III

(Actos preparatorios)

BANCO CENTRAL EUROPEO

DICTAMEN DEL BANCO CENTRAL EUROPEO

de 4 de junio de 2021

acerca de una propuesta de reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero

(CON/2021/20)

(2021/C 343/01)

Introducción y fundamento jurídico

El 22, 23 y 29 de diciembre de 2020 el Banco Central Europeo (BCE) recibió respectivamente del Consejo de la Unión Europea y del Parlamento Europeo una solicitud de dictamen acerca de una propuesta de reglamento del Parlamento Europeo y del Consejo 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 y (UE) n.º 909/2014 ([1]) (en lo sucesivo, el «reglamento propuesto»), y acerca de una propuesta de directiva por la que se modifican las Directivas 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 y (UE) 2016/2341 ([2]) (en lo sucesivo, la «directiva modificativa propuesta» y, conjuntamente con el reglamento propuesto, los «actos propuestos»).

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, puesto que los actos propuestos contienen disposiciones que afectan a las competencias del BCE, en particular, la definición y ejecución de la política monetaria, la promoción del buen funcionamiento de los sistemas de pago, la contribución a la buena gestión de las políticas que llevan a cabo las autoridades competentes con respecto a la estabilidad del sistema financiero, y las tareas encomendadas al BCE respecto de la supervisión prudencial de las entidades de crédito, conforme al artículo 127, apartado 2, guiones primero y cuarto, y al artículo 127, apartados 5 y 6, del Tratado. 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. Observaciones generales

1.1 El BCE acoge con satisfacción el reglamento propuesto, que pretende mejorar la ciberseguridad y la resiliencia operativa del sector financiero. En particular, el BCE celebra el propósito del reglamento propuesto de eliminar obstáculos al mercado interior de servicios financieros y mejorar su establecimiento y funcionamiento armonizando las normas aplicables en el ámbito de la gestión del riesgo de las tecnologías de la información y la comunicación (TIC), la presentación de informes, las pruebas y el riesgo de terceros relacionado con las TIC. El BCE celebra también el propósito del reglamento propuesto de simplificar y armonizar, evitando duplicidades, los requisitos regulatorios o expectativas de supervisión a que actualmente están sujetas según el derecho de la Unión las entidades financieras.

1.2 El BCE entiende que el reglamento propuesto es, respecto de las entidades financieras identificadas como operadores de servicios esenciales ([3]), un acto jurídico sectorial (una ley especial) en el sentido del artículo 1, apartado 7, de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([4]) (en lo sucesivo, la «Directiva SRI»), lo que significa que, en principio, las disposiciones del reglamento propuesto prevalecerían sobre las de la Directiva SRI. En la práctica, entre otras cosas, las entidades financieras identificadas como operadores de servicios esenciales ([5]) notificarían incidentes de acuerdo con el reglamento propuesto y no con

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Véase el artículo 1, apartado 2, del reglamento propuesto.
([4]) 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).
([5]) Véase el artículo 5 de la Directiva SRI.

la Directiva SRI. Aunque el BCE celebra que se reduzca el riesgo de duplicación de requisitos para las entidades financieras en materia de notificación de incidentes, debe prestarse más atención a la interacción entre el reglamento propuesto y la Directiva SRI. Por ejemplo, según el reglamento propuesto, un proveedor tercero de servicios de TIC ([6]) podría estar sujeto a las recomendaciones del supervisor principal ([7]). Al mismo tiempo, el mismo proveedor tercero de servicios de TIC puede clasificarse como operador de servicios esenciales conforme a la Directiva SRI y estar sujeto a las instrucciones vinculantes de la autoridad competente ([8]). En ese caso, el proveedor tercero de servicios de TIC podría recibir recomendaciones conforme al reglamento propuesto que fueran contrarias a las instrucciones vinculantes recibidas conforme a la Directiva SRI. El BCE sugiere que los órganos legislativos de la Unión examinen más detenidamente las posibles incoherencias entre el reglamento propuesto y la Directiva SRI que pueden impedir que se armonicen los requisitos para las entidades financieras y se evite la existencia de requisitos repetidos y contradictorios.

1.3 El BCE entiende asimismo que, según la propuesta de directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 ([9]) (en lo sucesivo, la «propuesta de directiva SRI 2»), los «cuasiincidentes» ([10]) deberán notificarse ([11]). Aunque el considerando 39 de la propuesta de directiva SRI 2 hace referencia al significado del término «cuasiincidente», no está claro si se pretende requerir que los cuasiincidentes sean notificados por las entidades financieras que se enumeran en el artículo 2 del reglamento propuesto. Sobre este punto, y teniendo en cuenta además que los cuasiincidentes solo pueden identificarse como tales una vez que ocurren, el BCE celebraría ser informado oportunamente de los cuasiincidentes importantes, como actualmente sucede con los ciberincidentes. El BCE sugiere que se coordine mejor el reglamento propuesto con la propuesta de directiva SRI 2 a fin de precisar el alcance de las obligaciones de notificación a que estén sujetas las entidades financieras conforme a estas dos normas de la Unión distintas pero conexas. Al mismo tiempo, habría que definir los «cuasiincidentes» y establecer normas relativas a su importancia.

1.4 El BCE celebra que se incentive a las entidades financieras a que compartan voluntariamente entre sí información sobre ciberamenazas para mejorar y reforzar su situación en materia de ciberresiliencia. El propio BCE ha contribuido a la iniciativa del mercado para el intercambio de información sobre ciberamenazas (*Cyber threat Intelligence Information Sharing Initiative* (CIISI-EU)) y pone el proyecto a disposición de quien quiera desarrollar y fomentar la iniciativa ([12]).

1.5 El BCE apoya la cooperación entre las autoridades competentes a los efectos del reglamento propuesto, las Autoridades Europeas de Supervisión (AES) y los equipos de respuesta a incidentes de seguridad informática (CSIRT) ([13]). Es esencial intercambiar información para garantizar la resiliencia operativa de la Unión, ya que el intercambio de información y la cooperación entre las autoridades puede contribuir a prevenir los ciberataques y a reducir la propagación de las amenazas de las TIC. Debe fomentarse un enfoque común a los riesgos relacionados con las TIC, y debe velarse por una evaluación coherente de dichos riesgos en toda la Unión. Es de suma importancia que las autoridades competentes ([14]) solo compartan la información con el punto de contacto único ([15]) y los CSIRT nacionales cuando se hayan establecido mecanismos claros de clasificación y de intercambio de información y, al mismo tiempo, salvaguardias adecuadas que garanticen la confidencialidad.

1.6 Por último, el BCE celebraría que el reglamento propuesto incluyera disposiciones sobre datos personales y retención de datos. Para determinar el plazo de retención deben tenerse en cuenta las tareas de investigación, inspección, solicitud de información, comunicación, publicación, evaluación, verificación y redacción de planes de vigilancia o supervisión, que las autoridades competentes pueden tener que desempeñar en el

([6]) Véase el artículo 3, punto 15, del reglamento propuesto.
([7]) Véase el artículo 31, apartado 1, letra d), del reglamento propuesto.
([8]) Véase el artículo 15, apartado 3, de la Directiva SRI.
([9]) COM(2020) 823 final.
([10]) Cualquier suceso que podría haber causado daños, pero cuya materialización completa se previno de manera satisfactoria. Véase el considerando 39 de la propuesta de directiva SRI 2.
([11]) Véase el artículo 11 de la propuesta de directiva SRI 2.
([12]) La *Cyber threat Intelligence Information Sharing Initiative* (CIISI-EU) está disponible en la dirección del BCE en internet, www.ecb.europa.eu.
([13]) Véase el artículo 42 del reglamento propuesto.
([14]) Véanse los artículos 11, 26 y 27 de la propuesta de directiva SRI 2.
([15]) Véase el artículo 8, apartado 3, de la Directiva SRI.

marco de sus respectivas obligaciones conforme al reglamento propuesto. Por ello, un plazo de retención de 15 años sería adecuado. Este plazo podría reducirse o ampliarse si lo exigieran las circunstancias de cada caso. Sobre este particular, el BCE sugiere que los órganos legislativos de la Unión, cuando formulen la disposición pertinente sobre datos personales y retención de datos, tengan también presentes el principio de minimización de datos y el ulterior tratamiento de estos con fines de archivo de interés público, científicos, de investigación histórica o estadísticos ([16]).

2. **Observaciones particulares sobre vigilancia y sobre compensación y liquidación de valores**

2.1 *Competencias del SEBC y del Eurosistema en materia de vigilancia*

2.1.1 Estrechamente vinculada a sus funciones básicas de política monetaria, el Tratado y los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo (en lo sucesivo, los «Estatutos del SEBC») encomiendan al Eurosistema la función de vigilar los sistemas de compensación y de pago. Conforme al artículo 127, apartado 2, cuarto guion, del Tratado, reproducido en el artículo 3.1 de los Estatutos del SEBC, una de las funciones básicas que deben llevarse a cabo a través del Sistema Europeo de Bancos Centrales (SEBC) es la de promover el buen funcionamiento de los sistemas de pago. En la ejecución de esta función básica, el BCE y los bancos centrales nacionales pueden proporcionar medios, y el BCE dictar reglamentos, destinados a garantizar unos sistemas de compensación y liquidación eficientes y solventes dentro de la Unión, así como con otros países ([17]). Conforme a su función de vigilancia, el BCE adoptó el Reglamento (UE) n.º 795/2014 del Banco Central Europeo (BCE/2014/28) (en lo sucesivo, el «Reglamento sobre los SIPS») ([18]). El Reglamento sobre los SIPS adopta en forma preceptiva los principios para las infraestructuras del mercado financiero publicados en abril de 2012 por el Comité de Sistemas de Pago y Liquidación y la Organización Internacional de Comisiones de Valores ([19]), que son jurídicamente vinculantes y abarcan los sistemas de importancia sistémica de grandes pagos y de pequeños pagos, tanto si se encarga de su funcionamiento un banco central del Eurosistema como una entidad privada. El marco de la política de vigilancia del Eurosistema ([20]) considera a los instrumentos de pago como parte integrante de los sistemas de pago, de modo que los incluye en el ámbito de su vigilancia. El marco de vigilancia de los instrumentos de pago está actualmente en proceso de revisión ([21]). Según este marco, un instrumento de pago (por ejemplo, tarjeta, transferencia, adeudo directo, transferencia de dinero electrónico o ficha de pago digital ([22])) es un dispositivo personalizado (o un conjunto de dispositivos personalizados) y/o un conjunto de procedimientos acordados entre el usuario de servicios de pago y el proveedor de servicios de pago y utilizado para iniciar una transferencia de valor ([23]).

2.1.2 En virtud de lo expuesto, el BCE celebra que no se incluyan en el artículo relativo al ámbito de aplicación personal del reglamento propuesto los operadores de sistemas según se definen en el artículo 2, letra p), de la Directiva 98/26/CE del Parlamento Europeo y del Consejo ([24]), ni los sistemas de pago (incluidos los

([16]) Véanse el artículo 4, letra b), y el artículo 13, del 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).

([17]) Véase el artículo 22 de los Estatutos del SEBC.

([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]) La versión revisada (julio de 2016) del *Eurosystem oversight policy framework* está disponible en la dirección del BCE en internet, www.ecb.europa.eu.

([21]) Véase la edición revisada y consolidada de octubre de 2020 del *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements* (marco PISA), disponible en la dirección del BCE en internet, www.ecb.europa.eu.

([22]) Una ficha de pago digital es una representación digital de valor que está respaldada por derechos o activos registrados en otro lugar y que permite transferir valor entre usuarios finales. Dependiendo del diseño subyacente, las fichas de pago digital pueden prever que el valor se transfiera sin que tenga que participar necesariamente un tercero central o tengan que utilizarse cuentas de pago.

([23]) La transferencia de valor es el acto, iniciado por el ordenante o en nombre del ordenante o por el beneficiario, de transferir fondos o fichas de pago digital, o depositar efectivo en una cuenta de usuario o retirarlo de ella, independiente de cualesquiera obligaciones subyacentes entre el ordenante y el beneficiario. En la transferencia pueden intervenir uno o varios proveedores de servicios de pago. Esta definición de transferencia de valor del marco PISA difiere de la definición de transferencia de «fondos» de la 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). Una transferencia de valor en el contexto de los instrumentos de pago según se definen en esa directiva solo puede ser una transferencia de fondos. En dicha directiva no se incluyen entre los fondos las fichas de pago digital salvo que las fichas puedan clasificarse como dinero electrónico (o más hipotéticamente como dinero escritural).

([24]) Directiva 98/26/CE del Parlamento Europeo y del Consejo, de 19 de mayo de 1998, sobre la firmeza de la liquidación en los sistemas de pagos y de liquidación de valores (DO L 166 de 11.6.1998, p. 45).

gestionados por bancos centrales), ni los regímenes o acuerdos de pago, en vista de la aplicación de los marcos de vigilancia a que se ha hecho referencia. Por consiguiente, las competencias del SEBC conforme al Tratado, y las del Eurosistema conforme al Reglamento sobre los SIPS, deben reflejarse con claridad en los considerandos del reglamento propuesto.

2.1.3 El BCE celebra igualmente que se excluya de la aplicación del marco de vigilancia establecido por el reglamento propuesto a los proveedores terceros de servicios de TIC que estén sujetos a marcos de vigilancia establecidos en apoyo de las tareas a que se refiere el artículo 127, apartado 2, del Tratado ([25]). En este punto, el BCE subraya que los bancos centrales del SEBC en sus funciones de política monetaria ([26]) y el Eurosistema cuando presta servicios por medio de TARGET2, TARGET2-Securites (T2S) ([27]) y el servicio de liquidación de pagos inmediatos de TARGET (TIPS) ([28]), no se incluyen en el ámbito de aplicación del reglamento propuesto ni pueden considerarse proveedores terceros de servicios de TIC ni, por lo tanto, clasificarse como proveedores terceros esenciales de servicios de TIC a los efectos del reglamento propuesto. El Eurosistema vigila T2S en virtud de su mandato de velar por unos sistemas de compensación y pago eficientes y solventes. Además, la AEVM aclaró que T2S no es un proveedor de un servicio esencial ([29]) en el sentido del Reglamento (UE) n.º 909/2014 del Parlamento Europeo y del Consejo ([30]) (en lo sucesivo, el «Reglamento sobre DCV»). Por consiguiente, la seguridad, eficiencia y resiliencia organizativa y operativa de T2S se garantizan por medio del marco legal, regulatorio y operacional y de los acuerdos de gobierno de T2S aplicables, y no por medio del Reglamento sobre DCV.

2.1.4 Además, el marco de la política de vigilancia del Eurosistema ([31]) alcanza a proveedores de servicios esenciales como la *Society for Worldwide Interbank Financial Telecommunication* (SWIFT). SWIFT es una sociedad cooperativa de responsabilidad limitada establecida en Bélgica que ofrece internacionalmente servicios de mensajería segura. El Nationale Bank van België/ Banque Nationale de Belgique actúa como supervisor principal de SWIFT y, sobre la base de un acuerdo de vigilancia cooperativo, ejerce la vigilancia de SWIFT en colaboración con los demás bancos centrales del G10, incluido el BCE. Los vigilantes del G10 reconocen que la vigilancia de SWIFT se centra en el riesgo operativo, pues este se considera el principal tipo de riesgo por el que SWIFT podría suponer un riesgo sistémico para el sistema financiero de la Unión. El Grupo de vigilancia cooperativa de SWIFT ha establecido un conjunto específico de principios y de expectativas de alto nivel aplicable a SWIFT y relacionado con la identificación y gestión del riesgo, la seguridad de la información, la fiabilidad y resiliencia, la planificación tecnológica y la comunicación con los usuarios. Los vigilantes del G10 esperan que SWIFT se adhiera a las directrices sobre ciberresiliencia del Comité de Sistemas de Pago y Liquidación (CPMI) y de la Organización Internacional de Comisiones de Valores (IOSCO) ([32]) y a otros estándares internacionales sobre la seguridad de las TIC que, en su conjunto, van más allá de los requisitos establecidos en el reglamento propuesto.

2.1.5 No se puede excluir que SWIFT y quizás otros proveedores de servicios sujetos al marco de la política de vigilancia del Eurosistema queden sujetos al reglamento propuesto como proveedores terceros de servicios de TIC si prestan servicios no comprendidos en el artículo 127, apartado 2, del Tratado. Por eso el BCE recomienda encarecidamente que los proveedores de servicios ya sujetos al marco de la política de vigilancia del Eurosistema, SWIFT entre otros, queden excluidos del ámbito de aplicación del marco de vigilancia del reglamento propuesto.

([25]) Véase el artículo 28, apartado 5, del reglamento propuesto.

([26]) Véase el apartado 1.3 del Dictamen del Banco Central Europeo, de 19 de febrero de 2021, sobre una propuesta de reglamento relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937 (CON/2021/4). Todos los dictámenes del BCE se publican en EUR-Lex.

([27]) Véanse el anexo II *bis* de la Orientación BCE/2012/27 del Banco Central Europeo, de 5 de diciembre de 2012, sobre el sistema automatizado transeuropeo de transferencia urgente para la liquidación bruta en tiempo real (TARGET2) (DO L 30 de 30.1.2013, p. 1); la Orientación BCE/2012/13 del Banco Central Europeo, de 18 de julio de 2012, sobre TARGET2-Securities (DO L 215 de 11.8.2012, p. 19), y la Decisión BCE/2011/20 del Banco Central Europeo, de 16 de noviembre de 2011, por la que se establecen normas y procedimientos detallados para la aplicación de los criterios de acceso de los depositarios centrales de valores a los servicios de TARGET2-Securities (DO L 319 de 2.12.2011, p. 117). Véanse también los acuerdos marco y colectivo de T2S.

([28]) Véase el anexo II *ter* de la Orientación BCE/2012/27.

([29]) Véanse el artículo 30, apartado 5, del 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), y el artículo 68 del Reglamento Delegado (UE) 2017/392 de la Comisión, de 11 de noviembre de 2016, por el que se completa el Reglamento (UE) n.º 909/2014 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación relativas a los requisitos operativos, de autorización y de supervisión aplicables a los depositarios centrales de valores (DO L 65 de 10.3.2017, p. 48).

([30]) 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).

([31]) La versión revisada (julio de 2016) del *Eurosystem oversight policy framework* está disponible en la dirección del BCE en internet, www.ecb.europa.eu.

([32]) Disponibles en la dirección del Banco de Pagos Internacionales en internet, www.bis.org.

2.2 *Competencias del SEBC en materia de liquidación de valores*

2.2.1 Los depositarios centrales de valores (DCV) son infraestructuras del mercado financiero estrictamente reguladas y vigiladas por diferentes autoridades con arreglo al Reglamento sobre DCV, que establece normas sobre la liquidación de instrumentos financieros y sobre la organización y gestión de los DCV. Además, los DCV deben tener en cuenta las directrices sobre ciberresiliencia de CPMI-IOSCO, que se han incorporado al documento *Cyber resilience oversight expectations for financial market infrastructures* ([33]) (de diciembre de 2018). Además de ejercer las competencias supervisoras que el Reglamento sobre DCV asigna a las autoridades nacionales competentes (ANC), los miembros del SEBC son «autoridades relevantes», en su condición de vigilantes de los sistemas de liquidación de valores gestionados por DCV, como bancos centrales emisores de las monedas más relevantes en las que tiene lugar la liquidación y como bancos centrales en cuyos libros se liquida el componente de efectivo de las operaciones ([34]). Sobre este particular, el considerando 8 del Reglamento sobre DCV dice que este debe aplicarse sin perjuicio de las responsabilidades del BCE y de los bancos centrales nacionales a la hora de 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 ([35]), incluida la vigilancia de los DCV y otras infraestructuras del mercado financiero ([36]).

2.2.2 Además, los miembros del SEBC suelen actuar como agentes de liquidación del componente de efectivo de las operaciones con valores, y el Eurosistema ofrece servicios de liquidación a través de T2S a los DCV. La vigilancia de T2S por el Eurosistema se vincula a su mandato de velar por unos sistemas de compensación y pago eficientes y solventes, mientras que las autoridades competentes y relevantes de los DCV velan por su buen funcionamiento, la seguridad y eficiencia de la liquidación, y el buen funcionamiento de los mercados financieros en sus jurisdicciones respectivas.

2.2.3 Conforme al reglamento propuesto ([37]), los bancos centrales del SEBC no participan en la elaboración de normas técnicas relativas a la especificación de los riesgos de TIC. También conforme al reglamento propuesto ([38]), no se informa a las autoridades pertinentes de los incidentes relacionados con las TIC. Los bancos centrales del SEBC deberían mantener el mismo nivel de participación que actualmente prevé el Reglamento sobre DCV, y deberían notificarse a las autoridades pertinentes los incidentes relacionados con las TIC. El Eurosistema es la autoridad pertinente para todos los DCV de la zona del euro y para algunos otros DCV de la UE. Los bancos centrales del SEBC necesitan estar al corriente de los incidentes relacionados con las TIC que interesan al ejercicio de sus funciones, incluida la de vigilar los DCV y otras infraestructuras del mercado financiero. Los riesgos a que están expuestos los DCV, incluidos los riesgos de TIC, pueden ser una amenaza para el buen funcionamiento de los DCV. Por lo tanto, los riesgos de TIC son importantes para las autoridades pertinentes, que deben tener una visión completa y detallada de ellos para evaluarlos e influir en la manera en que los DCV abordan la gestión del riesgo. El reglamento propuesto no debe establecer requisitos relacionados con los riesgos de TIC que sean menos rigurosos que los establecidos en el Reglamento sobre DCV y en las normas técnicas de regulación correspondientes en vigor.

2.2.4 Además, los órganos legislativos de la Unión deben clarificar la interacción entre el reglamento propuesto ([39]) y las normas técnicas de regulación que complementan el Reglamento sobre DCV. Concretamente, no está claro si debe eximirse a un DCV de la obligación de tener su propio centro secundario cuando su proveedor tercero de servicios de TIC tenga un centro secundario ([40]). En caso de que deba eximirse al DCV de la obligación de

([33]) Disponible en la dirección del BCE en internet, www.ecb.europa.eu.

([34]) Véase el artículo 12 del Reglamento (UE) n.º 909/2014.

([35]) Véanse también el artículo 13, el artículo 17, apartado 4, y el artículo 22, apartado 6, del Reglamento (UE) n.º 909/2014.

([36]) Véanse al apartado 7.3 del Dictamen del Banco Central Europeo, de 6 de abril de 2017, sobre la identificación de infraestructuras esenciales para la seguridad de las tecnologías de la información (CON/2017/10); el apartado 7.2 del Dictamen del Banco Central Europeo, de 8 de noviembre de 2018, sobre la designación de servicios esenciales y operadores de servicios esenciales para la seguridad de las redes y sistemas de información (CON/2018/47); el apartado 3.5.2 del Dictamen del Banco Central Europeo, de 2 de mayo de 2019, sobre la seguridad de las redes y sistemas de información (CON/2019/17), y el apartado 3.5.2 del Dictamen del Banco Central Europeo, de 11 de noviembre de 2019, sobre la seguridad de las redes y sistemas de información (CON/2019/38).

([37]) Véanse el artículo 54, apartado 5, del reglamento propuesto, y el artículo 45, apartado 7, del Reglamento (UE) n.º 909/2014.

([38]) Véanse el artículo 54, apartado 4, del reglamento propuesto, y el artículo 45, apartado 6, del Reglamento (UE) n.º 909/2014.

([39]) Véase el artículo 11, apartado 5, del reglamento propuesto.

([40]) Véase el artículo 78, apartado 3, del Reglamento Delegado (UE) 2017/392 de la Comisión, de 11 de noviembre de 2016, por el que se completa el Reglamento (UE) n.° 909/2014 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación relativas a los requisitos operativos, de autorización y de supervisión aplicables a los depositarios centrales de valores (DO L 65 de 10.3.2017, p. 48).

tener un centro secundario, no se entiende bien el valor jurídico de este requisito. Asimismo, el reglamento propuesto ([41]) hace referencia a los objetivos de tiempo y punto de recuperación para cada función ([42]), mientras que la norma técnica de regulación correspondiente distingue entre funciones esenciales ([43]) y operaciones esenciales ([44]) en cuanto al tiempo de recuperación establecido para las operaciones esenciales de los DCV. Es preciso que los órganos legislativos de la Unión examinen y aclaren mejor la interacción entre el reglamento propuesto y las normas técnicas de regulación que completan el Reglamento sobre DCV, a fin de evitar el riesgo de requisitos contradictorios. Por último, debe aclararse que las exenciones concedidas a los DCV gestionados por ciertas entidades públicas conforme al Reglamento sobre DCV ([45]) se extienden al reglamento propuesto.

2.3 *Competencias del SEBC en materia de compensación de valores*

2.3.1 Los bancos centrales del SEBC tienen atribuidas competencias de vigilancia de las entidades de contrapartida central (ECC), de modo que los bancos centrales nacionales del Eurosistema suelen cooperar con las autoridades nacionales competentes en la vigilancia y supervisión de las ECC y participan en el respectivo colegio de ECC establecido conforme al Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo ([46]) (en lo sucesivo, el «EMIR»). Los miembros pertinentes del Eurosistema ([47]) participan en los colegios del EMIR en sus funciones de vigilancia y representan al Eurosistema como banco central de emisión para las ECC en las que el euro es una de las monedas más importantes para los instrumentos financieros compensados (y para las ECC extraterritoriales que compensan una parte significativa de los instrumentos financieros en euros). El BCE es el banco central de emisión para las ECC de fuera de la zona del euro.

2.3.2 Conforme al reglamento propuesto ([48]), los bancos centrales del SEBC no participan en la elaboración de normas técnicas de regulación sobre la especificación de los riesgos de TIC. Además, el reglamento propuesto ([49]) no hace ninguna referencia a los requisitos del EMIR ([50]) sobre los objetivos de tiempo y punto de recuperación. La estructura regulatoria propuesta no debe establecer requisitos sobre los riesgos de TIC que sean menos restrictivos que los actualmente en vigor. Por eso, es esencial establecer unos objetivos claros de tiempo y punto de recuperación para disponer de un buen marco de gestión de la continuidad de la actividad. Disponer de objetivos específicos de tiempo y punto de recuperación es también uno de los principios de CPMI-IOSCO aplicables a las infraestructuras del mercado financiero ([51]). Debe mantenerse la actual norma del EMIR y adaptarse en consecuencia el reglamento propuesto. Los bancos centrales del SEBC deben participar en la elaboración de la legislación secundaria y en la labor de los órganos legislativos de la Unión de examinar y aclarar mejor la interacción entre el reglamento propuesto y las normas técnicas de regulación complementarias a fin de evitar el riesgo de que haya requisitos contradictorios o repetidos.

3. **Observaciones particulares sobre cuestiones de supervisión prudencial**

3.1 El Reglamento (UE) n.º 1024/2013 ([52]) (en lo sucesivo, el «Reglamento del MUS») 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 ANC participantes. En particular, el BCE se encarga de autorizar las entidades de crédito y de revocar su autorización, y tiene además, entre otras funciones, la de velar por el cumplimiento de la legislación aplicable de la Unión que establece requisitos prudenciales para las entidades de crédito, incluido el de que dispongan de estructuras sólidas de gobierno, tales como procesos de gestión de riesgos y mecanismos internos de control que sean eficaces ([53]). Con este fin, se otorgan al BCE todos los poderes supervisores para intervenir en la actividad de las entidades de crédito que el BCE necesite para desempeñar sus funciones. El BCE y las ANC pertinentes son, por consiguiente, las autoridades competentes que ejercen las

([41]) Véase el artículo 11, apartado 6, del reglamento propuesto.
([42]) Véase el artículo 3, punto 17, del reglamento propuesto.
([43]) Véase el artículo 76, apartado 2, letras d) y e), del Reglamento Delegado (UE) 2017/392 de la Comisión.
([44]) Véase el artículo 78, apartados 2 y 3, del Reglamento Delegado (UE) 2017/392 de la Comisión.
([45]) Véase el artículo 1, apartado 4, del Reglamento (UE) n.º 909/2014.
([46]) Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, de 4 de julio de 2012, relativo a los derivados extrabursátiles, las entidades de contrapartida central y los registros de operaciones (DO L 201 de 27.7.2012, p. 1).
([47]) Véase el artículo 18, apartado 2, letras g) y h), del EMIR.
([48]) Véanse el artículo 53, apartado 2, letra b), y el artículo 53, apartado 3, del reglamento propuesto, así como el artículo 34, apartado 3, del EMIR.
([49]) Véase el artículo 53, apartado 2, letra a), del reglamento propuesto.
([50]) Véase el artículo 34 del EMIR.
([51]) Véanse los Principios de CPMI-IOSCO aplicables a las infraestructuras del mercado financiero, disponibles en la dirección del Banco de Pagos Internacionales en internet, www.bis.org.
([52]) 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).
([53]) Véanse el artículo 4, apartado 1, letra e), y el artículo 6, apartado 4, del Reglamento (UE) n.º 1024/2013.

facultades de supervisión prudencial previstas en el Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo ([54]) (en lo sucesivo, el «Reglamento sobre requisitos de capital») y en la Directiva 2013/36/UE del Parlamento Europeo y del Consejo ([55]) (en lo sucesivo, la «Directiva sobre requisitos de capital»).

3.2 En el reglamento propuesto se dice que el código normativo único y el sistema de supervisión deben desarrollarse para abarcar la resiliencia operativa digital y la seguridad de las TIC, ampliando los mandatos de los supervisores financieros encargados de supervisar y proteger la estabilidad financiera y la integridad del mercado ([56]). El objetivo es fomentar un marco global del riesgo operativo o de TIC mediante la armonización de los requisitos clave de resiliencia operativa digital de todas las entidades financieras ([57]). En particular, el reglamento propuesto pretende consolidar y actualizar los requisitos relativos al riesgo de TIC abordados hasta ahora por separado en diferentes instrumentos normativos ([58]).

3.3 Los requisitos relacionados con el riesgo de TIC para el sector financiero se encuentran actualmente repartidos en varios actos del derecho de la Unión, incluidos la Directiva sobre requisitos de capital e instrumentos de derecho suasorio (como las directrices de la ABE), y son diversos y, a veces, incompletos. En algunos casos, el riesgo de TIC no se aborda en absoluto; en otros, solo implícitamente como parte del riesgo operativo. Este problema hay que solucionarlo armonizando el reglamento propuesto y esos actos. Para ello, la directiva modificativa propuesta presenta una serie de modificaciones necesarias para aportar claridad y coherencia jurídica a la aplicación de los diversos requisitos de resiliencia operativa digital. Sin embargo, las modificaciones de la Directiva sobre requisitos de capital incluidas actualmente en la directiva modificativa propuesta ([59]) solo se refieren a las disposiciones sobre los planes de emergencia y de continuidad de la actividad ([60]) porque se supone que sirven implícitamente de base para la gestión de los riesgos de TIC.

3.4 Además, el reglamento propuesto ([61]) ordena a las entidades financieras, incluidas las entidades de crédito, que dispongan de marcos internos de gobernanza y control que garanticen una gestión eficaz y prudente de todos los riesgos de TIC. El reglamento propuesto ([62]) dispone la aplicación de sus requisitos a nivel individual y consolidado, pero sin una coordinación suficiente con la legislación sectorial específica a que se refiere. Por último, el reglamento propuesto ([63]) dispone que, sin perjuicio de sus disposiciones relativas al marco de supervisión de los proveedores terceros esenciales de servicios de TIC ([64]), el cumplimiento de las obligaciones del reglamento propuesto lo garantizará, por lo que respecta a las entidades de crédito, la autoridad competente designada de conformidad con el artículo 4 de la Directiva sobre requisitos de capital, sin perjuicio de las tareas específicas que el Reglamento del MUS encomienda al BCE.

3.5 En vista de lo expuesto, el BCE entiende que, respecto de las entidades de crédito y salvo por las disposiciones del reglamento propuesto relativas al marco de supervisión de los proveedores terceros esenciales de servicios de TIC ([65]), el reglamento propuesto pretende establecer un marco prudencial de gobierno interno para la gestión del riesgo de TIC que se integre en el marco general de gobierno interno de la Directiva sobre requisitos de capital. Además, dada la naturaleza prudencial del marco propuesto, las autoridades competentes para supervisar el cumplimiento de las obligaciones en él establecidas, incluido el BCE, serán las autoridades encargadas de la supervisión bancaria de acuerdo con el Reglamento del MUS.

([54]) 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).

([55]) 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).

([56]) Véase el considerando 8 del reglamento propuesto.

([57]) Véase el considerando 11 del reglamento propuesto.

([58]) Véase el considerando 12 del reglamento propuesto.

([59]) Véanse los considerandos 4 y 5 de la directiva modificativa propuesta.

([60]) Véase el artículo 85 de la Directiva sobre requisitos de capital.

([61]) Véase el artículo 4, apartado 1, del reglamento propuesto.

([62]) Véase el artículo 25, apartados 3 y 4, del reglamento propuesto.

([63]) Véase el artículo 41 del reglamento propuesto.

([64]) Véase el capítulo V, sección II, del reglamento propuesto.

([65]) Véase el capítulo V, sección II, del reglamento propuesto.

3.6 Convendría, pues, que los órganos legislativos de la Unión tuvieran en cuenta lo siguiente para mejorar la claridad y la cohesión entre el reglamento propuesto y la Directiva sobre requisitos de capital. En primer lugar, los requisitos del reglamento propuesto pueden calificarse expresamente de prudenciales, como hace, entre otras normas, el Reglamento sobre DCV ([66]). En segundo lugar, los considerandos de la directiva modificativa propuesta ([67]) podrían redactarse de manera más amplia, ya que los requisitos del reglamento propuesto van más allá de la sola fase de los planes de emergencia y de continuidad de la actividad. Las medidas de gobierno del riesgo de TIC, en general, entran dentro del ámbito más amplio de los «sólidos sistemas de gobierno corporativo» a que se refiere el artículo 74 de la Directiva sobre requisitos de capital ([68]). En tercer lugar, el reglamento propuesto ([69]) debe modificarse para recordar en sus considerandos la competencia del BCE para supervisar prudencialmente las entidades de crédito, de acuerdo con el Tratado y el Reglamento del MUS. En cuarto lugar, debe revisarse la referencia a la aplicación a nivel individual y consolidado de los requisitos del reglamento propuesto ([70]), pues este no define los niveles subconsolidado y consolidado, y algunos tipos de intermediarios no están sujetos a supervisión consolidada según la legislación aplicable (por ejemplo, las entidades de pago). Además, el grado de aplicación de los requisitos del reglamento propuesto debe derivarse exclusivamente de la legislación aplicable a cada tipo de entidad financiera. En el caso de las entidades de crédito, se establece una clara conexión entre la Directiva sobre requisitos de capital y el reglamento propuesto, de manera que los requisitos de este se aplicarían automáticamente a los niveles individual, subconsolidado o consolidado ([71]), según procediera. Por último, los órganos legislativos de la Unión podrían considerar la posibilidad de establecer un régimen transitorio para el período comprendido entre la entrada en vigor del reglamento propuesto y la entrada en vigor de las normas técnicas de regulación en él previstas, dado que algunos intermediarios, incluidas las entidades de crédito, ya están sujetos a disposiciones sobre los riesgos de TIC que son aplicables a sectores específicos y que son más detalladas que las disposiciones generales del reglamento propuesto.

3.7 El Reglamento del MUS atribuye al BCE la función de garantizar el cumplimiento por las entidades de crédito de los requisitos del derecho de la Unión que les imponen disponer de procesos de gestión de riesgos y mecanismos internos de control eficaces ([72]). Esto significa que el BCE debe velar por que las entidades de crédito apliquen políticas y procedimientos de evaluación y gestión de su exposición al riesgo operativo, incluido el riesgo de modelo, y de cobertura de circunstancias poco frecuentes pero muy graves. Las entidades de crédito deben definir lo que constituye un riesgo operativo a efectos de dichas políticas y procedimientos ([73]).

3.8 En julio de 2017 el Consejo de Gobierno del Banco Central Europeo (BCE) aprobó el marco del MUS para la notificación de ciberincidentes, sobre la base de un proyecto propuesto por el Consejo de Supervisión conforme al artículo 26, apartado 8, y al artículo 6, apartado 2, del Reglamento del MUS, y conforme al artículo 21, apartado 1, del Reglamento (UE) n.º 468/2014 del Banco Central Europeo (BCE/2014/17) ([74]). El marco para la notificación de ciberincidentes se basa en una solicitud vinculante (decisiones individuales dirigidas a entidades de crédito) de presentación de información en virtud del artículo 10 del Reglamento del MUS ([75]). Algunos países ya disponen de procedimientos de notificación de incidentes que obligan a las entidades de crédito a notificar a sus ANC todo ciberincidente significativo. En esos países, las entidades de crédito significativas seguirán notificando los incidentes a las ANC, las cuales a su vez los notificarán sin demoras indebidas al BCE en nombre de las entidades supervisadas. Por consiguiente, las decisiones a que se ha hecho referencia se dirigen también a las ANC para que transmitan la información al BCE en virtud del marco para la notificación de ciberincidentes. El BCE respalda los esfuerzos de los órganos legislativos de la Unión por promover la armonización y simplificación del conjunto de normas y

([66]) Véase el capítulo II, sección 4, «Requisitos prudenciales», del Reglamento sobre DCV.

([67]) Véase el considerando 4 de la directiva modificativa propuesta.

([68]) El artículo 85 de la Directiva 2013/36/UE es una mera especificación. Sobre este particular, véanse también las páginas 4, 11 y 37 de las Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad, de 29 de noviembre de 2019 (en lo sucesivo, las «Directrices de la ABE»), que sitúan expresamente su base legal general en el artículo 74 de la Directiva 2013/36/UE.

([69]) Véase el artículo 41, apartado 1, del reglamento propuesto.

([70]) Véase el artículo 25, apartados 3 y 4, del reglamento propuesto.

([71]) Véase también el artículo 109 de la Directiva sobre requisitos de capital.

([72]) Véase el artículo 4, apartado 1, letra e), del Reglamento del MUS.

([73]) Véase el artículo 85 de la Directiva sobre requisitos de capital.

([74]) 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) (BCE/2014/17) (DO L 141 de 14.5.2014, p. 1).

([75]) Concretamente, un ciberincidente (presunta violación voluntaria o accidental de la seguridad de la información) debe notificarse al BCE si se da al menos una de las condiciones siguientes: 1) que su repercusión financiera potencial sea de 5 millones EUR o del 0,1 % del CET1; 2) que se haga público o cause un daño reputacional; 3) que sobrepase la notificación ordinaria y se eleve al jefe de información (CIO); 4) que la entidad de crédito lo notifique al CERT o CSIRT, a una agencia de seguridad o a la policía; 5) que provoque la activación de los procedimientos de recuperación en caso de desastre o de continuidad de la actividad, o que dé lugar a la presentación de una reclamación a un ciberseguro; 6) que se hayan infringido requisitos regulatorios legales, o 7) que la entidad de crédito, siguiendo sus criterios y pericia internos (inclusive sobre el posible impacto sistémico), decida informar al BCE.

obligaciones aplicables a las entidades de crédito en materia de notificación de incidentes. Por ello, el BCE manifiesta su disposición a modificar (y en su caso derogar) el marco para la notificación de ciberincidentes si fuera necesario en vista de la futura adopción del reglamento propuesto.

4. **Observaciones particulares sobre la gestión del riesgo de TIC, la notificación de incidentes, las pruebas de resiliencia operativa y el riesgo de terceros relacionado con las TIC**

4.1 *Gestión del riesgo de TIC*

4.1.1 El BCE celebra que el reglamento propuesto establezca un marco sólido y completo de gestión del riesgo de TIC que incorpora las directrices sobre ciberresiliencia de CPMI-IOSCO y sigue de cerca las mejores prácticas, incluidas las expectativas de vigilancia sobre ciberresiliencia para las infraestructuras del mercado financiero.

4.1.2 El BCE respalda que las entidades financieras deban llevar a cabo una evaluación del riesgo cada vez que se produzca un «cambio importante» en la infraestructura de las redes y los sistemas de información ([76]). Sin embargo, el reglamento propuesto no define qué es un «cambio importante», dando así pie a interpretaciones divergentes de las entidades financieras que no son deseables y que pueden en definitiva obstaculizar los fines armonizadores del reglamento propuesto. Para una mayor seguridad jurídica, convendría que los órganos legislativos de la Unión consideraran la posibilidad de incorporar al reglamento propuesto una definición de «cambio importante».

4.1.3 El BCE apoya en general que las entidades financieras que no sean microempresas deban informar a las autoridades competentes de los costes y pérdidas causados por perturbaciones de las TIC e incidentes relacionados con las TIC ([77]). Sin embargo, para garantizar la eficacia general del sistema y no agobiar a las autoridades competentes y a las entidades financieras con un número excesivo de notificaciones, convendría que los órganos legislativos de la Unión examinaran la posibilidad de introducir umbrales adecuados, posiblemente de carácter cuantitativo.

4.1.4 El BCE toma nota de la facultad de las entidades financieras, previa aprobación de las autoridades competentes, de delegar las tareas de verificación del cumplimiento de los requisitos de gestión del riesgo de TIC en empresas externas o de su mismo grupo ([78]). Al mismo tiempo, es importante que los órganos legislativos de la Unión aclaren cómo se concede la aprobación de las autoridades competentes cuando una determinada entidad financiera esté sujeta a varias, como es el caso de las entidades de crédito, los proveedores de servicios de criptoactivos o los proveedores de servicios de pago. Finalmente, en cuanto a la identificación y clasificación que corresponde efectuar a las entidades financieras según el reglamento propuesto ([79]), el BCE considera que sería prudente, a efectos de la clasificación de los activos, que el reglamento propuesto también exigiera a las entidades financieras que tuvieran en cuenta si esos activos son esenciales (es decir, si respaldan funciones esenciales).

4.2 *Notificación de incidentes*

4.2.1 El BCE acoge favorablemente los esfuerzos del reglamento propuesto por armonizar la notificación de incidentes de TIC en la Unión y avanzar hacia la notificación centralizada de los incidentes graves relacionados con las TIC ([80]). En principio, la introducción de un marco uniforme para la notificación de incidentes graves relacionados con las TIC ([81]) a las autoridades competentes simplificaría y armonizaría la carga informadora de las entidades financieras, incluidas las entidades de crédito. Las autoridades competentes se beneficiarían de una cobertura de incidentes superior a la cobertura que de los ciberincidentes ofrecen los marcos existentes ([82]). La futura adopción del reglamento propuesto exigiría revisar y tal vez derogar los marcos existentes, incluido el marco del MUS para la notificación de ciberincidentes. Dicho lo cual, a fin de lograr la simplificación y plena armonización de todos los marcos, es esencial velar por que el alcance de las disposiciones del reglamento propuesto sobre la notificación de incidentes, incluidas todas las definiciones pertinentes, se ajuste plenamente a los marcos pertinentes.

([76]) Véase el artículo 7, apartado 3, del reglamento propuesto.
([77]) Véase el artículo 10, apartado 9, del reglamento propuesto.
([78]) Véase el artículo 5, apartado 10, del reglamento propuesto.
([79]) Véase el artículo 7 del reglamento propuesto.
([80]) Véase el artículo 19 del reglamento propuesto.
([81]) Véanse el artículo 3, punto 7, y los artículos 17 y 18, del reglamento propuesto.
([82]) Véase por ejemplo el marco para la notificación de ciberincidentes.

Concretamente, es muy importante alinear el reglamento propuesto, por un lado, y, por el otro, la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo ([83]) (en lo sucesivo, la «PSD2») y las directrices de la ABE sobre la notificación de incidentes graves (en lo sucesivo, las «directrices de la ABE»). La directiva modificativa propuesta ([84]) contiene modificaciones de la PSD2 sobre la delimitación de la notificación de incidentes entre el reglamento propuesto y la PSD2 que afectarían principalmente a los proveedores de servicios de pago, que podrían tener también autorización como entidades de crédito, y a las autoridades competentes. Falta claridad en cuanto al proceso de notificación de incidentes, y hay un posible solapamiento en el caso de ciertos incidentes que deben notificarse tanto conforme al reglamento propuesto como conforme a las directrices de la ABE.

4.2.2 Los procedimientos de notificación de incidentes graves establecidos, respectivamente, en el reglamento propuesto ([85]), la PSD2 y las directrices correspondientes de la ABE, exigen de los proveedores de servicios de pago que notifiquen el incidente a su respectiva autoridad competente una vez clasificado este. En realidad, en las notificaciones iniciales no se registra la esencia y la causa del incidente ni la función a la que afecta, y los proveedores de servicios de pago solo pueden estar en condiciones de registrar esos datos en un momento posterior, cuando disponen de más información detallada sobre el incidente. Por lo tanto, los proveedores de servicios de pago podrían, bien presentar las notificaciones iniciales de incidentes tanto conforme al reglamento propuesto como conforme a las directrices de la ABE, bien optar por un solo marco de notificación y corregir la presentación posteriormente. La misma incertidumbre (en cuanto a, por ejemplo, la causa subyacente de un incidente) puede también afectar a los informes intermedios y finales, lo cual vuelve a suscitar la posibilidad de presentar a las autoridades competentes notificaciones paralelas, tanto conforme al reglamento propuesto como conforme a la PSD2.

4.2.3 Ciertos incidentes que pueden clasificarse como incidentes relacionados con las TIC pueden también afectar a otras áreas y, en consecuencia, tener que notificarse conforme a las directrices de la ABE. Así puede ocurrir cuando un incidente tenga repercusiones relacionadas con las TIC pero, al mismo tiempo, haya afectado a la prestación de servicios de pago directamente o a otras áreas o canales funcionales no relacionados con las TIC. Además, puede haber casos en los que no sea posible distinguir entre los incidentes operativos y los relacionados con las TIC. Asimismo, conforme al reglamento propuesto, si una misma entidad financiera es entidad de crédito significativa y proveedor de servicios de pago, tiene que notificar dos veces el incidente relacionado con las TIC, puesto que está sometida a dos autoridades competentes. En vista de lo expuesto, el reglamento propuesto debería expresar más claramente cómo funcionaría en la práctica la interacción entre la PSD2 y las directrices de la ABE. Y lo que es más importante, sería útil para la simplificación y armonización de las obligaciones de información que los órganos legislativos de la Unión examinaran la cuestión pendiente de la doble notificación y aclarasen si el reglamento propuesto, por un lado, y la PSD2 y las directrices de la ABE por el otro, van a coexistir o si, por el contrario, debe haber un único conjunto de requisitos para la notificación de incidentes.

4.2.4. El reglamento propuesto dispone que, cuando reciban una notificación, las autoridades competentes ([86]) acusen recibo de esta y proporcionen con la mayor celeridad posible todos los comentarios o la orientación que sean necesarios a la entidad financiera, en particular para estudiar medidas correctoras al nivel de la entidad o formas de minimizar las repercusiones negativas en los diversos sectores. Esto significa que las autoridades competentes deben contribuir activamente a gestionar y corregir los incidentes, al mismo tiempo que evalúan la respuesta de una entidad supervisada a los incidentes graves. El BCE subraya que debe quedar claro que la responsabilidad y el control de las medidas correctoras y de las consecuencias del incidente corresponden exclusivamente a la entidad financiera interesada. Por eso, el BCE sugiere limitar los comentarios y la orientación a los de carácter prudencial de alto nivel. Proporcionar unos comentarios y una orientación más amplios requeriría contar con unos profesionales especializados y con grandes conocimientos técnicos de los que no suelen disponer las autoridades prudenciales.

4.3 *Pruebas de resiliencia operativa digital*

4.3.1 El BCE celebra que el reglamento propuesto ([87]) disponga que las entidades financieras realicen pruebas de resiliencia operativa digital y que cada entidad tenga su propio programa de pruebas. El reglamento propuesto ([88]) describe diversos tipos de pruebas para orientar a las entidades financieras. Los tipos de pruebas no son del todo claros, y algunas pruebas, como las de compatibilidad, los cuestionarios o las pruebas basadas en escenarios, quedan a la interpretación de las AES, las autoridades competentes o las entidades financieras. Además, no se orienta acerca de

([83]) 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).

([84]) Véase el artículo 7, apartado 9, de la directiva modificativa propuesta.

([85]) Véase el artículo 17, apartado 3, del reglamento propuesto.

([86]) Véase el artículo 20 del reglamento propuesto.

([87]) Véanse los artículos 21 y 22 del reglamento propuesto.

([88]) Véase el artículo 22, apartado 1, del reglamento propuesto.

la frecuencia de cada prueba. Una posible solución sería que el reglamento propuesto estableciera los requisitos generales sobre las pruebas, y que fueran las normas técnicas de regulación y ejecución las que detallaran los diversos tipos de pruebas.

4.3.2 Las pruebas de penetración guiadas por amenazas son un buen instrumento para probar las defensas y el grado de preparación de seguridad. Por ello, el BCE es partidario de que las entidades financieras hagan este tipo de pruebas. Con este instrumento no se ponen a prueba solo las medidas técnicas sino también el personal y los procedimientos. Los resultados de estas pruebas pueden mejorar significativamente la concienciación en materia de seguridad de la alta dirección de las entidades que las hagan. El *European Framework for Threat Intelligence Based Ethical Red-teaming* (TIBER-EU) ([89]), y otras pruebas de penetración guiadas por amenazas ya disponibles fuera de la Unión, son instrumentos básicos para que las propias entidades evalúen, prueben, ensayen y mejoren sus posiciones y defensas de ciberresiliencia.

4.3.3 En la mayoría de los Estados miembros donde se ha aplicado el TIBER-EU, los encargados de las funciones de vigilancia y supervisión no desempeñan un papel activo en la implantación de programas localizados de TIBER-XX, y los ciberequipos del TIBER (TCT) se localizan en casi todos los casos fuera de esas funciones. Por ello, deben aplicarse las pruebas avanzadas del presente reglamento ([90]) basadas en pruebas de penetración guiadas por amenazas, como un instrumento para fortalecer el ecosistema financiero y aumentar la estabilidad financiera, más que como un instrumento puramente supervisor. Además, no es necesario crear un nuevo marco avanzado de pruebas de ciberresiliencia, pues son ya muchos los Estados miembros que han adoptado el TIBER-EU, que es actualmente el único marco de esta clase en la UE.

4.3.4 Los requisitos relativos a los encargados de las pruebas no deben incluirse en la parte principal del reglamento propuesto, pues el sector de las pruebas de penetración guiadas por amenazas está aún en fase de desarrollo, e imponer requisitos específicos podría obstaculizar la innovación. Dicho lo cual, el BCE considera que, a fin de asegurar un alto grado de independencia en la ejecución de las pruebas, las entidades financieras no deberían emplear o contratar como encargados de las pruebas a empleados o contratistas de entidades financieras de su mismo grupo o a personas que pertenezcan o estén sujetas al control de las entidades financieras objeto de las pruebas.

4.3.5 A fin de reducir el riesgo de fragmentación y asegurar la armonización, el reglamento propuesto debe establecer un marco de pruebas de penetración guiadas por amenazas aplicable al sector financiero del conjunto de la Unión. La fragmentación podría provocar mayores costes y necesidades de recursos técnicos, operativos y económicos, tanto para las autoridades competentes como para las entidades financieras, que podrían, en definitiva, repercutir negativamente en el reconocimiento recíproco de las pruebas. La falta de armonización y los problemas consiguientes de reconocimiento recíproco son cuestiones de suma importancia para las entidades financieras, que pueden tener varias autorizaciones y actuar en diversas jurisdicciones de la Unión. Las normas técnicas de regulación y ejecución que deben adoptarse respecto de las pruebas de penetración guiadas por amenazas conforme al reglamento propuesto, deben ser coherentes con el TIBER-EU. Además, el BCE celebra poder participar en la elaboración de esas normas técnicas de regulación y ejecución en colaboración con las AES.

4.3.6 La participación activa de las autoridades competentes en las pruebas podría originar un conflicto de intereses con la otra función que esas autoridades ejercen, a saber, la de evaluar el marco de pruebas de la entidad financiera. Por ello, el BCE sugiere que se suprima del reglamento propuesto la obligación de las autoridades competentes de validar la documentación y expedir certificados de ejecución de las pruebas de penetración guiadas por amenazas.

4.4 Riesgo de terceros relacionado con las TIC

4.4.1 El BCE aplaude la introducción de un amplio conjunto de principios esenciales y un marco de vigilancia sólido para identificar y gestionar los riesgos de TIC relacionados con los proveedores terceros de servicios de TIC, pertenezcan o no al mismo grupo de entidades financieras. No obstante, para lograr una identificación y gestión eficaz del riesgo de TIC, es importante entre otras cosas identificar y clasificar correctamente a los proveedores terceros esenciales de servicios de TIC. Sobre este particular, aunque celebra la introducción de actos delegados ([91]) que completen los criterios aplicables con fines de clasificación ([92]), el BCE considera que debe ser consultado antes de que esos actos delegados se adopten.

([89]) Disponible en la dirección del BCE en internet, www.ecb.europa.eu.
([90]) Artículos 23 y 24 del reglamento propuesto.
([91]) Véase el artículo 28, apartado 3, del reglamento propuesto.
([92]) Véase el artículo 28, apartado 2, del reglamento propuesto.

4.4.2 En cuanto al marco de supervisión ([93]), debe aclararse mejor la función del Comité Mixto. Al mismo tiempo, el BCE celebra ser parte del Foro de Supervisión como observador, pues esta condición le dará el mismo acceso a la documentación e información del que disfrutan los miembros con derecho de voto ([94]). El BCE señala a la atención de los órganos legislativos de la Unión que, en su condición de observador, el BCE contribuiría a la labor del Foro de Supervisión como banco central de emisión, con responsabilidad en la vigilancia de las infraestructuras del mercado, y también como supervisor prudencial de las entidades de crédito. Asimismo, el BCE señala que, además de ser observador en el Foro de Supervisión, formaría parte, como autoridad competente, del equipo de examen conjunto. Sobre este punto, convendría que los órganos legislativos de la Unión revisaran la composición de los equipos de examen conjunto ([95]) a fin de asegurar el peso adecuado de la participación de las autoridades competentes pertinentes. Además, el BCE considera que debería incrementarse el número máximo de participantes en los equipos de examen conjunto, teniendo en cuenta la importancia, la complejidad y el alcance de los servicios de TIC prestados por terceros.

4.4.3 El BCE observa que, conforme al reglamento propuesto, el supervisor principal puede impedir a los proveedores terceros esenciales de servicios de TIC que recurran a la subcontratación: i) si el subcontratista previsto es un proveedor tercero de servicios de TIC o un subcontratista de TIC establecido en un tercer país, y ii) si la subcontratación afecta a una función esencial o importante de la entidad financiera. El BCE subraya que esta facultad solo puede ejercerla el supervisor principal en supuestos de subcontratación en los que un proveedor tercero esencial de servicios de TIC subcontrate una función esencial o importante con una persona jurídica distinta establecida en un tercer país. El BCE entiende que el supervisor principal no podría ejercer semejante facultad para impedir que un proveedor tercero esencial de servicios de TIC externalizase funciones esenciales o importantes de la entidad financiera a un centro de dicho proveedor situado en un tercer país. Podría suceder, por ejemplo, que, desde el punto de vista operativo, se almacenasen o tratasen datos o informaciones esenciales en centros situados fuera del Espacio Económico Europeo (EEE), en cuyo caso, las facultades del supervisor principal podrían no bastar para habilitar debidamente a las autoridades competentes para acceder a la información, los locales, las infraestructuras y el personal relacionados con el ejercicio de todas las funciones esenciales o importantes de la entidad financiera. A fin de garantizar que las autoridades competentes puedan ejercer sus funciones sin obstáculos, el BCE sugiere que se faculte también al supervisor principal para limitar el uso por proveedores terceros esenciales de servicios de TIC de instalaciones situadas fuera del EEE. Esta facultad podría ejercerse en aquellos casos concretos en que no se hayan concluido los acuerdos administrativos con las autoridades de terceros países previstos en el reglamento propuesto ([96]), o en que los representantes de los proveedores terceros esenciales de servicios de TIC no den garantías suficientes, conforme al marco del tercer país pertinente, del acceso a la información, los locales, la infraestructura y el personal, necesario para el ejercicio de las funciones de vigilancia o supervisión.

4.4.4 Por último, exigir a las autoridades competentes que hagan un seguimiento de las recomendaciones del supervisor principal ([97]) podría no ser eficaz, pues es posible que dichas autoridades no tengan una visión integral de los riesgos planteados por cada proveedor tercero esencial de servicios de TIC. Además, puede que las autoridades competentes tengan que tomar medidas contra las entidades financieras que supervisan si los proveedores terceros esenciales no siguen las recomendaciones formuladas. Conforme al reglamento propuesto ([98]), las autoridades competentes pueden exigir a las entidades financieras que supervisan que suspendan temporalmente el servicio prestado por el proveedor tercero esencial o que pongan fin a los acuerdos contractuales en vigor con dicho proveedor. Es difícil traducir en acciones concretas el proceso de seguimiento previsto. En particular, no está claro que una entidad financiera supervisada esté en condiciones de suspender o rescindir un contrato con un proveedor tercero esencial de servicios de TIC si este es un proveedor importante de esa entidad financiera, o si la suspensión o rescisión puede acarrear a esta costes y compensaciones, contractuales o de otra índole. Además, esta solución no contribuye a la convergencia de la supervisión, pues las autoridades competentes pueden interpretar una misma recomendación de manera diferente, lo cual, en última instancia, podría obstaculizar el objetivo de armonizar la vigilancia del riesgo de terceros relacionado con las TIC al nivel de la Unión. En virtud de lo expuesto, convendría que los órganos legislativos de la Unión consideraran la posibilidad de otorgar a los supervisores legales unos poderes ejecutivos especiales, frente a los proveedores terceros esenciales de servicios de TIC, que tuvieran en cuenta los límites establecidos por la doctrina *Meroni* según los mitiga en parte el Tribunal de Justicia en su sentencia sobre el asunto AEVM ([99]).

([93]) Véase el artículo 29 del reglamento propuesto.
([94]) Véase el artículo 29, apartado 4, del reglamento propuesto.
([95]) Véase el artículo 35 del reglamento propuesto.
([96]) Véase el artículo 39, apartado 1, del reglamento propuesto.
([97]) Véanse el artículo 29, apartado 4, y el artículo 37, del reglamento propuesto.
([98]) Véase el artículo 37, apartado 3, del reglamento propuesto.
([99]) Véase la Sentencia del Tribunal de Justicia (Gran Sala), de 22 de enero de 2014, Reino Unido de Gran Bretaña e Irlanda del Norte contra Parlamento Europeo y Consejo de la Unión Europea - Reglamento (UE) n.º 236/2012 - Asunto C-270/12.

En un documento técnico de trabajo aparte figuran las propuestas de redacción específicas, acompañadas de explicaciones, correspondientes a los puntos del reglamento propuesto que el BCE recomienda modificar. El documento técnico de trabajo está disponible en inglés en EUR-Lex.

Hecho en Fráncfort del Meno el 4 de junio de 2021.

La presidenta del BCE
Christine LAGARDE