I

(Resoluções, recomendações e pareceres)

RECOMENDAÇÕES

COMITÉ EUROPEU DO RISCO SISTÉMICO

RECOMENDAÇÃO DO COMITÉ EUROPEU DO RISCO SISTÉMICO

de 2 de dezembro de 2021

sobre um quadro pan-europeu de coordenação para as autoridades competentes relativo a ciberincidentes sistémicos

(CERS/2021/17)

(2022/C 134/01)

O CONSELHO GERAL DO COMITÉ EUROPEU DO RISCO SISTÉMICO,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Acordo sobre o Espaço Económico Europeu ([1]), nomeadamente o anexo IX,

Tendo em conta o Regulamento (UE) n.º 1092/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, relativo à supervisão macroprudencial do sistema financeiro na União Europeia e que cria o Comité Europeu do Risco Sistémico ([2]), nomeadamente o artigo 3.º, n.º 2, alíneas b) e d), e os artigos 16.º a 18.º,

Tendo em conta a Decisão CERS/2011/1 do Comité Europeu do Risco Sistémico, de 20 de janeiro de 2011, que adota o Regulamento Interno do Comité Europeu do Risco Sistémico ([3]), nomeadamente os artigos18.º a 20.º,

Considerando o seguinte:

(1) Conforme referido no considerando 4 da Recomendação CERS/2013/1 do Comité Europeu do Risco Sistémico ([4]), a política macroprudencial tem por objetivo principal contribuir para a preservação da estabilidade do sistema financeiro no seu conjunto, nomeadamente através do reforço da resiliência do setor financeiro, e reduzir a acumulação de riscos sistémicos, assegurando assim uma contribuição sustentável do setor financeiro para o crescimento económico. O Comité Europeu do Risco Sistémico (CERS) é responsável pela supervisão macroprudencial do sistema financeiro na União. No cumprimento do seu mandato, o CERS deve contribuir para a prevenção e atenuação dos riscos sistémicos para a estabilidade financeira, incluindo os relacionados com ciberincidentes, e propor formas de atenuar esses riscos.

(2) Os ciberincidentes graves podem representar um risco sistémico para o sistema financeiro, dado o seu potencial de perturbação das operações e dos serviços financeiros essenciais. A amplificação de um choque inicial pode ocorrer quer através de um contágio operacional ou financeiro, quer através de uma erosão da confiança no sistema financeiro. Se o sistema financeiro não estiver em condições de absorver estes choques, a estabilidade financeira estará em risco e esta situação poderá dar lugar a numa cibercrise sistémica ([5]).

([1]) JO L 1 de 3.1.1994, p. 3.
([2]) JO L 331 de 15.12.2010, p. 1.
([3]) JO C 58 de 24.02.2011, p. 4.
([4]) Recomendação CERS/2013/1 do Comité Europeu do Risco Sistémico, de 4 de abril de 2013, relativa a objetivos intermédios e instrumentos de política macroprudencial (JO C 170 de 15 de junho de 2013, p. 1).
([5]) Ver *Systemic cyber risk*, CERS, fevereiro de 2020, disponível (em inglês) no sítio *web* do CERS em www.esrb.europa.eu

(3) A evolução constante do cenário de ciberameaças e o recente aumento dos ciberincidentes graves são indicadores de um risco acrescido para a estabilidade financeira da União. A pandemia de COVID-19 colocou em evidência a importância do papel desempenhado pela tecnologia ao permitir o funcionamento do sistema financeiro. As autoridades e instituições competentes viram-se na contingência de adaptar as suas infraestruturas técnicas e os seus quadros de gestão de riscos a um súbito crescimento do trabalho à distância, o que aumentou a exposição global do sistema financeiro às ciberameaças e permitiu que os infratores concebessem novos *modi operandi* e adaptassem os existentes para tirar partido da situação ([6]). Neste contexto, o número de ciberincidentes comunicados à Supervisão Bancária do BCE em 2020 aumentou 54 % em comparação com 2019 ([7]).

(4) Um ciberincidente de grande envergadura, velocidade e taxa de propagação exige uma resposta eficaz das autoridades competentes a fim de atenuar os potenciais efeitos negativos para a estabilidade financeira. Uma coordenação e comunicação rápidas entre as autoridades competentes ao nível da União pode contribuir para uma avaliação precoce do impacto de um ciberincidente grave sobre a estabilidade financeira, manter a confiança no sistema financeiro e limitar o contágio a outras instituições financeiras, contribuindo assim para evitar que um ciberincidente grave se torne um risco para a estabilidade financeira.

(5) O choque subjacente nasce de forma inédita relativamente às crises financeiras e de liquidez tradicionais com que as autoridades competentes se veem habitualmente confrontadas. Para além dos aspetos financeiros, a avaliação global dos riscos deve incluir a escala e o impacto das perturbações operacionais, uma vez que estas podem influenciar a escolha dos instrumentos macroprudenciais. Do mesmo modo, a estabilidade financeira pode também influenciar a escolha das medidas de atenuação operacionais por parte dos especialistas em cibersegurança. Tal exige uma coordenação estreita e rápida e uma comunicação aberta para, nomeadamente, desenvolver o conhecimento da situação.

(6) O risco de uma falha de coordenação por parte das autoridades existe e deve ser enfrentado. As autoridades competentes da União deverão coordenar-se entre si e com outras autoridades, como a Agência da União Europeia para a Cibersegurança (ENISA), com as quais possam não interagir habitualmente. Dado que um número significativo de instituições financeiras da União opera à escala mundial, um ciberincidente grave não se limitará, provavelmente, à União ou poderá ser desencadeado fora da União e poderá exigir uma resposta coordenada a nível global.

(7) As autoridades competentes devem estar preparadas para estas interações. Caso contrário, correriam o risco de tomar medidas incoerentes que contradigam ou comprometam as respostas de outras autoridades. Uma tal falha de coordenação poderia amplificar o choque para o sistema financeiro e provocar uma erosão da confiança no funcionamento do sistema financeiro, o que, no pior dos cenários, representaria um risco para a estabilidade financeira ([8]). Importa, por conseguinte, tomadas as medidas necessárias para fazer face ao risco para a estabilidade financeira decorrente de uma falta de coordenação em caso de ciberincidente grave.

(8) O relatório do CERS (2021) intitulado *Mitigating systemic Cyber risk* ([9]) (Atenuar o ciber-risco sitémico) evidencia a necessidade de estabelecer um quadro pan-europeu de coordenação em caso de ciberincidentes sistémicos (EU-SCICF) para as autoridades competentes da União. O EU-SCICF teria por objetivo aumentar o nível de preparação das autoridades competentes para facilitar uma resposta coordenada a um ciberincidente potencialmente grave. O relatório do CERS (2021) intitulado *Mitigating systematic Cyber risk* apresenta a avaliação pelo CERS das características do quadro que seriam necessárias, numa primeira leitura, para fazer face ao risco de uma falha de coordenação.

(9) A presente recomendação tem por objetivo primordial tirar partido de uma das funções previstas para as Autoridades Europeias de Supervisão (AES) no âmbito da proposta de regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro ([10]) (a seguir «Regulamento DORA»), para permitir a preparação gradual de uma resposta coordenada a nível da União em caso de incidente transfronteiriço grave relacionado com as tecnologias da informação e da comunicação (TIC) ou de ameaça conexa com impacto sistémico no setor financeiro da União no seu conjunto. Este processo conduzirá à criação do EU-SCICF para as autoridades competentes.

([6]) Ver *Internet Organised Crime Threat Assessment*, Europol, 2020, disponível (em inglês) no sítio *web* da Europol em www.europol.europa.eu
([7]) Ver *IT and cyber risk: a constant challenge*, BCE, 2021, disponível (em inglês) no sítio *web* da Supervisão Bancária do BCE em www.bankingsupervision.europa.eu
([8]) Ver *Systemic cyber risk*, CERS, fevereiro de 2020, disponível (em inglês) no sítio *web* do CERS em www.esrb.europa.eu
([9]) Ver *Mitigating systemic cyber risk*, C ERS, 2021, (em preparação).
([10]) COM(2020) 595 final.

(10) O EU-SCICF não deveria procurar substituir os quadros existentes, mas antes preencher eventuais lacunas de coordenação e comunicação entre as próprias autoridades competentes e com outras autoridades da União e outros intervenientes fundamentais a nível internacional. A este respeito, deve ser levado em conta o posicionamento do EU-SCICF no panorama dos quadros existentes em matéria de crises financeiras e ciberincidentes na União. No que diz respeito à coordenação entre as próprias autoridades competentes, devem ser levados em conta, entre outros, as funções e atividades do Grupo de Cooperação para as Redes e os Sistemas de Informação (RSI) para as entidades financeiras ao abrigo da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ([11]), e os mecanismos de coordenação previstos através da criação da unidade conjunta de cibersegurança, juntamente com a participação da ENISA.

(11) Em especial, a proposta de proceder à elaboração do EU-SCICF visa apoiar as funções potenciais das AES previstas na proposta de Regulamento DORA. O Regulamento DORA propõe que «As AES, através do Comité Conjunto e em colaboração com as autoridades competentes, o Banco Central Europeu (BCE) e o CERS, podem estabelecer mecanismos que permitam a partilha de práticas eficazes entre os setores financeiros, para melhorar o conhecimento da situação e identificar as vulnerabilidades e os riscos cibernéticos comuns entre setores» e «podem também desenvolver exercícios de gestão de crises e contingência que envolvam cenários de ciberataques com vista a desenvolver canais de comunicação e, gradualmente, permitir uma resposta coordenada eficaz a nível da UE caso ocorra um incidente grave transfronteiriço relacionado com as TIC ou caso uma ameaça conexa possa ter um impacto sistémico no setor financeiro da União como um todo» ([12]). Não existe ainda um quadro pan-europeu como o EU-SCICF, que deve ser estabelecido e desenvolvido no contexto do Regulamento DORA.

(12) Tendo em conta as implicações do risco cibernético para a estabilidade financeira da União, os trabalhos preparatórios para a criação gradual do EU-SCICF deverão, na medida do possível, começar ainda antes de ser plenamente aplicável o quadro jurídico e político necessário para o seu estabelecimento. Este quadro jurídico e político ficaria inteiramente completado e finalizado logo que as pertinentes disposições do Regulamento DORA e dos respetivos atos delegados se tornassem aplicáveis.

(13) Uma comunicação eficaz contribui para o conhecimento da situação pelas autoridades competentes, constituindo, por esse motivo, um pré-requisito indispensável da coordenação a nível da União aquando da ocorrência de ciberincidentes graves. A este respeito, importaria definir a infraestrutura de comunicação necessária para coordenar a resposta a um ciberincidente grave. Tal implicaria especificar o tipo de informações que devem ser partilhadas, os canais regulares a utilizar para partilhar essas informações e os pontos de contacto com os quais as informações devem ser partilhadas. A partilha de informações deve respeitar os requisitos legais em vigor. Além disso, as autoridades competentes podem ter que definir um plano de ação claro e os protocolos a seguir para assegurar uma boa coordenação entre as autoridades envolvidas no planeamento de uma resposta coordenada a um ciberincidente grave.

(14) Uma cibercrise sistémica exigirá o lançamento de uma cooperação plena a nível nacional e da União. Pode, por conseguinte, prever-se a designação de pontos de contacto para as AES, para o BCE e para cada Estado-Membro, escolhidos, neste caso, de entre as respetivas autoridades nacionais competentes, que devem ser comunicados às AES, a fim de estabelecer os principais interlocutores do mecanismo de coordenação do EU-SCICF que devem ser informados em caso de ciberincidente grave. A necessidade de designar pontos de contacto deve ser avaliada durante a elaboração do EU-SCICF, tendo em conta o ponto de contacto único designado pelos Estados-Membros nos termos da Diretiva (UE) 2016/1148, para os fins da segurança das redes e dos sistemas de informação, tendo em vista assegurar a cooperação transfronteiriça com outros Estados-Membros e com o Grupo de Cooperação RSI ([13]).

(15) A realização de exercícios de gestão de crises e de contingência poderá facilitar a aplicação do EU-SCICF e permitir que as autoridades avaliem o seu grau de prontidão e preparação para uma cibercrise sistémica ao nível da União. As autoridades poderiam retirar ensinamentos destes exercícios, o que permitiria uma melhoria e evolução contínuas do EU-SCICF.

([11]) Diretiva (UE) n.º 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação (JO L 194 de 19.7.2016, p. 1).
([12]) Ver projeto de artigo 43.º da proposta de Regulamento DORA.
([13]) Ver Comissão Europeia, Grupo de Cooperação SRI, disponível no sítio *web* da Comissão Europeia em www.ec.europa.eu

(16) Para a elaboração do EU-SCICF, é essencial que as AES realizem conjuntamente os trabalhos preparatórios pertinentes a fim de ponderar os potenciais elementos-chave do quadro e os recursos necessários ao seu desenvolvimento. Numa fase seguinte, as AES poderão começar a proceder a uma análise preliminar de eventuais impedimentos suscetíveis de prejudicar a capacidade das AES e das autoridades competentes para estabelecerem o EU-SCICF e partilharem informações relevantes através dos canais de comunicação em caso de ciberincidente grave. Uma tal análise constituiria um passo importante para orientar quaisquer medidas posteriores, sejam de natureza legislativa, ou outras iniciativas de apoio que a Comissão Europeia possa tomar na fase de aplicação posterior à adoção do Regulamento DORA,

ADOTOU A PRESENTE RECOMENDAÇÃO:

SECÇÃO 1

RECOMENDAÇÕES

Recomendação A — Criação de um quadro pan-europeu de coordenação para ciberincidentes sistémicos (EU-SCICF)

1. Recomenda-se que, tal como previsto na proposta da Comissão de regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro (a seguir «Regulamento DORA»), as Autoridades Europeias de Supervisão (AES), conjuntamente, através do Comité Conjunto, e juntamente com o Banco Central Europeu (BCE), o Comité Europeu do Risco Sistémico (CERS) e as autoridades nacionais competentes, deem início à preparação para o desenvolvimento gradual de uma resposta coordenada ao nível da União em caso de ciberincidente transfronteiriço grave ou ameaça conexa que possa ter um impacto sistémico no setor financeiro da União. Os trabalhos preparatórios para uma resposta coordenada ao nível da União devem implicar o desenvolvimento gradual do EU-SCICF para as AES, o BCE, o CERS e as autoridades nacionais competentes. Os trabalhos preparatórios devem incluir igualmente uma avaliação dos recursos necessários para o desenvolvimento eficaz do EU-SCICF.

2. Recomenda-se que as AES, levando em conta a recomendação A, n.º 1, e em consulta com o BCE e o CERS, realizem um levantamento e uma análise subsequente dos atuais impedimentos e dos obstáculos jurídicos e outros obstáculos operacionais ao desenvolvimento eficaz do EU-SCICF.

Recomendação B — Estabelecimento de pontos de contacto do EU-SCICF

Recomenda-se que as AES, o BCE e cada Estado-Membro, neste caso a escolher de entre as suas autoridades nacionais competentes, designem um ponto de contacto principal, que deverá ser comunicado às AES. Esta lista de contactos facilitará a elaboração do quadro; após a entrada em vigor do EU-SCICF, os pontos de contacto e o CERS devem ser informados da ocorrência de ciberincidentes graves. Deve igualmente prever-se a coordenação entre o EU-SCICF e o ponto de contacto único, designado pelos Estados-Membros ao abrigo da Diretiva (UE) 2016/1148 para efeitos de segurança das redes e dos sistemas de informação, com vista a assegurar a cooperação transfronteiriça com outros Estados-Membros e com o Grupo de Cooperação para as Redes e os Sistemas de Informação.

Recomendação C — Medidas adequadas ao nível da União

Recomenda-se que, com base nos resultados das análises efetuadas em conformidade com a recomendação A, a Comissão pondere as medidas adequadas necessárias para assegurar uma coordenação eficaz das respostas a ciberincidentes sistémicos.

SECÇÃO 2

APLICAÇÃO

1. **Definições**

Para efeitos da presente recomendação, entende-se por:

a) «Ciber», relacionado com, no âmbito de, ou através da infraestrutura de informação interligada de interações entre pessoas, processos, dados e sistemas de informação ([14]);

([14]) Ver *Cyber Lexicon*, CEF, 12 de novembro de 2018, disponível (em inglês) no sítio *web* do CEF em www.fsb.org.

b) «Ciberincidente grave», um incidente relacionado com as TIC suscetível de produzir um impacto adverso potencialmente elevado nas redes e nos sistemas de informação que apoiam as funções críticas das entidades financeiras ([15]);

c) «Cibercrise sistémica», um ciberincidente grave que causa um nível de perturbação no sistema financeiro da União suscetível de provocar consequências negativas graves para o bom funcionamento do mercado interno e para o funcionamento da economia real. Uma tal crise pode resultar de um ciberincidente grave que provoque choques em vários canais, nomeadamente operacionais, financeiros e de confiança;

d) «Autoridades europeias de supervisão» ou «AES», a Autoridade Europeia de Supervisão (Autoridade Bancária Europeia), instituída nos termos do Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho ([16]), a Autoridade Europeia de Supervisão (Autoridade Europeia dos Seguros e Pensões Complementares de Reforma), instituída nos termos do Regulamento (UE) n.º 1094/2010 do Parlamento Europeu e do Conselho ([17]) e a Autoridade Europeia de Supervisão (Autoridade Europeia dos Valores Mobiliários e dos Mercados), instituída nos termos do Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho ([18]);

e) «Comité Conjunto», o Comité Conjunto das Autoridades Europeias de Supervisão instituído nos termos do artigo 54.º do Regulamento (UE) n.º 1093/2010, do Regulamento (UE) n.º 1094/2010 e do Regulamento (UE) n.º 1095/2010;

f) «Autoridade nacional competente»,

1. uma autoridade competente ou de supervisão de um Estado-Membro, tal como especificado nos atos da União referidos no artigo 1.º, n.º 2, do Regulamento (UE) n.º 1093/2010, do Regulamento (UE) n.º 1094/2010 e do Regulamento (UE) n.º 1095/2010, e qualquer outra autoridade nacional competente especificada em atos da União que confiram atribuições às ESA;

2. uma autoridade competente de um Estado-Membro designada em conformidade com:

i) o artigo 4.º da Diretiva 2013/36/UE do Parlamento Europeu e do Conselho ([19]), sem prejuízo das atribuições específicas conferidas ao BCE pelo Regulamento (UE) n.º 1024/2013 do Conselho ([20]);

ii) o artigo 71.º da Diretiva (UE) n.º 2015/2366 do Parlamento Europeu de Conselho ([21]);

iii) o artigo 37.º da Diretiva 2009/110/CE do Parlamento Europeu e do Conselho ([22]);

iv) o artigo 4.º da Diretiva (UE) n.º 2019/2034 do Parlamento Europeu de Conselho ([23]);

([15]) Ver o artigo 3.º, ponto 7), da proposta de Regulamento DORA.

([16]) Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Bancária Europeia), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/78/CE da Comissão (JO L 331 de 15.12.2010, p. 12).

([17]) Regulamento (UE) n.º 1094/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Seguros e Pensões Complementares de Reforma), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/79/CE da Comissão (JO L 331 de 15.12.2010, p. 48).

([18]) Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Valores Mobiliários e dos Mercados), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/77/CE da Comissão (JO L 331 de 15.12.2010, p. 84).

([19]) Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).

([20]) Regulamento (UE) n.º 1024/2013 do Conselho, de 15 de outubro de 2013, que confere ao Banco Central Europeu atribuições específicas no que diz respeito às políticas relativas à supervisão prudencial das instituições de crédito (JO L 287 de 29.10.2013, p. 63).

([21]) Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE (JO L 337 de 23.12.2015, p. 35).

([22]) Diretiva 2009/110/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, relativa ao acesso à atividade das instituições de moeda eletrónica, ao seu exercício e à sua supervisão prudencial, que altera as Diretivas 2005/60/CE e 2006/48/CE e revoga a Diretiva 2000/46/CE (JO L 267 de 10.10.2009, p. 7).

([23]) Diretiva (UE) 2019/2034 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, relativa à supervisão prudencial das empresas de investimento e que altera as Diretivas 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE e 2014/65/UE (JO L 314 de 5.12.2019, p. 64).

v) o artigo 3.º, n.º 1, alínea ee), primeiro travessão, da proposta de regulamento do Parlamento Europeu e do Conselho relativo aos mercados de criptoativos e que altera a Diretiva (UE) 2019/1937 ([24]);

vi) o artigo 11.º do Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho ([25]);

vii) o artigo 22.º do Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho ([26]);

viii) o artigo 67.º da Diretiva 2014/65/CE do Parlamento Europeu e do Conselho ([27]);

ix) o artigo 22.º do Regulamento (UE) n.º 648/2012;"

x) o artigo 44.º da Diretiva 2011/61/UE do Parlamento Europeu e do Conselho ([28]);

xi) o artigo 97.º da Diretiva 2009/65/CE do Parlamento Europeu e do Conselho ([29]);

xii) o artigo 30.º da Diretiva 2009/138/CE do Parlamento Europeu e do Conselho ([30]);

xiii) o artigo 12.º da Diretiva (UE) n.º 2016/97 do Parlamento Europeu de Conselho ([31]);

xiv) o artigo 47.º da Diretiva (UE) n.º 2016/2341 do Parlamento Europeu de Conselho ([32]);

xv) o artigo 22.º do Regulamento (UE) n.º 1060/2009 do Parlamento Europeu e do Conselho ([33]);

xvi) o artigo 3.º, n.º 2, e o artigo 32.º da Diretiva 2006/43/CE do Parlamento Europeu e do Conselho ([34]);

xvii) o artigo 40.º do Regulamento (UE) n.º 2016/1011 do Parlamento Europeu e do Conselho ([35]);

xviii) o artigo 29.º do Regulamento (UE) n.º 2020/1503 do Parlamento Europeu e do Conselho ([36]);

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

([25]) Regulamento (EU) n.º do Parlamento Europeu e do Conselho, de 23 de julho de 2014 Regulamento (UE) n.º 909/2014, relativo à melhoria da liquidação de valores mobiliários na União Europeia e às Centrais de Valores Mobiliários (CSDs) e que altera as Diretivas 98/26/CE e 2014/65/UE e o Regulamento (UE) n.º 236/2012 (JO L 257 de 28.8.2014, p. 1).

([26]) Regulamento (UE) n.º 648/2012, do Parlamento Europeu e do Conselho, de 4 de julho de 2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações (JO L 201 de 27.7.2012, p. 1).

([27]) Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa aos mercados de instrumentos financeiros e que altera a Diretiva 2002/92/CE e a Diretiva 2011/61/UE (JO L 173 de 12.6.2014, p. 349).

([28]) Diretiva 2011/61/UE do Parlamento Europeu e do Conselho, de 8 de junho de 2011, relativa aos gestores de fundos de investimento alternativos e que altera as Diretivas 2003/41/CE e 2009/65/CE e os Regulamentos (CE) n.º 1060/2009 e (UE) n° 1095/2010 (JO L 174 de 1.7.2011, p. 1.

([29]) Diretiva 2009/65/CE do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que coordena as disposições legislativas, regulamentares e administrativas respeitantes a alguns organismos de investimento coletivo em valores mobiliários (OICVM) (JO L 302 de 17.11.2009, p. 32).

([30]) Diretiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, relativa ao acesso à atividade de seguros e resseguros e ao seu exercício (Solvência II) (JO L 335 de 17.12.2009, p.1).

([31]) Diretiva (UE) 2016/97 do Parlamento Europeu e do Conselho, de 20 de janeiro de 2016, sobre a distribuição de seguros (JO L 26 de 2.2.2016, p. 19).

([32]) Diretiva (UE) 2016/2341 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2016, relativa às atividades e à supervisão das instituições de realização de planos de pensões profissionais (IRPPP) (JO L 354 de 23.12.2016, p. 37).

([33]) Regulamento (CE) n.º 1060/2009 do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, relativo às agências de notação de risco (JO L 302 de 17.11.2009, p. 1).

([34]) Diretiva 2006/43/CE do Parlamento Europeu e do Conselho, de 17 de maio de 2006 , relativa à revisão legal das contas anuais e consolidadas, que altera as Diretivas 78/660/CEE e 83/349/CEE do Conselho e que revoga a Diretiva 84/253/CEE do Conselho (JO L 157 de 9.6.2006, p. 87).

([35]) Regulamento (UE) 2016/1011 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativo aos índices utilizados como índices de referência no quadro de instrumentos e contratos financeiros ou para aferir o desempenho de fundos de investimento e que altera as Diretivas 2008/48/CE e 2014/17/UE e o Regulamento (UE) n.º 596/2014 (JO L 171 de 29.6.2016, p. 1).

([36]) Regulamento (UE) 2020/1503 do Parlamento Europeu e do Conselho, de 7 de outubro de 2020, relativo aos prestadores europeus de serviços de financiamento colaborativo às empresas e que altera o Regulamento (UE) 2017/1129 e a Diretiva (UE) 2019/1937 (JO L 347 de 20.10.2020, p. 1).

3. uma autoridade responsável pela adoção e/ou ativação de medidas de política macroprudencial ou pelo desempenho de outras funções em matéria de estabilidade financeira, tais como análises de apoio conexas, incluindo, ainda que não exclusivamente:

   i) as autoridades designadas nos termos do título VII, capítulo 4, da Diretiva 2013/36/UE ou do artigo 458.º, n.º 1, do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho ([37]);

   ii) uma autoridade macroprudencial com os objetivos, mecanismos, funções, competências, instrumentos, obrigações de prestação de contas e outras características estabelecidas na Recomendação CESR/2011/3 do Comité Europeu do Risco Sistémico ([38]);

g) «Autoridade competente»,

   1. uma AES;

   2. o BCE, no que diz respeito às atribuições que lhe são conferidas nos termos dos artigos 4.º, n.ºs 1 e 2, e do artigo 5.º, n.º 2, do Regulamento (UE) n.º 1024/2013;

   3. uma autoridade nacional competente.

2. **Critérios de aplicação**

A aplicação da presente recomendação rege-se pelos critérios seguintes:

a) Deve ter-se devidamente em conta o princípio da necessidade de saber e o princípio da proporcionalidade, tomando em consideração o objetivo e o conteúdo de cada recomendação;

b) Devem ser cumpridos os critérios específicos de conformidade estabelecidos no anexo em relação a cada recomendação.

3. **Calendário para o seguimento**

Nos termos do artigo 17.º, n.º 1, do Regulamento (UE) n.º 1092/2010, os destinatários devem comunicar ao Parlamento Europeu, ao Conselho, à Comissão e ao ESRB as medidas tomadas em resposta à presente recomendação ou fundamentar a eventual não atuação. Os destinatários devem efetuar a referida comunicação em conformidade com os seguintes prazos.

1. Recomendação A

   a) Solicita-se às AES que, até 30 de junho de 2023, mas não antes de seis meses após a entrada em vigor do Regulamento DORA, apresentem ao Parlamento Europeu, ao Conselho, à Comissão e ao CERS um relatório intercalar sobre a aplicação da recomendação A, n.º 1.

   b) Solicita-se às AES que, até 30 de junho de 2024, mas não antes de 18 meses após a entrada em vigor do Regulamento DORA, apresentem ao Parlamento Europeu, ao Conselho, à Comissão e ao CERS um relatório final sobre a aplicação da recomendação A, n.º 1.

   c) Solicita-se às AES que, até 30 de junho de 2025, mas não antes de 30 meses após a entrada em vigor do Regulamento DORA, apresentem ao Parlamento Europeu, ao Conselho, à Comissão e ao CERS um relatório sobre a aplicação da recomendação A, n.º 2.

2. Recomendação B

   Solicita-se às AES, ao BCE e aos Estados-Membros que, até 30 de junho de 2023, mas não antes de 6 meses após a entrada em vigor do Regulamento DORA, apresentem ao Parlamento Europeu, ao Conselho, à Comissão e ao CERS um relatório sobre a aplicação da recomendação B.

3. Recomendação C

   a) Solicita-se à Comissão que, até 31 de dezembro de 2023, mas não antes de 12 meses após a entrada em vigor do Regulamento DORA, apresente ao Parlamento Europeu, ao Conselho e ao CERS um relatório sobre a aplicação da Recomendação C tendo em conta o relatório intercalar das AES previsto na recomendação A, n.º 1.

([37]) Regulamento (UE) N.o 575/2013 do Parlamento Europeu e do Conselho 26 de junho de 2013 relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.o 648/2012 (JO L 176 de 27.6.2013, p. 1).

([38]) Recomendação CERS/2011/3 do Comité Europeu do Risco Sistémico, de 22 de dezembro de 2011, relativa ao mandato macroprudencial das autoridades nacionais (JO C 41 de 14.2.2012, p. 1).

b) Solicita-se à Comissão que, até 31 de dezembro de 2025, mas não antes de 36 meses após a entrada em vigor do Regulamento DORA, apresente ao Parlamento Europeu, ao Conselho e ao CERS um relatório sobre a aplicação da Recomendação C tendo em conta o relatório intercalar das AES previsto na recomendação A, n.º 1.

4. **Acompanhamento e avaliação**

1. Compete ao Secretariado do CERS:

a) Prestar apoio aos destinatários, assegurando a coordenação do reporte e o fornecimento dos formulários pertinentes, e indicando, sempre que necessário, o procedimento e o calendário de seguimento;

b) Verificar o seguimento dado pelos destinatários, prestando-lhes assistência se o solicitarem, e apresentando relatórios sobre o seguimento ao Conselho Geral. As avaliações serão realizadas da seguinte forma:

i) no prazo de 12 meses após a entrada em vigor do Regulamento DORA, no que diz respeito à aplicação das recomendações A e B;

ii) no prazo de 18 meses após a entrada em vigor do Regulamento DORA, no que diz respeito à aplicação da recomendação C;

iii) no prazo de 24 meses após a entrada em vigor do Regulamento DORA, no que diz respeito à aplicação da recomendação A;

iv) no prazo de 36 meses após a entrada em vigor do Regulamento DORA, no que diz respeito à aplicação da recomendação A;

v) no prazo de 42 meses após a entrada em vigor do Regulamento DORA, no que diz respeito à aplicação da recomendação C.

2. O Conselho Geral avalia as medidas e as justificações apresentadas pelos destinatários e pode, se for caso disso, decidir que a presente recomendação não foi cumprida e que o destinatário não apresentou justificação adequada para a sua não atuação.

Feito em Frankfurt am Main, em 2 de dezembro de 2021.

O Chefe do Secretariado do CERS,
Em nome do Conselho Geral do CERS,
Francesco MAZZAFERRO

ANEXO

CRITÉRIOS DE OBSERVÂNCIA ESPECÍFICOS DAS RECOMENDAÇÕES

Recomendação A — Criação de um quadro pan-europeu de coordenação para ciberincidentes sistémicos (EU-SCICF)

Relativamente à recomendação A, n.º 1, são especificados os seguintes critérios de observância.

1. Ao preparar uma resposta coordenada e eficaz ao nível da União, que deverá implicar o desenvolvimento gradual do EU-SCICF, mediante o exercício das competências previstas no futuro Regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro (a seguir «Regulamento DORA»), as Autoridades Europeias de Supervisão (AES), agindo através do Comité Conjunto, e juntamente com o Banco Central Europeu (BCE), o Comité Europeu do Risco Sistémico (CERS) e as autoridades nacionais relevantes, e em consulta com a Agência da União Europeia para a Cibersegurança e com a Comissão, sempre que tal seja considerado necessário, devem ponderar a possibilidade de incluir, na preparação prevista para o EU-SCICF, pelo menos os seguintes aspetos:

   a) análise dos recursos necessários para o desenvolvimento eficaz do EU-SCICF;

   b) preparação de exercícios de gestão de crises e de contingência que envolvam cenários de ciberataque, com vista ao desenvolvimento de canais de comunicação;

   c) elaboração de um vocabulário comum;

   d) elaboração de uma classificação coerente dos ciberincidentes;

   e) estabelecimento de canais seguros e fiáveis de partilha de informação, incluindo sistemas de salvaguarda (*back-up*);

   f) estabelecimento de pontos de contacto;

   g) abordagem da questão da confidencialidade na partilha de informações;

   h) colaboração e iniciativas de partilha de informação com serviços de ciberinformação do setor financeiro;

   i) desenvolvimento de processos eficazes de ativação e escalonamento da informação eficazes através do conhecimento da situação;

   j) clarificação das responsabilidades dos participantes no quadro;

   k) desenvolvimento de interfaces para a coordenação intersetorial e, se for caso disso, com países terceiros;

   l) garantia de uma comunicação coerente das autoridades competentes com o público, a fim de preservar a confiança;

   m) estabelecimento de linhas de comunicação predefinidas para uma comunicação atempada;

   n) realização de exercícios adequados de teste do quadro, incluindo testes transjurisdicionais e a coordenação com países terceiros, e avaliações que permitam retirar ensinamentos e fazer evoluir o quadro;

   o) assegurar uma comunicação eficaz e medidas de combate à desinformação.

Recomendação B — Estabelecimento dos pontos de contacto do EU-SCICF

Relativamente à Recomendação B, são especificados os seguintes critérios de observância.

1. As AES, o BCE e cada um dos Estados-Membros, neste caso as respetivas autoridades nacionais competentes, devem acordar numa abordagem comum para partilhar e manter atualizada a lista dos pontos de contacto designados do EU-SCICF.

2. A designação do ponto de contacto deve ser avaliada tendo em conta o ponto de contacto único designado pelos Estados-Membros ao abrigo da Diretiva (UE) 2016/1148 para os fins da segurança das redes e dos sistemas de informação, tendo em vista assegurar a cooperação transfronteiriça com outros Estados-Membros e com o Grupo de Cooperação para as Redes e os Sistemas de Informação.

Recomendação C — Alterações ao quadro jurídico da União

Relativamente à Recomendação C, são especificados os seguintes critérios de observância.

A Comissão deve ponderar se, em resultado da análise efetuada em conformidade com a recomendação A, são necessárias medidas, incluindo alterações à legislação pertinente da União, tendentes a assegurar que as AES, através do Comité Conjunto e em conjunto com o BCE, o CERS e as autoridades nacionais competentes, possam desenvolver o EU-SCICF de acordo com a recomendação A, n.º 1, e assegurar que as AES, o BCE, o ESRB e as autoridades nacionais relevantes, bem como outras autoridades, possam participar em ações de coordenação e intercâmbio de informações suficientemente pormenorizadas e coerentes para apoiar um UE-SCICF eficaz.