DIRETIVA (UE) 2022/2556 DO PARLAMENTO EUROPEU E DO CONSELHO

de 14 de dezembro de 2022

que altera as Diretivas 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 no que diz respeito à resiliência operacional digital para o setor financeiro

(Texto relevante para efeitos do EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 53.º, n.º 1, e o artigo 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Banco Central Europeu ([1]),

Tendo em conta o parecer do Comité Económico e Social Europeu ([2]),

Deliberando de acordo com o processo legislativo ordinário ([3]),

Considerando o seguinte:

(1) A União precisa de abordar, de forma adequada e exaustiva, os riscos digitais para todas as entidades financeiras decorrentes de uma maior utilização das tecnologias da informação e comunicação (TIC) na prestação e utilização de serviços financeiros, contribuindo assim para a realização do potencial do financiamento digital, em matéria de promoção da inovação e da concorrência num ambiente digital seguro.

(2) As entidades financeiras dependem fortemente da utilização das tecnologias digitais nas suas atividades diárias. É, portanto, extremamente importante assegurar a resiliência operacional das suas operações digitais contra o risco associado às TIC. Esta necessidade tornou-se ainda mais premente devido ao crescimento das tecnologias revolucionárias no mercado, nomeadamente tecnologias que permitem que as representações digitais de valores ou direitos sejam transferidas e armazenadas eletronicamente recorrendo à tecnologia de registo distribuído ou a tecnologias semelhantes (criptoativos), bem como do mercado dos serviços relacionados com esses ativos.

([1]) JO C 343 de 26.8.2021, p. 1.
([2]) JO C 155 de 30.4.2021, p. 38.
([3]) Posição do Parlamento Europeu de 10 de novembro de 2022 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 28 de novembro de 2022.

(3) Ao nível da União, os requisitos relacionados com a gestão do risco associado às TIC no setor financeiro estão atualmente previstos nas Diretivas 2009/65/CE ([4]), 2009/138/CE ([5]), 2011/61/UE ([6]), 2013/36/UE ([7]), 2014/59/UE ([8]), 2014/65/UE ([9]), (UE) 2015/2366 ([10]) e (UE) 2016/2341 ([11]) do Parlamento Europeu e do Conselho.

Esses requisitos são diversificados, estando por vezes incompletos. Em alguns casos, o risco associado às TIC apenas foi abordado implicitamente, como parte do risco operacional, enquanto noutros nem sequer foi abordado. Essa situação é corrigida através da adoção do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho ([12]). Essas diretivas deverão, por conseguinte, ser alteradas para garantir a coerência com esse regulamento. Pela presente diretiva são adotadas um conjunto de alterações que se afiguram necessárias para proporcionar clareza e coerência jurídica no que se refere à aplicação, pelas entidades financeiras autorizadas e supervisionadas em conformidade com aquelas diretivas, de vários requisitos relativos à resiliência operacional digital necessários para o exercício das suas atividades e para a prestação de serviços, garantindo assim o bom funcionamento do mercado interno. É necessário assegurar a adequação desses requisitos no que se refere à evolução do mercado, promovendo simultaneamente a proporcionalidade em especial no que diz respeito à dimensão das entidades financeiras e aos regimes específicos a que estão sujeitas, com o objetivo de reduzir os custos de conformidade.

(4) No setor dos serviços bancários, a Diretiva 2013/36/UE atualmente estabelece apenas regras gerais de governação interna e disposições referentes ao risco operacional que contêm requisitos relativos aos planos de contingência e de continuidade das atividades que servem implicitamente de base para a gestão do risco associado às TIC. No entanto, a fim de fazer face a esse risco de forma expressa e clara, os requisitos relativos aos planos de contingência e de continuidade das atividades deverão ser alterados de modo a incluir também planos de continuidade das atividades e planos de resposta e recuperação no que se refere ao risco associado às TIC, em conformidade com os requisitos estabelecidos no Regulamento (UE) 2022/2554. Além disso, o risco associado às TIC só implicitamente – como parte da gestão do risco operacional – se encontra incluído no processo de revisão e avaliação pelo supervisor (SREP, do inglês *supervisory review and evaluation process*) conduzido pelas autoridades competentes, estando os critérios para a sua avaliação atualmente definidos nas Orientações relativas à avaliação do risco das TIC no âmbito do processo de revisão e avaliação pelo supervisor (SREP), emitidas pela Autoridade Europeia de Supervisão (Autoridade Bancária Europeia) (EBA), criada pelo Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho ([13]). A fim de proporcionar clareza jurídica e assegurar que os supervisores bancários identifiquem o risco

([4]) 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).

([5]) 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).

([6]) 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.º 1095/2010 (JO L 174 de 1.7.2011, p. 1).

([7]) 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).

([8]) Diretiva 2014/59/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, que estabelece um enquadramento para a recuperação e a resolução de instituições de crédito e de empresas de investimento e que altera a Diretiva 82/891/CEE do Conselho, e as Diretivas 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e os Regulamentos (UE) n.º 1093/2010 e (UE) n.º 648/2012 do Parlamento Europeu e do Conselho (JO L 173 de 12.6.2014, p. 190).

([9]) 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).

([10]) 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).

([11]) 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).

([12]) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (ver página 1 do presente Jornal Oficial).

([13]) 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).

associado às TIC e monitorizem a sua gestão por entidades financeiras, em consonância com o novo quadro relativo à resiliência operacional digital, o âmbito do SREP deverá também ser alterado de modo a incluir explicitamente os requisitos estabelecidos no Regulamento (UE) 2022/2554 e abranger, em particular, os riscos evidenciados pelas comunicações de incidentes de caráter severo relacionados com as TIC e pelos resultados dos testes de resiliência operacional digital realizados pelas entidades financeiras em conformidade com o referido regulamento.

(5) A resiliência operacional digital é essencial para preservar as funções críticas e as linhas de negócio críticas de uma entidade financeira em caso de resolução, evitando assim perturbações na economia real e no sistema financeiro. Os incidentes operacionais de caráter severo podem prejudicar a capacidade de uma entidade financeira para continuar a operar e podem comprometer os objetivos da resolução. A existência de certos acordos contratuais relativos à utilização de serviços de TIC é essencial para assegurar a continuidade operacional e fornecer os dados necessários em caso de resolução. A fim de ser harmonizada com os objetivos do quadro da União para a resiliência operacional, a Diretiva 2014/59/UE deverá ser alterada em conformidade, de modo a garantir que as informações relacionadas com a resiliência operacional sejam tidas em conta no contexto do planeamento da resolução e da avaliação da resolubilidade das entidades financeiras.

(6) A Diretiva 2014/65/UE determina regras mais rigorosas no domínio do risco associado às TIC para as empresas de investimento e as plataformas de negociação quando estas desenvolvam negociação algorítmica. Os serviços de comunicação de dados e os repositórios de transações são objeto de requisitos menos pormenorizados. Além disso, a Diretiva 2014/65/UE contém apenas referências limitadas a medidas de controlo e de segurança a nível dos seus sistemas de processamento de informações e à utilização de sistemas, recursos e procedimentos adequados com vista a assegurar a continuidade e regularidade dos serviços empresariais. Além disso, a diretiva em questão deverá ser harmonizada com o Regulamento (UE) 2022/2554 no que diz respeito à continuidade e regularidade no desempenho de serviços e atividades de investimento, à resiliência operacional, à capacidade dos sistemas de negociação e à eficácia dos mecanismos de continuidade das atividades e de gestão do risco.

(7) A Diretiva (UE) 2015/2366 estabelece regras específicas no que se refere às medidas de controlo da segurança e aos elementos de redução dos riscos em matéria de TIC para efeitos de obtenção de uma autorização para a prestação de serviços de pagamento. Essas regras de autorização deverão ser alteradas para fins de harmonização com o Regulamento (UE) 2022/2554. Além disso, a fim de reduzir os encargos administrativos e evitar a complexidade e a duplicação dos requisitos de comunicação de informações, as regras de notificação de incidentes previstas nessa diretiva deverão deixar de ser aplicáveis aos prestadores de serviços de pagamento que são regulados por essa diretiva e também sujeitos ao Regulamento (UE) 2022/2554, permitindo assim a esses prestadores de serviços de pagamento beneficiar de um mecanismo único e plenamente harmonizado de notificação de incidentes no que diz respeito a todos os incidentes operacionais ou de segurança relacionados com pagamentos, independentemente de tais incidentes estarem relacionados com as TIC.

(8) As Diretivas 2009/138/CE e (UE) 2016/2341 têm parcialmente em conta o risco associado às TIC nas suas disposições gerais referentes à governação e à gestão de riscos, deixando que determinados requisitos sejam especificados através de atos delegados com ou sem referências específicas ao risco associado às TIC. Analogamente, apenas regras muito gerais são aplicáveis aos gestores de fundos de investimento alternativos nos termos da Diretiva 2011/61/UE e às sociedades gestoras, nos termos da Diretiva 2009/65/CE. Essas diretivas deverão portanto ser alinhadas com os requisitos definidos no Regulamento (UE) 2022/2554 no que se refere à gestão dos sistemas e ferramentas de TIC.

(9) Em muitos casos, já foram estabelecidos requisitos adicionais relativos ao risco associado às TIC em atos delegados e de execução que foram adotados com base em projetos de normas técnicas de regulamentação e em projetos de execução elaborados pela Autoridade Europeia de Supervisão competente. Uma vez que as disposições do Regulamento (UE) 2022/2554 constituem a partir de agora o regime jurídico do risco associado às TIC no setor financeiro, certas habilitações para adotar atos delegados e atos de execução previstas nas Diretivas 2009/65/CE, 2009/138/CE, 2011/61/UE e 2014/65/UE deverão ser alteradas para eliminar as disposições referentes ao risco associado às TIC do âmbito dessas habilitações.

(10) Com o intuito de assegurar uma aplicação coerente do novo quadro referente à resiliência operacional digital do setor financeiro, os Estados-Membros deverão aplicar as disposições do direito nacional que transpõem a presente diretiva a partir da data de aplicação do Regulamento (UE) 2022/2554.

(11) As Diretivas 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 foram adotadas com base no artigo 53.º, n.º 1, ou no artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), ou em ambos. As alterações constantes da presente diretiva foram incluídas num único ato legislativo devido à interligação do objeto e dos objetivos dessas alterações. Consequentemente, a presente diretiva deverá ser adotada com base no artigo 53.º, n.º 1, e no artigo 114.º do TFUE.

(12) Atendendo a que os objetivos da presente diretiva não podem ser suficientemente alcançados pelos Estados-Membros, uma vez que implicam a harmonização de requisitos já contidos nas diretivas, mas podem, devido à dimensão e aos efeitos da ação, ser mais bem alcançados ao nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para alcançar esses objetivos.

(13) De acordo com a declaração política conjunta dos Estados-Membros e da Comissão, de 28 de setembro de 2011, sobre os documentos explicativos ([14]), os Estados-Membros assumiram o compromisso de fazer acompanhar a notificação das suas medidas de transposição, nos casos em que tal se justifique, de um ou mais documentos que expliquem a relação entre os componentes de uma diretiva e as partes correspondentes dos instrumentos nacionais de transposição. Em relação à presente diretiva, o legislador considera que a transmissão desses documentos se justifica,

ADOTARAM A PRESENTE DIRETIVA:

Artigo 1.º

Alteração da Diretiva 2009/65/CE

O artigo 12.º da Diretiva 2009/65/CE é alterado do seguinte modo:

1) No n.º 1, segundo parágrafo, a alínea a) passa a ter a seguinte redação:

«a) Aplique procedimentos administrativos e contabilísticos sólidos e disponha de mecanismos de controlo e segurança em matéria de tratamento eletrónico de dados, incluindo no que toca a sistemas de rede e informação criados e geridos em conformidade com o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*), bem como de procedimentos de controlo interno adequados, incluindo, em especial, regras relativas às transações pessoais dos seus empregados ou à detenção ou gestão de investimentos em instrumentos financeiros para investirem por conta própria e que garantam, pelo menos, que cada transação em que o OICVM participe possa ser reconstituída quanto à sua origem, às partes nela envolvidas, à sua natureza e ao momento e local em que foi efetuada, e que os ativos dos OICVM geridos pela sociedade gestora sejam investidos de acordo com o regulamento de gestão do fundo ou com os documentos constitutivos e com a legislação em vigor;

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»;

2) O n.º 3 passa a ter a seguinte redação:

«3. Sem prejuízo do disposto no artigo 116.º, a Comissão adota, através de atos delegados nos termos do artigo 112.º-A, medidas destinadas a especificar:

a) Os procedimentos e mecanismos referidos no n.º 1, segundo parágrafo, alínea a), com exceção dos procedimentos e mecanismos relativos aos sistemas de rede e informação;

b) As estruturas e requisitos organizativos necessários para minimizar os conflitos de interesses referidos no n.º 1, segundo parágrafo, alínea b).».

([14]) JO C 369 de 17.12.2011, p. 14.

Artigo 2.º

Alteração da Diretiva 2009/138/CE

A Diretiva 2009/138/CE é alterada do seguinte modo:

1) No artigo 41.º, o n.º 4 passa a ter a seguinte redação:

«4. As empresas de seguros e de resseguros devem tomar medidas razoáveis para assegurar a continuidade e a regularidade do exercício das suas atividades, incluindo o desenvolvimento de planos de contingência. Para esse efeito, as empresas empregam sistemas, recursos e procedimentos adequados e proporcionados e, em especial, criam e gerem sistemas de rede e informação em conformidade com o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*).

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»;

2) No artigo 50.º, n.º 1, as alíneas a) e b) passam a ter a seguinte redação:

«a) Os elementos dos sistemas referidos no artigo 41.º, no artigo 44.º, em particular os domínios enumerados no artigo 44.º, n.º 2, e nos artigos 46.º e 47.º, com exceção dos elementos relativos à gestão do risco associado às tecnologias da informação e da comunicação;

b) As funções referidas nos artigos 44.º, 46.º, 47.º e 48.º, com exceção das funções relacionadas com a gestão do risco associado às tecnologias da informação e da comunicação.».

Artigo 3.º

Alteração da Diretiva 2011/61/UE

O artigo 18.º da Diretiva 2011/61/UE passa a ter a seguinte redação:

«*Artigo 18.º*

Princípios gerais

1. Os Estados-Membros devem exigir que os GFIAs apliquem, a todo o tempo, os recursos humanos e técnicos adequados e apropriados que sejam necessários para a boa gestão dos FIAs.

Em especial, e tendo também em conta a natureza dos FIAs geridos pelo GFIA, as autoridades competentes do Estado-Membro de origem do GFIA devem exigir que este utilize procedimentos administrativos e contabilísticos sãos e disponha de mecanismos de controlo e segurança em matéria de tratamento eletrónico de dados, incluindo no que respeita aos sistemas de rede e informação criados e geridos em conformidade com o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*), bem como de procedimentos de controlo interno adequados, incluindo, em especial, regras relativas às transações pessoais dos seus empregados ou à detenção ou gestão de investimentos para investir por conta própria, e que assegurem, pelo menos, que cada transação em que os FIAs participem possa ser reconstituída quanto à sua origem, às partes nela envolvidas, à sua natureza e ao momento e local em que foi efetuada, e que os ativos dos FIAs geridos pelo GFIA sejam investidos de acordo com o regulamento ou os instrumentos constitutivos do FIA e com a legislação em vigor.

2. A Comissão adota, por meio de atos delegados nos termos do artigo 56.º e nas condições previstas nos artigos 57.º e 58.º, medidas para especificar os procedimentos e mecanismos a que se refere o n.º 1 do presente artigo, com exceção dos procedimentos e mecanismos relativos aos sistemas de rede e informação.

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).».

Artigo 4.º

Alteração da Diretiva 2013/36/UE

A Diretiva 2013/36/UE é alterada do seguinte modo:

1) No artigo 65.º, n.º 3, alínea a), a subalínea vi) passa a ter a seguinte redação:

«vi) terceiros aos quais as entidades a que se referem as subalíneas i) a iv) tenham subcontratado funções ou atividades, incluindo terceiros prestadores de serviços de TIC referidos no capítulo V do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*);

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»;

2) No artigo 74.º, n.º 1, o primeiro parágrafo passa a ter a seguinte redação:

«As instituições devem dispor de sistemas de governo sólidos, que incluam uma estrutura organizativa clara, com linhas de responsabilidade bem definidas, transparentes e coerentes, processos eficazes para identificar, gerir, monitorizar e comunicar os riscos a que estão ou podem vir a estar expostas, mecanismos adequados de controlo interno, incluindo procedimentos administrativos e contabilísticos sólidos, sistemas de rede e informação criados e geridos em conformidade com o Regulamento (UE) 2022/2554, e políticas e práticas de remuneração consentâneas com uma gestão sólida e eficaz do risco e que promovam esse tipo de gestão.»;

3) No artigo 85.º, o n.º 2 passa a ter a seguinte redação:

«2. As autoridades competentes asseguram que as instituições tenham políticas e planos adequados de contingência e de continuidade das atividades, incluindo políticas e planos de continuidade das atividades no domínio das TIC e planos de resposta e recuperação em matéria de TIC para a tecnologia que utilizam na comunicação de informações, e que esses planos sejam estabelecidos, geridos e testados em conformidade com o artigo 11.º do Regulamento (UE) 2022/2554, a fim de permitir que as instituições continuem a operar na eventualidade de uma perturbação grave da sua atividade de negócio e contenham as perdas incorridas em consequência dessa perturbação.»;

4) Ao artigo 97.º, n.º 1, é aditada a seguinte alínea:

«d) Os riscos revelados pelos testes de resiliência operacional digital realizados em conformidade com o capítulo IV do Regulamento (UE) 2022/2554».

Artigo 5.º

Alteração da Diretiva 2014/59/UE

A Diretiva 2014/59/UE é alterada do seguinte modo:

1) O artigo 10.º é alterado do seguinte modo:

a) No n.º 7, a alínea c) passa a ter a seguinte redação:

«c) Uma demonstração da forma como as funções críticas e as linhas de negócio críticas podem ser jurídica e economicamente separadas, na medida do necessário, de outras funções, a fim de assegurar a continuidade e a resiliência operacional digital em caso de insolvência da instituição;»;

b) No n.º 7, a alínea q) passa a ter a seguinte redação:

«q) Uma descrição das operações e dos sistemas essenciais para manter os processos operacionais da instituição em funcionamento contínuo, incluindo os sistemas de rede e informação a que se refere o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*);

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»;

c) Ao n.º 9, é aditado o seguinte parágrafo:

«Nos termos do artigo 10.º do Regulamento (UE) n.º 1093/2010, a EBA revê e, se necessário, atualiza as normas técnicas de regulamentação a fim de ter em conta, nomeadamente, as disposições do capítulo II do Regulamento (UE) 2022/2554.»;

2) O anexo é alterado do seguinte modo:

a) Na secção A, o ponto 16 passa a ter a seguinte redação:

«16) Mecanismos e medidas necessários para manter o funcionamento continuado dos processos operacionais da instituição, incluindo os sistemas de rede e informação criados e geridos em conformidade com o Regulamento (UE) 2022/2554;»;

b) A secção B é alterada do seguinte modo:

i) o ponto 14 passa a ter a seguinte redação:

«14) Identificação dos proprietários dos sistemas identificados no ponto 13, acordos de nível de serviço associados e programas, sistemas ou licenças informáticos, incluindo uma discriminação das respetivas entidades jurídicas, das operações críticas e das linhas de negócio críticas, bem como uma identificação dos terceiros prestadores de serviços de TIC críticos, tal como definido no artigo 3.º, ponto 23, do Regulamento (UE) 2022/2554;»,

ii) é inserido o seguinte ponto:

«14-A) Resultados dos testes de resiliência operacional digital das instituições realizados ao abrigo do Regulamento (UE) 2022/2554;»;

c) A secção C é alterada do seguinte modo:

i) o ponto 4 passa a ter a seguinte redação:

«4) Em que medida será possível garantir a solidez e o cabal cumprimento dos acordos de serviço, incluindo acordos contratuais relativos à utilização de serviços de TIC, mantidos pela instituição em caso de resolução da mesma.»,

ii) é inserido o seguinte ponto:

«4-A) A resiliência operacional digital dos sistemas de rede e informação que apoiam as funções críticas e as linhas de negócio críticas da instituição, tendo em conta a notificação de incidentes de caráter severo relacionados com as TIC e os resultados dos testes de resiliência operacional digital realizados ao abrigo do Regulamento (UE) 2022/2554».

Artigo 6.º

Alteração da Diretiva 2014/65/UE

A Diretiva 2014/65/UE é alterada do seguinte modo:

1) O artigo 16.º é alterado do seguinte modo:

a) O n.º 4 passa a ter a seguinte redação:

«4. As empresas de investimento tomam medidas razoáveis para assegurar a continuidade e a regularidade da execução dos serviços e atividades de investimento. Para esse efeito, as empresas de investimento empregam sistemas adequados e proporcionados, incluindo sistemas de tecnologias da informação e comunicação (TIC) criados e geridos em conformidade com o artigo 7.º do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*), bem como recursos e procedimentos adequados e proporcionados.

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»;

b) No n.º 5, os parágrafos segundo e terceiro passam a ter a seguinte redação:

«As empresas de investimento devem dispor de uma sólida organização administrativa e contabilística, mecanismos de controlo interno e procedimentos eficazes para a avaliação de riscos.

Sem prejuízo da capacidade das autoridades competentes para exigir o acesso às comunicações, nos termos da presente diretiva e do Regulamento (UE) n.º 600/2014, as empresas de investimento devem aplicar mecanismos de segurança sólidos para garantir, de acordo com os requisitos definidos no Regulamento (UE) 2022/2554, a segurança e a autenticação dos meios de transferência das informações, para minimizar o risco de corrupção de dados e de acesso não autorizado e para evitar fugas de informação, assim mantendo a confidencialidade dos dados em todos os momentos.»;

2) O artigo 17.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

«1. Uma empresa de investimento que desenvolva negociação algorítmica dispõe de sistemas e controlos de risco eficazes e adequados às atividades que desenvolve para assegurar que os seus sistemas de negociação sejam resilientes e tenham capacidade suficiente, em conformidade com os requisitos definidos no capítulo II do Regulamento (UE) 2022/2554, estão sujeitos a limiares e limites de negociação adequados e impedem o envio de ordens erradas ou impedem o sistema de funcionar de modo que possa criar ou contribuir para uma perturbação do mercado.

Essa empresa dispõe também de sistemas e controlos de risco eficazes, a fim de assegurar que os sistemas de negociação não possam ser utilizados para qualquer objetivo contrário ao disposto no Regulamento (UE) n.º 596/2014 ou às regras de uma plataforma de negociação a que esteja ligada.

A empresa de investimento dispõe ainda de mecanismos de continuidade das atividades eficazes para fazer face a qualquer falha dos seus sistemas de negociação, incluindo uma política e planos de continuidade das atividades no domínio das TIC e planos de resposta e recuperação em matéria de TIC estabelecidos em conformidade com o artigo 11.º do Regulamento (UE) 2022/2554, e assegura que os seus sistemas estão plenamente testados e são devidamente acompanhados, por forma a garantir que satisfazem os requisitos gerais constantes do presente número e quaisquer requisitos específicos definidos nos capítulos II e IV do Regulamento (UE) 2022/2554.»;

b) No n.º 7, a alínea a) passa a ter a seguinte redação:

«a) Os requisitos pormenorizados em matéria de organização estabelecidos nos n.ºs 1 a 6 – com exceção dos relacionados com a gestão do risco associado às TIC – que devem ser impostos às empresas de investimento que prestam diferentes serviços de investimento, atividades de investimento e serviços auxiliares ou combinações desses serviços, pelo que as especificações relativas aos requisitos em matéria de organização estabelecidos no n.º 5 definem os requisitos específicos para o acesso direto ao mercado e para o acesso patrocinado, de modo a assegurar que os controlos aplicados ao acesso patrocinado sejam, pelo menos, equivalentes aos aplicados ao acesso direto ao mercado;»;

3) No artigo 47.º, o n.º 1 é alterado do seguinte modo:

a) A alínea b) passa a ter a seguinte redação:

«b) Esteja dotado dos meios necessários para gerir os riscos a que está exposto, inclusive para gerir o risco associado às TIC de acordo com o capítulo II do Regulamento (UE) 2022/2554, para implementar mecanismos e sistemas adequados para identificar os riscos significativos para o seu funcionamento, bem como para instituir medidas eficazes para mitigar estes riscos;»;

b) É suprimida a alínea c);

4) O artigo 48.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

«1. Os Estados-Membros exigem que os mercados regulamentados criem e mantenham a sua resiliência operacional em conformidade com os requisitos estabelecidos no capítulo II do Regulamento (UE) 2022/2554 para garantir que os seus sistemas de negociação são resilientes, têm capacidade suficiente para lidarem com picos de ordens e grandes volumes de mensagens, são capazes de assegurar a negociação ordenada em condições de forte tensão no mercado, estão plenamente testados para garantir o cumprimento dessas condições e são regidos por mecanismos de continuidade das atividades eficazes, incluindo uma política e planos de continuidade das atividades no domínio das TIC e planos de resposta e recuperação em matéria de TIC estabelecidos em conformidade com o artigo 11.º do Regulamento (UE) 2022/2554, que asseguram a manutenção dos seus serviços, caso se verifique uma falha dos seus sistemas de negociação.»;

b) O n.º 6 passa a ter a seguinte redação:

«6. Os Estados-Membros exigem que os mercados regulamentados disponham de sistemas, procedimentos e mecanismos eficazes, incluindo a exigência de que os membros ou participantes realizem os testes apropriados aos algoritmos e proporcionem a criação de ambientes que facilitem a realização de tais testes, de acordo com os requisitos estabelecidos nos capítulos II e IV do Regulamento (UE) 2022/2554, para assegurar que os sistemas de negociação algorítmica não criam nem contribuem para a perturbação da negociação no mercado e para gerir quaisquer perturbações que afetem a negociação decorrentes desses sistemas de negociação algorítmica, incluindo sistemas que limitem o rácio de ordens não executadas face às transações que podem ser introduzidas no sistema por um membro ou participante, a fim de poder abrandar o fluxo de ordens, se se verificar o risco de ser atingida a capacidade máxima do sistema, e de limitar e fazer cumprir a variação mínima da oferta de preços (tick) que pode ser executada no mercado.»;

c) O n.º 12 é alterado do seguinte modo:

i) a alínea a) passa a ter a seguinte redação:

«a) Os requisitos para assegurar que os sistemas de negociação dos mercados regulamentados sejam resilientes e tenham a capacidade adequada, com exceção dos requisitos relacionados com a resiliência operacional digital;»,

ii) a alínea g) passa a ter a seguinte redação:

«g) Os requisitos para garantir a realização de testes apropriados aos algoritmos, com exceção dos testes de resiliência operacional digital, a fim de assegurar que os sistemas de negociação algorítmica, incluindo os sistemas de negociação algorítmica de alta frequência, não sejam passíveis de criar ou de contribuir para perturbações do processo de negociação no mercado.».

Artigo 7.º

Alteração da Diretiva (UE) 2015/2366

A Diretiva (UE) 2015/2366 é alterada do seguinte modo:

1) No artigo 3.º, a alínea j) passa a ter a seguinte redação:

«j) Aos serviços prestados por prestadores de serviços técnicos, que apoiam a prestação de serviços de pagamento sem nunca entrarem na posse dos fundos a transferir, incluindo o processamento e o armazenamento de dados, os serviços de proteção da confiança e da privacidade, a autenticação de dados e entidades, o fornecimento de tecnologias da informação e comunicação (TIC) e de redes de comunicação, e o fornecimento e manutenção de terminais e dispositivos utilizados para serviços de pagamento, com exceção dos serviços de iniciação de pagamentos e dos serviços de informação sobre contas;»;

2) O artigo 5.º, n.º 1, é alterado do seguinte modo:

a) O primeiro parágrafo é alterado do seguinte modo:

i) a alínea e) passa a ter a seguinte redação:

«e) Uma descrição dos seus sistemas de governo e dos seus mecanismos de controlo interno, designadamente os procedimentos administrativos, de gestão de riscos e contabilísticos, bem como dos seus acordos relativos à utilização de serviços de TIC nos termos do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*), que demonstre que esses sistemas de governo e mecanismos de controlo interno são proporcionados, adequados, sólidos e suficientes;

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»,

ii) a alínea f) passa a ter a seguinte redação:

«f) Uma descrição do procedimento criado para verificar, tratar e acompanhar incidentes de segurança e reclamações dos clientes relacionadas com a segurança, incluindo um mecanismo de comunicação de incidentes que tenha em conta as obrigações de notificação da instituição de pagamento previstas no capítulo III do Regulamento (UE) 2022/2554;»,

iii) a alínea h) passa a ter a seguinte redação:

«h) Uma descrição dos mecanismos de continuidade das atividades, incluindo uma identificação clara das operações críticas, uma política e planos de continuidade das atividades no domínio das TIC e planos de resposta e recuperação em matéria de TIC eficazes, bem como um procedimento para testar regularmente esses planos, avaliando a sua adequação e eficácia, em conformidade com o Regulamento (UE) 2022/ /2554;»;

b) O terceiro parágrafo passa a ter a seguinte redação:

«A descrição das medidas de controlo da segurança e de redução dos riscos a que se refere o primeiro parágrafo, alínea j), indica a forma como essas medidas garantem um elevado nível de resiliência operacional digital, em conformidade com o capítulo II do Regulamento (UE) 2022/2554, em particular em relação à segurança técnica e à proteção de dados, inclusive a nível do software e dos sistemas de TIC utilizados pelas instituições requerentes ou pelas empresas a que essas instituições externalizem a totalidade ou parte das suas operações. Essas medidas incluem igualmente as medidas de segurança previstas no artigo 95.º, n.º 1, da presente diretiva. Essas medidas têm em conta as orientações da EBA sobre medidas de segurança a que se refere o artigo 95.º, n.º 3, da presente diretiva, uma vez elaboradas.»;

3) No artigo 19.º, n.º 6, o segundo parágrafo passa a ter a seguinte redação:

«A externalização de funções operacionais importantes, incluindo sistemas de TIC, não pode ser efetuada de um modo que prejudique significativamente a qualidade do controlo interno da instituição de pagamento nem a capacidade das autoridades competentes para verificarem e reconstituírem o cumprimento, por parte da instituição de pagamento, de todas as obrigações previstas na presente diretiva.»;

4) Ao artigo 95.º, n.º 1, é aditado o seguinte parágrafo:

«O primeiro parágrafo não prejudica a aplicação do capítulo II do Regulamento (UE) 2022/2554:

a) Aos prestadores de serviços de pagamento a que se refere o artigo 1.º, n.º 1, alíneas a), b) e d), da presente diretiva;

b) Aos prestadores de serviços de informação sobre contas a que se refere o artigo 33.º, n.º 1, da presente diretiva;

c) Às instituições de pagamento isentas nos termos do artigo 32.º, n.º 1, da presente diretiva; nem

d) Às instituições de moeda eletrónica que beneficiem de uma isenção nos termos do artigo 9.º, n.º 1, da Diretiva 2009/110/CE.»;

5) Ao artigo 96.º é aditado o seguinte número:

«7. Os Estados-Membros asseguram que os n.ºs 1 a 5 do presente artigo não se aplicam:

a) Aos prestadores de serviços de pagamento a que se refere o artigo 1.º, n.º 1, alíneas a), b) e d), da presente diretiva;

b) Aos prestadores de serviços de informação referidos no artigo 33.º, n.º 1 da presente diretiva;

c) Às instituições de pagamento isentas nos termos do artigo 32.º, n.º 1 da presente diretiva; nem

d) Às instituições de moeda eletrónica que beneficiem de uma isenção nos termos do artigo 9.º, n.º 1, da Diretiva 2009/110/CE.»;

6) No artigo 98.º, o n.º 5 passa a ter a seguinte redação:

«5. Nos termos do artigo 10.º do Regulamento (UE) n.º 1093/2010, a EBA revê e, se necessário, atualiza periodicamente as normas técnicas de regulamentação a fim de ter em conta, nomeadamente, a inovação e a evolução tecnológica, bem como as disposições do capítulo II do Regulamento (UE) 2022/2554».

Artigo 8.º

Alteração da Diretiva (UE) 2016/2341

O artigo 21.º, n.º 5, da Diretiva (UE) 2016/2341, passa a ter a seguinte redação:

«5. Os Estados-Membros asseguram que as IRPPP tomem medidas razoáveis para assegurar a continuidade e a regularidade do exercício das suas atividades, incluindo a elaboração de planos de contingência. Para esse efeito, as

IRPPP devem utilizar sistemas, recursos e procedimentos adequados e proporcionados, e devem, em especial, criar e gerir sistemas de rede e informação em conformidade com o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*), quando aplicável.

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).».

Artigo 9.º

Transposição

1. Os Estados-Membros adotam e publicam até 17 de janeiro de 2025, as disposições necessárias para dar cumprimento à presente diretiva. Do facto informam imediatamente a Comissão.

Os Estados-Membros aplicam essas disposições a partir de 17 de janeiro de 2025.

As disposições adotadas pelos Estados-Membros fazem referência à presente diretiva ou são acompanhadas dessa referência aquando da sua publicação oficial. Os Estados-Membros estabelecem o modo como é feita a referência.

2. Os Estados-Membros comunicam à Comissão o texto das principais disposições de direito interno que adotarem no domínio regulado pela presente diretiva.

Artigo 10.º

Entrada em vigor

A presente diretiva entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Artigo 11.º

Destinatários

Os destinatários da presente diretiva são os Estados-Membros.

Feito em Estrasburgo, em 14 de dezembro de 2022.

Pelo Parlamento Europeu	*Pelo Conselho*
A Presidente	*O Presidente*
R. METSOLA	M. BEK