III

(Atos preparatórios)

BANCO CENTRAL EUROPEU

PARECER DO BANCO CENTRAL EUROPEU

de 4 de junho de 2021

sobre uma proposta de regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro

(CON/2021/20)

(2021/C 343/01)

Introdução e base jurídica

Nos dias 22, 23 e 29 de dezembro de 2020 o Banco Central Europeu (BCE) recebeu do Conselho da União Europeia e do Parlamento Europeu, respetivamente, pedidos de parecer sobre uma proposta de regulamento 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 e (UE) n.º 909/2014 ([1]) (a seguir «regulamento proposto») e, ainda, sobre uma proposta de diretiva que altera as Diretivas 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 ([2]) (a seguir «diretiva de alteração proposta»), conjuntamente designados por «diplomas legislativos propostos».

A competência do BCE para emitir parecer baseia-se no artigo 127.º, n.º 4, e no artigo 282.º, n.º 5, do Tratado sobre o Funcionamento da União Europeia, uma vez que os diplomas legislativos propostos contêm disposições que se inserem nas competências do BCE, nomeadamente de definição e execução da política monetária, de promoção do bom funcionamento dos sistemas de pagamentos e de contribuição para a boa condução das políticas prosseguidas pelas autoridades competentes relativas à estabilidade do sistema financeiro, bem como nas atribuições do BCE relativas à supervisão prudencial das instituições de crédito previstas no artigo 127.º, n.º 2, primeiro e quarto travessões, no artigo 127.º, n.º 5, e no artigo 127.º, n.º 6, do Tratado. O presente parecer foi aprovado pelo Conselho do BCE, em conformidade com o disposto no artigo 17.º-5, primeiro período, do Regulamento Interno do Banco Central Europeu.

1. Observações genéricas

1.1 O BCE acolhe favoravelmente o regulamento proposto, que visa reforçar a cibersegurança e a resiliência operacional do setor financeiro. O BCE acolhe com especial agrado o objetivo do regulamento proposto de melhorar o estabelecimento e o funcionamento do mercado interno de serviços financeiros, e de eliminar obstáculos aos mesmos por meio da harmonização das regras aplicáveis no domínio da gestão do risco associado às tecnologias da informação e comunicação (TIC), à comunicação de incidentes, à realização de testes e à monitorização do risco de terceiros no domínio das TIC. O BCE congratula-se igualmente com o objetivo do regulamento proposto de simplificar e harmonizar qualquer sobreposição de requisitos regulamentares ou expectativas de supervisão a que as entidades financeiras estão atualmente sujeitas ao abrigo da legislação da União.

1.2 O BCE entende que, de acordo com o espírito do artigo 1.º, n.º 7, da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ([3]) (a seguir «Diretiva SRI»), o regulamento proposto constitui legislação sectorial específica (*lex specialis*) no que respeita às entidades financeiras identificadas como operadores de serviços essenciais ([4]), o que implica que, em princípio, as obrigações impostas pelo regulamento proposto prevaleceriam sobre a Diretiva SRI. Na prática, isso significa que as entidades financeiras identificadas como operadores de serviços essenciais ([5]) deveriam, nomeadamente, notificar incidentes em conformidade com o

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Diretiva (UE) n.º 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, 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).
([4]) Ver o artigo 1.º, n.º 2, do regulamento proposto.
([5]) Ver o artigo 5.º, da Diretiva SRI.

regulamento proposto, e não com a Diretiva SRI. Embora o BCE se congratule com a diminuição de uma possível sobreposição de obrigações das entidades financeiras no domínio da comunicação de incidentes, deveria prestar-se mais atenção à interação entre o regulamento proposto e a Diretiva SRI. Por exemplo, ao abrigo do regulamento proposto, um terceiro prestador de serviços no domínio das TIC ([6]) poderia ficar obrigado a seguir as recomendações da autoridade fiscalizadora principal ([7]). Mas, simultaneamente, o mesmo prestador de serviços no domínio das TIC pode ser classificado como operador de serviços essenciais ao abrigo da Diretiva SRI, ficando assim sujeito a instruções vinculativas emitidas pela autoridade competente ([8]). Em tal caso, o terceiro prestador de serviços no domínio das TIC poderia vir a ser destinatário de recomendações (emitidas ao abrigo do regulamento proposto) e de instruções vinculativas (emitidas ao abrigo da Diretiva SRI) que estejam em contradição. O BCE sugere que os órgãos legislativos da União reflitam mais aprofundadamente sobre potenciais incoerências entre o regulamento proposto e a Diretiva SRI, suscetíveis de dificultar a harmonização e a redução de sobreposições e requisitos contraditórios aplicáveis às entidades financeiras.

1.3 O BCE entende ainda que, nos termos da proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a assegurar um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 ([9]) (a seguir «Diretiva SRI 2 proposta»), os «quase incidentes» ([10]) ficarão sujeitos a obrigações de notificação ([11]). Embora o considerando 39 da diretiva proposta SRI 2 se refira ao significado da expressão «quase incidentes», não está claro se a intenção é exigir que estes sejam notificados pelas entidades financeiras enumeradas no artigo 2.º do regulamento proposto. A este respeito, e tendo também em conta que os «quase incidentes» só podem ser identificados como tal após terem ocorrido, o BCE gostaria de receber atempadamente a notificação de quase incidentes de caráter significativo, como já acontece atualmente no caso dos ciberincidentes. O BCE sugere uma maior coordenação entre o regulamento proposto e a diretiva proposta SRI 2, para tornar claro o âmbito das obrigações de notificação a que qualquer entidade financeira pode estar sujeita ao abrigo destes dois atos legislativos da União, que são distintos, mas estão interligados. Paralelamente, seria necessário definir os «quase incidentes» e elaborar disposições que justifiquem o seu caráter significativo.

1.4 O BCE congratula-se com o facto de se incentivarem as entidades financeiras a voluntariamente partilhar entre si informação sobre ciberameaças, a fim de reforçar e promover a sua ciber-resiliência. O próprio BCE colaborou na *Cyber threat Intelligence Information Sharing Initiative (CIISI-EU)* (Iniciativa para a Partilha de Informação sobre Ciberameaças) impulsionada pelo mercado, tendo colocado à disposição do público os modelos necessários para qualquer pessoa poder desenvolver e promover tal iniciativa ([12]).

1.5 O BCE é a favor da cooperação entre as autoridades competentes para efeitos do regulamento proposto, as Autoridades Europeias de Supervisão (AES) e as Equipas de Resposta a Incidentes de Segurança Informática (*Computer Security Incident Response Teams /CSIRT*) ([13]). É essencial proceder-se ao intercâmbio de informações a fim de assegurar a resiliência operacional da União, uma vez que a partilha de informações e a cooperação entre as autoridades podem contribuir para a prevenção de ciberataques e ajudar a reduzir a propagação de ameaças no domínio das TIC. Há que promover um entendimento comum dos riscos relacionados com as TIC, e garantir uma avaliação coerente desses riscos em toda a União. É da maior importância que as informações sejam partilhadas pelas autoridades competentes com o ponto de contacto único ([14]) e com as CSIRT nacionais ([15]) apenas quando existam mecanismos de classificação e de partilha de informações claramente definidos, juntamente com salvaguardas adequadas para garantir a confidencialidade.

1.6 Por último, o BCE veria com agrado a introdução, ao abrigo do regulamento proposto, de regras relativas aos dados pessoais e à conservação de dados. A fixação do período de retenção deveria ter em atenção as atividades de investigação, inspeção, pedido de informação, comunicação, publicação, avaliação, verificação, avaliação e elaboração de planos de superintendência ou supervisão que as autoridades competentes possam ter de levar a cabo no âmbito das respetivas obrigações e deveres ao abrigo do regulamento proposto. A este respeito, considerar-se-ia apropriado um período de retenção dados de 15 anos. Este período de retenção de dados poderia ser encurtado ou alargado, em função de circunstâncias específicas. Relativamente a este

([6]) Ver o artigo 3.º, n.º 15, do regulamento proposto.
([7]) Ver artigo 31.º, n.º 1, alínea d), do regulamento proposto.
([8]) Ver o artigo 15.º, n.º 3, da Diretiva SRI.
([9]) COM(2020) 823 final.
([10]) Um evento que poderia ter causado danos, mas que foi impedido de se materializar plenamente; ver considerando 39 da diretiva proposta SRI 2.
([11]) Ver o artigo 11.º da diretiva proposta SRI 2.
([12]) *Cyber threat Intelligence Information Sharing Initiative (CIISI-EU)*, disponível [em inglês] no sítio *web* do BCE: www.ecb.europa.eu.
([13]) Ver o artigo 42.º do regulamento proposto.
([14]) Ver o artigo 8, n.º 3, da Diretiva SRI.
([15]) Ver igualmente os artigos 11.º, 26.º e 27.º da Diretiva proposta SRI 2.

aspeto, o BCE sugere que os órgãos legislativos da União, na formulação da disposição pertinente respeitante aos dados pessoais e à retenção da informação, levem igualmente em conta o princípio da minimização dos dados, bem como o seu tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos ([16]).

2. **Observações específicas sobre a fiscalização, compensação e liquidação de valores mobiliários**

2.1 *Competências de fiscalização do SEBC e do Eurosistema*

2.1.1 Por se encontrarem estreitamente relacionados com as suas atribuições fundamentais de política monetária, o Tratado e os Estatutos do Sistema Europeu de Bancos Centrais e do Banco Central Europeu (a seguir «Estatutos do SEBC») regulam a ação do Eurosistema em matéria de superintendência dos sistemas de compensação e de pagamentos. Nos termos do artigo 127.º, n.º 2, quarto travessão, do Tratado, refletido no artigo 3.º-1 dos Estatutos, uma das atribuições fundamentais cometidas ao SEBC consiste na promoção do bom funcionamento dos sistemas de pagamento. No desempenho desta atribuição, «[O] BCE e os bancos centrais nacionais podem conceder facilidades e o BCE pode adotar regulamentos, a fim de assegurar a eficiência e a solidez dos sistemas de compensação e de pagamentos no interior da União e com países terceiros» ([17]). No exercício da sua função de superintendência, o BCE adotou o Regulamento (UE) n.º 795/2014 do Banco Central Europeu (BCE/2014/28) (a seguir «Regulamento *SIPS*») ([18]). O Regulamento SIPS implementa os princípios aplicáveis às infraestruturas dos mercados financeiros emitidos pelo Comité dos Sistemas de Pagamento e Liquidação (*Committee on Payment and Settlement Systems/CPSS*) e pela Organização Internacional das Comissões de Valores Mobiliários (*International Organization of Securities Commissions/IOSCO*) (a seguir designados «princípios CPSS-IOSCO») ([19]), os quais são juridicamente vinculativos e abrangem os sistemas de pagamentos, tanto de importâncias avultadas como de pequeno montante, com importância sistémica, operados quer por um banco central do Eurosistema quer por uma entidade privada. O quadro de política de superintendência do Eurosistema ([20]) classifica os instrumentos de pagamento como «parte integrante dos sistemas de pagamentos», pelo que os inclui no âmbito da sua superintendência. O quadro de fiscalização dos instrumentos de pagamento está atualmente a ser objeto de revisão ([21]). De acordo com o referido quadro, um instrumento de pagamento (por exemplo, um cartão, uma transferência de crédito, um débito direto, uma transferência de moeda eletrónica ou uma criptoficha de pagamento digital ([22])) é definido como sendo um dispositivo personalizado (ou conjunto de dispositivos) e/ou um conjunto de procedimentos acordados entre o utilizador do serviço de pagamento e o prestador de serviços de pagamento, utilizado para iniciar uma transferência de valor ([23]).

2.1.2 À luz do que precede, e face à aplicação dos quadros de superintendência acima referidos, o BCE congratula-se com a exclusão do âmbito de aplicação do regulamento proposto dos operadores de sistemas, tal como definidos no artigo 2.º, alínea p), da Diretiva 98/26/CE do Parlamento Europeu e do Conselho ([24]), dos sistemas

([16]) Ver o artigo 4.º, alínea b), e o artigo 13.º do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

([17]) Ver o artigo 22.º dos Estatutos do SEBC.

([18]) Regulamento (UE) n.º 795/2014 do Banco Central Europeu, de 3 de julho de 2014, relativo aos requisitos de superintendência de sistemas de pagamentos sistemicamente importantes (BCE/2014/28) (JO L 217 de 23.7.2014, p. 16).

([19]) Disponível [em inglês] no sítio *web* do Banco de Pagamentos Internacionais, www.bis.org.

([20]) *Eurosystem oversight policy framework* (Quadro de política de superintendência do Eurosistema), versão revista (julho de 2016) disponível [em inglês] no sítio *web* do BCE em www.ecb.europa.eu.

([21]) *Eurosystem oversight framework for electronic payment instruments, schemes and arrangements* (Quadro de superintendência revisto e consolidado do Eurosistema relativo a instrumentos, esquemas e acordos de pagamento eletrónico), de outubro de 2020 (quadro PISA), disponível [em inglês] no sítio *web* do BCE em www.ecb.europa.eu..

([22]) Uma criptoficha de pagamento digital é uma representação digital de valor, garantida por créditos ou ativos registados noutro local, que permite a transferência de valor entre utilizadores finais. Dependendo da conceção subjacente, as criptofichas de pagamento digitais podem prever uma transferência de valor sem envolver necessariamente uma central terceira e/ou utilizar contas de pagamento.

([23]) «Transferência de valor», «o ato, iniciado pelo ordenante ou em seu nome, ou pelo beneficiário, de transferir fundos ou criptofichas de pagamento digitais, ou de colocar ou levantar numerário numa conta de utilizador, independentemente de quaisquer obrigações subjacentes entre o ordenante e o beneficiário. A transferência pode envolver um único ou vários prestadores de serviços de pagamento.» A definição de «transferência de valor» constante do quadro PISA diverge do que é referido como uma transferência de «fundos» na 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). Uma «transferência de valor» no contexto de um «instrumento de pagamento», na aceção da diretiva citada apenas se pode referir a uma transferência de «fundos». Nos termos da referida diretiva, os «fundos» não incluem criptofichas de pagamento digitais, a menos que as criptofichas possam ser classificadas como moeda eletrónica (ou, mais hipoteticamente, como moeda escritural).

([24]) Diretiva 98/26/CE do Parlamento Europeu e do Conselho, de 19 de maio de 1998, relativa ao carácter definitivo da liquidação nos sistemas de pagamentos e de liquidação de valores mobiliários (JO L 166 de 11.6.1998, p. 45).

de pagamento (incluindo os geridos por bancos centrais), dos sistemas de pagamento e dos acordos de pagamento. Pelas razões acima referidas, as competências do SEBC ao abrigo do Tratado e as competências do Eurosistema ao abrigo do Regulamento SIPS deveriam ser claramente enumeradas nos considerandos do regulamento proposto.

2.1.3 Pela mesma razão o BCE congratula-se com a exclusão, do âmbito de aplicação do quadro de fiscalização previsto no regulamento proposto, dos terceiros prestadores de serviços no domínio das TIC que estão sujeitos a quadros de fiscalização criados com a finalidade de apoiar as atribuições indicadas no artigo 127.º, n.º 2, do Tratado ([25]). A este respeito, o BCE gostaria de salientar que os bancos centrais do SEBC, quando atuam enquanto autoridades monetárias ([26]), e o Eurosistema, quando presta serviços através do TARGET2, TARGET2-Securites (*T2S*) ([27]) e do T*ARGET Instant Payment Settlement (TIPS*) ([28]) não estão sujeitos aos disposto no artigo referente ao âmbito de aplicação do regulamento proposto, nem podem ser considerados terceiros prestadores de serviços no domínio das TIC não podendo, por conseguinte, ser considerados, para efeitos do regulamento proposto, como terceiros prestadores de serviços de TIC críticos O Eurosistema supervisiona o T2S no âmbito do seu mandato de assegurar a eficiência e a solidez dos sistemas de compensação e de pagamentos. Além disso, a ESMA esclareceu que o T2S não é um prestador de serviços críticos ([29]) para efeitos do Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho ([30]) (a seguir «Regulamento CSD»). Por conseguinte, a segurança, a eficiência e a resiliência organizativas e operacionais do T2S são asseguradas mediante o quadro jurídico, regulamentar e operacional aplicável e dos mecanismos de governação acordados relativos ao T2S, em vez do Regulamento CSD.

2.1.4 Além disso, o quadro de política de superintendência do Eurosistema ([31]) abrange prestadores de serviços críticos, como a Society for Worldwide Interbank Financial Telecommunication (SWIFT). A SWIFT é uma sociedade cooperativa de responsabilidade limitada estabelecida na Bélgica, que presta serviços de transmissão segura de mensagens a nível internacional. O Nationale Bank van België/Banque Nationale de Belgique atua como autoridade fiscalizadora principal da SWIFT, exercendo, em cooperação com os outros bancos centrais do G10, incluindo o BCE, a superintendência da SWIFT com base num acordo de superintendência colaborativa. Os superintendentes do G10 reconhecem que o principal objetivo da sua fiscalização é o risco operacional da SWIFT, uma vez que esta é considerada a principal categoria de risco através do qual a SWIFT poderia representar um risco sistémico para o sistema financeiro da União. A este respeito, o *Cooperative Oversight Group* (grupo responsável pela fiscalização colaborativa) da SWIFT desenvolveu um conjunto específico de princípios e expectativas de alto nível aplicáveis à SWIFT, tais como a identificação e gestão de riscos, a segurança da informação, a fiabilidade e resiliência, o planeamento tecnológico e a comunicação com os utilizadores. Os superintendentes do G10 esperam que a SWIFT adira às orientações do Comité das Infraestruturas de Pagamento e do Mercado (CPMI) e da Organização Internacional das Comissões de Valores Mobiliários (IOSCO) em matéria de ciber-resiliência ([32]), bem como a outras normas internacionais em matéria de segurança das TIC, as quais, globalmente consideradas, excedem os requisitos estabelecidos no regulamento proposto.

2.1.5 Não é possível ter a certeza de que a SWIFT e, eventualmente, outros prestadores de serviços sujeitos ao regime de superintendência do Eurosistema não ficariam sujeitos ao regulamento proposto como prestadores terceiros de serviços no domínio das TIC, caso prestem serviços não abrangidos pelo artigo 127.º, n.º 2, do Tratado. Por conseguinte, o BCE congratula-se vivamente com o facto de os prestadores de serviços já sujeitos ao regime de superintendência do Eurosistema, incluindo, mas não exclusivamente, a SWIFT, serem excluídos do âmbito de aplicação do quadro de fiscalização estabelecido no regulamento proposto.

([25]) Ver o artigo 28.º, n.º 5, do regulamento proposto.

([26]) Ver o ponto 1.3 do Parecer do BCE, de 19 de fevereiro de 2021, sobre uma proposta de regulamento relativo aos mercados de criptoativos e que altera a Diretiva (UE) 2019/1937 (CON/2021/4). Todos os pareceres do BCE estão publicados no EUR-Lex.

([27]) Ver o anexo II-A da Orientação BCE/2012/27 do Banco Central Europeu, de 5 de dezembro de 2012, relativa a um sistema de transferências automáticas transeuropeias de liquidação por bruto em tempo real (TARGET2) (JO L 30 de 30.1.2013, p. 1); a Orientação BCE/2012/13 do Banco Central Europeu, de 18 de julho de 2012, relativa ao TARGET2-Securities (JO L 215 de 11.8.2012, p.19); e a Decisão BCE/2011/20 do Banco Central Europeu, de 16 de Novembro de 2011, que estabelece regras e procedimentos detalhados para implementação dos critérios de elegibilidade aplicáveis ao acesso das centrais de depósito de valores mobiliários aos serviços do TARGET2-Securities (JO L 319 de 2.12.2011, p. 117). Ver também a convenção-quadro T2S e a convenção coletiva.

([28]) Ver o anexo II-B da Orientação BCE/2012/27.

([29]) Ver o artigo 30.º, n.º 5, do Regulamento (UE) n.º 909/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 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) e o artigo 68.º do Regulamento Delegado (UE) 2017/392 da Comissão, de 11 de novembro de 2016, que complementa o Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas aos requisitos em matéria de autorização e supervisão e aos requisitos operacionais aplicáveis às Centrais de Valores Mobiliários (JO L 65 de 10.3.2017, p. 48).

([30]) Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 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).

([31]) *Eurosystem oversight policy framework* (Quadro da política de superintendência do Eurosistema), versão revista (julho de 2016) disponível [em inglês] no sítio *web* do BCE em www.ecb.europa.eu.

([32]) Disponível [em inglês] no sítio *web* do Banco de Pagamentos Internacionais, em www.bis.org.

2.2 *Competências no domínio da liquidação de títulos do SEBC*

2.2.1 As *CSD* (centrais de depósito de valores mobiliários) são infraestruturas dos mercados financeiros (IMF) estritamente regulamentadas e supervisionadas por diferentes autoridades nos termos do Regulamento CSD, o qual estabelece requisitos em matéria de liquidação de instrumentos financeiros e regras sobre a organização e a conduta das CSD. Além disso, as CSD devem levar em conta o *CPMI-IOSCO Guidance on cyber resilience* (Guia de ciber-resiliência CPMI-IOSCO), cujas orientações foram implementadas no documento *Cyber resilience oversight expectations for financial market infrastructures* (Expectativas de superintendência relativas à ciber-resiliência das infraestruturas do mercado financeiro, de dezembro 2018) ([33]). Para além das competências de supervisão atribuídas às autoridades nacionais competentes (ANC) nos termos do Regulamento CSD, os membros do SEBC atuam como «autoridades relevantes» na sua qualidade de superintendentes de sistemas de liquidação de valores mobiliários operados por CSD, de bancos centrais que emitem as moedas mais relevantes em que a liquidação tem lugar e, ainda, de bancos centrais em cujos livros é liquidada a componente de numerário das transações ([34]). A este respeito, o considerando 8 do Regulamento CSD refere que a aplicação deste não deverá prejudicar as responsabilidades que cabem ao BCE e aos bancos centrais nacionais de assegurar a eficiência e a solidez dos sistemas de compensação e de pagamentos na União e noutros países O mesmo considerando refere ainda que o Regulamento CSD não deverá impedir o acesso dos membros do SEBC às informações relevantes para o desempenho das suas funções ([35]), incluindo o exercício da superintendência das CSD e de outras IMF ([36]).

2.2.2 Além disso, os membros do SEBC atuam frequentemente como agentes de liquidação relativamente à componente de numerário das transações de valores mobiliários e o Eurosistema oferece serviços de liquidação através do T2S às CSD. A superintendência do T2S pelo Eurosistema está relacionada com o seu mandato de garantia da eficiência e solidez dos sistemas de compensação e de pagamentos, enquanto que as autoridades competentes e relevantes das CSD visam assegurar o seu bom funcionamento, a segurança e eficiência da liquidação e o bom funcionamento dos mercados financeiros nas respetivas jurisdições.

2.2.3 Nos termos do regulamento proposto ([37]), os bancos centrais do SEBC não estão envolvidos na elaboração de normas técnicas no que diz respeito à especificação do risco associado à TIC. Do mesmo modo, nos termos do regulamento proposto, ([38]) as autoridades competentes não são informadas de quaisquer incidentes relacionados com as TIC. O banco central do SEBC deve manter o mesmo nível de envolvimento que o atualmente previsto no Regulamento CSD, devendo as autoridades competentes ser notificadas de incidentes relacionados com as TIC. O Eurosistema é a autoridade relevante para todas as CSD da área do euro e para várias outras CSD da UE. Os bancos centrais do SEBC teriam de ser informados sobre incidentes relacionados com o TIC que sejam relevantes para o desempenho das suas funções, incluindo a superintendência das CSD e de outras IMF. Os riscos a que as CSD estão expostas, incluindo os riscos associados às TIC, podem ameaçar o bom funcionamento das CSD. Por conseguinte, os riscos associados às TIC são importantes para as autoridades competentes, que devem dispor de uma panorâmica completa e pormenorizada desses riscos, a fim de os avaliar e influenciar a abordagem de gestão de riscos das CSD. O regulamento proposto não deve prever requisitos menos restritivos no que diz respeito aos riscos associados às TIC em comparação com os previstos no Regulamento CSD e nas atuais normas técnicas de regulamentação conexas.

2.2.4 Além disso, os órgãos legislativos da União deveriam clarificar a interação entre o regulamento proposto ([39]) e as normas técnicas de regulamentação que complementam o regulamento CSD. Não está claro, nomeadamente, se uma CSD deve ser dispensada da obrigação de manter o seu próprio local secundário de tratamento de dados no mesmo local em que o seu terceiro prestador de serviços no domínio das TIC mantenha o seu próprio local de tratamento de dados ([40]). Se uma CSD estiver isenta da obrigação de manter

([33]) Disponível no sítio *web* do BCE em www.ecb.europa.eu.

([34]) Ver o artigo 12.º do Regulamento (UE) n.º 909/2014.

([35]) Ver também o artigo 13.º, o artigo 17.º, n.º 4, e o artigo 22.º, n.º 6, do Regulamento (UE) n.º 909/2014.

([36]) Ver o ponto 7.3 do Parecer do Banco Central Europeu, de 6 de abril de 2017, sobre a identificação de infraestruturas essenciais para a segurança informática (CON/2017/10); o ponto 7.2 do Parecer do Banco Central Europeu, de 8 de novembro de 2018, sobre a designação dos serviços essenciais e dos operadores desses serviços para fins de segurança das redes e dos sistemas de informação (CON/2018/47); o ponto 3.5.2 do Parecer do Banco Central Europeu, de 2 de maio de 2019, sobre a segurança das redes e dos sistemas de informação (CON/2019/17); bem como o ponto 3.5.2 do Parecer do Banco Central Europeu, de 11 de novembro de 2019, sobre a segurança das redes e sistemas informáticos (CON/2019/38).

([37]) Ver o artigo 54.º, n.º 5, do regulamento proposto e o artigo 45.º, n.º 7, do Regulamento (UE) n.º 909/2014.

([38]) Ver o artigo 54.º, n.º 4, do regulamento proposto e o artigo 45.º, n.º 6, do Regulamento (UE) n.º 909/2014.

([39]) Ver o artigo 11.º, n.º 5, do regulamento proposto.

([40]) Ver o artigo 78.º, n.º 3, do Regulamento Delegado (UE) 2017/392 da Comissão, de 11 de novembro de 2016, que complementa o Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas aos requisitos em matéria de autorização e supervisão e aos requisitos operacionais aplicáveis às Centrais de Valores Mobiliários (JO L 65 de 10.3.2017, p. 48).

um sítio secundário, não se percebe qual seria o valor jurídico deste requisito. Seguindo a mesma linha de raciocínio, o regulamento proposto ([41]) faz referência a um objetivo temporal de recuperação e a objetivos de ponto de recuperação para cada função ([42]), ao passo que a norma técnica regulamentar pertinente estabelece uma distinção entre funções críticas ([43]) e operações críticas ([44]) em relação ao tempo de recuperação fixado para as operações críticas das CSD. Justifica-se uma maior clarificação e reflexão por parte dos órgãos legislativos da União sobre a interação entre o regulamento proposto e as normas técnicas de regulamentação que complementam o Regulamento CSD, para evitar o risco de requisitos contraditórios. Por último, importa esclarecer que o regulamento proposto alarga as isenções concedidas pelo Regulamento CSD ([45]) às CSD operadas por determinadas entidades públicas.

2.3 *Competências do SEBC no domínio da compensação de títulos*

2.3.1 Os bancos centrais do SEBC gozam de poderes de superintendência em relação às contrapartes centrais (CP). Nesta matéria, os bancos centrais nacionais do Eurosistema cooperam frequentemente com as autoridades nacionais competentes relevantes na superintendência e supervisão das CP e participam no respetivo colégio de CP criado ao abrigo do Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho ([46]) (a seguir «*EMIR* »- *European Market Infrastructure Regulation*). Os membros relevantes do Eurosistema ([47]) participam nos colégios EMIR na sua qualidade de superintendentes. e representam o Eurosistema como banco central emissor em relação às CP em que o euro seja uma das moedas mais relevantes para os instrumentos financeiros compensados (e, também, para as CP *offshore* que compensam uma proporção significativa de instrumentos financeiros em euros). O BCE é o banco central emissor para as CP não pertencentes à área do euro.

2.3.2 Nos termos do regulamento proposto ([48]) os bancos centrais do SEBC não estão envolvidos na elaboração de normas técnicas no que diz respeito à especificação do risco associado às TIC. Além disso, o regulamento proposto ([49]) não contém qualquer referência ao objetivo do prazo de recuperação nem aos requisitos relativos ao ponto de recuperação estabelecidos no EMIR ([50]). A estrutura regulamentar proposta não deve prever requisitos menos restritivos do que os atuais em matéria de riscos associados às TIC. Por conseguinte, é fundamental definir objetivos claros em termos de calendário e de pontos de recuperação, a fim de se dispor de um quadro sólido de gestão da continuidade da atividade. A manutenção de objetivos específicos em matéria de prazos e pontos de recuperação faz igualmente parte dos Princípios CPMI-IOSCO para as Infraestruturas do Mercado Financeiro ([51]). Deve manter-se a atual disposição do EMIR, e adaptar em conformidade o regulamento proposto. Os bancos centrais do SEBC deveriam ser envolvidos na preparação de qualquer legislação secundária, bem como numa maior clarificação e reflexão por parte dos órgãos legislativos da União sobre a interação entre o regulamento proposto e as normas técnicas de regulamentação complementares, para prevenir o risco de requisitos contraditórios ou duplicados.

3. **Observações específicas sobre aspetos de supervisão prudencial**

3.1 O Regulamento do Conselho (UE) n.º 1024/2013 ([52]) (a seguir «Regulamento MUS») confere ao BCE atribuições específicas no que diz respeito à supervisão prudencial das instituições de crédito na área do euro, e responsabiliza o BCE pelo funcionamento eficaz e coerente do Mecanismo Único de Supervisão (MUS), no âmbito do qual responsabilidades específicas de supervisão prudencial são repartidas entre o BCE e as ANC participantes. Ao BCE compete, em particular, autorizar e revogar as autorizações de todas as instituições de crédito. O BCE tem também por missão, designadamente, assegurar o cumprimento da legislação aplicável da União que impõe requisitos prudenciais às instituições de crédito, incluindo a obrigação de dispor de mecanismos de governação sólidos, tais como processos de gestão do risco robustos e mecanismos de controlo interno ([53]). Para o efeito, são conferidos ao

([41]) Ver o artigo 11.º, n.º 6, do regulamento proposto.
([42]) Ver o artigo 3.º n.º 17, do regulamento proposto.
([43]) Ver o artigo 76.º, n.º 2, alíneas d) e e), do Regulamento Delegado (UE) 2017/392 da Comissão.
([44]) Ver o artigo 78.º, n.ºs 2 e 3, do Regulamento Delegado (UE) 2017/392 da Comissão.
([45]) Ver o artigo 1.º, n.º 4, do Regulamento (UE) n.º 909/2014.
([46]) 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).
([47]) Ver artigo 18.º, n.º 2, alíneas g) e h), do EMIR.
([48]) Ver o artigo 53.º, n.º 2, alínea b), e n.º 3, do regulamento proposto, e o artigo 34.º, n.º 3, do EMIR.
([49]) Ver o artigo 53.º, n.º 2, alínea a), do regulamento proposto.
([50]) Ver o artigo 34.º do EMIR.
([51]) Ver os Princípios para as infraestruturas dos mercados financeiros do CPMI-IOSCO, disponíveis [em inglês] no sítio *web* do Banco de Pagamentos Internacionais em www.bis.org.
([52]) 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).
([53]) Ver o artigo 4.º, n.º 1, alínea e), e o artigo 6.º, n.º 4, do Regulamento (UE) n.º 1024/2013.

BCE todos os poderes de supervisão para intervir na atividade das instituições de crédito necessárias ao exercício das suas funções. O BCE e as ANC relevantes são, por conseguinte, as autoridades competentes que exercem poderes específicos de supervisão prudencial ao abrigo do Regulamento 2013/575/UE do Parlamento Europeu e do Conselho ([54]) (a seguir designado «Regulamento Requisitos de Fundos Próprios») e da Diretiva 2013/36/UE do Parlamento Europeu e do Conselho ([55]) (a seguir designada «Diretiva Requisitos de Fundos Próprios»).

3.2 O regulamento proposto estabelece que o conjunto único de regras («*single rulebook*») e o sistema de supervisão devem continuar a ser desenvolvidos para passarem a incluir a resiliência operacional digital e a segurança das TIC, mediante o reforço dos mandatos dos supervisores financeiros encarregados de acompanhar e proteger a estabilidade financeira e a integridade do mercado ([56]). O objetivo é promover um quadro abrangente em matéria de TIC ou de risco operacional através da harmonização dos principais requisitos de resiliência operacional digital e sua aplicação a todas as entidades financeiras ([57]). Mais concretamente, o regulamento proposto visa consolidar e atualizar os requisitos em matéria de risco no domínio das TIC que, até à data, têm sido abordados de forma isolada em diferentes atos legislativos ([58]).

3.3 Os requisitos relacionados com o risco das TIC para o setor financeiro estão atualmente dispersos por vários atos legislativos da União, incluindo a Diretiva Requisitos de Fundos Próprios, e instrumentos jurídicos não vinculativos (como as orientações da EBA), e revelam-se diversos e, ocasionalmente, incompletos. Em alguns casos, o risco das TIC foi apenas implicitamente abordado como parte do risco operacional, ao passo que noutros não foi abordado de todo. Esta situação deve ser corrigida através do alinhamento do regulamento proposto e com os referidos atos. Para o efeito, a proposta de diretiva de alteração apresenta um conjunto de alterações que se afiguram necessárias para conferir clareza e coerência jurídicas à aplicação dos vários requisitos de resiliência operacional digital. No entanto, as alterações à Diretiva Requisitos de Fundos Próprios agora sugeridas pela diretiva de alteração proposta ([59]) referem-se apenas às disposições relativas aos planos de contingência ([60]), e de continuidade da atividade, uma vez que, alegadamente, os mesmos servem implicitamente de base para abordar a gestão do risco associado à TIC.

3.4 Além disso, o regulamento proposto ([61]) prevê que as entidades financeiras, incluindo as instituições de crédito, devem dispor de quadros de governação e controlo internos que assegurem uma gestão eficaz e prudente de todos os riscos associados às TIC. O regulamento proposto ([62]) prevê a aplicação, a nível individual e consolidado, dos requisitos nele estabelecidos, mas sem coordenação suficiente com a legislação setorial específica referida. Por último, o regulamento proposto ([63]) prevê que, sem prejuízo das disposições relativas ao quadro de superintendência dos terceiros prestadores de serviços de TIC críticos referidos no regulamento proposto ([64]), o cumprimento das obrigações nele estabelecidas seja assegurado, no que se refere às instituições de crédito, pela autoridade competente designada nos termos do artigo 4.º da Diretiva Requisitos de Fundos Próprios, sem prejuízo das atribuições específicas conferidas ao BCE pelo Regulamento MUS.

3.5 Tendo em conta o que precede, o BCE entende que, em relação às instituições de crédito, e com exceção das disposições do regulamento proposto relativas ao quadro de fiscalização aplicável a terceiros prestadores de serviços de TIC críticos ([65]), o regulamento proposto pretende estabelecer um quadro de governação interna prudencial para a gestão do risco das TIC, integrado no quadro geral de governação interna ao abrigo da Diretiva Requisitos de Fundos Próprios. Além disso, dada a natureza prudencial do quadro proposto, as autoridades competentes responsáveis pela supervisão do cumprimento das obrigações estabelecidas no quadro proposto, incluindo o BCE, serão as autoridades responsáveis pela supervisão bancária em conformidade com o Regulamento MUS.

([54]) Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 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).

([55]) 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 e empresas de investimento, 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).

([56]) Ver o considerando 8 do regulamento proposto.

([57]) Ver o considerando 11 do regulamento proposto.

([58]) Ver o considerando 12 do regulamento proposto.

([59]) Ver os considerandos 4 e 5 da diretiva de alteração proposta.

([60]) Ver o artigo 85.º da Diretiva Requisitos de Fundos Próprios.

([61]) Ver o artigo 4.º, n.º 1, do regulamento proposto.

([62]) Ver o artigo 25.º, n.ºs 3 e 4, do regulamento proposto.

([63]) Ver o artigo 41.º do regulamento proposto.

([64]) Ver o Capítulo V, Secção II do regulamento proposto.

([65]) Ver o Capítulo V, Secção II do regulamento proposto.

3.6 Assim sendo, e para aumentar a clareza e a coordenação entre o regulamento proposto e a Diretiva Requisitos de Fundos Próprios, os órgãos legislativos da União poderão querer levar em conta as seguintes sugestões: Em primeiro lugar, os requisitos previstos no regulamento proposto poderiam ser expressamente qualificados de prudenciais, tal como foi feito, nomeadamente, no Regulamento CSD ([66]). Em segundo lugar, os considerandos da diretiva de alteração proposta ([67]) poderiam ter uma redação mais genérica, uma vez que os requisitos previstos no regulamento proposto vão além da única fase dos planos de contingência e de continuidade das atividades. As medidas de governação do risco associado à TIC, em geral, inserem-se no âmbito mais geral dos mecanismos de governação sólidos nos termos do artigo 74.º da Diretiva Requisitos de Fundos Próprios ([68]). Em terceiro lugar, o regulamento proposto ([69]) deveria ser alterado a fim de recordar, nos considerandos, a competência do BCE no que toca à supervisão prudencial das instituições de crédito ao abrigo do Tratado e do Regulamento MUS. Em quarto lugar, a referência à aplicação a nível individual e consolidado dos requisitos nela previstos ([70]) deve ser revista, uma vez que os níveis subconsolidado e consolidado não estão definidos no regulamento proposto, e que determinados tipos de intermediários não estão sujeitos a supervisão numa base consolidada ao abrigo da legislação pertinente (por exemplo, instituições de pagamento). Além disso, o nível de aplicação dos requisitos previstos no regulamento proposto deve derivar, exclusivamente, da legislação aplicável a cada tipo de entidade financeira. No caso das instituições de crédito, está prevista uma ligação clara entre a Diretiva Requisitos de Fundos Próprios e o regulamento proposto, pelo que os requisitos previstos no regulamento proposto seriam automaticamente aplicáveis a nível individual, subconsolidado ou consolidado ([71]),consoante o caso. Por último, os órgãos legislativos da União poderiam considerar a possibilidade de prever um regime transitório para gerir o período compreendido entre a entrada em vigor do regulamento proposto e a entrada em vigor das normas técnicas de regulamentação previstas no regulamento proposto, dado que alguns intermediários, incluindo as instituições de crédito, já estão sujeitos a regras sobre os riscos associados às TIC aplicáveis a setores específicos, e são mais pormenorizadas do que as disposições gerais do regulamento proposto.

3.7 Ao abrigo do Regulamento MUS, foi confiada ao BCE a missão de assegurar o cumprimento, por parte das instituições de crédito, dos requisitos da legislação da União que exigem que as instituições de crédito disponham de processos sólidos de gestão de riscos e de mecanismos de controlo interno ([72]). Tal significa que o BCE deve zelar para que as instituições apliquem políticas e procedimentos destinados a avaliar e gerir a respetiva exposição ao risco operacional, incluindo o risco associado aos modelos financeiros, incluindo os acontecimentos de reduzida frequência, mas de grande impacto. As instituições devem definir o que entendem por risco operacional para efeitos das referidas políticas e procedimentos ([73]).

3.8 Em julho de 2017, o Conselho do Banco Central Europeu (BCE) adotou o *MUS Cyber Incident Reporting Framework* (Quadro de reporte de ciberincidentes no âmbito do MUS (a seguir designado por «Quadro») com base num projeto de proposta do Conselho de Supervisão de acordo com os artigos 26.º, n.º 8 e do artigo 6.º, n.º 2, do Regulamento MUS e do artigo 21.º, n.º 1, do Regulamento (UE) n.º 468/2014 do Banco Central Europeu (BCE/2014/17) ([74]). O referido quadro consiste num pedido vinculativo (decisões individuais dirigidas a instituições de crédito) de informação e/ou comunicação de informações na base do artigo 10.º do Regulamento MUS ([75]). Alguns países já dispõem de um processo de comunicação de incidentes, exigindo que as instituições de crédito comuniquem todos os ciberincidentes significativos às respetivas ANC. Nesses países, as instituições de crédito significativas

([66]) Ver título do Capítulo II, Secção 4, «Requisitos prudenciais» do Regulamento CSD.

([67]) Ver o considerando 4 da diretiva de alteração proposta.

([68]) O artigo 85.º da Diretiva 2013/36/UE é uma mera especificação. A este respeito, ver também as páginas 4, 11 e 37 das Orientações da Autoridade Bancária Europeia relativas à gestão dos riscos associados às TIC e à segurança (*EBA Guidelines on ICT and security risk management*), de 29 de novembro de 2019 (a seguir designadas «Orientações da EBA»), cuja base jurídica geral consta expressamente do artigo 74.º da Diretiva 2013/36/UE.

([69]) Ver o artigo 41.º, n.º 1, do regulamento proposto.

([70]) Ver o artigo 25.º, n.ºs 3 e 4, do regulamento proposto.

([71]) Ver o artigo 109.º da Diretiva Requisitos de Fundos Próprios.

([72]) Ver o artigo 4.º, n.º 1, alínea e), do Regulamento do MUS.

([73]) Ver o artigo 85.º da Diretiva Requisitos de Fundos Próprios.

([74]) Regulamento (UE) n.º 468/2014 do Banco Central Europeu, de 16 de abril de 2014, que estabelece o quadro de cooperação, no âmbito do Mecanismo Único de Supervisão, entre o Banco Central Europeu e as autoridades nacionais competentes e com as autoridades nacionais designadas (Regulamento-Quadro do MUS) (BCE/2014/17) (JO L 141 de 14.5.2014, p. 1).

([75]) Um ciberincidente – isto é, uma possível violação da segurança da informação (tanto de caráter malicioso como acidental) identificada – deve ser reportado ao BCE, caso se verifique, pelo menos, uma das seguintes condições: 1) o incidente tem um potencial impacto financeiro de 5 milhões de euros ou 0,1% dos fundos próprios principais de nível 1; 2) o incidente foi divulgado publicamente ou causa danos reputacionais; 3) o incidente foi comunicado ao responsável pelos sistemas de informação (*CIO*) fora do processo de reporte regular; 4) a instituição de crédito notificou o incidente à equipa de resposta a emergências informáticas (CERT)/à equipa de resposta a incidentes de segurança informática (CSIRT), a uma agência de segurança ou à polícia; 5) foram acionados procedimentos de recuperação em caso de catástrofe ou de continuidade da atividade, ou solicitada uma indemnização de seguro por ciberincidente; 6) ocorreu uma violação de requisitos legais ou regulamentares; ou 7) a instituição de crédito utiliza critérios internos e apreciações de especialistas (incluindo sobre um potencial impacto sistémico) e decide informar o BCE.

continuarão a comunicar os incidentes às ANC que, em nome das entidades supervisionadas, os transmitirão, sem demora injustificada, ao BCE. Por conseguinte, as decisões acima referidas são também dirigidas a estas autoridades nacionais competentes, as quais devem transmitir essa informação ao BCE também com base no Quadro. O BCE apoia os esforços dos órgãos legislativos da União para promover a harmonização e a racionalização, nomeadamente no que diz respeito ao conjunto de regras e obrigações aplicáveis às instituições de crédito em matéria de comunicação de incidentes. Tendo em conta o que precede, o BCE está disposto a alterar (e, potencialmente, revogar) o Quadro, se necessário, à luz da eventual adoção do regulamento proposto.

4. **Observações específicas sobre a gestão de riscos associados às TIC, a comunicação de incidentes, os testes de resiliência operacional e o risco de terceiros no domínio das TIC**

4.1 *Gestão do risco associado às TIC*

4.1.1 O BCE congratula-se com a introdução, pelo regulamento proposto, de um quadro sólido e abrangente de gestão do risco associado às TIC, que engloba as orientações do CPMI-IOSCO em matéria de ciber-resiliência e está estreitamente alinhado com as melhores práticas, incluindo as Expectativas de superintendência relativas às ciber--resiliência quanto às infraestruturas do mercado financeiro.

4.1.2 O BCE apoia a noção de que as entidades financeiras deveriam ter de realizar avaliações de risco relativamente a cada «grande alteração» na infraestrutura da rede e do sistema de informação respetivos ([76]). Dito isto, o regulamento proposto não contém qualquer definição de «alteração importante», criando uma margem indesejável para interpretações divergentes por parte das entidades financeiras, o que poderia, em última análise, prejudicar os objetivos de harmonização do regulamento proposto. Por razões de segurança jurídica, os órgãos legislativos da União poderão querer considerar a introdução de uma definição de «alteração importante» no regulamento proposto.

4.1.3 De um modo geral, o BCE apoia a ideia de que as entidades financeiras que não sejam microempresas devem comunicar às autoridades competentes os custos e perdas relevantes causados por perturbações das TIC e incidentes relacionados com as TIC ([77]). No entanto, a fim de assegurar a eficácia global do sistema e evitar sobrecarregar as autoridades competentes e as entidades financeiras com um número excessivo de relatórios, a introdução de limiares relevantes, possivelmente de natureza quantitativa, poderia ser explorada de forma útil pelos órgãos legislativos da União.

4.1.4 O BCE reconhece a possibilidade de as entidades financeiras delegarem em empresas intragrupo ou externas as funções de verificação do cumprimento dos requisitos de gestão de riscos associados às TIC, mediante aprovação pelas autoridades competentes ([78]). Ao mesmo tempo, é importante que os órgãos legislativos da União clarifiquem a forma como é que as autoridades competentes concederiam a sua aprovação quando uma entidade financeira estiver sujeita a várias autoridades competentes. Tal pode acontecer se a entidade financeira for, simultaneamente, uma instituição de crédito, um prestador de serviços criptoativos e/ou um prestador de serviços de pagamento. Por último, no que diz respeito à identificação e classificação a efetuar pelas entidades financeiras nos termos do regulamento proposto ([79]), o BCE considera prudente, para efeitos da classificação dos ativos, que o regulamento proposto exija igualmente que as entidades financeiras tenham em conta o carácter crítico desses ativos (ou seja, se apoiam funções críticas).

4.2 *Notificação de incidentes*

4.2.1 O BCE congratula-se com os esforços delineados no regulamento proposto para harmonizar o panorama de comunicação de incidentes nas TIC na União e trabalhar no sentido de uma comunicação centralizada dos principais incidentes relacionados com as TIC ([80]). A introdução de um quadro harmonizado para a comunicação de incidentes graves relacionados com as TIC ([81]) às autoridades competentes simplificaria e harmonizaria, em princípio, os encargos em matéria de comunicação de informações das entidades financeiras, incluindo as instituições de crédito. As autoridades competentes beneficiariam do conhecimento de um maior âmbito dos incidentes abrangidos, para além dos incidentes relacionados com o ciberespaço atualmente abrangidos pelos quadros existentes ([82]). A futura adoção do regulamento proposto exigiria a revisão e a eventual revogação dos quadros existentes, incluindo o quadro de comunicação de incidentes de cibersegurança do MUS. Dito isto, a fim de conseguir uma verdadeira racionalização e harmonização total de todos os enquadramentos, é fundamental assegurar que o âmbito de aplicação das disposições relativas à comunicação de incidentes ao abrigo do

([76]) Ver o artigo 7.º, n.º 3, do regulamento proposto.
([77]) Ver o artigo 10.º, n.º 9, do regulamento proposto.
([78]) Ver o artigo 5.º, n.º 10, do regulamento proposto.
([79]) Ver o artigo 7.º do regulamento proposto.
([80]) Ver o artigo 19.º do regulamento proposto.
([81]) Ver os artigos 3.º, n.º 7, 17.º e 18.º do regulamento proposto.
([82]) Ver, por exemplo, o Quadro.

regulamento proposto, incluindo todas as definições, limiares e parâmetros de comunicação pertinentes, esteja plenamente alinhado com os quadros pertinentes. Em especial, é da maior importância assegurar o alinhamento entre, por um lado, o regulamento proposto e, por outro, a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho ([83]) (a seguir designada por «DSP2») e as Orientações da EBA relativas à comunicação de incidentes graves (a seguir designadas «Orientações da EBA»). A diretiva de alteração proposta ([84]) contém alterações à DSP2 no que diz respeito à delimitação da comunicação de incidentes entre o regulamento proposto e a DSP2, a qual afetaria principalmente os prestadores de serviços de pagamento, que também poderiam ser autorizados como instituições de crédito, bem como as autoridades competentes. O processo de notificação de incidentes não é claro, e pode haver sobreposição de alguns dos incidentes que têm de ser comunicados ao abrigo do regulamento proposto e das Orientações da EBA.

4.2.2 Os processos de notificação de incidentes graves ao abrigo, respetivamente, do regulamento proposto ([85]), da DSP2 e das correspondentes Orientações da EBA, exigiriam que os prestadores de serviços de pagamento apresentassem um relatório de incidente à respetiva autoridade competente após a classificação do incidente. Com efeito, os relatórios iniciais não captam a essência, a causa ou a área funcional afetada pelo incidente, e os prestadores de serviços de pagamento poderão só estar em condições de efetuar essas distinções numa fase posterior, quando estiverem disponíveis informações mais pormenorizadas sobre o incidente. Em consequência, os relatórios de incidentes iniciais poderiam ser apresentados tanto ao abrigo do regulamento proposto como das orientações da EBA, ou os prestadores de serviços de pagamento poderiam decidir sobre um quadro único de comunicação de informações e corrigir a sua apresentação numa data posterior. A mesma incerteza (no que diz respeito, por exemplo, à causa principal de qualquer incidente) pode também refletir-se nos relatórios intercalar e final. Tal aumentaria, mais uma vez, o potencial de apresentação paralela de relatórios às autoridades competentes ao abrigo do regulamento proposto e da DSP2.

4.2.3 Alguns incidentes que podem ser classificados como incidentes relacionados com as TIC podem também ter impacto noutras áreas, pelo que teriam de ser notificados ao abrigo das orientações da EBA. Pode ser esse o caso quando um incidente tem impacto do ponto de vista das TIC, mas, ao mesmo tempo, também afetou diretamente a prestação de serviços de pagamento, e/ou outras áreas funcionais ou canais não relacionados com as TIC. Além disso, poderá haver casos em que não seja possível distinguir entre incidentes operacionais e incidentes relacionados com as TIC. Acresce que, no caso de a mesma entidade financeira ser uma instituição de crédito significativa e de um prestador de serviços de pagamento, nos termos do regulamento proposto essa entidade teria de comunicar o incidente relacionado com as TIC duas vezes, ficando sujeita a duas autoridades competentes. Tendo em conta o que precede, o regulamento proposto deve especificar de forma mais clara a forma como se pretende que funcione, na prática, a interação entre a DSP2 e as Orientações da EBA. Mas, sobretudo, seria importante, por razões de harmonização e racionalização das obrigações de comunicação, que os órgãos legislativos da União refletissem sobre questões residuais de dupla comunicação, e que esclarecesse se o regulamento proposto, por um lado, e as orientações da DSP2 e EBA, por outro, irão coexistir, ou se deveria haver um conjunto único de requisitos de comunicação de incidentes.

4.2.4. O regulamento proposto introduz a obrigação para as autoridades competentes ([86]) de, após a receção de um relatório, acusarem a receção da notificação e, o mais rapidamente possível, fornecerem todas as informações ou orientações necessárias à entidade financeira, em especial para discutir as medidas corretivas a nível da entidade ou formas de minimizar o impacto negativo em todos os setores. Tal significaria que as autoridades competentes deveriam contribuir ativamente para a gestão e a reparação de incidentes e, ao mesmo tempo, avaliar a resposta de uma entidade supervisionada a incidentes críticos. O BCE salienta que a responsabilidade e a titularidade da reparação e as consequências de um incidente devem caber exclusiva e claramente à entidade financeira em causa. O BCE proporia, por conseguinte, limitar o retorno de informação e as orientações apenas às reações e orientações prudenciais de alto nível. Se o retorno de informação fosse mais amplo, exigiria profissionais especializados com conhecimentos técnicos muito consideráveis, normalmente não disponíveis na reserva de talentos à disposição das autoridades prudenciais.

4.3 *Ensaio de resiliência operacional digital*

4.3.1 O BCE congratula-se com os requisitos estabelecidos no regulamento proposto ([87]) relativo aos testes de resiliência operacional digital de todas as entidades financeiras, e com a necessidade de cada instituição dispor do seu próprio programa de testes. O regulamento proposto ([88]) descreve diferentes tipos de testes como indicativos para as

([83]) 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).

([84]) Ver o artigo 7.º, n.º 9, da diretiva proposta.

([85]) Ver o artigo 17.º, n.º 3, do regulamento proposto.

([86]) Ver o artigo 20.º do regulamento proposto.

([87]) Ver os artigos 21.º e 22.º do regulamento proposto.

([88]) Ver o artigo 22.º, n.º 1, do regulamento proposto.

entidades financeiras. Os tipos de testes não são muito claros e alguns testes, tais como testes de compatibilidade, questionários ou testes baseados em cenários, são suscetíveis de interpretação pelas AES, autoridades competentes ou entidades financeiras. Além disso, também não há orientações quanto à frequência de cada teste. Uma abordagem possível seria que o regulamento proposto estabelecesse requisitos genéricos em matéria de testes, com uma descrição mais precisa dos tipos de testes definidos nas normas técnicas de regulamentação e de execução.

4.3.2 Os testes de penetração baseados em ameaças (*Threat-led penetration testing*/TLPT) são um instrumento poderoso para testar as defesas de segurança e o grau de preparação. Por conseguinte, o BCE incentiva o emprego de TLPT por parte de entidades financeiras. Com esta ferramenta, são testadas não só medidas técnicas, mas também pessoal e processos. Os resultados destes testes podem aumentar significativamente a sensibilização dos quadros superiores das entidades testadas para aspetos de segurança. O quadro europeu para a comunicação de informação baseada nas ameaças digitais (*European Framework for Threat Intelligence Based Ethical Red-teaming (TIBER-EU)* ([89]) e outras ferramentas TLPT já disponíveis, fora da União, são instrumentos fundamentais para as próprias entidades avaliarem, testarem, praticarem e melhorarem a sua atitude e defesas em matéria de ciber-resiliência.

4.3.3 Na maioria dos Estados-Membros em que o TIBER-UE foi implementado, os superintendentes e supervisores não desempenham um papel ativo na execução de um programa TIBER-XX localizado, e a Equipa Tiber Cyber (TCT) opera, em quase todos os casos, independentemente destas funções. Por este motivo, os testes avançados contemplados no regulamento proposto ([90]), mediante TLPT, devem ser implementados não como um mero instrumento de supervisão, mas como um instrumento para reforçar o ecossistema financeiro e reforçar a estabilidade financeira, Além disso, não é necessário desenvolver um novo quadro avançado de testes de ciber--resiliência, uma vez que já muitos Estados-Membros adotaram o TIBER-EU, , o único quadro atualmente existente na UE.

4.3.4 Os requisitos aplicáveis aos testadores não devem constar do texto principal do regulamento proposto, uma vez que o setor relacionado com TLTP ainda está a desenvolver-se, e a inovação pode ser dificultada pela imposição de requisitos específicos. Posto isto, o BCE considera que, a fim de assegurar um elevado grau de independência na realização de testes, as entidades financeiras não devem empregar ou contratar testadores que sejam empregados de, ou contratados por entidades financeiras do seu próprio grupo, ou de alguma outra forma detidas e/ou controladas pelas entidades financeiras a testar.

4.3.5 A fim de reduzir o risco de fragmentação e assegurar a harmonização, o regulamento proposto deve prever um quadro TLPT aplicável ao setor financeiro em toda a União. A fragmentação pode conduzir a um aumento dos custos e das necessidades de recursos técnicos, operacionais e financeiros, tanto para as autoridades competentes como para as instituições financeiras. Estes custos e requisitos acrescidos podem, em última análise, ter um impacto negativo no reconhecimento mútuo dos testes. Esta falta de harmonização e as consequentes questões de reconhecimento mútuo revestem-se de particular importância para as entidades financeiras, que podem ser titulares de múltiplas licenças e/ou operar em várias jurisdições em toda a União. As normas técnicas de regulamentação e de execução, que deverão ser elaboradas para o TLPT ao abrigo do regulamento proposto, deveriam estar em conformidade com o TIBER-UE. Além disso, o BCE encara com agrado a oportunidade de participar na preparação destas normas técnicas de regulamentação e de execução, em cooperação com as AES.

4.3.6 A participação ativa das autoridades competentes nos testes pode resultar num potencial conflito de interesses com as outras funções que desempenham, ou seja, a avaliação do quadro de testes da entidade financeira. Neste contexto, o BCE propõe suprimir do regulamento proposto qualquer obrigação para as autoridades competentes no que respeita à validação de documentos e à emissão de um certificado de teste TLPT.

4.4 Risco de terceiros no domínio das TIC

4.4.1 O BCE congratula-se com a introdução de um conjunto abrangente de princípios fundamentais e de um sólido quadro de fiscalização para identificar e gerir os riscos associados às TIC de terceiros prestadores de serviços no domínio das TIC, independentemente de pertencerem, ou não, ao mesmo grupo de entidades financeiras. Dito isto, para conseguir uma identificação e gestão eficazes do risco associado à TIC, é importante identificar e classificar corretamente, nomeadamente, os terceiros prestadores de serviços de TIC críticos. A este respeito, embora seja de saudar a introdução de atos delegados ([91]) que complementarão os critérios a utilizar para fins de classificação ([92]), o BCE deve ser consultado antes da adoção desses atos delegados.

([89]) Disponível no sítio *web* do BCE em www.ecb.europa.eu.
([90]) Artigos 23.º e 24.º do regulamento proposto.
([91]) Ver o artigo 28.º, n.º 3, do regulamento proposto.
([92]) Ver o artigo 28.º, n.º 2, do regulamento proposto.

4.4.2 No que diz respeito à estrutura do quadro de superintendência ([93]), é necessário clarificar melhor o papel a desempenhar pelo Comité Misto. Paralelamente, o BCE congratula-se com a sua inclusão no Fórum de Fiscalização como observador, uma vez que este papel proporcionará ao BCE o mesmo acesso à documentação e à informação que os membros com direito de voto ([94]). O BCE gostaria de chamar a atenção dos órgãos legislativos da União para o facto de, na sua qualidade de observador, contribuir para o trabalho do Fórum de Fiscalização, tanto na sua qualidade de banco central emissor, com responsabilidade pela superintendência das infraestruturas de mercado, como como supervisor prudencial das instituições de crédito. Além disso, o BCE observa que, para além de ser observador no Fórum de Fiscalização, enquanto autoridade competente também fará parte da equipa de análise conjunta. A este respeito, os órgãos legislativos da União poderiam continuar a refletir sobre a composição das equipas de exame conjuntas ([95]), a fim de assegurar uma participação adequada das autoridades competentes relevantes. Do mesmo modo, o BCE considera que o número máximo de participantes nas equipas de exame conjuntas deve ser aumentado, tendo em conta a importância crítica, a complexidade e o âmbito dos serviços de terceiros no domínio das TIC.

4.4.3 O BCE observa que, nos termos do regulamento proposto, a autoridade fiscalizadora principal pode impedir que terceiros prestadores de serviços de TIC críticos celebrem outros acordos de subcontratação quando i) o subcontratante previsto for um terceiro prestador de serviços no domínio das TIC ou um subcontratante de TIC estabelecido num país terceiro e ii) a subcontratação disser respeito a uma função crítica ou importante da entidade financeira. O BCE gostaria de salientar que estes poderes só podem ser exercidos pela autoridade fiscalizadora principal no contexto de acordos de subcontratação em que um terceiro prestador de serviços no domínio das TIC crítico subcontrate uma função crítica ou importante a uma entidade jurídica distinta estabelecida num país terceiro. O BCE entende que a autoridade fiscalizadora principal não pode exercer poderes comparáveis para impedir que um terceiro prestador de serviços de TIC crítico externalize funções críticas ou importantes da entidade financeira para instalações desse prestador de serviços localizadas num país terceiro. Pode acontecer, por exemplo, que, do ponto de vista operacional, os dados e/ou informações críticos possam ser armazenados ou tratados por instalações situadas fora do Espaço Económico Europeu (EEE). Nesse caso, os poderes da autoridade fiscalizadora principal podem não conferir às autoridades competentes poderes adequados para aceder a todas as informações, instalações, infraestruturas e pessoal relevantes para o desempenho de todas as funções essenciais ou importantes da entidade financeira. A fim de assegurar a capacidade das autoridades competentes para desempenharem sem entraves as suas funções, o BCE sugere que seja conferido à autoridade fiscalizadora principal o poder de restringir também a utilização de instalações localizadas fora do EEE por terceiros prestadores de serviços críticos de TIC críticos. Este poder pode ser exercido nos casos específicos em que não existam acordos administrativos com as autoridades competentes do país terceiro, tal como previsto no regulamento proposto ([96]), ou em que os representantes dos terceiros prestadores de serviços de TIC críticos não prestem garantias suficientes, no âmbito do quadro do país terceiro em causa, quanto ao acesso às informações, instalações, infraestruturas e pessoal necessário para exercer as funções de superintendência ou supervisão..

4.4.4 Por último, exigir que as autoridades competentes deem seguimento às recomendações da autoridade fiscalizadora principal ([97]) corre o risco de se revelar ineficaz, uma vez que as autoridades competentes podem não ter uma visão holística dos riscos gerados por cada terceiro prestador de serviços de TIC crítico. Além disso, as autoridades competentes podem ser obrigadas a tomar medidas contra as suas entidades financeiras supervisionadas, caso as recomendações não sejam tidas em conta pelos terceiros prestadores de serviços críticos. Nos termos do regulamento proposto ([98]), as autoridades competentes podem exigir que as suas entidades financeiras supervisionadas suspendam temporariamente o serviço prestado por terceiros críticos, ou que rescindam contratos pendentes com terceiros prestadores de serviços críticos. É difícil traduzir em ações concretas o processo de acompanhamento previsto. Concretamente, não é claro se uma entidade financeira supervisionada estará em condições de suspender ou rescindir um contrato com um terceiro prestador de serviços críticos. Tal deve-se ao facto de o terceiro prestador de serviços de TIC críticos poder ser um prestador significativo para essa entidade financeira, ou devido aos custos e indemnizações, contratuais ou não, que a entidade financeira pode sofrer em consequência dessa suspensão ou cessação. Além disso, esta abordagem não serve a convergência da supervisão, uma vez que as autoridades competentes podem interpretar a mesma recomendação de forma divergente. Tal poderia, em última análise, prejudicar a harmonização prevista e uma abordagem coerente na monitorização, a nível da União, do risco de terceiros no domínio das TIC. Tendo em conta o que precede, os órgãos legislativos da União podem pretender considerar a possibilidade de conceder aos supervisores legais poderes de execução específicos em relação a terceiros prestadores de serviços de TIC críticos, tendo em conta os limites impostos pela doutrina Meroni, parcialmente mitigados pelo Tribunal de Justiça no seu acórdão no processo ESMA ([99]).

([93]) Ver o artigo 29.º do regulamento proposto.
([94]) Ver o artigo 29.º, n.º 3, do regulamento proposto.
([95]) Ver o artigo 35.º do regulamento proposto.
([96]) Ver o artigo 39.º, n.º 1, do regulamento proposto.
([97]) Ver o artigo 29.º, n.º 4, e o artigo 37.º do regulamento proposto.
([98]) Ver o artigo 37.º, n.º 3, do regulamento proposto.
([99]) Ver o Acórdão do Tribunal de Justiça (Grande Secção), de 22 de janeiro de 2014, no processo C-270/12, Reino Unido da Grã-Bretanha e da Irlanda do Norte contra Parlamento Europeu e Conselho da União Europeia, relativo ao Regulamento (UE) n.º 236/2012 (ECLI: EU:C:2014:18)

Nos casos em que o BCE recomenda alterações ao regulamento proposto, as sugestões de reformulação específicas constam de um documento técnico de trabalho separado, acompanhadas de um texto explicativo para o efeito. O documento técnico de trabalho está disponível em versão inglesa no EUR-Lex.

Feito em Frankfurt am Main, em 4 de junho de 2021.

A Presidente do BCE
Christine LAGARDE