BANCO CENTRAL EUROPEO

EUROSISTEMA

ES **ECB-PUBLIC**

DICTAMEN DEL BANCO CENTRAL EUROPEO

de 11 de noviembre de 2019

sobre la seguridad de las redes y sistemas de información

(CON/2019/38)

Introducción y fundamento jurídico

El 10 de octubre de 2019 el Banco Central Europeo (BCE) recibió del Banco de España, en nombre de la Secretaría de Estado para el Avance Digital (SEAD), una solicitud de dictamen sobre un proyecto de real decreto sobre la seguridad de las redes y sistemas de información (en lo sucesivo, el «proyecto de real decreto»). El proyecto de real decreto desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información[1].

La competencia consultiva del BCE se basa en el artículo 127, apartado 4, y en el artículo 282, apartado 5, del Tratado de Funcionamiento de la Unión Europea, así como en el artículo 2, apartado 1, guiones tercero, quinto y sexto, de la Decisión 98/415/CE del Consejo[2], ya que el proyecto de real decreto afecta al Banco de España, a los sistemas de pago y liquidación, a normas aplicables a las entidades financieras que influyen significativamente en la estabilidad de las entidades y los mercados financieros, y a las tareas encomendadas al BCE conforme al artículo 127, apartado 6, del Tratado, respecto de la supervisión prudencial de las entidades de crédito. De conformidad con la primera frase del artículo 17.5 del Reglamento interno del Banco Central Europeo, el presente dictamen ha sido adoptado por el Consejo de Gobierno.

1. Objeto del proyecto de real decreto

1.1 El objeto del proyecto de real decreto es desarrollar ciertos aspectos del Real Decreto-ley 12/2018. Estas normas incorporan al derecho interno la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo[3] y complementan la legislación pertinente en vigor en España antes de adoptarse la Directiva (UE) 2016/1148, en particular la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas[4].

1.2 *Designación del Banco de España y de la Comisión Nacional del Mercado de Valores como autoridades competentes*

1 BOE núm. 2018, de 8 de septiembre de 2018.

2 Decisión 98/415/CE del Consejo, de 29 de junio de 1998, relativa a la consulta de las autoridades nacionales al Banco Central Europeo acerca de los proyectos de disposiciones legales (DO L 189 de 3.7.1998, p. 42).

3 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

4 BOE núm. 102, de 29 de abril de 2011.

1.3 A efectos de la seguridad de las redes y sistemas de información, el proyecto de real decreto designa al Banco de España como la autoridad competente para las entidades de crédito, en cuanto operadores de servicios esenciales, siempre que no estén clasificadas como operadores críticos. Ni el Real Decreto-ley 12/2018 ni el proyecto de real decreto determinan quiénes son los operadores de servicios esenciales. Si una entidad de crédito se clasificara como operador crítico, la autoridad competente sería el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), que es parte de la Secretaría de Estado de Seguridad, que a su vez está integrada en el Ministerio del Interior.

1.4 El proyecto de real decreto encomienda a las autoridades competentes la supervisión del cumplimiento por los operadores de servicios esenciales de sus obligaciones en materia de seguridad de las redes y sistemas de información y de notificación de incidentes. Los operadores de servicios esenciales deben cooperar con la autoridad competente y proporcionarle toda la información que precise. El proyecto de real decreto faculta a las autoridades competentes para llevar a cabo inspecciones en el desempeño de sus funciones. De acuerdo con el proyecto de real decreto, el Banco de España, como autoridad competente, puede además adoptar circulares para asegurar una comunicación eficaz con las entidades de crédito y supervisar el cumplimiento de los requisitos que les sean aplicables.

1.5 El proyecto de real decreto dispone que sus disposiciones se entiendan sin perjuicio de las competencias y funciones atribuidas al Banco de España, al BCE y al Sistema Europeo de Bancos Centrales, de conformidad con el Tratado, los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo (en lo sucesivo, los «Estatutos del SEBC»), y el Reglamento (UE) n.º 1024/2013 del Consejo[5]. Las disposiciones del proyecto de real decreto se entienden también sin perjuicio de la Ley 13/1994, de 1 de junio, de autonomía del Banco de España[6]. Las disposiciones del proyecto de real decreto solo se aplican al Banco de España en lo no previsto en su normativa específica y en la medida en que sean compatibles con la naturaleza, funciones e independencia del Banco de España.

1.6 El proyecto de real decreto designa también, a efectos de la seguridad de las redes y sistemas de información, a la Comisión Nacional del Mercado de Valores (CNMV) como autoridad competente para las entidades que prestan servicios de inversión y las sociedades gestoras de instituciones de inversión colectiva. Si una entidad o sociedad de esta clase fuera clasificada como operador crítico, la autoridad competente sería la Secretaría de Estado de Seguridad, a través del CNPIC.

1.7 *Obligaciones de los operadores de servicios esenciales*

1.8 El proyecto de real decreto establece los siguientes requisitos de seguridad para los operadores de servicios esenciales, incluidas las entidades de crédito designadas como tales: i) aprobar políticas de seguridad que consideren, como mínimo, los siguientes aspectos: análisis y gestión de riesgos, gestión de riesgos de terceros o proveedores, detección y gestión de incidentes, planes de recuperación y aseguramiento de la continuidad de las operaciones, e interconexión de sistemas; y ii) designar un responsable de la seguridad de la información que actúe de punto de

5 Reglamento (UE) n.º 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito (DO L 287 de 29.10.2013 p. 63).

6 BOE núm. 131, de 2 de junio de 1994.

contacto con la autoridad competente y se coordine con ella si se produce un incidente de seguridad. Las funciones del responsable de la seguridad de la información comprenden la elaboración de las políticas de seguridad, la supervisión de su aplicación, y la notificación de incidentes a la autoridad competente. Según el proyecto de real decreto, el responsable de la seguridad de la información debe contar con personal con conocimientos especializados y experiencia, así como con los recursos necesarios para desarrollar sus funciones, y ser independiente de los responsables de las redes y los sistemas de información.

1.9 Los operadores de servicios esenciales deben gestionar y resolver los incidentes de seguridad que afecten a las redes y los sistemas de información que utilicen para prestar sus servicios, tanto los detectados por ellos mismos como los notificados por la autoridad competente o el equipo de respuesta a incidentes de seguridad informática (*Computer Security Incident Response Team*, CSIRT) de referencia. Los operadores de servicios esenciales deben además notificar a la autoridad competente, a través del CSIRT de referencia, los incidentes que tengan un nivel de impacto crítico, muy alto o alto. También deben notificar a la autoridad competente los incidentes que puedan afectar a las redes y los sistemas de información que se utilicen para prestar servicios esenciales, aun cuando no hayan tenido todavía efectos adversos reales.

1.10 *Otras medidas*

1.11 El proyecto de real decreto dispone asimismo la cooperación entre los diversos CSIRT, y entre estos y las autoridades competentes, por medio de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, que garantiza el intercambio seguro de la información.

1.12 El proyecto de real decreto incluye un anexo con la instrucción nacional de notificación y gestión de ciberincidentes, que establece los criterios de clasificación de los ciberincidentes y de su asignación a un nivel de peligrosidad determinado y que contiene un cuadro donde figura la información que los operadores de servicios esenciales deben notificar a la autoridad competente.

2. Observaciones generales

2.1 Como ha manifestado anteriormente[7], El BCE apoya el objetivo de la Directiva (UE) 2016/1148 de garantizar un alto nivel común de seguridad de las redes y de la información en la Unión y de conseguir que este campo se aborde de modo coherente en todos los sectores económicos y todos los Estados miembros. Es importante garantizar que el mercado interior sea un lugar seguro para hacer negocios y que todos los Estados miembros tengan un cierto nivel mínimo de preparación frente a los incidentes de ciberseguridad. Debe garantizarse al mismo tiempo que las disposiciones nacionales que transponen la Directiva (UE) 2016/1148 se coordinen con las competencias del Eurosistema[8] y respeten el principio de independencia de los bancos centrales establecido en el artículo 130 del Tratado. Conforme a la recomendación del BCE, el considerando 14 de la Directiva (UE) 2016/1148 afirma que esta no afecta al régimen de supervisión por el

7 Véanse el apartado 2.1 del Dictamen CON/2014/58, el apartado 2.1 del Dictamen CON/2017/10, el apartado 2.2 del Dictamen CON/2018/22, el apartado 2.2 del Dictamen CON/2018/27, y el apartado 2.2 del Dictamen CON/2019/17. Todos los dictámenes del BCE se publican en su dirección en internet, www.ecb.europa.eu.

8 Véanse también el apartado 2.2 del Dictamen CON/2014/58, el apartado 2.2 del Dictamen CON/2017/10, y el apartado 3.1.1 del Dictamen CON/2018/22.

Eurosistema de los sistemas de pago y liquidación[9]. Por otra parte, la seguridad de las redes y sistemas de información se beneficia de las sinergias y de las economías de escala. En particular, las autoridades nacionales competentes pueden convertirse en repositorios de unos recursos y una experiencia considerables a los que puede recurrir el Eurosistema en materia de seguridad de las redes y sistemas de información. Además, el reconocimiento de la independencia de BCE y de sus órganos rectores no tiene como consecuencia desvincular al Eurosistema por completo de la Unión ni eximirlo de toda norma jurídica de esta[10]. No cabe excluir en principio la aplicación al Eurosistema de las medidas nacionales de ejecución de la Directiva (UE) 2016/1148[11].

2.2 En virtud de lo expuesto, el BCE celebra que el Banco de España sea designado autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información y que las disposiciones del proyecto de real decreto se entiendan sin perjuicio de las competencias y funciones atribuidas al Banco de España, al BCE y al SEBC, de conformidad con el Tratado, los Estatutos del SEBC, el Reglamento (UE) n.º 1024/2013 y la Ley 13/1994[12], de manera que el proyecto de real decreto solo se aplique al Banco de España en lo no previsto en su normativa específica y en la medida en que sea compatible con su naturaleza, sus funciones y su independencia.

2.3 La designación del Banco de España como autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información garantiza que este se beneficie de los recursos y la información específicos de este ámbito y que, en particular, reciba puntual y eficazmente información sobre los ciberincidentes o ciberamenazas reales y potenciales que afecten a los sistemas e infraestructuras del sector financiero[13]. Además, el proyecto de real decreto garantiza que el Banco de España pueda llevar a cabo sus funciones de autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información sin perjuicio de sus funciones como integrante del Eurosistema y del Mecanismo Único de Supervisión (MUS). Sobre este particular, el BCE entiende que la clarificación de que el proyecto de real decreto se entiende sin perjuicio de las competencias y funciones, incluidas las relacionadas con el SEBC y el MUS, atribuidas al Banco de España conforme al Tratado, a los Estatutos del SEBC, al Reglamento (UE) n.º 1024/2013 y a la Ley 13/1994, significa que el proyecto de real decreto se aplica respecto de todas las competencias y funciones del Banco de España y no solo respecto de su designación como autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información.

2.4 El BCE celebra que el proyecto de real decreto se aplique sin perjuicio de las competencias y funciones atribuidas al BCE de conformidad con el Tratado, los Estatutos del SEBC y el Reglamento (UE) n.º 1024/2013.

2.5 Asimismo, el BCE manifiesta su disposición a cooperar con las autoridades españolas por lo que respecta a los sistemas e infraestructuras cuya vigilancia o funcionamiento dependa del Eurosistema, como los sistemas e instrumentos de pago, y por lo que respecta a la supervisión

9 Véanse el apartado 3.1 del Dictamen CON/2014/58 y el apartado 3.5 del Dictamen CON/2017/10.

10 Véase la sentencia del Tribunal de Justicia de 10 de julio de 2003, *Comisión contra BCE*, C-11/00, ECLI:EU:C:2003:395, apartados 134 a 136.

11 Véase el apartado 2.2 del Dictamen CON/2019/17.

12 Disposición adicional cuarta del proyecto de real decreto.

13 Véanse los apartados 3.2.4 y 3.4.3 del Dictamen CON/2018/22 y el apartado 4.4 del Dictamen CON/2018/47.

prudencial de las entidades de crédito, a fin de asegurar la adopción y el seguimiento de las mejores prácticas en materia de seguridad de las redes y sistemas de información[14]. El BCE ya pidió que se establecieran tales mecanismos eficaces de cooperación e intercambio de información entre las autoridades nacionales encargadas de la seguridad de las redes y sistemas de información y, por medio de los bancos centrales nacionales (BCN), el BCE[15]. En este punto, el BCE entiende[16] que el Banco de España puede compartir con el BCE puntual y eficientemente y conforme a sus responsabilidades respectivas la información pertinente que reciba de diversos interesados como autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información[17].

3. Efectos del proyecto de real decreto en los sistemas de pago y en los sistemas de liquidación de valores

3.1 *Efectos en otros operadores de servicios esenciales del sector estratégico financiero y tributario*

3.1.1 La Ley 8/2011 considera al «sistema financiero y tributario» como un sector estratégico, esto es, un área de actividad económica que proporciona un servicio esencial. Los servicios esenciales se definen tanto en la Ley 8/2011 como en el Real Decreto-ley 12/2018 como los servicios que son necesarios para mantener: i) las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o ii) el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas, y que dependen de las redes y sistemas de information. El Real Decreto-ley 12/2018 aclara que los operadores de servicios esenciales son entidades públicas o privadas que prestan servicios esenciales en alguno de los sectores estratégicos definidos en la Ley 8/2011. El Real Decreto-ley 12/2018 aclara además que un operador se considerará operador de servicios esenciales cuando los incidentes que sufra puedan tener efectos perturbadores significativos en la prestación de los servicios, en función, entre otros factores, de las alternativas disponibles o del número de usuarios.

3.1.2 El proyecto de real decreto designa expresamente las autoridades competentes, a los efectos de la seguridad de las redes y sistemas de información, para las entidades de crédito, las entidades aseguradoras, las sociedades gestoras de instituciones de inversión colectiva y las entidades que prestan servicios de inversión clasificadas como operadores de servicios esenciales para el sistema financiero y tributario, siempre que no estén clasificadas como operadores críticos. Sin embargo, el proyecto de real decreto no designa expresamente las autoridades competentes, a los efectos de la seguridad de las redes y sistemas de información, para otras entidades, en la medida en que no sean operadores críticos, que también forman parte del sistema financiero y tributario, como los gestores de centros de negociación o las entidades de contrapartida central, que son objeto de referencia expresa en el anexo II de la Directiva (UE) 2016/1148, u otros sistemas de

14 Véase el apartado 6.3 del Dictamen CON/2018/22.

15 Véanse los apartados 2.3 y 6.2 del Dictamen CON/2018/22 y los apartados 2.4, 3.1.6, 3.2.4 y 4.7 del Dictamen CON/2019/17.

16 Esta interpretación se basa en el artículo 14 del Real Decreto-ley 12/2018,que permite el intercambio de información entre autoridades, y en las disposiciones generales sobre confidencialidad aplicables al Banco de España.

17 Véanse el apartado 4.3 del Dictamen CON/2018/27, el apartado 6.2 del Dictamen CON/2018/47 y el apartado 2.4 del Dictamen CON/2019/17.

pago y de liquidación de valores, y tampoco facilita orientación adicional en cuanto a qué constituye a una entidad en operador de servicios esenciales. El BCE entiende que estas otras infraestructuras, sujetas a la vigilancia del BCE o del Banco de España, podrían designarse como operadores críticos, en cuyo caso la autoridad competente a los efectos de la seguridad de las redes y sistemas de información sería la Secretaría de Estado de Seguridad, a través del CNPIC, sobre la base de la designación del Real Decreto-ley 12/2018. En este punto, no está claro si el propio Banco de España, en calidad de operador de un sistema de pago de importancia sistémica como el componente español de TARGET2, es decir, TARGET2-Banco de España, estaría sujeto a las obligaciones que el proyecto de real decreto impone a los operadores de servicios esenciales.

3.2 *Efectos en los operadores de infraestructuras del mercado: sistemas de pago de importancia sistémica (SIPS)*

3.2.1 De acuerdo con sus funciones de vigilancia, y en virtud de los artículos 3.1 y 22, y del artículo 34.1, primer guion, de los Estatutos del SEBC, el BCE adoptó el Reglamento (UE) n.º 795/2014 del Banco Central Europeo (BCE/2014/28)[18], que incorpora los principios sobre las infraestructuras del mercado financiero adoptados por el Comité de Pagos e Infraestructuras del Mercado (CPMI) y la Organización Internacional de Comisiones de Valores (IOSCO) (los principios CPMI-IOSCO)[19], que son jurídicamente vinculantes y se aplican a los sistemas de grandes o pequeños pagos, sean operados por un banco central del Eurosistema o por una entidad privada.

3.2.2 Por tanto, los SIPS están sujetos a una evaluación regular del cumplimiento de los requisitos del Reglamento (UE) n.º 795/2014 (BCE/2014/28) relativos al riesgo operativo[20], lo que faculta al banco central pertinente del Eurosistema, como autoridad competente, para verificar dicho cumplimiento. En caso de incumplimiento, el banco central pertinente del Eurosistema puede imponer al SIPS sanciones o medidas correctoras que garanticen el cumplimiento de los requisitos aplicables[21]. El Reglamento (UE) n.º 795/2014 (BCE/2014/28) se ha modificado recientemente[22] para imponer una serie de nuevos requisitos a los operadores de SIPS respecto de nuevos riesgos, como los riesgos operativo y de seguridad, incluida la ciberresiliencia[23], teniendo en cuenta, entre otras cosas, la guía sobre ciberresiliencia de las infraestructuras del mercado

---

18 Reglamento (UE) n.º 795/2014 del Banco Central Europeo, de 3 de julio de 2014, sobre los requisitos de vigilancia de los sistemas de pago de importancia sistémica (BCE/2014/28) (DO L 217 de 23.7.2014, p. 16).

19 Disponibles en la dirección del Banco de Pagos Internacionales en internet, www.bis.org.

20 Véase el artículo 15 del Reglamento (UE) n.º 795/2014 (BCE/2014/28), que obliga a los operadores de SIPS a tomar medidas como: a) fijar políticas de seguridad de la información y seguridad física completas que identifiquen, valoren y gestionen de forma adecuada todas las posibles vulnerabilidades y amenazas, y b) garantizar que los sistemas críticos de tecnología de la información puedan volver a operar en plazos específicos contados desde que se produzca una situación que suponga un riesgo significativo de perturbar las operaciones del SIPS.

21 Véase el apartado 3.4 del Dictamen CON/2017/10.

22 Por el Reglamento (UE) 2017/2094 del Banco Central Europeo, de 3 de noviembre de 2017, por el que se modifica el Reglamento (UE) n.º 795/2014 sobre los requisitos de vigilancia de los sistemas de pago de importancia sistémica (BCE/2014/28) (BCE/2017/32) (DO L 299 de 16.11.2017, p. 11).

23 Véase el artículo 15, apartados 1 *bis* y 4 *bis*, del Reglamento (UE) n.º 795/2014 (ECB/2014/28), que obliga a los operadores de SIPS a tomar las medidas siguientes: i) revisar, auditar y comprobar los sistemas, políticas, procedimientos y controles periódicamente y cada vez que se introduzcan cambios significativos; ii) establecer un marco efectivo de ciberresistencia que incluya medidas de gobierno apropiadas para gestionar el ciberriesgo; iii) determinar sus operaciones críticas y los activos que las respaldan, y disponer de medidas adecuadas para detectar ciberataques y responder a ellos y para proteger esas operaciones de ciberataques y hacer que se recuperen de ellos; iv) comprobar periódicamente las medidas adoptadas, y v) garantizar un nivel adecuado de conocimiento de las ciberamenazas, incluso mediante la aplicación de un proceso continuo de aprendizaje.

financiero publicada en 2016 por CPMI-IOSCO[24] (en lo sucesivo, la «Guía sobre ciberresiliencia de CPMI-IOSCO»).

3.2.3 Además, en consonancia con los requisitos de la Directiva (UE) 2016/1148, el Reglamento (UE) n.º 795/2014 (BCE/2014/28) ya faculta a los bancos centrales del Eurosistema para obtener de los operadores de SIPS la información relativa a, entre otras cosas, los incidentes graves y leves, la naturaleza y el tipo de los incidentes y su gravedad y duración[25]. Dicho reglamento se modificó para facultar además a los bancos centrales del Eurosistema para llevar a cabo inspecciones in situ y para exigir a los operador de SIPS que designen expertos independientes que lleven a cabo investigaciones o exámenes independientes sobre el funcionamiento de los sistemas[26].

3.2.4 De entre los SIPS de la lista del BCE, TARGET2 tiene un carácter especial al ser propiedad del Eurosistema, que lo gestiona, y estar sujeto a normas estrictas de regulación y vigilancia[27]. Aunque el proyecto de real decreto no se refiere expresamente a los SIPS, el BCE entiende que el componente español de TARGET2, TARGET2-Banco de España, operado por el Banco de España, podría estar comprendido en el ámbito de aplicación del proyecto de real decreto. En virtud de la Decisión BCE/2014/35 del Banco Central Europeo[28], se ha determinado que TARGET2 es un SIPS y que está sujeto a la vigilancia del BCE como autoridad competente conforme al Reglamento (UE) n.º 795/2014 (BCE/2014/28).

3.2.5 El BCE entiende que el proyecto de real decreto en nada afecta a la competencia del Eurosistema respecto de la vigilancia de los SIPS, ya que dicha vigilancia tiene lugar sobre la base de reglamentos del BCE. Conforme a lo expuesto en el apartado 2.5, el BCE entiende que el Banco de España puede compartir puntual y eficazmente con el BCE la información que el Banco de España, como autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información, reciba acerca de ciberincidentes reales o potenciales o medidas previstas o adoptadas que puedan afectar a los SIPS y a TARGET2.

3.3 *Efectos en los sistemas de pago sin importancia sistémica*

3.3.1 Entre los sistemas de pago sin importancia sistémica se incluyen sistemas de grandes pagos y sistemas de pequeños pagos. Conforme al marco de vigilancia de los sistemas de pequeños pagos[29], los sistemas de pequeños pagos sin importancia sistémica se dividen en dos claros grupos: los sistemas de pequeños pagos muy importantes (*prominently important retail payments systems*, PIRPS), y los otros sistemas de pequeños pagos. El Sistema Nacional de Compensación Electrónica (el sistema español de pequeños pagos) se clasifica en el grupo de los PIRPS[30]. El BCE entiende que sus servicios podrían incluirse en la relación de servicios esenciales del

24 Disponible en la dirección del Banco de Pagos Internacionales en internet.

25 Véase el artículo 21, apartado 1, letra a), del Reglamento (UE) n.º 795/2014 (BCE/2014/28).

26 Véase el artículo 21, apartado 1, letras b) y c), del Reglamento (UE) n.º 795/2014 (BCE/2014/28).

27 Véase el apartado 3.1.5 del Dictamen CON/2019/17.

28 Decisión BCE/2014/35 del Banco Central Europeo, de 13 de agosto de 2014, acerca de la identificación de TARGET2 como sistema de pago de importancia sistémica de conformidad con el Reglamento (UE) n.º 795/2014 sobre los requisitos de vigilancia de los sistemas de pago de importancia sistémica (DO L 245 de 20.8.2014, p. 5).

29 Véase el documento del Eurosistema «Revised oversight framework for retail payment systems» (febrero de 2016), disponible en la dirección del BCE en internet, www.ecb.europa.eu.

30 Véase el documento del Eurosistema «Overview of payment systems», disponible en la dirección del BCE en internet.

proyecto de real decreto y que los operadores de este sistema podrían designarse como operadores de servicios esenciales.

3.3.2 En el marco de la política de vigilancia del Eurosistema, los sistemas de pequeños pagos sin importancia sistémica deben seguir los principios CPMI-IOSCO y las expectativas de vigilancia aplicables a los enlaces entre sistemas de pequeños pagos[31]. Tanto los principios como las expectativas son instrumentos de derecho suasorio, lo cual significa que los sistemas de grandes pagos, los sistemas de pequeños pagos muy importantes y los otros sistemas de pequeños pagos, que no tengan importancia sistémica, están sujetos a estándares de vigilancia comparables a los del Reglamento (UE) n.º 795/2014 (BCE/2014/28), aunque no existe legislación de la Unión que regule su vigilancia o supervisión[32]. Las competencias del Banco de España respecto de la vigilancia de los sistemas de pago sin importancia sistémica se basan también en la Ley 13/1994[33].

3.3.3 En el marco revisado para la vigilancia de los sistemas de pequeños pagos se especifica que todos los sistemas de esta clase son parte integrante del panorama de pago y liquidación de la zona del euro y, por consiguiente, entran dentro del ámbito de la vigilancia. Por lo tanto, el Eurosistema tiene interés en velar por que el marco de vigilancia y los estándares aplicables a dichos sistemas no se altere como resultado de la aplicación de la Directiva (UE) 2016/1148 o de la aprobación de otras normas relacionadas con la seguridad de las redes y sistemas de información[34].

3.3.4 Si se pretende que los sistemas de pago sin importancia sistémica entren en el ámbito de aplicación del proyecto de real decreto, el BCE entiende que este no afecta a la competencia del Banco de España para llevar a cabo sus funciones de vigilancia. Conforme a lo expuesto en el apartado 2.5, el BCE entiende que el Banco de España puede compartir con el BCE toda información pertinente sobre sistemas de pago sin importancia sistémica que reciba en calidad de autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información.

3.4 *Efectos en los servicios e instrumentos de pago*

3.4.1 En el marco de la política de vigilancia del Eurosistema, los instrumentos de pago (como las tarjetas, las transferencias, el adeudo directo y el dinero electrónico) se consideran parte integrante de los sistemas de pago y, por lo tanto, se incluyen en el ámbito de aplicación de la vigilancia del banco central. En el caso de los instrumentos de pago, la función de vigilancia principal se asigna al Eurosistema por el vínculo nacional de dichos instrumentos y la personalidad jurídica de su autoridad de gobierno. Respecto de las transferencias y los sistemas de adeudo directo de la Zona única de pagos para el euro, y de algunos de los sistemas internacionales de pagos con tarjeta, la función principal de vigilancia corresponde al BCE. Los proveedores de servicios de pago (PSP), incluidas las entidades de crédito, las entidades de pago y las entidades

---

31 Véase el documento «Oversight expectations for links between retail payment systems», disponible en la dirección del BCE en internet.

32 Véanse el apartado 2.4.4 del Dictamen CON/2017/31, el apartado 3.2.3 del Dictamen CON/2018/22, y el apartado 3.2.2 del Dictamen CON/2019/17.

33 Véanse los artículos 7 y 16 de la Ley 13/1994.

34 Véanse el apartado 3.4.2 del Dictamen CON/2018/22, el apartado 4.3 del Dictamen CON/2018/47, y el apartado 3.2.3 del Dictamen CON/2019/17.

de dinero electrónico, están sujetos a la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo[35], aplicable desde enero de 2018, según su transposición al derecho interno. El marco jurídico y regulador establece requisitos relativos a los riesgos operativo y de seguridad y a la comunicación de incidentes. No obstante, los supervisores prudenciales deben actuar con cautela, al decidir si publican información referente a incidentes de ciberseguridad concretos, a fin de garantizar que no merme la confianza del público en las entidades afectadas. Además, la Autoridad Bancaria Europea (ABE) ha publicado directrices sobre las medidas de seguridad para la gestión de los riesgos operativos y de seguridad de los servicios de pago objeto de la Directiva (UE) 2015/2366[36] y trabaja en un proyecto de directrices sobre tecnología de la información y la comunicación (ICT) y gestión del riesgo de seguridad[37] destinadas a armonizar los estándares aplicables a los PSP respecto de la seguridad de la ICT, la comunicación de incidentes, la gestión de proyectos, y la continuidad operativa. Por lo tanto, los PSP están sujetos a la legislación de la Unión, a la legislación española, y a los reglamentos basados en la legislación de la Unión. En cambio, los sistemas nacionales e internacionales de tarjetas de pago no están sujetos a la legislación de la Unión como tal[38].

3.4.2 El BCE entiende que los diversos instrumentos de pago y PSP pueden entrar en el ámbito de aplicación del proyecto de real decreto, y reitera que a su juicio el Banco de España puede compartir puntual y eficazmente con el BCE, conforme a sus responsabilidades respectivas, toda la información pertinente que reciba como autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información.

3.5 *Efectos en los depositarios centrales de valores*

3.5.1 Los depositarios centrales de valores (DCV) están sujetos a la regulación y supervisión estrictas de diversas autoridades, según el Reglamento (UE) n.º 909/2014 del Parlamento Europeo y del Consejo[39], que establece requisitos relacionados con el riesgo operativo. Por otra parte, los DCV deben tener en cuenta las directrices de CPMI-IOSCO en materia de ciberresiliencia, destinadas a todas las infraestructuras del mercado financiero.

3.5.2 Además de las competencias supervisoras asignadas a las autoridades nacionales competentes (ANC) en el Reglamento (UE) n.º 909/2014, las autoridades nacionales, en particular los miembros del SEBC, intervienen en la autorización y supervisión de los DCV en calidad de «autoridades relevantes»[40]. A este respecto, el considerando 8 del Reglamento (UE) n.º 909/2014 afirma que este debe entenderse sin perjuicio de las responsabilidades del BCE y de los BCN a la hora de

---

35 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).

36 Directrices sobre las medidas de seguridad para los riesgos operativos y de seguridad asociados a los servicios de pago en virtud de la Directiva (UE) 2015/2366 (PSD2) (EBA/GL/2017/17), de 12 de enero de 2018.

37 Véanse la Directrices de la ABE sobre gobierno interno conforme a la Directiva 2013/36/UE, de 26 de septiembre de 2017 (EBA/GL/2017/11) y el proyecto de directrices de la ABE sobre tecnología de la información y la comunicación (ICT) y gestión del riesgo de seguridad, de 13 de diciembre de 2018 (EBA/CP/2018/15), disponibles en la dirección de la ABE en internet, www.eba.europa.eu.

38 Véanse el apartado 2.4.3 del Dictamen CON/2017/31, el apartado 3.4.2 del Dictamen CON/2018/22 y el apartado 3.4.1 del Dictamen CON/2019/17.

39 Reglamento (UE) n.º 909/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, sobre la mejora de la liquidación de valores en la Unión Europea y los depositarios centrales de valores y por el que se modifican las Directivas 98/26/CE y 2014/65/UE y el Reglamento (UE) n.º 236/2012 (DO L 257 de 28.8.2014. p. 1).

40 Véase el artículo 12 del Reglamento (UE) n.º 909/2014.

velar por la existencia de sistemas de compensación y de pago eficientes y sólidos dentro de la Unión y en otros países, y que no debe impedir a los miembros del SEBC acceder a la información pertinente para el ejercicio de sus funciones[41], en particular la vigilancia de los DCV y otras infraestructuras de los mercados financieros[42].

3.5.3 Iberclear es el DCV español, autorizado conforme al Reglamento (UE) n.º 909/2014 y supervisado por la CNMV. Conforme a dicho reglamento, Iberclear es el operador de un sistema de liquidación de valores que vigilan conjuntamente el Banco de España y la CNMV. En la medida en que Iberclear puede ser operador de servicios esenciales y entrar en el ámbito de aplicación del proyecto de real decreto, el BCE entiende que este se aplicaría sin perjuicio de las funciones de vigilancia del Banco de España, teniendo en cuenta además que estas se ejercen en virtud de la legislación de la Unión.

3.6 *Estrategia del Eurosistema en cuanto a la ciberresiliencia de las infraestructuras del mercado financiero*

3.6.1 El BCE entiende que las disposiciones del proyecto de real decreto se aplican sin perjuicio de la estrategia del Eurosistema en cuanto a la ciberresiliencia de las infraestructuras del mercado financiero[43], que pretende apoyar la aplicación de las directrices de CPMI-IOSCO sobre ciberresiliencia desde la perspectiva de la vigilancia. Los objetivos de dicha estrategia son: i) aumentar la ciberresiliencia del sector financiero de la zona del euro en su conjunto mejorando la «ciberalerta» de infraestructuras concretas del mercado financiero vigiladas por los bancos centrales del Eurosistema, y ii) fomentar la colaboración entre las infraestructuras del mercado financiero, sus proveedores de servicios críticos y las autoridades pertinentes. Como parte de esa estrategia, el Eurosistema ha creado una serie de mecanismos que pueden emplear las infraestructuras del mercado financiero para mejorar su ciberresiliencia, como el TIBER[44], además de las «ciberencuestas» y los exámenes enfocados en evaluar la «cibermadurez» de los sistemas de pago del Eurosistema y establecer expectativas en materia de vigilancia de la ciberresiliencia[45], y que proporcionarán a los operadores de los sistemas de pago una orientación más detallada.

4. Efectos del proyecto de real decreto en las entidades de crédito

4.1 El considerando 13 de la Directiva (UE) 2016/1148 afirma que los requisitos relativos a los sistemas de información a menudo son más estrictos que los establecidos en dicha directiva y se recogen en una serie de actos jurídicos de la Unión que incluyen normas sobre el acceso a la actividad de las entidades de crédito y la supervisión prudencial de las entidades de crédito y las empresas de inversión. Dice también que los Estados miembros deben tener en cuenta esos requisitos al aplicar la transposición de dicha directiva como ley especial. Ciertamente, entre los actos jurídicos de la Unión que armonizan el área de la supervisión de las entidades de crédito se

41 Véanse también el artículo 13 y el artículo 17, apartado 4, del Reglamento (UE) n.º 909/2014.

42 Véanse el apartado 7.3 del Dictamen CON/2017/10, el apartado 7.2 del Dictamen CON/2018/47, y el apartado 3.5.2 del Dictamen CON/2019/17.

43 Para más información, véase https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html.

44 Véase el documento «Eurosystem's Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU)» (mayo de 2018), disponible en la dirección del BCE en internet.

45 Véase el documento del Eurosistema «Cyber resilience oversight expectations for financial market infrastructures» (CROE) (diciembre de 2018), disponible en la dirección del BCE en internet.

incluyen el Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo[46] y la Directiva 2013/36/UE del Parlamento y del Consejo[47], que constituyen conjuntamente el marco CRR/CRD IV.

4.2 El BCE y el Banco de España son las autoridades competentes que ejercen las facultades supervisoras del marco CRR/CRD IV en virtud del Reglamento (UE) n.º 1024/2013, que encomienda al BCE tareas específicas respecto de la supervisión prudencial de las entidades de crédito de la zona del euro y le hace responsable del funcionamiento eficaz y coherente del Mecanismo Único de Supervisión (MUS), dentro del cual las funciones específicas de supervisión se distribuyen entre el BCE y las autoridades nacionales competentes participantes, incluido el Banco de España. En particular, el BCE se encarga de la autorización y la revocación de la autorización de todas las entidades de crédito. Respecto de las entidades de crédito significativas, el BCE tiene además la función, entre otras, de garantizar el cumplimiento del derecho aplicable de la Unión por el que se imponen requisitos prudenciales a las entidades de crédito, incluido el requisito de que se doten de estructuras sólidas de gobierno, tales como procesos de gestión de riesgos y mecanismos de control interno fiables[48]. Con este fin, se otorgan al BCE todas las facultades de supervisión para intervenir en la actividad de las entidades de crédito que sean necesarias para el desempeño de sus funciones.

4.3 La supervisión prudencial de las entidades de crédito conforme la ejercen el BCE y el Banco de España dentro del MUS comprende varios aspectos relacionados con la ciberseguridad como parte de la supervisión prudencial del riesgo operativo, es decir, el riesgo de pérdidas debido a la inadecuación o el fallo de los procedimientos, las personas y los sistemas internos, o a acontecimientos externos[49]. Además, la ABE ha publicado directrices sobre gobierno interno que cubren ciertos aspectos de los riesgos de la tecnología de la información (IT)[50], y, como se ha dicho en el apartado 3.4.1, un proyecto de directrices sobre tecnología de la información y la comunicación (ICT) y gestión del riesgo de seguridad[51], con las que se pretende armonizar los requisitos aplicables a las entidades de crédito, las empresas de servicios de inversión y los proveedores de servicios de pagos, por lo que respecta a la seguridad de la ICT, la comunicación de incidentes, la gestión de proyectos y la continuidad operativa. Están en preparación otras directrices de la ABE relativas a la inclusión de ciertos aspectos del ciberriesgo en el Proceso de Revisión y Evaluación Supervisora (PRES)[52]. El BCE ha elaborado cuestionarios detallados sobre

---

46 Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 176 de 27.6.2013, p. 1).

47 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 y las empresas de inversión, 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).

48 Véanse el artículo 4, apartado 1, letra e), y el artículo 6, apartado 4, del Reglamento (UE) n.º 1024/2013.

49 Véase el artículo 4, apartado 1, punto 52, del Reglamento (UE) n.º 575/2013.

50 Directrices sobre gobierno interno (EBA/GL/2017/11), de 21 de marzo de 2018.

51 Véanse la Directrices de la ABE sobre gobierno interno conforme a la Directiva 2013/36/UE, de 26 de septiembre de 2017 (EBA/GL/2017/11) y el proyecto de directrices de la ABE sobre tecnología de la información y la comunicación (ICT) y gestión del riesgo de seguridad, de 13 de diciembre de 2018 (EBA/CP/2018/15), disponibles en la dirección de la ABE en internet.

52 Véase el proyecto de directrices de la ABE sobre la evaluación del riesgo de ICT en el PRES, de 6 de octubre de 2016 (EBA/CP/2016/14), disponible en la dirección de la ABE en internet.

el riesgo de IT destinados a las entidades de crédito supervisadas e incorporados a sus resultados del PRES, y también tiene en cuenta la información sobre cuestiones de ciberseguridad que puede obtener de las revisiones temáticas, de las inspecciones in situ y de los informes sobre ciberincidentes[53]. Dicha información puede servir de base para recomendaciones específicas dirigidas a determinadas entidades y para comparaciones y directrices generales para todo el sector. Al mismo tiempo, los supervisores prudenciales deben actuar con cautela, al decidir si publican información referente a incidentes de ciberseguridad concretos, para no socavar la confianza del público en las entidades de crédito afectadas.

4.4 Además, el BCE y las ANC del MUS se encargan de evaluar los planes de recuperación y adoptar medidas de intervención temprana conforme a la Directiva 2014/59/UE del Parlamento Europeo y del Consejo[54] (según su incorporación al derecho interno). Asimismo, la responsabilidad principal de determinar si una entidad de crédito significativa, como condición para su resolución, es inviable o puede serlo, corresponde al BCE[55]. Uno de los objetivos de la resolución es mantener la continuidad de las funciones esenciales de la entidad de crédito[56], lo que puede incluir la continuidad del funcionamiento de sus sistemas de pago y circulación de efectivo.

4.5 Los bancos centrales están fuera del ámbito de aplicación de la Directiva 2013/36/UE y no son, pues, entidades supervisadas objeto del Reglamento (UE) n.º 575/2013. Por consiguiente, ni el BCE ni el Banco de España entran en la definición de «banca» a los efectos del anexo II, punto 3, de la Directiva (UE) 2016/1148[57].

4.6 En este contexto, el BCE celebra la designación del Banco de España como autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información para las entidades de crédito, como operadores de servicios esenciales, no clasificadas como operadores críticos, aunque, indudablemente, la supervisión prudencial del riesgo operativo de las entidades de crédito se solapa con la vigilancia del cumplimiento por dichas entidades de sus obligaciones como operadores de servicios esenciales. El BCE celebra igualmente que el proyecto de real decreto aclare expresamente que el Banco de España debe desempeñar sus funciones en materia de seguridad de las redes y sistemas de información sin perjuicio de sus funciones supervisoras en el marco del MUS. En este sentido, el BCE observa que, conforme al derecho de la Unión, existe la obligación de velar por el intercambio de información entre el BCE y las ANC, que deben proporcionar al primero toda la información necesaria para el desempeño de las funciones que le

53 Véase también el artículo del boletín informativo (Newsletter) de 13 de febrero de 2019 «IT and cyber risk - the SSM perspective», disponible en la dirección del BCE en internet.

54 Véanse los artículos 27 a 30 de la Directiva 2014/59/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, por la que se establece un marco para la reestructuración y la resolución de entidades de crédito y empresas de servicios de inversión, y por la que se modifican la Directiva 82/891/CEE del Consejo, y las Directivas 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE y 2013/36/UE, y los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 648/2012 del Parlamento Europeo y del Consejo (DO L 173 de 12.6.2014, p. 190).

55 Véase el artículo 32, apartado 1, letra a), de la Directiva 2014/59/UE.

56 Véase el artículo 31, apartado 2, letra a), de la Directiva 2014/59/UE.

57 Véanse el apartado 2.4 del Dictamen CON/2017/10 y el apartado 4.5 del Dictamen CON/2019/17.

encomienda el Reglamento (UE) n.º 1024/2013[58]. En este punto, el BCE reitera que entiende que el Banco de España puede compartir puntual y eficazmente con el BCE, conforme a sus responsabilidades respectivas, la información pertinente que obtenga como autoridad sectorial a los efectos de la seguridad de las redes y sistemas de información.

5. Funciones del Banco de España en materia de seguridad de las redes y sistemas de información

5.1 El proyecto de real decreto designa al Banco de España como autoridad competente para las entidades de crédito, como operadores de servicios esenciales, siempre que no estén clasificadas como operadores críticos. Su supervisión consiste en vigilar que las entidades de crédito, como operadores de servicios esenciales, cumplan sus obligaciones en materia de seguridad de las redes y sistemas de información, e incluye la facultad de solicitar documentos y llevar a cabo inspecciones en caso necesario. El Banco de España debe además cooperar con otras autoridades competentes en el desempeño de sus funciones de seguridad de las redes y sistemas de información, incluida la prestación de asesoramiento técnico sobre la adecuación de las medidas de seguridad de las entidades de crédito. El Banco de España debe coordinarse y cooperar con los CSIRT de referencia. El Real Decreto-ley 12/2018 faculta a las autoridades competentes para sancionar los incumplimientos graves o menores de las obligaciones de seguridad de las redes y sistemas de información.

5.2 Muchas de las funciones del Banco de España como autoridad sectorial, incluidas las de vigilar el cumplimiento de las obligaciones de las entidades de crédito y coordinarse con otras autoridades, ya las desempeña el Banco de España como supervisor prudencial de las entidades de crédito. El proyecto de real decreto da lugar a un solapamiento considerable con las funciones de supervisión prudencial del Banco de España en el marco del MUS, en particular respecto de la supervisión del riesgo operativo, que conlleva el examen de la adecuación de los procesos internos, los procedimientos de gestión de crisis, los planes de continuidad y los riesgos de IT. Por tanto, las funciones que el proyecto de real decreto asigna al Banco de España guardan relación y se solapan con las funciones de supervisión prudencial encomendadas al BCE y a los BCN por el Tratado y los Estatutos del SEBC. Estas funciones no son atípicas. Muchos BCN tienen asignadas funciones de supervisión prudencial, y hay algunos Estados miembros a cuyos BCN se encomiendan funciones específicas de seguridad de las redes y sistemas de información, incluidas las de determinar quiénes son los operadores de servicios esenciales y vigilar que cumplen las

58 Véanse el artículo 6, apartado 2, y el artículo 6, apartado 7, letra c), incisos i) y iii), del Reglamento (UE) n.º 1024/2013, y el artículo 21, apartado 1, y los artículos 97 y 98, del Reglamento (UE) n.º 468/2014 del Banco Central Europeo, de 16 de abril de 2014, por el que se establece el marco de cooperación en el Mecanismo Único de Supervisión entre el Banco Central Europeo y las autoridades nacionales competentes y con las autoridades nacionales designadas (Reglamento Marco del MUS) (DO L 141 de 14.5.2014, p. 1).

obligaciones de ciberseguidad[59]. La ciberseguridad afecta claramente a la seguridad nacional pero, dado su notable solapamiento con las funciones de supervisión prudencial del Banco de España, en particular la supervisión del riesgo operativo, puede concluirse que el proyecto de real decreto no asigna al respecto al Banco de España funciones realmente nuevas.

El presente dictamen se publicará en la dirección del BCE en internet.

Hecho en Fráncfort del Meno el 11 de noviembre de 2019

[firmado]

La presidenta del BCE
Christine LAGARDE

59 En Bélgica, el Nationale Bank van België/Banque Nationale de Belgique fue designado conforme a la Ley de 1 de julio de 2011, sobre la seguridad y protección de infraestructuras críticas, como autoridad sectorial para el sector financiero encargada de designar y vigilar las infraestructuras críticas. Dicho BCN fue además designado, conforme a la legislación nacional de transposición de la Directiva (UE) 2016/1148, como autoridad sectorial encargada de velar por el cumplimiento por las entidades de crédito y las entidades de contrapartida central, en cuanto operadores de servicios esenciales, de sus obligaciones de notificación de incidentes. Las normas sobre requisitos de seguridad, auditoría interna y externa, control, verificaciones e inspecciones, aplicables a los demás sectores, no se aplican a los operadores de servicios esenciales del sector financiero. Véanse los apartados 1.2, 1.3 y 1.5 del Dictamen CON/2018/27. En Croacia, la Ley de ciberseguridad que transpone la Directiva (UE) 2016/1148, adoptada en julio de 2018, encomendó al Hrvatska Narodna Banka (HNB) funciones relacionadas con la determinación de los operadores de servicios esenciales, su supervisión, y la recepción de la notificación de incidentes. El HNB vigila el cumplimiento por los operadores de servicios esenciales de sus obligaciones de ciberseguridad, supervisándolos una vez cada dos años o cuando incumplan sus obligaciones legales. El HNB está facultado para recibir de ellos la información necesaria para evaluar el nivel de seguridad de sus redes y sistemas de información, incluidas sus normas de seguridad documentadas y pruebas de su aplicación efectiva. El HNB está también facultado para emitir orientaciones vinculantes, presentar denuncias y recibir informes de incidentes. En Irlanda, el «Statutory Instrument No 360 of 2018 European Union (Measures for a high common level of security of network and information systems) Regulations 2018» asignó las siguientes funciones al Banc Ceannais na hÉireann/Central Bank of Ireland: i) elaborar y mantener la lista de servicios esenciales del sector pertinente; ii) designar a los operadores de servicios esenciales del sector pertinente; iii) crear y llevar un registro de operadores de servicios esenciales con los detalles de los pertenecientes al sector bancario y de las IFM, y iv) perseguir sumariamente las infracciones cometidas por los operadores de servicios esenciales. En los Países Bajos, el artículo 28 de la Ley de seguridad de las redes y sistemas de información (*Wet beveiliging netwerk- en informatiesystemen*) y la Orden del Consejo de seguridad de las redes y sistemas de información (*Besluit beveiliging netwerk- en informatiesystemen*) facultan a las autoridades competentes para iniciar una auditoría de seguridad, dar instrucciones vinculantes, e imponer sanciones administrativas y medidas coercitivas. Las obligaciones relativas a la auditoría y las instrucciones de seguridad no se aplican a las infraestructuras y entidades financieras, que sí están sujetas a la obligación de notificar incidentes. Por tanto, las funciones principales del De Nederlandsche Bank son recibir la notificación de incidentes e imponer medidas coercitivas y sanciones por el incumplimiento de la obligación de notificar incidentes.