2025/1190

18.6.2025

REGLAMENTO DELEGADO (UE) 2025/1190 DE LA COMISIÓN

de 13 de febrero de 2025

por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación que especifican los criterios utilizados para determinar qué entidades financieras están obligadas a realizar pruebas de penetración basadas en amenazas, los requisitos y normas que rigen el uso de probadores internos, los requisitos en relación con el alcance, la metodología y el enfoque de realización de pruebas en las fases de prueba, resultados, conclusión y adopción de medidas correctoras, y el tipo de cooperación en materia de supervisión y otros tipos de cooperación pertinente necesarios para la realización de las pruebas de penetración basadas en amenazas y para facilitar el reconocimiento mutuo

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el 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 ([1]), y en particular su artículo 26, apartado 11, párrafo cuarto,

Considerando lo siguiente:

(1) El presente Reglamento se ha elaborado de conformidad con el marco TIBER-EU y refleja la metodología, el proceso y la estructura de las pruebas de penetración basadas en amenazas descritas en dicho marco. Las entidades financieras sujetas a pruebas de penetración basadas en amenazas podrán hacer referencia al marco TIBER-EU, o a una de sus adaptaciones nacionales, y aplicarlo, en la medida en que dicho marco o adaptación sea coherente con los requisitos establecidos en los artículos 26 y 27 del Reglamento (UE) 2022/2554 y en el presente Reglamento. La designación de una única autoridad pública en el sector financiero que sea responsable de las cuestiones relacionadas con las pruebas de penetración basadas en amenazas a escala nacional de conformidad con el artículo 26, apartado 9, del Reglamento (UE) 2022/2554 debe entenderse sin perjuicio de la competencia de las autoridades correspondientes confiada a escala de la Unión para la supervisión de determinadas entidades financieras de conformidad con el artículo 46 de dicho Reglamento, como, por ejemplo, el Banco Central Europeo en relación con las entidades de crédito significativas que deben considerarse competentes en materia de pruebas de penetración basadas en amenazas. Cuando solo se deleguen algunas de las tareas relacionadas con las pruebas de penetración basadas en amenazas en otra autoridad nacional del sector financiero de conformidad con el artículo 26, apartado 10, del Reglamento (UE) 2022/2554, la autoridad competente sobre la entidad financiera a que se refiere el artículo 46 de dicho Reglamento debe seguir siendo la autoridad competente en relación con las tareas vinculadas a las pruebas de penetración basadas en amenazas que no se hayan delegado.

(2) Teniendo en cuenta la complejidad de la prueba de penetración basada en amenazas y los riesgos que conlleva, su uso debe limitarse a las entidades financieras para las que esté justificado. Por lo tanto, las autoridades responsables de los asuntos relacionados con las pruebas de penetración basadas en amenazas (autoridades competentes en relación con dichas pruebas, ya sea a escala de la Unión o nacional) deben excluir del ámbito de aplicación de estas pruebas a las entidades financieras que operen en subsectores esenciales de los servicios financieros para los que no esté justificado realizarlas. Esto significa que las entidades de crédito, las entidades de pago y de dinero electrónico, los depositarios centrales de valores, las entidades de contrapartida central, los centros de negociación y las empresas de seguros y reaseguros, aunque cumplan los criterios cuantitativos, podrían quedar exentas del requisito de realizar las pruebas de penetración basadas en amenazas a la luz de una evaluación global de su perfil de riesgo relacionado con las TIC y el grado de madurez de sus TIC, su impacto en el sector financiero y las preocupaciones relativas a la estabilidad financiera.

(3) Las autoridades competentes en relación con las pruebas de penetración basadas en amenazas deben evaluar, a la luz de una evaluación global del perfil de riesgo relacionado con las TIC y del grado de madurez de las TIC, del impacto en el sector financiero y de las preocupaciones relativas a la estabilidad financiera, si cualquier tipo de entidad financiera distinta de las entidades de crédito, las entidades de pago, las entidades de dinero electrónico, las entidades de contrapartida central, los depositarios centrales de valores, los centros de negociación y las empresas de seguros y reaseguros debe estar sujeta a la realización de pruebas de penetración basadas en amenazas. La evaluación de si dichas entidades financieras cumplen esos criterios cualitativos debe tener por objeto determinar para qué entidades

([1]) DO L 333 de 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

financieras es adecuada la prueba de penetración basada en amenazas, utilizando para ello indicadores intersectoriales y objetivos. Al mismo tiempo, la evaluación de si una entidad financiera cumple esos criterios cualitativos debe limitar las entidades sujetas a pruebas de penetración basadas en amenazas a aquellas para las que la prueba esté justificada. También debe evaluarse si una entidad financiera cumple esos criterios cualitativos a la luz de la evolución reciente de los mercados y de la creciente importancia de los nuevos participantes en el mercado para el sector financiero en el futuro, incluidos los proveedores de servicios de criptoactivos autorizados de conformidad con el artículo 59 del Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo ([2]).

(4) Las entidades financieras podrán tener el mismo proveedor intragrupo de servicios de TIC o pertenecer al mismo grupo y recurrir al uso de sistemas de TIC compartidos. En ese caso, es importante que las autoridades competentes en relación con las pruebas de penetración basadas en amenazas tengan en cuenta la estructura y el carácter sistémico o la importancia para el sector financiero de dicha entidad financiera a escala nacional o de la Unión al evaluar si una entidad financiera debe estar sujeta a la mencionada prueba y si esta debe llevarse a cabo a nivel de entidad o de grupo (a través de una prueba de penetración basada en amenazas compartida).

(5) Para imitar el marco TIBER-EU, es necesario que la metodología de la prueba prevea la participación de los siguientes agentes principales: la entidad financiera, con un equipo de control (a imagen del «equipo de control» de TIBER-EU) y un equipo azul (a imagen del «equipo azul» de TIBER-EU), y la autoridad competente en relación con las pruebas de penetración basadas en amenazas, en forma de equipo cibernético encargado de las pruebas de penetración basadas en amenazas (a imagen de los «equipos cibernéticos TIBER» de TIBER-EU), un proveedor de inteligencia de amenazas y probadores (los cuales son reflejo del «proveedor de equipo rojo» de TIBER-EU).

(6) Para garantizar que las pruebas de penetración basadas en amenazas se beneficien de la experiencia adquirida en el marco de la aplicación del marco TIBER-EU y reducir los riesgos asociados a la ejecución de las pruebas, debe garantizarse que las responsabilidades de los equipos cibernéticos que se creen en el seno de las autoridades competentes en relación con las pruebas de penetración basadas en amenazas se asemejen lo máximo posible a las de los equipos cibernéticos TIBER-EU. Por lo tanto, los equipos cibernéticos encargados de las pruebas de penetración basadas en amenazas deben contar con gestores de pruebas que sean responsables de supervisar, planificar y coordinar cada prueba. Los equipos cibernéticos encargados de las pruebas de penetración basadas en amenazas deben servir de punto de contacto único para la comunicación relacionada con las pruebas dirigida a las partes interesadas internas y externas, para la recogida y el tratamiento de las observaciones recibidas y las lecciones aprendidas de las pruebas realizadas previamente, y para apoyar a las entidades financieras sometidas a pruebas de penetración basadas en amenazas.

(7) Para imitar la metodología del marco TIBER-EU, los gestores de pruebas deben poseer las competencias y capacidades necesarias para prestar asesoramiento y cuestionar las propuestas de los probadores. La experiencia adquirida en el marco de TIBER-EU ha demostrado la utilidad de contar con un equipo de al menos dos gestores asignados a cada prueba. Para reflejar que la prueba de penetración basada en amenazas se utiliza para fomentar la experiencia de aprendizaje y proteger la confidencialidad de las pruebas, se alienta vivamente a las autoridades competentes en relación con las pruebas de penetración basadas en amenazas (a menos que presenten limitaciones de recursos o conocimientos técnicos) a que consideren la posibilidad de que, mientras esté en curso una prueba de este tipo, los gestores de la prueba no lleven a cabo actividades de supervisión sobre la misma entidad financiera sometida a la prueba.

(8) En aras de la coherencia con el marco TIBER-EU, es importante que la autoridad competente en relación con las pruebas de penetración basadas en amenazas lleve a cabo un seguimiento estrecho de las pruebas en cada una de sus fases. Teniendo en cuenta la naturaleza de las pruebas y los riesgos asociados, es fundamental que la autoridad competente participe en cada fase específica de las pruebas. En particular, la autoridad competente en relación con las pruebas de penetración basadas en amenazas debe ser consultada y validar las evaluaciones o decisiones de las entidades financieras que, por una parte, puedan influir en la eficacia de la prueba y, por otra, incidan en los riesgos que conlleva esta. Entre los pasos fundamentales en los que es necesaria una participación específica de la autoridad competente cabe citar la validación de determinada documentación fundamental de las pruebas, así como la selección de proveedores de inteligencia sobre amenazas y probadores, y de medidas de gestión de riesgos. La participación de las autoridades competentes en relación con las pruebas de penetración basadas en amenazas, en particular en las validaciones, no debe suponer una carga excesiva para dichas autoridades y, por tanto, debe limitarse a la documentación y las decisiones que afecten directamente a la realización de la prueba. Mediante la participación activa en cada fase de las pruebas, las autoridades competentes en relación con estas podrán evaluar eficazmente el cumplimiento de los requisitos pertinentes por parte de las entidades financieras, lo que debe permitir a dichas autoridades expedir informes de validación de conformidad con el artículo 26, apartado 7, del Reglamento (UE) 2022/2554.

([2]) Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937 (DO L 150 de 9.6.2023, p. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

(9) Es de suma importancia garantizar la confidencialidad de las pruebas de penetración basadas en amenazas para asegurar que las condiciones de las pruebas sean realistas. Por este motivo, las pruebas deben mantenerse en secreto y se deben tomar precauciones para preservar su confidencialidad, incluida la elección de las claves que deben diseñarse para impedir la identificación de la prueba de penetración basada en amenazas por parte de terceros. En el caso de que los miembros del personal responsables de la seguridad del equipo financiero tengan conocimiento de que se está llevando a cabo o está previsto realizar una prueba de penetración basada en amenazas, es probable que permanezcan más atentos y alerta que en las condiciones de trabajo normales, lo que alteraría el resultado de las pruebas. Por lo tanto, los miembros del personal de la entidad financiera ajenos al equipo de control solo deben ser informados de cualquier prueba de penetración basada en amenazas prevista o en curso cuando existan razones convincentes para ello y previo acuerdo de los gestores de la prueba, a fin de garantizar, entre otras cosas, el secreto de la prueba en caso de que un miembro del equipo azul la haya detectado.

(10) Como demuestra la experiencia adquirida en el marco de TIBER-EU con respecto al «equipo de control», la selección de un responsable del equipo de control adecuado es indispensable para la realización segura de las pruebas de penetración basadas en amenazas. El responsable del equipo de control debe tener el mandato necesario dentro de la entidad financiera para guiar todos los aspectos de la prueba, sin comprometer su confidencialidad. Por la misma razón, los miembros del equipo de control deben poseer un profundo conocimiento de la entidad financiera, del cargo desempeñado por el responsable del equipo de control y de su posicionamiento estratégico, pero además deben tener la antigüedad requerida y disponer de acceso al consejo de administración. Para reducir el riesgo de comprometer la prueba de penetración basada en amenazas, el equipo de control debe ser lo más pequeño posible.

(11) Existen elementos inherentes a los riesgos asociados a las pruebas de penetración basadas en amenazas, ya que las funciones esenciales se someten a prueba en un entorno de producción activo, lo que puede provocar incidentes de denegación de servicio, interrupciones imprevistas del sistema, daños a los sistemas de producción activos esenciales o la pérdida, modificación o divulgación de datos. Estos riesgos ponen de relieve la necesidad de adoptar medidas sólidas de gestión de riesgos. Para garantizar que la prueba de penetración basada en amenazas se lleve a cabo de manera controlada en su totalidad, es muy importante que las entidades financieras sean conscientes, en todos los puntos, de los riesgos específicos que surgen en una prueba de este tipo y que dichos riesgos se mitiguen. A este respecto, sin perjuicio de los procesos internos de la entidad financiera y de la responsabilidad y las facultades ya delegadas en el responsable del equipo de control, puede ser adecuado informar sobre las medidas de gestión de los riesgos que entrañan las pruebas o, en casos particulares, contar con la aprobación de dichas medidas por parte del propio órgano de dirección de la entidad financiera. Para poder prestar servicios profesionales eficaces y más cualificados y reducir esos riesgos, también es esencial que los probadores y los proveedores de inteligencia sobre amenazas (a los que en lo sucesivo se denominará conjuntamente «proveedores de pruebas de penetración basadas en amenazas») posean el máximo nivel de capacidades, conocimientos técnicos y experiencia adecuada en materia de inteligencia sobre amenazas y pruebas de penetración basadas en amenazas en el sector de los servicios financieros.

(12) Las pruebas de penetración convencionales proporcionan una evaluación detallada y útil de las vulnerabilidades técnicas y de configuración a menudo de un único sistema o entorno aislado, pero, a diferencia de la prueba de equipo rojo basada en inteligencia, no evalúan el escenario completo de un ataque selectivo contra toda una entidad, de manera que abarque la totalidad de las personas que la integran y de sus procesos y tecnologías. Por lo tanto, durante el proceso de selección de los proveedores de pruebas de penetración basadas en amenazas, las entidades financieras deben garantizar que dichos proveedores cuenten con las capacidades necesarias para realizar pruebas de equipo rojo en función de la inteligencia, y no solo pruebas de penetración. Así pues, es necesario establecer criterios exhaustivos para los probadores, tanto internos como externos, y para los proveedores de inteligencia sobre amenazas, siempre externos. Cuando los proveedores de pruebas de penetración basadas en amenazas pertenezcan a la misma empresa, el personal asignado a una prueba de este tipo debe ser convenientemente separado.

(13) Puede haber circunstancias excepcionales en las que las entidades financieras no puedan contratar proveedores de pruebas de penetración basadas en amenazas que cumplan los criterios generales. Por lo tanto, las entidades financieras, tras demostrar la falta de disponibilidad de dichos proveedores de inteligencia sobre amenazas, deben poder contratar a personas que no cumplan todos los criterios generales, siempre que mitiguen adecuadamente los riesgos adicionales resultantes y que la autoridad competente en relación con las pruebas de penetración basadas en amenazas evalúe todos esos criterios.

(14) Cuando varias entidades financieras y varias autoridades competentes en relación con las pruebas de penetración basadas en amenazas participen en una prueba de este tipo, deben especificarse las funciones de todas las partes en el proceso de prueba para llevar a cabo la prueba más eficiente y segura. A efectos de las pruebas conjuntas, se necesitan requisitos concretos para especificar el papel de la entidad financiera designada, a saber, que debe encargarse de proporcionar toda la documentación necesaria a la autoridad principal competente en relación con las pruebas de penetración basadas en amenazas y de supervisar el proceso de prueba. La entidad financiera designada también debe encargarse de los aspectos comunes de la evaluación de la gestión de riesgos. Sin perjuicio del papel de la entidad financiera designada, las obligaciones de cada entidad financiera que participe en el proceso de la prueba de penetración basada en amenazas conjunta no deben verse afectadas durante la prueba conjunta. El mismo principio debe aplicarse a las pruebas de penetración basadas en amenazas compartidas.

(15) Como demuestra la experiencia adquirida en el contexto de la aplicación del marco TIBER-EU, celebrar reuniones presenciales o virtuales en las que participen todas las partes interesadas (entidades financieras, autoridades, probadores y proveedores de inteligencia sobre amenazas) es la manera más eficiente de garantizar una adecuada realización de las pruebas. En consecuencia, deben celebrarse reuniones presenciales y virtuales en diversas fases del proceso y, en particular, durante la fase de preparación, en el momento de la puesta en marcha de la prueba de penetración basada en amenazas y con el fin de ultimar su alcance, durante la fase de prueba, para finalizar el informe de inteligencia sobre amenazas y el plan de pruebas del equipo rojo y para las actualizaciones semanales, así como durante la fase de conclusión, para reproducir las acciones de los probadores y los equipos azules, el trabajo en equipo morado y el intercambio de opiniones sobre la prueba de penetración basada en amenazas.

(16) Para garantizar el buen funcionamiento de la prueba de penetración basada en amenazas, la autoridad competente en la materia debe presentar claramente a la entidad financiera sus expectativas con respecto a la prueba. A este respecto, los gestores de la prueba deben garantizar que se establezca un flujo adecuado de información con el equipo de control de la entidad financiera y con los proveedores de pruebas de penetración basadas en amenazas.

(17) La entidad financiera debe seleccionar las funciones esenciales o importantes que se incluirán en el alcance de la prueba. Al seleccionar estas funciones, la entidad financiera debe basarse en diversos criterios relativos a la importancia de cada función para la propia entidad financiera y para el sector financiero, a escala de la Unión y nacional, no solo en términos económicos, sino también teniendo en cuenta el estatus simbólico o político de la función. Para facilitar una transición fluida a la fase de recopilación de inteligencia sobre amenazas, el equipo de control debe proporcionar a los probadores y proveedores de inteligencia sobre amenazas que no participen en el proceso de delimitación del alcance de la prueba, información detallada sobre el alcance acordado.

(18) A fin de proporcionar a los probadores la información necesaria para simular un ataque real y realista a los sistemas activos de la entidad financiera que sustentan sus funciones esenciales o importantes, el proveedor de inteligencia sobre amenazas debe recopilar inteligencia o información que abarque al menos dos ámbitos clave de interés: los objetivos, señalando posibles superficies de ataque en toda la entidad financiera, y las amenazas, indicando los agentes que suponen una amenaza y los escenarios de amenaza probables. Para garantizar que el proveedor de inteligencia sobre amenazas tenga en cuenta las amenazas pertinentes para la entidad financiera, los probadores, el equipo de control y los gestores de la prueba deben proporcionar información sobre el proyecto de informe de inteligencia sobre amenazas. El proveedor de inteligencia sobre amenazas (si se dispone de él) podrá utilizar un panorama genérico de amenazas para el sector financiero de un Estado miembro, facilitado por la autoridad competente en relación con las pruebas de penetración basadas en amenazas, como base de referencia para el panorama de amenazas nacional. Sobre la base de la aplicación del marco TIBER-EU, el proceso de recopilación de inteligencia sobre amenazas suele durar unas cuatro semanas.

(19) Para que los probadores puedan conocer mejor y seguir revisando el documento de especificación del alcance y el informe de inteligencia sobre amenazas específicas con objeto de ultimar el plan de pruebas del equipo rojo, es esencial que, antes de la fase de pruebas del equipo rojo en el marco de la prueba de penetración basada en amenazas, el proveedor de inteligencia sobre amenazas facilite a los probadores explicaciones detalladas acerca del informe de inteligencia sobre amenazas específicas y el análisis de posibles escenarios de amenaza.

(20) Para que los probadores puedan llevar a cabo pruebas realistas y exhaustivas en las que se ejecuten todas las fases del ataque y se alcancen los marcadores, debe asignarse tiempo suficiente para la fase activa de pruebas del equipo rojo. Sobre la base de la experiencia adquirida con el marco TIBER-EU, el tiempo asignado debe ser de al menos 12 semanas y debe determinarse teniendo en cuenta el número de partes implicadas, el alcance de la prueba de penetración basada en amenazas, los recursos de la entidad o entidades financieras implicadas, cualquier requisito externo y la disponibilidad de información complementaria facilitada por la entidad financiera.

(21) Durante la fase activa de pruebas del equipo rojo, los probadores deben desplegar una serie de tácticas, técnicas y procedimientos para probar adecuadamente los sistemas de producción activos de la entidad financiera. Dichas tácticas, técnicas y procedimientos deben incluir, según proceda, el reconocimiento (es decir, la recopilación de la mayor cantidad posible de información sobre un objetivo), la instrumentalización (es decir, el análisis de información sobre la infraestructura, las instalaciones y los empleados y la preparación para las operaciones específicas del objetivo), la ejecución (es decir, el inicio activo de la operación completa contra el objetivo), la explotación (es decir, cuando el objetivo de los probadores sea comprometer los servidores y las redes de la entidad financiera y explotar a su personal a través de la ingeniería social), el control y movimiento (es decir, intentos de pasar de los sistemas comprometidos a otros más vulnerables o de alto valor) y acciones en relación con el objetivo (es decir, conseguir un mayor acceso a los sistemas comprometidos y obtener acceso a la información y los datos sobre los objetivos previamente acordados en el plan de pruebas del equipo rojo).

(22) Al llevar a cabo una prueba de penetración basada en amenazas, los probadores deben actuar teniendo en cuenta el tiempo disponible para llevar a cabo el ataque, los recursos y los límites éticos y jurídicos. En el caso de que los probadores no puedan avanzar a la siguiente fase programada del ataque, el equipo de control deberá prestar asistencia ocasional, previo acuerdo de la autoridad competente en relación con las pruebas de penetración basadas en amenazas. Dicha asistencia puede clasificarse, en términos generales, como asistencia relacionada con la información y asistencia relacionada con el acceso, y puede consistir en la provisión de acceso a sistemas de TIC o a redes internas para continuar con la prueba y centrarse en las fases siguientes del ataque.

(23) Durante el trabajo activo del equipo rojo en la fase de prueba, si es necesario para permitir la continuación de la prueba de penetración basada en amenazas como último recurso en circunstancias excepcionales y una vez agotadas todas las opciones alternativas, debe utilizarse una actividad de prueba colaborativa en la que participen tanto los probadores como el equipo azul. En el contexto de un ejercicio de trabajo en equipo morado tan limitado, pueden utilizarse los siguientes métodos: «captura y liberación», en el que los probadores intentan continuar con los escenarios, ser detectados y, a continuación, reanudar las pruebas, a modo de «juegos de guerra», lo que permite probar la toma de decisiones estratégicas en escenarios más complejos, o de «prueba de concepto colaborativa», que permite a los probadores y a los miembros del equipo azul validar conjuntamente medidas, herramientas o técnicas de seguridad específicas en un entorno controlado y cooperativo.

(24) La prueba de penetración basada en amenazas debe utilizarse como experiencia de aprendizaje para mejorar la resiliencia operativa digital de las entidades financieras. A este respecto, el equipo azul y los probadores deben reproducir el ataque y revisar las medidas adoptadas para aprender de la experiencia de las pruebas en colaboración con los probadores. A tal fin, y para permitir una preparación adecuada, el informe de pruebas del equipo rojo y el informe de pruebas del equipo azul deben ponerse a disposición de todas las partes implicadas en las actividades de reproducción, antes de llevar a cabo cualquier actividad de este tipo. Además, debe llevarse a cabo un ejercicio de trabajo en equipo morado, en la fase de conclusión, para maximizar la experiencia de aprendizaje. Los métodos que pueden utilizarse para el trabajo en equipo morado en la fase de conclusión deben incluir el debate de escenarios de ataque alternativos, la exploración de sistemas activos de escenarios alternativos o una segunda exploración de escenarios previstos sobre sistemas activos que los probadores no hayan podido completar o ejecutar durante la fase de prueba.

(25) Para facilitar aún más la experiencia de aprendizaje de todas las partes implicadas en la prueba de penetración basada en amenazas, en beneficio de futuras pruebas, y con el objetivo de fomentar la resiliencia operativa digital de las entidades financieras, las partes interesadas deben informarse mutuamente sobre el proceso general y, en particular, determinar qué actividades transcurrieron satisfactoriamente o podrían haberse mejorado, y qué aspectos del proceso de las pruebas de penetración basadas en amenazas funcionaron de forma adecuada o podrían mejorarse.

(26) Las autoridades competentes a que se refiere el artículo 46 del Reglamento (UE) 2022/2554 y las autoridades competentes en relación con las pruebas de penetración basadas en amenazas, cuando sean diferentes, deberán cooperar para incorporar pruebas avanzadas a los procesos de supervisión existentes mediante la realización de pruebas de penetración basadas en amenazas. A este respecto, y a fin de compartir la correcta comprensión de las conclusiones de la prueba de penetración basada en amenazas y de cómo deben interpretarse, es conveniente que, en particular en lo que se refiere al informe resumido de la prueba y los planes de introducción de medidas correctoras, se establezca una cooperación estrecha entre los gestores de pruebas que participaron en la prueba de penetración basada en amenazas y los supervisores responsables.

(27) El artículo 26, apartado 8, párrafo primero, del Reglamento (UE) 2022/2554 exige a las entidades financieras que contraten probadores externos cada tres pruebas. Cuando las entidades financieras incluyan en el equipo probadores tanto internos como externos, la prueba de penetración basada en amenazas deberá considerarse realizada con probadores internos a efectos de dicho artículo.

(28) El presente Reglamento se basa en los proyectos de normas técnicas de regulación presentados a la Comisión por la Autoridad Bancaria Europea, la Autoridad Europea de Seguros y Pensiones de Jubilación y la Autoridad Europea de Valores y Mercados (Autoridades Europeas de Supervisión), de acuerdo con el Banco Central Europeo.

(29) Las Autoridades Europeas de Supervisión han llevado a cabo consultas públicas abiertas sobre los proyectos de normas técnicas de regulación en que se basa el presente Reglamento, han analizado los costes y beneficios potenciales conexos y han recabado el asesoramiento del Grupo de Partes Interesadas del Sector Bancario establecido de conformidad con el artículo 37 del Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo ([3]), del Grupo de Partes Interesadas del Sector de Seguros y de Reaseguros y el Grupo de Partes Interesadas del Sector de Pensiones de Jubilación establecidos de conformidad con el artículo 37 del Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo ([4]), y del Grupo de Partes Interesadas del Sector de los Valores y Mercados establecido de conformidad con el artículo 37 del Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo ([5]).

(30) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([6]), emitió su dictamen el 20 de agosto de 2024.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Definiciones

A efectos del presente Reglamento, se entenderá por:

1) «equipo de control»: el equipo compuesto por personal de la entidad financiera sometida a prueba y, en su caso, teniendo en cuenta el alcance de la prueba de penetración basada en amenazas, el personal de sus proveedores terceros de servicios y cualquier otra parte que gestiona la prueba;

2) «responsable del equipo de control»: el miembro del personal de la entidad financiera responsable de la realización de todas las actividades relacionadas con la prueba de penetración basada en amenazas en el contexto de una prueba determinada;

3) «equipo azul»: el personal de la entidad financiera y, en su caso, el personal de los proveedores terceros de servicios de la entidad financiera y cualquier otra parte que se considere pertinente, teniendo en cuenta el alcance de la prueba de penetración basada en amenazas, de los proveedores terceros de servicios de la entidad financiera, que defiendan el uso de redes y sistemas de información por parte de una entidad financiera manteniendo su postura de seguridad frente a ataques simulados o reales y que no tenga conocimiento de la prueba de penetración basada en amenazas;

4) «tareas del equipo azul»: tareas que normalmente lleva a cabo el equipo azul, como el centro de operaciones de seguridad (COS), los servicios de infraestructura de TIC, los servicios de asistencia y los servicios de gestión de incidentes a nivel operativo;

5) «equipo rojo»: los probadores, internos o externos, contratados o asignados a una prueba de penetración basada en amenazas;

6) «trabajo en equipo morado»: actividad de prueba colaborativa en la que participan tanto los probadores como el equipo azul;

([3]) Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión (DO L 331 de 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/79/CE de la Comisión (DO L 331 de 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/77/CE de la Comisión (DO L 331 de 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7) «autoridad competente en relación con las pruebas de penetración basadas en amenazas»: cualquiera de las siguientes:

   a) la autoridad pública única del sector financiero designada de conformidad con el artículo 26, apartado 9, del Reglamento (UE) 2022/2554;

   b) la autoridad del sector financiero en la que se delega el ejercicio de algunas o todas las tareas en relación con las pruebas de penetración basadas en amenazas, de conformidad con el artículo 26, apartado 10, del Reglamento (UE) 2022/2554;

   c) cualquiera de las autoridades competentes a que se refiere el artículo 46 del Reglamento (UE) 2022/2554;

8) «equipo cibernético encargado de las pruebas de penetración basadas en amenazas» o «TCT» (por sus siglas en inglés): el personal de las autoridades competentes en relación con las pruebas de penetración basadas en amenazas que es responsable de las cuestiones relacionadas con dichas pruebas;

9) «gestores de pruebas»: el personal designado para dirigir las actividades de la autoridad competente en relación con las pruebas de penetración basadas en amenazas en lo referente a una prueba de penetración basada en amenazas específica a fin de supervisar el cumplimiento del presente Reglamento;

10) «proveedor de inteligencia sobre amenazas»: los expertos contratados por la entidad financiera para cada prueba de penetración basada en amenazas y externos a la entidad financiera y, en su caso, a los proveedores intragrupo de servicios de TIC, que recopilan y analizan información específica sobre amenazas pertinente para las entidades financieras incluidas en el ámbito de una prueba de penetración basada en amenazas específica y desarrollan escenarios de amenaza pertinentes y realistas;

11) «proveedores de pruebas de penetración basadas en amenazas»: los probadores y los proveedores de inteligencia sobre amenazas;

12) «asistencia»: ayuda o información facilitada por el equipo de control a los probadores para que estos puedan proseguir con la ejecución de una trayectoria de ataque cuando no puedan avanzar por sí solos y cuando no exista ninguna otra alternativa razonable, incluso debido a la falta de tiempo o recursos suficientes en una determinada prueba de penetración basada en amenazas;

13) «trayectoria de ataque»: la ruta que siguen los probadores durante la fase activa de pruebas del equipo rojo, en el marco de la prueba de penetración basada en amenazas, para llegar a las banderas especificadas para dicha prueba;

14) «banderas»: objetivos clave de los sistemas de TIC que sustenten funciones esenciales o importantes de una entidad financiera que los probadores intentan alcanzar a través de la prueba;

15) «información sensible»: información que puede aprovecharse fácilmente para cometer ataques contra los sistemas de TIC de la entidad financiera, la propiedad intelectual, los datos empresariales confidenciales o los datos personales, que puede perjudicar de forma directa o indirecta a la entidad financiera y a su ecosistema si cae en manos de agentes malintencionados;

16) «agrupación»: todas las entidades financieras que participan en una prueba de penetración basada en amenazas conjunta de conformidad con el artículo 26, apartado 4, del Reglamento (UE) 2022/2554;

17) «Estado miembro de acogida»: el Estado miembro de acogida de conformidad con el Derecho sectorial de la Unión aplicable a cada entidad financiera;

18) «prueba de penetración basada en amenazas compartida»: prueba de penetración basada en amenazas, distinta de las pruebas de penetración basadas en amenazas conjuntas a que se refiere el artículo 26, apartado 4, del Reglamento (UE) 2022/2554, en la que participan varias entidades financieras que utilizan el mismo proveedor intragrupo de servicios de TIC, o que pertenecen al mismo grupo y comparten sistemas de TIC.

Artículo 2

Determinación de las entidades financieras obligadas a realizar pruebas de penetración basadas en amenazas

1. Las autoridades competentes en relación con las pruebas de penetración basadas en amenazas evaluarán si una entidad financiera está obligada a realizar dichas pruebas teniendo en cuenta el impacto de dichas entidades financieras, su carácter sistémico y su perfil de riesgo relacionado con las TIC, sobre la base de todos los criterios que se enumeran a continuación:

a) factores relacionados con el impacto y el carácter sistémico:

   i) el tamaño de la entidad financiera, determinado en función de si la entidad financiera presta servicios financieros en uno o varios Estados miembros y comparando las actividades de la entidad financiera con las de otras entidades financieras que presten servicios similares,

   ii) el alcance y la naturaleza de la interconexión de la entidad financiera con otras entidades financieras del sector financiero de uno o varios Estados miembros,

   iii) el carácter esencial o la importancia de los servicios que la entidad financiera presta al sector financiero,

iv) la sustituibilidad de los servicios que presta la entidad financiera,

v) la complejidad del modelo de negocio de la entidad financiera y los servicios y procesos conexos,

vi) si la entidad financiera forma parte de un grupo de carácter sistémico a escala de la Unión o nacional en el sector financiero que comparte sistemas de TIC;

b) factores vinculados al riesgo relacionado con las TIC:

i) el perfil de riesgo de la entidad financiera,

ii) el panorama de amenazas a que se enfrenta la entidad financiera,

iii) el grado de dependencia de las funciones esenciales o importantes de la entidad financiera o de sus funciones de apoyo respecto de los sistemas y procesos de TIC,

iv) la complejidad de la arquitectura de TIC de la entidad financiera,

v) los servicios y funciones de TIC sustentados por proveedores terceros de servicios de TIC, y la cantidad y el tipo de acuerdos contractuales con proveedores terceros de servicios de TIC o proveedores intragrupo de servicios de TIC,

vi) los resultados de cualquier revisión supervisora pertinentes para la evaluación de la madurez de las TIC de la entidad financiera,

vii) la madurez de los planes de continuidad de la actividad en materia de TIC y de los planes de respuesta y recuperación en materia de TIC,

viii) la madurez de las medidas operativas de detección y mitigación de la seguridad de las TIC, incluida la capacidad de:

1) efectuar un seguimiento permanente de la infraestructura de TIC de la entidad financiera;

2) detectar incidentes relacionados con las TIC en tiempo real;

3) analizar los incidentes a que se refiere el punto 2;

4) responder a los incidentes a que se refiere el punto 2 de manera oportuna y eficaz,

ix) si la entidad financiera forma parte de un grupo activo en el sector financiero a escala de la Unión o nacional que comparte sistemas de TIC.

A efectos de la letra a), inciso i), la autoridad competente en relación con las pruebas de penetración basadas en amenazas analizará, cuando sea posible, los aspectos siguientes:

a) la cuota de mercado de la entidad financiera a escala nacional y de la Unión;

b) la gama de actividades que ofrece la entidad financiera;

c) la cuota de mercado de los servicios prestados por la entidad financiera o de las actividades que lleva a cabo a escala nacional y de la Unión.

A efectos de la letra a), inciso v), la autoridad competente en relación con las pruebas de penetración basadas en amenazas analizará, cuando sea posible, los aspectos siguientes:

a) si la entidad financiera opera con más de un modelo de negocio;

b) la interconexión de los diferentes procesos empresariales y los servicios conexos.

2. Las autoridades competentes en relación con las pruebas de penetración basadas en amenazas exigirán a todas las entidades financieras siguientes que realicen pruebas de este tipo, a menos que la evaluación a que se refiere el apartado 1 con respecto a una entidad financiera indique que su impacto, los problemas de estabilidad financiera relacionados con dicha entidad financiera o su perfil de riesgo relacionado con las TIC no justifican la realización de una prueba de dicha naturaleza:

a) las entidades de crédito que cumplan alguna de las condiciones siguientes:

i) haber sido identificadas como entidades de importancia sistémica mundial (EISM) de conformidad con el artículo 131 de la Directiva 2013/36/UE del Parlamento Europeo y del Consejo ([7]),

ii) haber sido identificadas como otras entidades de importancia sistémica (OEIS) de conformidad con el artículo 131 de la Directiva 2013/36/UE,

iii) formar parte de una EISM u OEIS;

([7]) Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (DO L 176 de 27.6.2013, p. 338, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) las entidades de pago que hayan realizado operaciones de pago, tal como se definen en el artículo 4, punto 5, de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo ([8]), por un valor total superior a 150 000 millones EUR en cada uno de los dos años naturales anteriores a la evaluación por parte de la autoridad competente en relación con las pruebas de penetración basadas en amenazas;

c) las entidades de dinero electrónico que hayan realizado operaciones de pago, tal como se definen en el artículo 4, apartado 5, de la Directiva (UE) 2015/2366, por un valor total superior a 150 000 millones EUR, en cada uno de los dos años naturales anteriores a la evaluación por parte de la autoridad competente en relación con las pruebas de penetración basadas en amenazas, o registrado una cantidad de dinero electrónico en circulación por un importe total superior a 40 000 millones EUR;

d) los depositarios centrales de valores;

e) las entidades de contrapartida central;

f) los centros de negociación con un sistema electrónico de negociación que cumplan cualquiera de los criterios siguientes:

i) que el centro de negociación ostente la mayor cuota de mercado en términos de volumen de negocios de cualquiera de los títulos siguientes a nivel nacional en cada uno de los dos años naturales anteriores a la evaluación por parte de la autoridad competente en relación con las pruebas de penetración basadas en amenazas:

1) valores negociables de acuerdo con la definición del artículo 4, apartado 1, punto 44, letra a), de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo ([9]);

2) valores negociables, de acuerdo con la definición del artículo 4, apartado 1, punto 44, letra b), de la Directiva 2014/65/UE;

3) derivados, de acuerdo con la definición del artículo 2, apartado 1, punto 29, del Reglamento (UE) n.º 600/2014 del Parlamento Europeo y del Consejo ([10]);

4) productos de titulización, de acuerdo con la definición del artículo 2, apartado 1, punto 28, del Reglamento (UE) n.º 600/2014;

5) los derechos de emisión a que se refiere el anexo I, sección C, punto 11, de la Directiva 2014/65/UE,

ii) que el centro de negociación ostente una cuota de mercado en términos de volumen de negocios a escala de la Unión en cualquiera de los títulos siguientes superior al 5 % en cada uno de los dos años naturales anteriores a la evaluación por parte de la autoridad competente en relación con las pruebas de penetración basadas en amenazas:

1) acciones de sociedades y otros valores equiparables a las acciones de sociedades, asociaciones u otras entidades, y certificados de depósito de valores representativos de acciones;

2) bonos y obligaciones u otras formas de deuda titulizada, incluidos los certificados de depósito de valores representativos de tales valores;

3) derivados, de acuerdo con la definición del artículo 2, apartado 1, punto 29, del Reglamento (UE) n.º 600/2014;

4) productos de titulización, de acuerdo con la definición del artículo 2, apartado 1, punto 28, del Reglamento (UE) n.º 600/2014;

5) los derechos de emisión a que se refiere el anexo I, sección C, punto 11, de la Directiva 2014/65/UE;

([8]) Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE (DO L 337 de 23.12.2015, p. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (DO L 173 de 12.6.2014, p. 349, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Reglamento (UE) n.º 600/2014 del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 173 de 12.6.2014, p. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) las empresas de seguros y reaseguros que cumplan todos los criterios siguientes:

i) tener una prima bruta suscrita superior a 1 500 000 000 EUR,

ii) tener provisiones técnicas superiores a 10 000 000 000 EUR,

iii) las empresas de seguros que ejerzan únicamente actividades de vida o que ejerzan actividades tanto de vida como de no vida y cuyos activos totales superen el 3,5 % de la suma de los activos totales de las empresas de seguros y reaseguros establecidas en el Estado miembro, valorados de conformidad con el artículo 75 de la Directiva 2009/138/CE del Parlamento Europeo y del Consejo ([11]).

A efectos de la letra f), inciso ii), cuando el centro de negociación forme parte de un grupo que comparta sistemas de TIC o el mismo proveedor intragrupo de servicios de TIC, se tendrá en cuenta el volumen de negocios de los contratos de valores y derivados en todos los centros de negociación pertenecientes al mismo grupo y establecidos en la Unión.

A efectos de la letra g), las autoridades competentes en relación con las pruebas de penetración basadas en amenazas determinarán un subconjunto de todas las empresas de seguros y reaseguros aplicando los criterios establecidos en la letra g), incisos i), ii) y iii). Las empresas de seguros y reaseguros incluidas en ese subconjunto estarán obligadas a realizar pruebas de penetración basadas en amenazas cuando también cumplan cualquiera de los criterios siguientes:

a) tener una prima bruta suscrita superior a 3 000 000 000 EUR;

b) tener provisiones técnicas superiores a 30 000 000 000 EUR;

c) tener unos activos totales que superen el 10 % de la suma de los activos totales de las empresas de seguros y reaseguros establecidas en el Estado miembro, valorados de conformidad con el artículo 75 de la Directiva 2009/138/CE.

3. Cuando más de una entidad financiera perteneciente al mismo grupo y que comparta sistemas de TIC, o más de una entidad financiera que utilice el mismo proveedor intragrupo de servicios de TIC, cumplan los criterios establecidos en el apartado 2, las autoridades competentes en relación con las pruebas de penetración basadas en amenazas de las citadas entidades financieras decidirán, de conformidad con el artículo 16, apartado 2, si el requisito de realizar dichas pruebas de forma individual es pertinente para las citadas entidades financieras.

Cuando la autoridad competente en relación con las pruebas de penetración basadas en amenazas de la sociedad matriz de un grupo de entidades financieras a que se refiere el párrafo primero sea diferente de las autoridades competentes en relación con las pruebas de penetración basadas en amenazas de las entidades financieras del grupo, las autoridades competentes en relación con las pruebas de penetración basadas en amenazas de estas últimas consultarán a dicha autoridad si es conveniente realizar pruebas de penetración basadas en amenazas de forma individual.

Artículo 3

Equipo de ciberseguridad y gestores de pruebas de penetración basadas en amenazas

1. Una autoridad competente en relación con las pruebas de penetración basadas en amenazas asignará a un equipo de ciberseguridad de dichas pruebas de penetración la responsabilidad de coordinar las actividades relacionadas con tales pruebas. Un equipo de ciberseguridad de pruebas de penetración basadas en amenazas estará compuesto por los gestores de pruebas asignados a la supervisión de una prueba concreta de penetración basada en amenazas.

2. Para cada prueba, la autoridad competente designará un gestor de pruebas y al menos un sustituto.

3. Los gestores de pruebas supervisarán si se cumplen los requisitos establecidos en el presente Reglamento y se asegurarán de que se cumplan.

([11]) Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II) (DO L 335 de 17.12.2009, p. 1, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. El gestor de pruebas comunicará los datos de contacto del equipo de ciberseguridad de pruebas a la entidad financiera a través de la notificación a que se refiere el artículo 9, apartado 1.

5. La autoridad competente en relación con la prueba de penetración basada en amenazas participará en todas las fases de la prueba.

Artículo 4

Disposiciones organizativas para las entidades financieras

1. Las entidades financieras designarán un equipo de control que será responsable de la gestión cotidiana de la prueba de penetración basada en amenazas y de las decisiones y acciones del equipo de control.

2. Las entidades financieras establecerán medidas organizativas y de procedimiento para garantizar que:

a) el acceso a la información relativa a cualquier prueba de penetración basada en amenazas prevista o en curso está limitado, en función de la necesidad de conocerla, al equipo de control, al órgano de dirección, a los probadores, al proveedor de inteligencia sobre amenazas y a la autoridad competente en relación con la prueba de penetración basada en amenazas;

b) el equipo de control consulta a los gestores de la prueba antes de implicar a cualquier miembro del equipo azul en una prueba de penetración basada en amenazas;

c) el equipo de control es informado de cualquier detección de la prueba de penetración basada en amenazas por parte de miembros del personal de la entidad financiera o de sus proveedores terceros de servicios; en caso de traslado de la respuesta al incidente resultante a un nivel de decisión superior, cuando sea necesario, el equipo de control bloquea dicho traslado;

d) existen disposiciones relativas a la confidencialidad de la prueba de penetración basada en amenazas aplicables al personal de la entidad financiera, al personal de los proveedores terceros de servicios de TIC afectados, a los probadores y al proveedor de inteligencia sobre amenazas;

e) el equipo de control facilita a los gestores de la prueba, previa solicitud, cualquier información relativa a la prueba de penetración basada en amenazas;

f) en la medida de lo posible, las partes implicadas en la prueba solo hacen referencia a ella por su nombre clave.

Artículo 5

Gestión de riesgos de las pruebas de penetración basadas en amenazas

1. Durante la fase de preparación a que se refiere el artículo 9, el equipo de control evaluará los riesgos asociados a la prueba de los sistemas de producción activos de funciones esenciales o importantes de la entidad financiera, incluidas las posibles repercusiones en:

a) el sector financiero;

b) la estabilidad financiera a escala de la Unión o nacional.

El equipo de control revisará dichas repercusiones a lo largo de las pruebas.

2. A efectos de la evaluación y gestión de los riesgos, el equipo de control tendrá en cuenta, como mínimo, los siguientes tipos de riesgos relacionados con:

a) la concesión de acceso al proveedor de inteligencia sobre amenazas y a los probadores externos, cuando proceda, a información delicada sobre la entidad financiera;

b) la falta de conformidad de la prueba de penetración basada en amenazas con el Reglamento (UE) 2022/2554 y con el presente Reglamento cuando tal incumplimiento dé lugar a la no expedición del informe de validación a que se refiere el artículo 26, apartado 7, del Reglamento (UE) 2022/2554, incluso cuando dicho incumplimiento se deba a violaciones de la confidencialidad de la prueba de penetración basada en amenazas o a la falta de ética;

c) el traslado de crisis e incidentes a instancias de decisión superiores;

d) la fase activa del equipo rojo, incluidos los riesgos relacionados con la interrupción de actividades esenciales y la corrupción de datos debido a las actividades de los probadores, y sus posibles repercusiones en terceros;

e) la actividad del equipo azul, incluidos los riesgos relacionados con la interrupción de actividades esenciales y la corrupción de datos debido a las actividades del equipo azul, y sus posibles repercusiones en terceros;

f) la restauración incompleta de los sistemas afectados por la prueba de penetración basada en amenazas.

Artículo 6

Gestión del riesgo de las pruebas de penetración basadas en amenazas conjuntas o compartidas

1. En el caso de una prueba de penetración basada en amenazas conjunta o compartida, el equipo de control de cada entidad financiera llevará a cabo su propia evaluación del riesgo y establecerá sus propias medidas de gestión de riesgos.

2. El equipo de control de la entidad financiera designada a que se refiere el artículo 16, apartado 3, letra b), del presente Reglamento, o la entidad financiera designada de conformidad con el artículo 26, apartado 4, del Reglamento (UE) 2022/2554, evaluará los riesgos relacionados con la participación de múltiples entidades financieras en la prueba de penetración basada en amenazas. Los equipos de control de las entidades financieras implicadas cooperarán con el equipo de control de la entidad financiera designada para detectar posibles riesgos conjuntos.

Artículo 7

Selección de proveedores de pruebas de penetración basadas en amenazas

1. El equipo de control tomará medidas para gestionar los riesgos relacionados con la prueba de penetración basada en amenazas y, en particular, velará por que, para cada prueba de este tipo:

a) el proveedor de inteligencia sobre amenazas y los probadores externos faciliten al equipo de control un currículum vítae detallado y copias de las certificaciones que, con arreglo a normas de mercado reconocidas, sean adecuadas para el desempeño de sus actividades;

b) el proveedor de inteligencia sobre amenazas y el probador externo estén debida y completamente cubiertos por seguros adecuados de responsabilidad civil profesional, también frente a los riesgos de falta intencionada y negligencia;

c) el proveedor de inteligencia sobre amenazas proporcione al menos tres referencias de encargos anteriores en el contexto de las pruebas de penetración y las pruebas de equipo rojo;

d) los probadores externos proporcionen al menos cinco referencias de encargos anteriores relacionados con pruebas de penetración y pruebas de equipo rojo;

e) el personal del proveedor de inteligencia sobre amenazas asignado a la prueba de penetración basada en amenazas:

   i) esté compuesto por al menos un responsable con al menos cinco años de experiencia en inteligencia sobre amenazas y al menos un miembro adicional con al menos dos años de experiencia en inteligencia sobre amenazas,

   ii) posea una amplia variedad y un nivel adecuado de conocimientos y capacidades profesionales, en particular:

      1) tácticas, técnicas y procedimientos de recopilación de información;

      2) conocimientos geopolíticos, técnicos y sectoriales;

      3) capacidades de comunicación adecuadas para presentar claramente el resultado de la intervención e informar al respecto,

   iii) haya participado en total en al menos tres misiones anteriores de inteligencia sobre amenazas en el contexto de pruebas de penetración y pruebas de equipo rojo,

   iv) no realice simultáneamente tareas de equipo azul u otros servicios que puedan presentar un conflicto de intereses con respecto a la entidad financiera, el proveedor tercero de servicios de TIC o un proveedor intragrupo de servicios de TIC que participe en las pruebas de penetración basadas en amenazas a las que estén asignados,

   v) esté separado del personal del mismo proveedor de pruebas de penetración basadas en amenazas que proporcione probadores externos para la misma prueba y no esté bajo la dirección de dicho personal;

f) en el caso de los probadores externos, que el equipo rojo asignado a la prueba de penetración basada en amenazas:

i) esté compuesto por al menos un responsable con al menos cinco años de experiencia en pruebas de penetración y pruebas de equipo rojo, así como por al menos dos probadores adicionales, cada uno de ellos con una experiencia de al menos dos años en pruebas de penetración y pruebas de equipo rojo,

ii) posea una amplia variedad y un nivel adecuado de conocimientos y capacidades profesionales, en particular conocimientos sobre la actividad de la entidad financiera, reconocimiento, gestión de riesgos, explotación de oportunidades, penetración física, ingeniería social y análisis de vulnerabilidades, así como capacidades de comunicación adecuadas para presentar e informar claramente sobre el resultado de la intervención,

iii) haya participado en total en al menos cinco encargos anteriores relacionados con pruebas de penetración y pruebas de equipo rojo,

iv) no tenga una relación laboral con un proveedor de inteligencia sobre amenazas que realice simultáneamente tareas de equipo azul para una entidad financiera, un proveedor tercero de servicios de TIC o un proveedor intragrupo de servicios de TIC que participe en la prueba de penetración basada en amenazas, ni preste servicios a un proveedor de tales características,

v) esté separado del personal del mismo proveedor de pruebas de penetración basadas en amenazas que preste simultáneamente servicios de inteligencia sobre amenazas en relación con la misma prueba;

g) los probadores y el proveedor de inteligencia sobre amenazas lleven a cabo procedimientos de restauración al final de las pruebas, incluida la supresión segura de información relacionada con contraseñas, credenciales y otras claves secretas comprometidas durante la prueba de penetración basada en amenazas, la comunicación segura de las cuentas comprometidas a las entidades financieras, así como la recogida, el almacenamiento, la gestión y la eliminación seguros de otros datos recogidos durante la prueba;

h) los probadores, además de los procedimientos de restauración al término de la prueba a que se refiere la letra g), lleven a cabo los siguientes procedimientos de restauración:

i) desactivación del mando y el control,

ii) interruptores de seguridad para el alcance y la fecha,

iii) eliminación de programas maliciosos de tipo *backdoor* y de otra índole,

iv) notificación de posibles infracciones,

v) procedimientos para la restauración futura de copias de seguridad que puedan guardar relación con programas maliciosos o herramientas instalados durante la prueba,

vi) seguimiento de las actividades del equipo azul y notificación al equipo de control de cualquier posible detección;

i) los probadores y el proveedor de inteligencia sobre amenazas no realicen ni participen en ninguna de las actividades siguientes:

i) destrucción no autorizada de equipos de la entidad financiera y de sus proveedores terceros de servicios de TIC, en su caso,

ii) modificación incontrolada de la información y los activos de TIC de la entidad financiera y de sus proveedores terceros de servicios de TIC, en su caso,

iii) comprometer intencionadamente la continuidad de las funciones esenciales o importantes de la entidad financiera,

iv) inclusión no autorizada de sistemas no contemplados en el alcance de la prueba,

v) divulgación no autorizada de los resultados de la prueba.

2. El equipo de control llevará un registro de la documentación facilitada por los probadores y los proveedores de inteligencia sobre amenazas para demostrar el cumplimiento de lo dispuesto en el apartado 1, letras a) a f).

En circunstancias excepcionales, las entidades financieras podrán contratar a probadores externos y proveedores de inteligencia sobre amenazas que no cumplan uno o varios de los requisitos establecidos en el apartado 1, letras a) a f), siempre que dichas entidades financieras adopten medidas adecuadas para mitigar los riesgos relacionados con el incumplimiento de esas disposiciones y registren dichas medidas.

Artículo 8

Especificidades de las pruebas de penetración basadas en amenazas conjuntas o compartidas

1. Salvo decisión en contrario de la autoridad principal competente en relación con las pruebas de penetración basadas en amenazas, cuando varias entidades financieras, identificadas de conformidad con el artículo 16, apartados 2 o 4, participen en una prueba de penetración basada en amenazas conjunta o compartida, cada entidad financiera seguirá cada uno de los pasos descritos en los artículos 9 a 15.

2. Salvo disposición en contrario del presente Reglamento, cuando varias autoridades competentes en relación con las pruebas de penetración basadas en amenazas participen en una prueba de este tipo conjunta o compartida, tal como se contempla en el artículo 16, apartados 3 o 5, las referencias incluidas en los artículos 9 a 15 a la «autoridad competente en relación con las pruebas de penetración basadas en amenazas» se entenderán hechas a la autoridad principal competente en relación con dicha prueba conjunta o compartida.

Artículo 9

Fase de preparación

1. Una entidad financiera determinada con arreglo al artículo 26, apartado 8, párrafo tercero, del Reglamento (UE) 2022/2554 iniciará una prueba de penetración basada en amenazas tras la notificación de la autoridad competente en la materia sobre la conveniencia de llevar a cabo ese tipo de prueba.

2. En el plazo de tres meses a partir de la recepción de la notificación a que se refiere el apartado 1, la entidad financiera presentará a los gestores de la prueba de penetración basada en amenazas toda la información siguiente relativa a la puesta en marcha de la prueba:

a) una carta del proyecto que incluya un plan general del proyecto, en el que se recoja la información que figura en el anexo I;

b) los datos de contacto de la persona responsable del equipo de control;

c) información sobre el recurso previsto a probadores internos o externos, o a ambos, cuando proceda, tal como se detalla en el artículo 15;

d) información sobre los canales de comunicación que deben utilizarse durante la prueba de penetración basada en amenazas;

e) el nombre clave de la prueba.

3. Cuando la información a que se refiere el apartado 2, letras a) a e), sea completa y garantice la idoneidad y la eficaz realización de la prueba de penetración basada en amenazas, la autoridad competente en relación con la prueba validará la información de puesta en marcha y se lo notificará a la entidad financiera.

4. Tras la validación de la información de inicio de la prueba por parte de la autoridad competente, la entidad financiera creará un equipo de control para ayudar al responsable de dicho equipo a dirigir sus tareas de:

a) especificación de los canales y procesos de comunicación en el seno del equipo de control con los probadores y los proveedores de inteligencia sobre amenazas en todos los asuntos relacionados con la prueba;

b) información al órgano de dirección de la entidad financiera sobre el avance de la prueba de penetración basada en amenazas y los riesgos asociados;

c) toma de decisiones basadas en conocimientos especializados a lo largo de toda la prueba;

d) ejecución de la prueba de penetración basada en amenazas de acuerdo con lo dispuesto en el presente Reglamento;

e) selección del proveedor de inteligencia sobre amenazas para la prueba;

f) selección de probadores externos, internos o ambos;

g) elaboración del documento de especificación del alcance de la prueba.

5. Cuando la autoridad competente en relación con la prueba de penetración basada en amenazas considere que la composición inicial del equipo de control y cualquier modificación posterior de este son adecuadas para la realización de las tareas a que se refiere el apartado 4, dicha autoridad validará el equipo de control y lo notificará al responsable de este.

6. La entidad financiera presentará a los gestores de la prueba un documento de especificación del alcance de esta que contendrá toda la información establecida en el anexo II en un plazo de seis meses a partir de la recepción de la notificación de la autoridad competente en relación con la prueba a que se refiere el apartado 1. El órgano de dirección de la entidad financiera aprobará el documento de especificación del alcance de la prueba.

7. Las entidades financieras tendrán en cuenta los criterios siguientes para la inclusión de funciones esenciales o importantes en el ámbito de aplicación de la prueba de penetración basada en amenazas:

a) el carácter esencial o la importancia de la función y su posible repercusión en el sector financiero y en la estabilidad financiera a escala nacional y de la Unión;

b) la importancia de la función para las operaciones comerciales cotidianas de la entidad financiera;

c) la intercambiabilidad de la función;

d) la interconexión con otras funciones;

e) la ubicación geográfica de la función;

f) la dependencia sectorial de la función por parte de otras entidades;

g) inteligencia sobre amenazas relacionadas con la función, cuando se disponga de ella.

8. El equipo de control compartirá la información de inicio de la prueba de penetración basada en amenazas y el documento de especificación del alcance de la prueba con los probadores y los proveedores de inteligencia sobre amenazas una vez contratados. El equipo de control informará a los probadores y a los proveedores de inteligencia sobre amenazas acerca del proceso de prueba que debe seguirse.

9. La entidad financiera velará por que la contratación o asignación de probadores y proveedores de inteligencia sobre amenazas finalice antes del inicio de la fase de prueba.

10. Antes de comenzar la fase de prueba, el equipo de control consultará a los gestores de la prueba sobre la evaluación del riesgo de la prueba y sobre las medidas de gestión de riesgos. El equipo de control revisará la evaluación del riesgo o las medidas de gestión de riesgos cuando la autoridad competente en relación con la prueba considere que no abordan adecuadamente los riesgos de esta prueba.

11. El equipo de control evaluará la conformidad de los proveedores de inteligencia sobre amenazas y de los probadores que consideren involucrados en la prueba de penetración basada en amenazas con los requisitos establecidos en el artículo 27 del Reglamento (UE) 2022/2554 y con el artículo 7, apartado 1, del presente Reglamento, y documentará el resultado de dicha evaluación. El equipo de control seleccionará a los proveedores de inteligencia sobre amenazas de conformidad con dicha evaluación y con sus prácticas de gestión de riesgos. Antes de contratar a los proveedores de inteligencia sobre amenazas y a los probadores externos seleccionados, el equipo de control proporcionará evidencias a los gestores de la prueba de que dichos proveedores de inteligencia sobre amenazas y probadores cumplen los requisitos establecidos en el artículo 27 del Reglamento (UE) 2022/2554 y el artículo 7, apartado 1, del presente Reglamento. El equipo de control no procederá a contratar a los proveedores de inteligencia sobre amenazas y los probadores externos seleccionados cuando la autoridad competente en relación con la prueba de penetración basada en amenazas considere que los proveedores de inteligencia sobre amenazas y los probadores externos seleccionados no cumplen los requisitos establecidos en el artículo 27 del Reglamento (UE) 2022/2554, los requisitos establecidos en el artículo 7, apartado 1, del presente Reglamento o los requisitos adicionales derivados de la legislación nacional en materia de seguridad de conformidad con el Derecho de la Unión, o cuando la entidad financiera no cumpla lo dispuesto en el artículo 7, apartado 2, párrafo primero, del presente Reglamento, o cuando no concurran las circunstancias a que se refiere el artículo 7, apartado 2, párrafo segundo, del presente Reglamento.

12. Cuando el documento de especificación del alcance de la prueba esté completo y garantice la realización de una prueba de penetración basada en amenazas adecuada y eficaz, la autoridad competente aprobará dicho documento e informará de ello al responsable del equipo de control.

Artículo 10

Fase de prueba: inteligencia sobre amenazas

1. Tras la aprobación del documento de especificación del alcance de la prueba por parte de la autoridad competente, el proveedor de inteligencia sobre amenazas analizará la inteligencia sobre amenazas genérica y sectorial pertinente para la entidad financiera. Cuando la autoridad competente en relación con la prueba haya facilitado un panorama genérico de amenazas para el sector financiero de un Estado miembro, el proveedor de inteligencia sobre amenazas podrá utilizar dicho panorama como base de referencia para el panorama nacional de amenazas. El proveedor de inteligencia sobre amenazas detectará las ciberamenazas y las vulnerabilidades existentes o potenciales que afecten a la entidad financiera. Además, el proveedor de inteligencia sobre amenazas recopilará información y analizará inteligencia concreta, ejecutable y contextualizada sobre los objetivos y amenazas relativos a la entidad financiera, consultando en particular al equipo de control y a los gestores de la prueba.

2. El proveedor de inteligencia sobre amenazas presentará las amenazas pertinentes y la inteligencia sobre amenazas específicas, y propondrá los escenarios necesarios al equipo de control, a los probadores y a los gestores de la prueba. Los escenarios propuestos diferirán en cuanto a los agentes de amenaza detectados y las tácticas, técnicas y procedimientos asociados, y se centrarán en cada función esencial o importante incluida en el alcance de la prueba de penetración basada en amenazas.

3. El responsable del equipo de control seleccionará al menos tres escenarios para llevar a cabo la prueba de penetración basada en amenazas, basándose en todos los elementos siguientes:

a) la recomendación del proveedor de servicios de inteligencia sobre amenazas y la naturaleza de cada escenario provocado por la amenaza;

b) los datos aportados por los gestores de la prueba;

c) la viabilidad de los escenarios propuestos para la ejecución, sobre la base del criterio experto de los probadores;

d) el tamaño, la complejidad y el perfil de riesgo general de la entidad financiera y la naturaleza, escala y complejidad de sus servicios, actividades y operaciones.

4. Como máximo uno de los escenarios seleccionados podrá no estar provocado por amenazas y basarse en una amenaza prospectiva y potencialmente ficticia con un elevado valor predictivo, anticipativo, oportunista o prospectivo, habida cuenta de la evolución prevista del panorama de amenazas que afecten a la entidad financiera.

En el caso de las pruebas de penetración basadas en amenazas conjuntas, sin perjuicio de los escenarios dirigidos directamente contra funciones esenciales o importantes de las entidades financieras que participen en las pruebas, al menos un escenario incluirá los sistemas, procesos y tecnologías de TIC subyacentes pertinentes del proveedor tercero de servicios de TIC que sustenten las funciones esenciales o importantes de las entidades financieras incluidas en el alcance de la prueba.

Cuando la prueba sea una prueba de penetración basada en amenazas compartida en la que participe un proveedor intragrupo de servicios de TIC, sin perjuicio de los escenarios dirigidos directamente contra funciones esenciales o importantes de las entidades financieras que participen en la prueba, al menos un escenario incluirá los sistemas, procesos y tecnologías de TIC subyacentes pertinentes del proveedor intragrupo de servicios de TIC que sustenten las funciones esenciales o importantes de las entidades financieras incluidas en el alcance de la prueba.

5. El proveedor de inteligencia sobre amenazas facilitará el informe de inteligencia sobre amenazas específicas al equipo de control, incluidos los escenarios seleccionados de conformidad con los apartados 3 y 4. El informe de inteligencia sobre amenazas contendrá la información establecida en el anexo III.

6. El equipo de control presentará el informe de inteligencia sobre amenazas específicas al gestor de la prueba para su aprobación. Cuando el informe de inteligencia sobre amenazas específicas esté completo y garantice la realización de una prueba de penetración basada en amenazas eficaz, la autoridad competente aprobará el informe de inteligencia sobre amenazas específicas e informará de ello al responsable del equipo de control.

Artículo 11

Fase de prueba: pruebas del equipo rojo

1. Tras la aprobación del informe de inteligencia sobre amenazas específicas por parte de la autoridad competente, los probadores elaborarán el plan de pruebas del equipo rojo, que contendrá la información que figura en el anexo IV. Los probadores utilizarán el documento de especificación del alcance y el informe de inteligencia sobre amenazas específicas como base para elaborar los escenarios de ataque.

2. Los probadores consultarán al equipo de control, al proveedor de inteligencia sobre amenazas y a los gestores de la prueba sobre el plan de pruebas del equipo rojo, incluido el sistema de comunicación, procedimiento y gestión del proyecto, la preparación y los casos de uso para la activación de la asistencia, así como los mecanismos de presentación de informes al equipo de control y a los gestores de la prueba.

3. Cuando el plan de pruebas del equipo rojo esté completo y garantice la realización de una prueba de penetración basada en amenazas eficaz, el equipo de control y la autoridad competente aprobarán el plan de pruebas del equipo rojo, y la autoridad competente informará de ello al responsable del equipo de control.

4. Una vez aprobado el plan de pruebas del equipo rojo de conformidad con el apartado 3, los probadores llevarán a cabo la prueba de penetración basada en amenazas durante la fase activa de pruebas del equipo rojo.

5. La duración de la fase activa de pruebas del equipo rojo activo será proporcional al alcance de la prueba de penetración basada en amenazas, a la dimensión, la actividad, la complejidad y el número de entidades financieras y de proveedores terceros o intragrupo de servicios de TIC que participen en la prueba, y en cualquier caso tendrá una duración mínima de 12 semanas. Los escenarios de ataque pueden ejecutarse de manera secuencial o simultánea. El equipo de control, el proveedor de inteligencia sobre amenazas, los probadores y los gestores de la prueba acordarán el final de la fase activa de pruebas del equipo rojo.

6. Siempre que se garantice que el plan de pruebas del equipo rojo siga siendo completo y permita la realización de una prueba de penetración basada en amenazas eficaz, el responsable del equipo de control y los gestores de la prueba aprobarán cualquier cambio en el plan de pruebas del equipo rojo tras su aprobación, incluidos los que afecten al calendario, el alcance, los sistemas objetivo o las banderas.

7. Durante toda la fase activa de pruebas del equipo rojo, los probadores informarán, al menos una vez por semana, al equipo de control y a los gestores de la prueba sobre los avances de esta, y el proveedor de inteligencia sobre amenazas seguirá estando disponible para responder a consultas y ofrecer información adicional sobre amenazas cuando así lo solicite el equipo de control.

8. El equipo de control facilitará oportunamente asistencia diseñada con base en el plan de pruebas del equipo rojo. Se podrá añadir asistencia adicional o adaptar la proporcionada previa aprobación del equipo de control y de los gestores de la prueba.

9. En el caso de que cualquier miembro del personal de la entidad financiera o de sus proveedores terceros o intragrupo de servicios de TIC, cuando proceda, detecten las actividades de la prueba, el equipo de control, en consulta con los probadores y sin perjuicio de lo dispuesto en el apartado 10, propondrá y presentará medidas que permitan continuar con la prueba de penetración basada en amenazas, garantizando al mismo tiempo su confidencialidad a los gestores de la prueba a efectos de validación.

10. En circunstancias excepcionales que entrañen el riesgo de que los datos se vean afectados, o de provocar daños a los activos y perturbaciones en funciones, servicios u operaciones esenciales o importantes de la propia entidad financiera o de sus proveedores terceros o intragrupo de servicios de TIC, o perturbaciones en sus contrapartes o en el sector financiero, el responsable del equipo de control podrá suspender la prueba o, como último recurso, cuando no sea posible continuar con ella y siempre que así lo valide previamente la autoridad competente en relación con la prueba, proseguir con ella utilizando un ejercicio limitado de trabajo en equipo morado. La duración de dicho ejercicio limitado computará a efectos de la duración mínima de 12 semanas de la fase activa de pruebas del equipo rojo a que se refiere el apartado 5.

Artículo 12

Fase de conclusión

1. Una vez finalizada la fase activa de pruebas del equipo rojo, el responsable del equipo de control informará al equipo azul de que se ha llevado a cabo una prueba de penetración basada en amenazas.

2. En el plazo de cuatro semanas a contar desde la finalización de la fase activa de pruebas del equipo rojo, los probadores presentarán al equipo de control un informe de pruebas del equipo rojo, que contendrá la información establecida en el anexo V.

3. El equipo de control facilitará sin demora indebida el informe de pruebas del equipo rojo al equipo azul y a los gestores de la prueba.

Si así lo solicitan los gestores de la prueba, el informe a que se refiere el párrafo primero no contendrá información sensible.

4. Una vez recibido el informe de pruebas del equipo rojo, y en un plazo máximo de diez semanas a contar desde la finalización de la fase activa de pruebas del equipo rojo, el equipo azul presentará al equipo de control un informe de pruebas del equipo azul, que contendrá la información indicada en el anexo VI. El equipo de control facilitará sin demora indebida el informe de pruebas del equipo azul a los probadores y a los gestores de la prueba.

Si así lo solicitan los gestores de la prueba, el informe a que se refiere el párrafo primero no contendrá información sensible.

5. En un plazo máximo de diez semanas desde la finalización de la fase activa de pruebas del equipo rojo, el equipo azul y los probadores reproducirán las acciones ofensivas y defensivas llevadas a cabo durante la prueba de penetración basada en amenazas. El equipo de control también llevará a cabo un ejercicio de trabajo en equipo morado sobre los temas determinados conjuntamente por el equipo azul y los probadores, basado en las vulnerabilidades detectadas durante la prueba y, en su caso, en cuestiones que no pudieran probarse durante la fase activa de pruebas del equipo rojo.

6. Una vez concluidos los ejercicios de reproducción y trabajo en equipo morado, el equipo de control, el equipo azul, los probadores y los proveedores de inteligencia sobre amenazas se facilitarán mutuamente observaciones sobre el proceso de la prueba de penetración basada en amenazas. Los gestores de la prueba podrán formular observaciones.

7. Una vez que la autoridad competente en relación con la prueba de penetración basada en amenazas haya notificado al responsable del equipo de control que, a partir de su evaluación, ha concluido que el informe de pruebas del equipo azul y el informe de pruebas del equipo rojo contienen la información establecida en los anexos V y VI, la entidad financiera presentará a la autoridad competente, en un plazo de ocho semanas, el informe de síntesis de los hallazgos pertinentes de la prueba de penetración basada en amenazas a que se refiere el artículo 26, apartado 6, del Reglamento (UE) 2022/2554, que deberá contener los elementos establecidos en el anexo VII para su aprobación.

Si así lo solicita la autoridad competente, el informe a que se refiere el párrafo primero no contendrá información sensible.

Artículo 13

Plan corrector

1. En el plazo de ocho semanas a contar desde la notificación a que se refiere el artículo 12, apartado 7, del presente Reglamento, la entidad financiera presentará los planes correctores y la documentación a que se refiere el artículo 26, apartado 6, del Reglamento (UE) 2022/2554 a la autoridad competente en relación con las pruebas de penetración basadas en amenazas y, cuando sea diferente, a la autoridad competente sobre la entidad financiera.

2. El plan corrector a que se refiere el apartado 1 incluirá, para cada incidencia producida en el marco de la prueba de penetración basada en amenazas:

a) una descripción de las deficiencias detectadas;

b) una descripción de las medidas correctoras propuestas y de su orden de prioridad y finalización prevista, incluidas, cuando proceda, las medidas dirigidas a mejorar las capacidades de identificación, protección, detección y respuesta;

c) un análisis de las causas profundas;

d) el personal o las funciones de la entidad financiera responsables de aplicar las medidas correctoras o las mejoras propuestas;

e) los riesgos asociados a la no aplicación de las medidas a que se refiere la letra b) y, en su caso, los riesgos asociados a la aplicación de dichas medidas.

Artículo 14

Informe de validación

1. El informe de validación a que se refiere el artículo 26, apartado 7, del Reglamento (UE) 2022/2554 contendrá la información que figura en el anexo VIII.

2. Cuando varias autoridades competentes en relación con las pruebas de penetración basadas en amenazas hayan participado en una prueba de este tipo, la autoridad principal competente expedirá el informe de validación a que se refiere el artículo 26, apartado 7, del Reglamento (UE) 2022/2554 a las entidades financieras sometidas a prueba.

Artículo 15

Recurso a probadores internos

1. Las entidades financieras establecerán todas las disposiciones siguientes para el recurso a probadores internos:

a) el establecimiento y la aplicación de una política para la gestión de probadores internos en el marco de una prueba de penetración basada en amenazas;

b) medidas para garantizar que el recurso a probadores internos para llevar a cabo una prueba de penetración basada en amenazas no afecte negativamente a las capacidades generales defensivas o de resiliencia de la entidad financiera frente a incidentes relacionados con las TIC ni afecte de manera significativa a la disponibilidad de recursos dedicados a tareas relacionadas con las TIC durante una prueba de esta naturaleza;

c) medidas para garantizar que los probadores internos dispongan de recursos y capacidades suficientes para llevar a cabo una prueba de penetración basada en amenazas.

La política a que se refiere la letra a):

a) contendrá criterios para evaluar la idoneidad, la competencia y los posibles conflictos de intereses de los probadores internos, así como para especificar las responsabilidades de gestión en el proceso de la prueba;

b) se documentará y será objeto de revisiones periódicas;

c) dispondrá que el equipo de pruebas interno incluya un responsable y al menos dos miembros adicionales;

d) exigirá que todos los miembros del equipo de pruebas hayan sido contratados por la entidad financiera o por un proveedor intragrupo de servicios de TIC durante los 12 meses anteriores;

e) incluirá disposiciones relativas a la formación sobre cómo los probadores internos han de realizar pruebas de penetración y pruebas de equipo rojo.

2. Cuando una autoridad competente en relación con las pruebas de penetración basadas en amenazas apruebe el recurso a probadores internos de conformidad con el artículo 27, apartado 2, letra a), del Reglamento (UE) 2022/2554, dicha autoridad tendrá en cuenta los requisitos establecidos en el artículo 7, apartado 1, del presente Reglamento.

3. Cuando se recurra a probadores internos, la entidad financiera se asegurará de que dicha medida se mencione en los documentos siguientes:

a) la información relativa al inicio de la prueba a que se refiere el artículo 9;

b) el informe de pruebas del equipo rojo a que se refiere el artículo 12, apartado 2;

c) el informe de síntesis de los hallazgos pertinentes de la prueba de penetración basada en amenazas a que se refiere el artículo 26, apartado 6, del Reglamento (UE) 2022/2554.

4. Los probadores a los que recurra un proveedor intragrupo de servicios de TIC se considerarán probadores internos de la entidad financiera.

Artículo 16

Cooperación y reconocimiento mutuo

1. A efectos de la realización de una prueba de penetración basada en amenazas en relación con una entidad financiera que preste servicios en más de un Estado miembro, incluso a través de una sucursal, su autoridad competente en relación con este tipo de pruebas:

a) determinará qué autoridades competentes en relación con este tipo de pruebas deberán participar en la prueba en el Estado miembro de acogida, teniendo en cuenta si se ejerce o comparte una o varias funciones esenciales o importantes en los Estados miembros de acogida;

b) informará a las autoridades competentes determinadas de conformidad con la letra a) de la decisión de someter a una prueba de penetración basada en amenazas a la entidad financiera;

c) a menos que las autoridades competentes en relación con las pruebas de penetración basadas en amenazas acuerden otra cosa, la autoridad competente sobre la entidad financiera dirigirá la prueba.

En un plazo de veinte días hábiles a partir de la recepción de la información sobre la futura realización de una prueba de penetración basada en amenazas, las autoridades competentes de los Estados miembros de acogida podrán manifestar su interés en seguir la prueba en calidad de observadores o designar a un gestor de pruebas para que participe en la prueba. La autoridad principal competente proporcionará a todas las autoridades competentes que participen en calidad de observadores el documento de especificación del alcance de la prueba, el informe de síntesis de esta, el plan corrector y el informe de validación.

La autoridad principal competente en relación con las pruebas de penetración basadas en amenazas coordinará a todas las autoridades participantes a lo largo de toda la prueba y adoptará todas las decisiones necesarias para llevarla a cabo de manera adecuada y eficaz. La autoridad principal competente podrá fijar un número máximo de autoridades participantes en la prueba cuando, de no hacerlo, se pudiera poner en peligro la eficiencia de su realización.

2. Cuando una entidad financiera utilice el mismo proveedor intragrupo de servicios de TIC que entidades financieras establecidas en otros Estados miembros, o pertenezca a un grupo y comparta sistemas de TIC con entidades financieras del mismo grupo establecidas en otros Estados miembros, la autoridad competente sobre la entidad financiera se pondrá en contacto con las autoridades competentes sobre las demás entidades financieras que utilicen el mismo proveedor intragrupo de servicios de TIC o compartan sistemas de TIC como parte del grupo y evaluarán con ellas la viabilidad y la idoneidad de llevar a cabo una prueba de penetración basada en amenazas compartida. Será preferible realizar una prueba de penetración basada en amenazas compartida frente a una individual cuando pueda dar lugar a una reducción de costes y del consumo de recursos para las entidades financieras y para las autoridades competentes en relación con este tipo de pruebas, siempre que la solidez y eficacia de las pruebas no se vean perjudicadas por ello.

3. A efectos de la realización de una prueba de penetración basada en amenazas compartida:

a) las autoridades competentes sobre las entidades financieras en relación con este tipo de pruebas acordarán qué entidad financiera será designada para llevarla a cabo, teniendo en cuenta la estructura del grupo y la eficiencia de la prueba;

b) la autoridad competente sobre la entidad financiera designada de conformidad con la letra a) dirigirá la prueba, salvo acuerdo en contrario de las autoridades competentes sobre las entidades financieras que participen en la prueba compartida;

c) las autoridades competentes sobre las entidades financieras distintas de la entidad financiera designada para dirigir la prueba compartida podrán manifestar su interés en seguir la prueba en calidad de observadores o asignar un gestor para dicha prueba.

La autoridad principal competente coordinará a todas las autoridades competentes que participen en la prueba compartida y adoptará todas las decisiones necesarias para llevarla a cabo de manera sólida y eficaz.

4. Cuando una entidad financiera tenga la intención de llevar a cabo una prueba de penetración basada en amenazas conjunta, tal como se contempla en el artículo 26, apartado 4, del Reglamento (UE) 2022/2554, en la que puedan participar entidades financieras establecidas en otros Estados miembros, su autoridad competente en relación con este tipo de pruebas se pondrá en contacto con las autoridades competentes sobre las demás entidades financieras y evaluará con ellas la viabilidad y la idoneidad de llevar a cabo una prueba conjunta de conformidad con el artículo 26, apartado 4, del Reglamento (UE) 2022/2554.

5. A efectos de la realización de una prueba de penetración basada en amenazas conjunta a que se refiere el artículo 26, apartado 4, del Reglamento (UE) 2022/2554:

a) las autoridades competentes en relación con las pruebas de penetración basadas en amenazas de las entidades financieras acordarán qué entidad financiera será la designada para llevar a cabo la prueba conjunta de penetración basada en amenazas teniendo en cuenta los servicios de TIC prestados por el proveedor tercero de servicios de TIC a las entidades financieras y la eficiencia de la prueba;

b) la autoridad competente sobre la entidad financiera designada de conformidad con la letra a) dirigirá la prueba, salvo acuerdo en contrario de las autoridades competentes sobre las entidades financieras que participen en la prueba conjunta;

c) las autoridades competentes en relación con las pruebas de penetración basadas en amenazas sobre las entidades financieras distintas de la entidad financiera designada para dirigir la prueba conjunta podrán manifestar su interés en seguir la prueba en calidad de observadores o asignar un gestor para dicha prueba.

La autoridad principal competente coordinará a todas las autoridades competentes que participen en la prueba conjunta y adoptará todas las decisiones necesarias para llevarla a cabo de manera sólida y eficaz.

6. Cuando, en relación con una entidad financiera obligada a realizar una prueba de penetración basada en amenazas, su autoridad competente en relación con este tipo de pruebas difiera de la autoridad competente sobre ella a que se refiere el artículo 46 del Reglamento (UE) 2022/2554, dichas autoridades compartirán cualquier información pertinente con respecto a todas las cuestiones relacionadas con la prueba a efectos de llevar a cabo esta o de desempeñar sus funciones de conformidad con dicho Reglamento.

Artículo 17

Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 13 de febrero de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

Contenido de la carta del proyecto [artículo 9, apartado 2, letra a)]

Elemento de información	Información exigida
Persona responsable del plan del proyecto, es decir, responsable del equipo de control	Nombre Datos de contacto
Probadores	☐ internos ☐ externos ☐ ambos
Canales de comunicación seleccionados de conformidad con el artículo 9, apartado 2, letra d), y el artículo 9, apartado 4, letra a), en particular: a) el cifrado de correo electrónico que se utilizará b) las salas de datos en línea que se utilizarán c) el servicio de mensajería instantánea que se utilizará	
Nombre clave de la prueba de penetración basada en amenazas	
En su caso, funciones esenciales o importantes que la entidad financiera realice en otros Estados miembros	1. lista de funciones esenciales o importantes realizadas en otro Estado miembro 2. para cada función esencial o importante, indicación del Estado o Estados miembros en los que se realizan
En su caso, funciones esenciales o importantes sustentadas por proveedores terceros de servicios de TIC	3. lista de funciones esenciales o importantes sustentadas por proveedores terceros de servicios de TIC 4. para cada función, identificación del proveedor tercero de servicios de TIC
Plazos previstos para la finalización de:	
(1) la fase de preparación, de conformidad con el artículo 9	aaaa-mm-dd
(2) la fase de prueba, de conformidad con los artículos 10 y 11	aaaa-mm-dd
(3) la fase de conclusión, de conformidad con el artículo 12	aaaa-mm-dd
(4) el plan corrector, de conformidad con el artículo 13	aaaa-mm-dd

ANEXO II

Contenido del documento de especificación del alcance de la prueba (artículo 9, apartado 6)

1. El documento de especificación del alcance de la prueba contendrá una lista de todas las funciones esenciales o importantes señaladas por la entidad financiera.

2. Para cada función esencial o importante señalada se incluirá la información siguiente:
   a) cuando la función esencial o importante no esté incluida en el alcance de la prueba de penetración basada en amenazas, la explicación de los motivos por los que no se incluye;
   b) cuando la función esencial o importante esté incluida en el ámbito de aplicación de la prueba:
      i) la explicación de los motivos de su inclusión,
      ii) el sistema o sistemas de TIC identificados que sustenten esa función esencial o importante,
      iii) para cada sistema de TIC identificado:
         1. si se ha subcontratado y, en caso afirmativo, el nombre del proveedor tercero de servicios de TIC;
         2. las jurisdicciones en las que se utiliza el sistema de TIC;
         3. una descripción general de la(s) bandera(s) preliminar(es), en la que se indique qué aspecto de protección de la confidencialidad, integridad, autenticidad o disponibilidad está cubierto por cada bandera.

ANEXO III

Contenido del informe de inteligencia sobre amenazas específicas (artículo 10, apartado 5)

El informe de inteligencia sobre amenazas específicas contendrá información sobre todos los aspectos siguientes:

1. El alcance general de la investigación de inteligencia, incluidos, como mínimo, los elementos siguientes:
   a) funciones esenciales o importantes incluidas en el alcance de la prueba;
   b) ubicación geográfica de dichas funciones esenciales o importantes;
   c) lengua oficial de la UE utilizada;
   d) proveedores terceros de servicios de TIC pertinentes;
   e) período durante el cual se lleva a cabo la investigación.
2. La evaluación general de qué información concreta aplicable puede encontrarse sobre la entidad financiera, en particular:
   a) los nombres de usuario y las contraseñas de los empleados;
   b) los dominios similares que pueden confundirse con los dominios oficiales de la entidad financiera;
   c) reconocimiento técnico: programas informáticos, sistemas y tecnologías vulnerables o susceptibles de ser explotados;
   d) la información enviada por los empleados a través de internet relacionada con la entidad financiera y que pueda utilizarse para un ataque;
   e) información destinada a la venta en la red oscura;
   f) cualquier otra información pertinente disponible en internet o en redes públicas;
   g) cuando proceda, información sobre objetivos físicos, incluidas las formas de acceso a las instalaciones de la entidad financiera.
3. Un análisis de la inteligencia sobre amenazas teniendo en cuenta el panorama general de amenazas y la situación particular de la entidad financiera, que incluya, como mínimo:
   a) el entorno geopolítico;
   b) el entorno económico;
   c) las tendencias tecnológicas y cualquier otra tendencia relacionada con las actividades llevadas a cabo en el sector de los servicios financieros.
4. Perfiles de amenaza de los agentes malintencionados (persona o grupo específico, o clase genérica) que puedan actuar contra la entidad financiera, incluidos los sistemas de la entidad financiera que los agentes malintencionados tengan más probabilidades de comprometer o perseguir, la posible motivación, intención y justificación del posible ataque y el posible *modus operandi* de los atacantes.
5. Escenarios de amenaza: al menos tres escenarios de amenaza de extremo a extremo para los perfiles de amenaza determinados de conformidad con el punto 4 que presenten las puntuaciones más altas en cuanto a gravedad de la amenaza. Los escenarios de amenaza describirán la trayectoria de ataque de extremo a extremo e incluirán, como mínimo:
   a) un escenario que incluya, entre otras cosas, la puesta en peligro de la disponibilidad del servicio;
   b) un escenario que incluya, entre otras cosas, la puesta en peligro de la integridad de los datos;
   c) un escenario que incluya, entre otras cosas, la puesta en peligro de la confidencialidad de la información.
6. Cuando proceda, una descripción del escenario no provocado por amenazas a que se refiere el artículo 10, apartado 4.

ANEXO IV

Contenido del plan de pruebas del equipo rojo (artículo 11, apartado 1)

El plan de pruebas del equipo rojo contendrá información sobre todos los aspectos siguientes:

a) los canales y procedimientos de comunicación;

b) las tácticas, técnicas y procedimientos permitidos y no permitidos para su uso en el ataque, incluidos los límites éticos a la ingeniería social;

c) las medidas de gestión de riesgos que deberán seguir los probadores;

d) una descripción de cada escenario, que incluya:

   i) el agente de riesgo simulado,

   ii) su intención, motivación y objetivos,

   iii) la función o funciones objetivo y el sistema o sistemas de TIC que las sustenten,

   iv) los aspectos relacionados con la confidencialidad, integridad, disponibilidad y autenticidad objetivo del ataque,

   v) las banderas;

e) una descripción detallada de cada trayectoria de ataque prevista, incluidos los requisitos previos y la posible asistencia que deberá proporcionar el equipo de control, incluidos los plazos para su puesta a disposición y su posible uso;

f) el calendario de las actividades de trabajo en equipo rojo, incluida la planificación temporal para la ejecución de cada escenario, desglosada como mínimo en función de las tres fases que el probador lleva a cabo a lo largo de la fase de prueba, a saber, la introducción en los sistemas de TIC de las entidades financieras, la navegación por dichos sistemas y la ejecución de acciones sobre objetivos y, en su caso, su extracción de los sistemas de TIC (fases de entrada, actuación y salida);

g) las particularidades de la infraestructura de las entidades financieras que deben tenerse en cuenta durante la prueba;

h) en su caso, información adicional u otros recursos necesarios para los probadores a efectos de la ejecución de los escenarios.

ANEXO V

Contenido del informe de pruebas del equipo rojo (artículo 12, apartado 2)

El informe de pruebas del equipo rojo contendrá información sobre, como mínimo, todos los elementos siguientes:

a) información sobre el ataque perpetrado, en particular:
   i) las funciones esenciales o importantes específicas y los sistemas, procesos y tecnologías de TIC identificados que sustenten la función esencial o importante, tal como se indique en el plan de pruebas del equipo rojo,
   ii) un resumen de cada escenario,
   iii) las banderas alcanzadas y no alcanzadas,
   iv) las trayectorias de ataque seguidas con éxito y sin éxito,
   v) las tácticas, técnicas y procedimientos utilizados con éxito y sin éxito,
   vi) las desviaciones del plan de pruebas del equipo rojo, en su caso,
   vii) la asistencia concedida, en su caso;

b) todas las acciones de las que los probadores tengan conocimiento que llevó a cabo el equipo azul para reconstruir el ataque y mitigar sus efectos;

c) las vulnerabilidades detectadas y otras constataciones, en particular:
   i) una descripción de las vulnerabilidades y otras constataciones, incluido su carácter esencial,
   ii) un análisis de las causas profundas de los ataques que tuvieron éxito,
   iii) recomendaciones sobre la introducción de medidas correctoras, indicando su prioridad.

ANEXO VI

Contenido del informe de pruebas del equipo azul (artículo 12, apartado 4)

El informe de prueba del equipo azul contendrá información sobre, como mínimo, todos los elementos siguientes:

1. para cada paso del ataque descrito por los probadores en el informe de pruebas del equipo rojo:
   a) lista de acciones de ataque detectadas;
   b) anotaciones de registro correspondientes a esas detecciones;
2. evaluación de las conclusiones y recomendaciones de los probadores;
3. pruebas del ataque por los probadores recopiladas por el equipo azul;
4. análisis del equipo azul sobre las causas profundas de los ataques llevados a cabo por los probadores que tuvieron éxito;
5. relación de lecciones aprendidas y posibilidades de mejora detectadas;
6. lista de temas que se abordarán en el trabajo en equipo morado.

ANEXO VII

Detalles del informe de síntesis de los hallazgos pertinentes de la prueba de penetración basada en amenazas a que se refiere el artículo 26, apartado 6, del Reglamento (UE) 2022/2554

El informe de síntesis de la prueba contendrá información, como mínimo, sobre todos los elementos siguientes:

a) partes implicadas;

b) plan del proyecto;

c) alcance validado de la prueba, incluida la justificación de la inclusión o exclusión de funciones esenciales o importantes y los sistemas, procesos y tecnologías de TIC identificados que sustenten las funciones esenciales o importantes cubiertas por la prueba;

d) escenarios seleccionados y cualquier desviación significativa del informe de inteligencia sobre amenazas específicas;

e) vías de ataque ejecutadas y tácticas, técnicas y procedimientos utilizados;

f) banderas capturadas y no capturadas;

g) desviaciones del plan de pruebas del equipo rojo, en su caso;

h) detecciones del equipo azul, en su caso;

i) trabajo en equipo morado en la fase de prueba, cuando se haya llevado a cabo, y las condiciones en que se realizó;

j) asistencia utilizada, en su caso;

k) medidas de gestión de riesgos adoptadas;

l) vulnerabilidades detectadas y otras constataciones, incluido su carácter esencial;

m) análisis de las causas profundas de los ataques que tuvieron éxito;

n) un plan corrector general en el que se establezca la relación entre las vulnerabilidades y otras constataciones, sus causas profundas y la prioridad de las medidas correctoras;

o) lecciones extraídas de las observaciones recibidas.

ANEXO VIII

Detalles del informe de validación de la prueba de penetración basada en amenazas a que se refiere el artículo 26, apartado 7, del Reglamento (UE) 2022/2554

El informe de validación contendrá, como mínimo, toda la información siguiente:

a) sobre la prueba de penetración basada en amenazas realizada:
   i) las fechas de inicio y finalización de la prueba,
   ii) las funciones esenciales o importantes incluidas en el alcance de la prueba,
   iii) cuando proceda, información sobre las funciones esenciales o importantes incluidas en el alcance de la prueba en relación con las cuales no se haya realizado esta,
   iv) cuando proceda, otras entidades financieras que participaron en la prueba,
   v) cuando proceda, los proveedores terceros de servicios de TIC que participaron en la prueba,
   vi) en lo que respecta a los probadores:
      1. si se recurrió a probadores internos;
      2. si la entidad financiera hizo uso del artículo 5, apartado 3, párrafo segundo,
   vii) la duración, en días naturales, de la fase activa de pruebas del equipo rojo;
b) cuando participasen varias autoridades competentes en relación con la prueba de penetración basada en amenazas, el resto de las autoridades competentes en relación con dicha prueba y en qué calidad participaron;
c) la lista de los documentos examinados por la autoridad competente en relación con la prueba de penetración basada en amenazas a efectos de la validación.