I

(Resoluciones, recomendaciones y dictámenes)

RECOMENDACIONES

JUNTA EUROPEA DE RIESGO SISTÉMICO

RECOMENDACIÓN DE LA JUNTA EUROPEA DE RIESGO SISTÉMICO

de 2 de diciembre de 2021

sobre un marco paneuropeo de coordinación de ciberincidentes sistémicos para las autoridades pertinentes

(JERS/2021/17)

(2022/C 134/01)

LA JUNTA GENERAL DE LA JUNTA EUROPEA DE RIESGO SISTÉMICO,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Acuerdo sobre el Espacio Económico Europeo ([1]), en particular, su anexo IX,

Visto el Reglamento (UE) n.º 1092/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, relativo a la supervisión macroprudencial del sistema financiero en la Unión Europea y por el que se crea una Junta Europea de Riesgo Sistémico ([2]), en particular el artículo 3, apartado, 2, letras b) y d), y los artículos 16 y 18,

Vista la Decisión JERS/2011/1 de la Junta Europea de Riesgo Sistémico, de 20 de enero 2011, por la que se adopta el Reglamento interno de la Junta Europea de Riesgo Sistémico ([3]), en particular los artículos 18 a 20,

Considerando lo siguiente:

(1) Como se señala en el considerando 4 de la Recomendación JERS/2013/1 de la Junta Europea de Riesgo Sistémico ([4]), el objetivo final de la política macroprudencial es contribuir a la protección de la estabilidad del sistema financiero en su conjunto, incluso mediante el refuerzo de la capacidad de resistencia del sistema financiero y la atenuación de los riesgos sistémicos, garantizando así una aportación sostenible del sector financiero al crecimiento económico. La Junta Europea de Riesgo Sistémico (JERS) se encarga de la vigilancia macroprudencial del sistema financiero de la Unión. En el cumplimiento de su mandato, la JERS debe contribuir a prevenir y reducir los riesgos sistémicos para la estabilidad financiera, inclusive los relacionados con ciberincidentes, y proponer cómo atenuarlos.

(2) Los ciberincidentes graves pueden suponer un riesgo sistémico para el sistema financiero, dado que pueden interrumpir operaciones y servicios financieros esenciales. La amplificación de una perturbación inicial puede producirse a través del contagio operativo o financiero o a través de una erosión de la confianza en el sistema financiero. Si el sistema financiero no puede absorber estas perturbaciones, la estabilidad financiera correrá peligro, y esta situación puede dar lugar a una crisis cibernética sistémica ([5]).

([1]) DO L 1 de 3.1.1994, p. 3.
([2]) DO L 331 de 15.12.2010, p. 1.
([3]) DO C 58 de 24.2.2011, p. 4.
([4]) Recomendación de la Junta Europea de Riesgo Sistémico, de 4 de abril de 2013, sobre objetivos intermedios e instrumentos de política macroprudencial (JERS/2013/1) (OJ C 170, 15.6.2013, p. 1).
([5]) Véase «Systemic cyber risk», JERS, febrero de 2020, disponible en inglés en la dirección de la JERS en Internet: www.esrb.europa.eu

(3) El panorama de ciberamenazas en constante evolución y el reciente aumento de ciberincidentes graves son indicadores de mayor riesgo para la estabilidad financiera de la Unión. La pandemia de COVID-19 ha puesto de relieve la importancia del papel que desempeña la tecnología en el funcionamiento del sistema financiero. Las autoridades e instituciones pertinentes deben adaptar su infraestructura técnica y sus marcos de gestión de riesgos a un aumento repentino del trabajo a distancia, que ha elevado la exposición global del sistema financiero a las ciberamenazas y ha permitido a los delincuentes concebir nuevos modos de operar y adaptar los existentes para aprovechar la situación ([6]). En este contexto, el número de ciberincidentes notificados a la supervisión bancaria del BCE en 2020 se incrementó en un 54 % en comparación con 2019 ([7]).

(4) La gran escala, velocidad y tasa de propagación de un ciberincidente grave exigen una respuesta eficaz por parte de las autoridades competentes para atenuar los posibles efectos negativos sobre la estabilidad financiera. Una rápida coordinación y comunicación entre las autoridades pertinentes de la Unión puede contribuir a la evaluación temprana de los efectos de un ciberincidente grave en la estabilidad financiera, mantener la confianza en el sistema financiero y limitar el contagio a otras entidades financieras, contribuyendo así a evitar que un ciberincidente grave se convierta en un riesgo para la estabilidad financiera.

(5) La perturbación subyacente tiene su origen en una forma novedosa en comparación con las crisis financieras y de liquidez tradicionales a las que se suelen enfrentar las autoridades pertinentes. Además de los aspectos financieros, la evaluación global de riesgos debe incluir la magnitud y los efectos de las perturbaciones operativas, ya que podrían influir en la elección de los mecanismos macroprudenciales. Del mismo modo, la estabilidad financiera también podría influir en la elección de medidas operativas por parte de los ciberexpertos. Esto requiere una coordinación estrecha y rápida y una comunicación abierta para, entre otras cosas, facilitar el conocimiento de la situación.

(6) El riesgo de fallo de coordinación por parte de las autoridades existe y debe abordarse. Las autoridades pertinentes de la Unión tendrán que coordinarse entre sí y con otras autoridades, como la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), con las que normalmente no interactúan. Dado que un número significativo de instituciones financieras de la Unión operan a escala mundial, es probable que un ciberincidente grave no se limite a la Unión o pueda desencadenarse fuera de esta y requiera una coordinación global de la respuesta.

(7) Las autoridades pertinentes deben estar preparadas para estas interacciones. De lo contrario, podrían adoptar medidas incoherentes que contradigan o pongan en peligro las respuestas de otras autoridades. Este fallo de coordinación podría amplificar la perturbación del sistema financiero al provocar una erosión de la confianza en su funcionamiento que, en el peor de los casos, supondría un riesgo para la estabilidad financiera ([8]). Por lo tanto, deben adoptarse las medidas necesarias para abordar el riesgo para la estabilidad financiera derivado de un fallo de coordinación en caso de ciberincidente grave.

(8) El informe de la JERS (2021) *Mitigating systemic cyber risk* ([9]) identifica la necesidad de establecer un marco paneuropeo de coordinación de ciberincidentes sistémicos (EU-SCICF) para las autoridades pertinentes de la Unión. El objetivo del EU-SCICF sería aumentar el nivel de preparación de las autoridades pertinentes para facilitar una respuesta coordinada a un ciberincidente potencialmente grave. El informe de la JERS (2021) *Mitigating system cyber risk* presenta la evaluación de la JERS sobre las características marco que serían necesarias, a primera vista, para hacer frente al riesgo de fallo de coordinación.

(9) El objetivo principal de la presente recomendación es basarse en una de las funciones previstas de las Autoridades Europeas de Supervisión (AES) en virtud de la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero ([10]) (en lo sucesivo, «DORA») para permitir gradualmente una respuesta coordinada eficaz a nivel de la Unión en caso de un incidente transfronterizo grave relacionado con las tecnologías de la información y la comunicación (TIC) o una amenaza conexa que tenga efectos sistémicos en el sector financiero de la Unión en su conjunto. Este proceso dará lugar a la creación del EU-SCICF para las autoridades pertinentes.

([6]) Véase la Evaluación de la amenaza de la delincuencia organizada en Internet, Europol, 2020, disponible en la dirección de Europol en Internet: www.europol.europa.eu

([7]) Véase «IT and cyber risk: a constant challenge», BCE, 2021, disponible en inglés en la dirección de supervisión bancaria del BCE en internet, www.bankingsupervision.europa.eu

([8]) Véase «Systemic cyber risk», JERS, febrero de 2020, disponible en inglés en la dirección de la JERS en Internet: www.esrb.europa.eu

([9]) Véase «Mitigating systemic cyber risk», JERS, 2021, (disponible).

([10]) COM(2020) 595 final.

(10) El EU-SCICF no debe tener como objetivo sustituir los marcos existentes, sino colmar las lagunas de coordinación y comunicación entre las propias autoridades pertinentes y con otras autoridades de la Unión y otros actores esenciales en el ámbito internacional. A este respecto, debe tenerse en cuenta el posicionamiento del EU-SCICF en el actual marco de crisis financiera y en el panorama del marco de ciberincidentes de la Unión. Por lo que respecta a la coordinación entre las propias autoridades pertinentes, deben considerarse, entre otras cosas, las funciones y actividades del Grupo de Cooperación sobre Redes y Sistemas de Información (SRI) para las entidades financieras en virtud de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo ([11]), y los mecanismos de coordinación previstos a través de la creación de la Unidad Informática Conjunta junto con la participación de la ENISA.

(11) En particular, la propuesta de poner en marcha la preparación del EU-SCICF tiene por objeto respaldar las funciones potenciales de las AES, tal como se prevé en la propuesta de DORA. La DORA propone que «las AES, a través del Comité Mixto y en colaboración con las autoridades competentes, el Banco Central Europeo (BCE) y la JERS, podrán establecer mecanismos que permitan compartir prácticas eficaces en todos los sectores financieros a fin de mejorar la conciencia situacional y detectar las vulnerabilidades y los riesgos cibernéticos comunes a los diversos sectores» y «podrán organizar ejercicios de gestión de crisis y contingencia que incluyan escenarios de ciberataques con el fin de desarrollar los canales de comunicación y hacer posible gradualmente una respuesta coordinada eficaz a nivel de la UE en caso de que se produzca un incidente grave relacionado con las TIC de alcance transfronterizo o una amenaza conexa que tenga un impacto sistémico en el sector financiero de la Unión en su conjunto» ([12]). Todavía no existe un marco paneuropeo como el EU-SCICF, que debe establecerse y desarrollarse en el contexto de la DORA.

(12) Habida cuenta del riesgo para la estabilidad financiera de la Unión derivado del riesgo cibernético, los trabajos preparatorios para el establecimiento gradual del EU-SCICF deben comenzar, en la medida de lo posible, incluso antes de que el marco jurídico y político necesario para su establecimiento sea plenamente aplicable. Este marco jurídico y político se completaría plenamente y se concluiría una vez sean aplicables las disposiciones pertinentes de la DORA y de sus actos delegados.

(13) Una comunicación eficaz contribuye al conocimiento de la situación entre las autoridades pertinentes y, por lo tanto, es un requisito previo indispensable para la coordinación a escala de la Unión durante los ciberincidentes graves. A este respecto, debe definirse la infraestructura de comunicación necesaria para coordinar una respuesta a un ciberincidente grave. Esto implicaría especificar el tipo de información que debe compartirse, los canales regulares que deben utilizarse para compartir dicha información y los puntos de contacto con los que debe compartirse la información. El intercambio de información debe respetar los requisitos legales existentes. Además, las autoridades pertinentes pueden tener que definir un plan de acción claro y los protocolos que deben seguirse para garantizar una coordinación adecuada entre las autoridades implicadas en la planificación de una respuesta coordinada a un ciberincidente grave.

(14) Una crisis cibernética sistémica requerirá la puesta en marcha de una plena cooperación a nivel nacional y de la Unión. Por consiguiente, puede preverse la designación de puntos de contacto para las AES, el BCE y cada Estado miembro entre sus autoridades nacionales pertinentes, que deben comunicarse a las AES, a fin de establecer los principales interlocutores en el sistema de coordinación del EU-SCICF que deben ser informados en caso de ciberincidente grave. La necesidad de designar puntos de contacto debe evaluarse durante el desarrollo del EU-SCICF, teniendo en cuenta el punto de contacto único designado en virtud de la Directiva (UE) 2016/1148 que los Estados miembros han establecido sobre la seguridad de las redes y sistemas de información para garantizar la cooperación transfronteriza con otros Estados miembros y con el Grupo de Cooperación SRI ([13]).

(15) La realización de ejercicios de gestión de crisis y contingencias podría facilitar la aplicación del EU-SCICF y permitir a las autoridades evaluar su disposición y preparación ante una cibercrisis sistémica a escala de la Unión. Estos ejercicios proporcionarían a las autoridades las enseñanzas extraídas y permitirían una mejora y evolución continuas del EU-SCICF.

([11]) 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).

([12]) Véase el proyecto de artículo 43 de la propuesta de la DORA.

([13]) Véase Comisión Europea, Grupo de cooperación SRI, disponible en la dirección de la Comisión Europea en Internet: www.ec.europa.eu

(16) Para la creación del EU-SCICF es esencial que las AES lleven a cabo conjuntamente los trabajos preparatorios pertinentes a fin de considerar los posibles elementos esenciales del marco y los recursos necesarios para su creación. A continuación, las AES podrían empezar a trabajar en un análisis preliminar de cualquier impedimento que pudiera dificultar su capacidad y la de las autoridades pertinentes para establecer el EU-SCICF y compartir información pertinente a través de canales de comunicación en caso de ciberincidente grave. Este análisis sería un paso importante para dar a conocer cualquier otra medida, ya sea de carácter legislativo u otras iniciativas de apoyo que la Comisión Europea pueda adoptar en la fase de aplicación posterior a la DORA.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

SECCIÓN 1

RECOMENDACIONES

Recomendación A – Establecimiento de un marco paneuropeo de coordinación de ciberincidentes sistémicos (EU-SCICF)

1. Se recomienda que, tal como se prevé en la propuesta de la Comisión de Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero (en lo sucesivo, «DORA»), las Autoridades Europeas de Supervisión (AES), conjuntamente a través del Comité Mixto y junto con el Banco Central Europeo (BCE), la Junta Europea de Riesgo Sistémico (JERS) y las autoridades nacionales pertinentes, comiencen a prepararse para el establecimiento gradual de una respuesta coordinada eficaz a escala de la Unión en caso de ciberincidente transfronterizo grave o amenaza conexa que pueda tener un impacto sistémico en el sector financiero de la Unión. El trabajo preparatorio para lograr una respuesta coordinada a nivel de la Unión debe conllevar el establecimiento gradual del EU-SCICF para las AES, el BCE, la JERS y las autoridades nacionales pertinentes. Esto también debe incluir una evaluación de las necesidades de recursos para la creación efectiva del EU-SCICF.

2. Se recomienda a las AES, a la vista de la recomendación A, apartado 1, que, en consulta con el BCE y la JERS, emprendan un inventario y un análisis posterior de los obstáculos actuales, jurídicos y de otra índole para la creación efectiva del EU-SCICF.

Recomendación B – Establecimiento de puntos de contacto del EU-SCICF

Se recomienda a las AES, al BCE y a cada Estado miembro, que, entre sus autoridades nacionales pertinentes, designen un punto de contacto principal que debe comunicarse a las AES. Esta lista de contactos facilitará la creación del marco y, una vez establecido el EU-SCICF, los puntos de contacto y la JERS deben ser informados en caso de ciberincidente grave. También debe preverse la coordinación entre el EU-SCICF y el punto de contacto único designado en virtud de la Directiva (UE) 2016/1148 que los Estados miembros hayan establecido sobre la seguridad de las redes y sistemas de información para garantizar la cooperación transfronteriza con otros Estados miembros y con el Grupo de Cooperación sobre Redes y Sistemas de Información.

Recomendación C – Medidas adecuadas a escala de la Unión

Se recomienda que, sobre la base de los resultados de los análisis realizados de conformidad con la recomendación A, la Comisión considere las medidas adecuadas necesarias para garantizar una coordinación eficaz de las respuestas a los ciberincidentes sistémicos.

SECCIÓN 2

APLICACIÓN

1. **Definiciones**

A efectos de la presente recomendación, se entenderá por:

(a) «cibernético», relacionado con, dentro o a través del soporte de la infraestructura de información interconectada de las interacciones entre personas, procesos, datos y sistemas de información ([14]);

([14]) Véase «Cyber Lexicon», FSB, 12 de noviembre de 2018, disponible en inglés en la dirección del FSB de internet en www.fsb.org

(b) «ciberincidente grave», un incidente relacionado con las TIC que puede tener efectos negativos importantes en las redes y los sistemas de información que respaldan las funciones esenciales de las entidades financieras ([15]);

(c) «crisis cibernética sistémica», un ciberincidente grave que causa un nivel de perturbación del sistema financiero de la Unión que puede acarrear graves consecuencias negativas para el buen funcionamiento del mercado interior y el funcionamiento de la economía real. Una crisis de estas características podría ser consecuencia de un ciberincidente grave que provoque perturbaciones en una serie de canales, incluidos los aspectos operativos, de confianza y financieros;

(d) «Autoridades Europeas de Supervisión» o «AES», la Autoridad Europea de Supervisión (Autoridad Bancaria Europea), creada en virtud del Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo ([16]), la Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación), creada en virtud del Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo ([17]), y la Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados), creada en virtud del Reglamento (UE) n.º 1095/2010 del Parlamento Europeo y del Consejo ([18]);

(e) «Comité Mixto», el Comité Mixto de las Autoridades Europeas de Supervisión previsto en el artículo 54 del Reglamento (UE) n.º 1093/2010, del Reglamento (UE) n.º 1094/2010 y del Reglamento (UE) n.º 1095/2010;

(f) «autoridad nacional pertinente»,

1. una autoridad competente o de supervisión de un Estado miembro especificada en los actos de la Unión a que se refiere el artículo 1, apartado 2, del Reglamento (UE) n.º 1093/2010, del Reglamento (UE) n.º 1094/2010 y del Reglamento (UE) n.º 1095/2010, y cualquier otra autoridad nacional competente especificada en los actos de la Unión que confieran funciones a las AES;

2. una autoridad competente de un Estado miembro designada de conformidad con:

i. el artículo 4 de la Directiva 2013/36/UE del Parlamento Europeo y del Consejo ([19]), sin perjuicio de las funciones específicas atribuidas al BCE por el Reglamento (UE) n.º 1024/2013 del Consejo ([20]);

ii. el artículo 22 del Reglamento (UE) n.º 2015/2366 del Parlamento Europeo y del Consejo ([21]);

iii. el artículo 37 de la Directiva 2009/110/CE del Parlamento Europeo y del Consejo ([22]);

iv. el artículo 4 de la Directiva (UE) 2019/2034 del Parlamento Europeo y del Consejo ([23]);

([15]) Véase el proyecto de artículo 3, punto 7, de la propuesta de la DORA.

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

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

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

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

([20]) 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).

([21]) 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).

([22]) Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE (DO L 267 de 10.10.2009, p. 7).

([23]) Directiva (UE) 2019/2034 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019, relativa a la supervisión prudencial de las empresas de servicios de inversión, y por la que se modifican las Directivas 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE y 2014/65/UE (DO L 314 de 5.12.2019, p. 64).

v. el artículo 3, apartado 1, *sexies sexies*, primer guion, de la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937 ([24]);

vi. el artículo 11 del Reglamento (UE) n.º 909/2014 del Parlamento Europeo y del Consejo ([25]);

vii. el artículo 22 del Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo ([26]);

viii. el artículo 67 de la Directiva 2014/65/CE del Parlamento Europeo y del Consejo ([27]);

ix. el artículo 22 del Reglamento (UE) n.º 648/2012,

x. el artículo 44 de la Directiva 2011/61/UE del Parlamento Europeo y del Consejo ([28]);

xi. el artículo 97 de la Directiva 2009/65/UE del Parlamento Europeo y del Consejo ([29]);

xii. el artículo 30 de la Directiva 2009/138/CE del Parlamento Europeo y del Consejo ([30]);

xiii. el artículo 12 de la Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo ([31]);

xiv. el artículo 47 de la Directiva (UE) 2016/2341 del Parlamento Europeo y del Consejo ([32]);

xv. el artículo 22 del Reglamento (CE) n.º 1060/2009 del Parlamento Europeo y del Consejo ([33]);

xvi. el artículo 3, apartado 2, y el artículo 32, de la Directiva 2006/43/CE del Parlamento Europeo y del Consejo ([34]);

xvii. el artículo 40 del Reglamento (UE) n.º 2016/1011 del Parlamento Europeo y del Consejo ([35]);

xviii. el artículo 29 del Reglamento (UE) n.º 2020/1503 del Parlamento Europeo y del Consejo ([36]);

([24]) COM(2020) 593 final.

([25]) 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).

([26]) 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).

([27]) Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (DO L 173 de 12.6.2014, p. 349).

([28]) Directiva 2011/61/UE, del Parlamento Europeo y del Consejo, de 8 de junio de 2011, relativa a los gestores de fondos de inversión alternativos y por la que se modifican las Directivas 2003/41/CE y 2009/65/CE y los Reglamentos (CE) n.º 1060/2009 y (UE) n.º 1095/2010 (DO L 174 de 1.7.2011, p. 1).

([29]) Directiva 2009/65/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, por la que se coordinan las disposiciones legales, reglamentarias y administrativas sobre determinados organismos de inversión colectiva en valores mobiliarios (OICVM) (DO L 302 de 17.11.2009, p. 32).

([30]) Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, relativa al acceso a la actividad de seguro y reaseguro y a su ejercicio (Solvencia II) (DO L 335 de 17.12.2009, p. 1).

([31]) Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros (versión refundida) (DO L 26 de 2.2.2016, p. 19).

([32]) Directiva (UE) 2016/2341 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2016, relativa a las actividades y la supervisión de los fondos de pensiones de empleo (FPE) (DO L 354 de 23.12.2016, p.37).

([33]) Reglamento (CE) n.º 1060/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre las agencias de calificación crediticia (DO L 302 de 17.11.2009, p. 1).

([34]) Directiva 2006/43/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas, por la que se modifican las Directivas 78/660/CEE y 83/349/CEE del Consejo y se deroga la Directiva 84/253/CEE (DO L 157 de 9.6.2006, p.87).

([35]) Reglamento (UE) 2016/1011 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, sobre los índices utilizados como referencia en los instrumentos financieros y en los contratos financieros o para medir la rentabilidad de los fondos de inversión, y por el que se modifican las Directivas 2008/48/CE y 2014/17/UE y el Reglamento (UE) n.º 596/2014 (DO L 171 de 29.6.2016, p.1).

([36]) Reglamento (UE) 2020/1503 del Parlamento Europeo y del Consejo, de 7 de octubre de 2020, relativo a los proveedores europeos de servicios de financiación participativa para empresas, y por el que se modifican el Reglamento (UE) 2017/1129 y la Directiva (UE) 2019/1937 (DO L 347 de 20.10.2020, p. 1).

3. una autoridad a la que se haya encomendado la adopción o la activación de medidas de política macroprudencial, u otras funciones de estabilidad financiera, como, por ejemplo, el análisis de apoyo correspondiente, entre otras, a modo de ejemplo:

   i. una autoridad designada de conformidad con el capítulo 4, del título VII, de la Directiva 2013/36/UE, o con el artículo 458, apartado 1, del Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo ([37]);

   ii. una autoridad macroprudencial con los objetivos, los acuerdos, las funciones, las competencias, los instrumentos, los requisitos de rendición de cuentas y otras características establecidos en la Recomendación JERS/2011/3 de la Junta Europea de Riesgo Sistémico ([38]);

(g) «autoridad pertinente»,

1. una AES;

2. el BCE en lo que respecta a las funciones que se le atribuyen de conformidad con el artículo 4, apartados 1 y 2, y artículo 5, apartado 2, del Reglamento (UE) n.º 1024/2013;

3. una autoridad nacional pertinente.

2. **Criterios de aplicación**

La aplicación de la presente recomendación se regirá por los siguientes criterios:

(a) Debe prestarse la debida consideración al principio de necesidad de conocer y al principio de proporcionalidad, teniendo en cuenta el objetivo y el contenido de cada recomendación.

(b) Se deben satisfacer los criterios específicos de cumplimiento establecidos en el anexo en relación con cada recomendación.

3. **Plazos de seguimiento**

De acuerdo con el artículo 17, apartado 1, del Reglamento (UE) n.º 1092/2010, los destinatarios de la presente recomendación deben comunicar al Parlamento Europeo, al Consejo, a la Comisión, y a la JERS, las medidas que tomen al respecto, así como la justificación adecuada de cualquier inacción. Se pide a los destinatarios que realicen dicha comunicación de conformidad con los siguientes plazos:

1. Recomendación A

(a) A más tardar el 30 de junio de 2023, pero no antes de seis meses después de la entrada en vigor de la DORA, se pide a las AES que presenten al Parlamento Europeo, al Consejo, a la Comisión y a la JERS un informe provisional sobre la aplicación de la recomendación A, apartado 1.

(b) A más tardar el 30 de junio de 2024, pero no antes de 18 meses después de la entrada en vigor de la DORA, se pide a las AES que presenten al Parlamento Europeo, al Consejo, a la Comisión y a la JERS un informe final sobre la aplicación de la recomendación A, apartado 1.

(c) A más tardar el 30 de junio de 2025, pero no antes de 30 meses después de la entrada en vigor de la DORA, se pide a las AES que presenten al Parlamento Europeo, al Consejo, a la Comisión y a la JERS un informe sobre la aplicación de la recomendación A, apartado 2.

2. Recomendación B

A más tardar el 30 de junio de 2023, pero no antes de seis meses después de la entrada en vigor de la DORA, se pide a las AES, al BCE y a los Estados miembros que presenten al Parlamento Europeo, al Consejo, a la Comisión y a la JERS un informe sobre la aplicación de la recomendación B.

3. Recomendación C

(a) A más tardar el 31 de diciembre de 2023, pero no antes de 12 meses después de la entrada en vigor de la DORA, se pide a la Comisión que presente al Parlamento Europeo, al Consejo y a la JERS un informe sobre la aplicación de la recomendación C en vista del informe provisional de las AES de conformidad con la recomendación A, apartado 1.

([37]) Reglamento (UE) No 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) no 648/2012 (DO L 176 de 27.6.2013, p. 1).

([38]) Recomendación de la Junta Europea de Riesgo Sistémico, de 22 de diciembre de 2011, sobre el mandato macroprudencial de las autoridades nacionales (JERS/2011/3) (DO C 41 de 14.2.2012, p. 1).

(b) A más tardar el 31 de diciembre de 2025, pero no antes de 36 meses después de la entrada en vigor de la DORA, se pide a la Comisión que presente al Parlamento Europeo, al Consejo y a la JERS un informe sobre la aplicación de la recomendación C en vista de los informes de las AES de conformidad con la recomendación A.

4. **Vigilancia y evaluación**

1. La Secretaría de la JERS:

(a) prestará asistencia a los destinatarios garantizando la coordinación de la presentación de información, facilitando las plantillas pertinentes y especificando, en caso necesario, el procedimiento y los plazos de seguimiento;

(b) verificará el seguimiento realizado por los destinatarios, les prestará asistencia si así lo solicitan y presentará informes de seguimiento a la Junta General. Las evaluaciones se iniciarán de la manera siguiente:

(i) en un plazo de 12 meses a partir de la entrada en vigor de la DORA, en relación con la aplicación de las recomendaciones A y B;

(ii) en un plazo de 18 meses a partir de la entrada en vigor de la DORA, en relación con la aplicación de la recomendación C;

(iii) en un plazo de 24 meses a partir de la entrada en vigor de la DORA, en relación con la aplicación de la recomendación A;

(iv) en un plazo de 36 meses a partir de la entrada en vigor de la DORA, en relación con la aplicación de la recomendación A;

(v) en un plazo de 42 meses a partir de la entrada en vigor de la DORA, en relación con la aplicación de la recomendación C;

2. La Junta General evaluará las medidas y justificaciones que comuniquen los destinatarios de la presente recomendación y, cuando proceda, podrá decidir que la presente recomendación no se ha aplicado y que el destinatario pertinente no ha justificado adecuadamente su inacción.

Hecho en Fráncfort del Meno el 2 de diciembre de 2021.

El Jefe de la Secretaría de la JERS,
en nombre de la Junta General de la JERS
Francesco MAZZAFERRO

ANEXO

CRITERIOS DE APLICACIÓN ESPECÍFICOS DE LAS RECOMENDACIONES

Recomendación A – Establecimiento de un marco paneuropeo de coordinación de ciberincidentes sistémicos (EU-SCICF)

Se especifican los siguientes criterios de cumplimiento para la recomendación A, apartado 1.

1. A la hora de preparar una respuesta coordinada eficaz a nivel de la Unión, que debería implicar el establecimiento gradual del EU-SCICF mediante el ejercicio de las competencias previstas en el futuro Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero (en lo sucesivo, «DORA»), las Autoridades Europeas de Supervisión (AES), actuando a través del Comité Mixto, y junto con el Banco Central Europeo (BCE), la Junta Europea de Riesgo Sistémico (JERS) y las autoridades nacionales pertinentes, y en consulta con la Agencia de Seguridad de las Redes y de la Información de la Unión Europea y la Comisión, cuando se considere necesario, deben considerar la posibilidad de incluir en la preparación prevista para el EU-SCICF al menos los aspectos siguientes:

   a. análisis de las necesidades de recursos para un establecimiento eficaz del EU-SCICF;

   b. preparación de ejercicios de gestión de crisis y contingencias que impliquen escenarios de ciberataque con vistas a desarrollar canales de comunicación;

   c. elaboración de un vocabulario común;

   d. creación de una clasificación coherente de ciberincidentes;

   e. establecimiento de canales de intercambio de información seguros y fiables, incluidos sistemas de respaldo;

   f. establecimiento de puntos de contacto;

   g. abordar la confidencialidad en el intercambio de información;

   h. iniciativas de colaboración e intercambio de información con la ciberinteligencia del sector financiero;

   i. desarrollo de procesos eficaces de activación y escalada a través del conocimiento de la situación;

   j. aclaración de las responsabilidades de los participantes en el marco;

   k. creación de interfaces para la coordinación intersectorial y, en su caso, de terceros países;

   l. garantizar una comunicación coherente de las autoridades pertinentes con el público para preservar la confianza;

   m. establecimiento de líneas de comunicación predefinidas para la comunicación oportuna;

   n. realización de ejercicios de pruebas marco adecuados, incluidas pruebas interjurisdiccionales y coordinación con terceros países, y evaluaciones de las que se extraigan las enseñanzas obtenidas y que contribuyan a la evolución del marco;

   o. garantizar una comunicación eficaz y contramedidas contra la desinformación.

Recomendación B – Establecimiento de puntos de contacto del EU-SCICF

Se especifican los siguientes criterios de cumplimiento para la recomendación B.

1. Las autoridades nacionales pertinentes de las AES, del BCE y de cada Estado miembro deben acordar un enfoque común para compartir y mantener actualizada la lista de puntos de contacto designados del EU-SCICF.

2. La designación del punto de contacto debe evaluarse atendiendo al punto de contacto único designado en virtud de la Directiva (UE) 2016/1148 que los Estados miembros hayan establecido respecto a la seguridad de las redes y sistemas de información para garantizar la cooperación transfronteriza con otros Estados miembros y con el Grupo de Cooperación sobre Redes y Sistemas de Información.

Recomendación C – Medidas adecuadas a escala de la Unión

Se especifican los siguientes criterios de cumplimiento para la recomendación C.

La Comisión debe considerar si son necesarias medidas, incluidos cambios en la legislación pertinente de la Unión, como resultado del análisis realizado de conformidad con la recomendación A, a fin de garantizar que las AES, a través del Comité Mixto y junto con el BCE, la JERS y las autoridades nacionales pertinentes, puedan establecer el EU-SCICF de conformidad con la recomendación A, apartado 1, y garantizar que las AES, el BCE, la JERS y las autoridades nacionales pertinentes, así como otras autoridades, puedan emprender acciones de coordinación e intercambio de información que sea lo suficientemente detallada y coherente como para apoyar un EU-SCICF eficaz.