EBA/REC/2017/03

28/03/2018

Recomendações

relativas à subcontratação externa a prestadores de serviços de computação em nuvem

1. Obrigações de cumprimento e de comunicação de informação

Natureza das presentes recomendações

1. O presente documento contém orientações emitidas ao abrigo do artigo 16.º do Regulamento (UE) n.º 1093/2010[1]. Nos termos do artigo 16.º, n.º 3, do referido Regulamento, as autoridades competentes e as instituições financeiras desenvolvem todos os esforços para dar cumprimento a essas orientações e recomendações.

2. As recomendações refletem a posição da EBA sobre o que constituem práticas de supervisão adequadas no âmbito do Sistema Europeu de Supervisão Financeira ou sobre o modo como a legislação da União deve ser aplicada num domínio específico. As autoridades competentes, na aceção do artigo 4.º, n.º 2, do Regulamento (UE) n.º 1093/2010, às quais as presentes recomendações se aplicam, dão cumprimento às mesmas incorporando-as nas respetivas práticas de supervisão conforme se revele mais adequado (por exemplo, mediante a alteração do respetivo quadro jurídico ou dos respetivos processos de supervisão), incluindo os casos em que determinadas orientações são dirigidas, em primeira linha, às instituições.

Requisitos de notificação

3. Nos termos do disposto no artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes confirmam à EBA se dão ou tencionam dar cumprimento às presentes recomendações, ou, em caso contrário, indicam as razões para o não cumprimento até 28.05.2018. Na ausência de qualquer notificação até à referida data, a EBA considera que as autoridades competentes em causa não cumprem as orientações. As notificações efetuam-se mediante o envio do formulário disponível no sítio Web da EBA para o endereço compliance@eba.europa.eu com a indicação de referência «EBA/REC/2017/03». As notificações são efetuadas por pessoas devidamente autorizadas a comunicar a situação de cumprimento em nome das respetivas autoridades competentes. Qualquer alteração no que respeita à situação de cumprimento deve igualmente ser comunicada à EBA.

4. As notificações serão publicadas no sítio Web da EBA, em conformidade com o disposto no artigo 16.º, n.º 3.

[1] 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).

2. Objeto, âmbito de aplicação e definições

Objeto e âmbito de aplicação

1. As presentes recomendações especificam mais pormenorizadamente as condições para a subcontratação externa, conforme referido nas orientações "Guidelines on outsourcing" do Comité das Autoridades Europeias de Supervisão Bancária (CEBS) sobre subcontratação externa ("outsourcing") de 14 de dezembro de 2006, e são aplicáveis à subcontratação externa por parte das instituições, na aceção do ponto 3 do artigo 4.º, n.º 1, do Regulamento (UE) n.º 575/2013 para prestadores de serviços de computação em nuvem.

Destinatários

2. As presentes recomendações destinam-se às autoridades competentes, na aceção do artigo 4.º, n.º 2, do Regulamento (UE) n.º 1093/2010, bem como às instituições, na aceção no ponto 3 do artigo 4.º, n.º 1, do Regulamento n.º 575/2013.[2]

Definições

3. Salvo especificação em contrário, os termos utilizados e definidos na Diretiva 2013/36/UE[3] sobre requisitos de capital e nas orientações do CEBS têm o mesmo significado nas recomendações. Adicionalmente, para efeitos das presentes recomendações, aplicam-se as seguintes definições:

Serviços de computação em nuvem ("cloud services")	Serviços fornecidos através de computação em nuvem, ou seja, um modelo que oferece um acesso em rede em qualquer local, prático e a pedido a um conjunto partilhado de recursos informáticos configuráveis (por exemplo, redes, servidores, sistemas de armazenamento, aplicações e serviços) que podem ser rapidamente disponibilizados e libertados com um esforço mínimo de gestão ou de interação com o fornecedor de serviço.
Nuvem pública	Infraestrutura em nuvem disponível para utilização em sistema aberto pelo público em geral.
Nuvem privada	Infraestrutura em nuvem disponível para utilização exclusiva por uma única instituição.

[2] 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.

[3] 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.

Nuvem comunitária	Infraestrutura em nuvem disponível para utilização exclusiva por uma comunidade específica de instituições, incluindo várias instituições de um único grupo.
Nuvem híbrida	Infraestrutura em nuvem composta por duas ou mais infraestruturas em nuvem distintas.

3. Aplicação

Data de aplicação

5. As presentes recomendações são aplicáveis a partir de 1 de julho de 2018.

4. Recomendações relativas à subcontratação externa a prestadores de serviços de computação em nuvem

4.1 Avaliação da materialidade

1. As instituições que procedem à subcontratação externa devem, antes de subcontratarem externamente as respetivas atividades, avaliar quais as atividades que devem ser consideradas relevantes. As instituições devem realizar esta avaliação da materialidade das atividades com base na orientação 1, alínea f) das orientações do CEBS relativas à subcontratação externa e, relativamente a subcontratação externa a prestadores de serviços de computação em nuvem em particular, ter em consideração todos os critérios abaixo:

    (a) a criticidade e o perfil de risco inerente das atividades a subcontratar externamente, ou seja, se são atividades essenciais para a continuidade/viabilidade operacional da instituição e das suas obrigações para com os clientes;

    (b) o impacto operacional direto dos períodos de indisponibilidade e dos riscos legais e de reputação associados;

    (c) o impacto que qualquer perturbação da atividade possa ter nas perspetivas de receita da instituição;

    (d) o potencial impacto que uma violação de confidencialidade ou falha da integridade dos dados possa ter na instituição e nos respetivos clientes.

4.2 Dever de informar devidamente os supervisores

2. As instituições que procedem à subcontratação externa devem informar devidamente as autoridades competentes acerca das atividades relevantes que serão subcontratadas externamente para prestadores de serviços de computação em nuvem. As instituições devem fazê-lo com base no número 4.3 das orientações do CEBS e, em todo o caso, disponibilizar às autoridades competentes as seguintes informações:

    (a) o nome do prestador de serviços de computação em nuvem e o nome da respetiva empresa-mãe (se aplicável);
    (b) uma descrição das atividades e dados a subcontratar externamente;
    (c) o país ou países em que o serviço será realizado (incluindo a localização dos dados);
    (d) a data de início da prestação do serviço;
    (e) a data da última renovação do contrato (quando aplicável);
    (f) a lei aplicável que rege o contrato;

(g) a data de expiração da prestação do serviço ou a data da próxima renovação do contrato (quando aplicável).

3. Para além das informações fornecidas em conformidade com o número anterior, a autoridade competente pode solicitar informações adicionais à instituição que procede à subcontratação externa sobre a sua análise de risco para as atividades relevantes a subcontratar externamente, nomeadamente:

   (a) se o prestador de serviços de computação em nuvem possui um plano de continuidade de negócio adequado para os serviços fornecidos à instituição que procede à subcontratação externa;
   (b) se a instituição que procede à subcontratação externa possui uma estratégia de saída em caso de cessação do contrato por uma das partes ou interrupção da prestação dos serviços pelo prestador de serviços de computação em nuvem;
   (c) se a instituição que procede à subcontratação externa mantém as competências e recursos necessários para monitorizar de forma adequada as atividades subcontratadas externamente.

4. A instituição que procede à subcontratação externa deve manter um registo atualizado da informação sobre as suas atividades relevantes e não relevantes subcontratadas externamente a prestadores de serviços de computação em nuvem ao nível da instituição e do grupo. A instituição que procede à subcontratação externa deve disponibilizar à autoridade competente, a pedido, uma cópia do acordo de subcontratação externa e informações relacionadas constantes no registo, independentemente da atividade subcontratada externamente para um prestador de serviços de computação em nuvem ter sido avaliada ou não como relevante pela instituição.

5. No registo referido no número anterior, devem ser incluídas, no mínimo, as seguintes informações:

   (a) as informações referidas no número 2, alíneas a) a g), se ainda não tiverem sido fornecidas;
   (b) o tipo de subcontratação externa (o modelo do serviço de computação em nuvem e o modelo de implementação da nuvem, ou seja, nuvem pública/privada/híbrida/comunitária);
   (c) as partes que recebem serviços de computação em nuvem ao abrigo do acordo de subcontratação externa;
   (d) provas da aprovação para subcontratação externa pelo órgão de administração ou pelos comités delegados, se aplicável;
   (e) os nomes de eventuais subcontratantes, se aplicável;
   (f) o país onde o prestador de serviços de computação em nuvem/principal subcontratante está registado;
   (g) se a subcontratação externa foi avaliada como relevante (sim/não);
   (h) a data da última avaliação da materialidade da instituição relativamente às atividades subcontratadas externamente;
   (i) se o prestador de serviços de computação em nuvem/subcontratante(s) suporta operações comerciais em que o tempo é um fator crítico (sim/não);

(j) uma avaliação da capacidade de substituição do prestador de serviços de computação em nuvem (como fácil, difícil ou impossível);
(k) identificação de um prestador de serviços alternativo, se possível;
(l) a data da última avaliação do risco da subcontratação externa ou acordo de subcontratação.

4.3 Direitos de acesso e de auditoria

Para instituições

6. Com base na orientação 8, n.º 2, alínea g) das orientações do CEBS e para efeitos de subcontratação externa da nuvem, as instituições que procedem à subcontratação externa devem igualmente garantir que se encontra em vigor um acordo por escrito com o prestador de serviços de computação em nuvem, pelo qual este último compromete-se a:

   (a) fornecer à instituição, a terceiros designados pela instituição para o efeito e ao revisor oficial de contas da instituição acesso total às instalações (sedes e centros de operações), incluindo a todos os dispositivos, sistemas, redes e dados utilizados para o fornecimento dos serviços subcontratados externamente (direito de acesso);

   (b) conceder à instituição, a terceiros designados pela instituição para o efeito e ao revisor oficial de contas da instituição direitos ilimitados de inspeção e auditoria relativamente aos serviços subcontratados externamente (direito de auditoria).

7. O exercício efetivo dos direitos de acesso e de auditoria não deverão ser impedidos ou limitados por disposições contratuais. Se a realização de auditorias ou a utilização de determinadas técnicas de auditoria forem suscetíveis de criar um risco para o ambiente de outro cliente, devem ser acordadas formas alternativas para proporcionar um nível de garantia similar ao exigido pela instituição.

8. A instituição que procede à subcontratação externa deve exercer os seus direitos de auditoria e de acesso com base no risco. Nos casos em que a instituição que procede à subcontratação externa não utilize os seus recursos de auditoria próprios, esta deve considerar utilizar, pelo menos, uma das seguintes ferramentas:

   (a) Auditorias comuns organizadas conjuntamente com outros clientes do mesmo prestador de serviços de computação em nuvem e realizadas por esses clientes ou por terceiros designados pelos mesmos, a fim de se utilizar os recursos de auditoria com mais eficácia e de se reduzir os encargos administrativos para os clientes e para o prestador de serviços de computação em nuvem.

   (b) Certificações de terceiros e relatórios de auditoria interna ou de terceiros disponibilizados pelo prestador de serviços de computação em nuvem, desde que:

      i. A instituição que procede à subcontratação externa garanta que o âmbito da certificação ou relatório de auditoria abranja os sistemas (ou seja, processos,

aplicações, infraestruturas, centros de dados, etc.) e os controlos considerados fundamentais pela instituição que procede à subcontratação externa.

ii. A instituição que procede à subcontratação externa avalie de forma exaustiva o conteúdo das certificações ou relatórios de auditoria de forma contínua e, em especial, garanta que os controlos chave continuam a estar abrangidos em futuras versões de um relatório de controlo e verifique que a certificação ou relatório de controlo não se encontra obsoleto.

iii. A instituição que procede à subcontratação externa esteja satisfeita com a aptidão da entidade de certificação ou auditoria (por exemplo, no que se refere à rotatividade da empresa de certificação ou auditoria, qualificações, conhecimentos especializados, repetição/verificação das provas no ficheiro de auditoria subjacente).

iv. As certificações sejam emitidas e as auditorias sejam realizadas com base em normas amplamente reconhecidas e incluam um teste da eficácia operacional dos controlos chave existentes.

v. A instituição que procede à subcontratação externa detenha o direito contratual de solicitar o alargamento do âmbito das certificações ou relatórios de auditoria a alguns sistemas e/ou controlos relevantes. O número e a frequência desses pedidos de alteração do âmbito devem ser razoáveis e legítimos de uma perspetiva de gestão do risco.

9. Considerando que as soluções de computação em nuvem têm um elevado nível de complexidade técnica, a instituição que procede à subcontratação externa deve verificar se o pessoal que realiza a auditoria – quer sejam auditores internos, o grupo de auditores que atua em nome da instituição ou os auditores designados pelo prestador de serviço de computação em nuvem – ou, conforme apropriado, o pessoal que supervisiona a certificação de terceiros ou os relatórios de auditoria do prestador de serviços adquiriram as competências e conhecimentos adequados para realizar auditorias eficazes e relevantes e/ou avaliações das soluções de computação na nuvem.

Para autoridades competentes

10. Com base na orientação 8, n.º 2, alínea h), das orientações do CEBS e para efeitos de subcontratação externa na nuvem, as instituições que procedem à subcontratação externa devem garantir que se encontra em vigor um acordo por escrito com o prestador de serviços de computação na nuvem, pelo qual este último compromete-se a:

(a) fornecer à autoridade competente que supervisiona a instituição que procede à subcontratação externa (ou a terceiros designados por essa autoridade para o efeito) acesso total às instalações do prestador de serviços de computação em nuvem (sedes e centros de operações), incluindo a todos os dispositivos, sistemas, redes e dados utilizados para o fornecimento de serviços à instituição que procede à subcontratação externa (direito de acesso);

(b) conceder à autoridade competente que supervisiona a instituição que procede à subcontratação externa (ou a terceiros designados por essa autoridade para o efeito)

direitos ilimitados de inspeção e auditoria relativamente aos serviços subcontratados externamente (direito de auditoria).

11. A instituição que procede à subcontratação externa deve garantir que as disposições contratuais não impedem que a respetiva autoridade competente execute a sua função e objetivos de supervisão.

12. As informações que as autoridades competentes obtêm pelo exercício dos direitos de acesso e de auditoria devem estar sujeitas aos requisitos de sigilo profissional e de confidencialidade referidos no artigo 53 e seguintes da Diretiva 2013/36/UE (CRD IV). As autoridades competentes devem abster-se de celebrar qualquer tipo de acordo contratual ou declaração que as impeça de cumprir as disposições do direito da União em matéria de confidencialidade, sigilo profissional e troca de informações.

13. Com base nas constatações da auditoria, a autoridade competente deve endereçar eventuais deficiências identificadas, se necessário, impondo medidas diretamente sobre a instituição que procede à subcontratação externa.

4.4 Especialmente em relação ao direito de acesso

14. O acordo referido nos números 6 e 10 deve incluir as seguintes disposições:

(a) A parte que pretende exercer o seu direito de acesso (instituição, autoridade competente, auditor ou terceiros que representam a instituição ou a autoridade competente) deve, antes de realizar uma visita planeada ao local, comunicar, num período de tempo razoável, a realização da visita ao local onde se situam instalações relevantes, a não ser que não tenha sido possível proceder a uma notificação prévia devido a uma emergência ou situação de crise.

(b) É necessário que o prestador de serviços de computação em nuvem coopere plenamente com as autoridades competentes, bem como com a instituição e o respetivo auditor, relativamente à visita ao local.

4.5 Segurança dos dados e sistemas

15. Tal como especificado na orientação 8, n.º 2, alínea e), das orientações do CEBS, o contrato de subcontratação externa deve obrigar o prestador de serviços de computação em nuvem a proteger a confidencialidade das informações transmitidas pela instituição financeira. Conforme a orientação 6, n.º 6, alínea e), das orientações do CEBS, as instituições devem implementar medidas para garantir a continuidade dos serviços fornecidos pelos prestadores de serviços de subcontratação externa. Com base nas orientações 8, n.º 2, alínea b), e 9 das orientações do CEBS, as necessidades das instituições que procedem à subcontratação externa no que diz respeito à qualidade e desempenho devem ser integradas em contratos de subcontratação

externa e acordos de níveis de serviço por escrito. Estes aspetos referentes à segurança devem também ser monitorizados de forma contínua (orientação 7).

16. Para efeitos do número anterior, a instituição deve realizar, antes de proceder à subcontratação externa e a fim de comunicar a decisão relevante, no mínimo, o seguinte:

    (a) identificar e classificar as suas atividades, processos e dados e sistemas relacionados, quanto à sensibilidade e às proteções necessárias;

    (b) efetuar uma seleção completa, com base no risco, das atividades, processos e dados e sistemas relacionados cuja subcontratação externa para uma solução de computação em nuvem esteja a ser equacionada;

    (c) definir e decidir um nível adequado de proteção da confidencialidade dos dados, continuidade das atividades subcontratadas externamente e integridade e rastreabilidade dos dados e sistemas no contexto da subcontratação externa pretendida para a nuvem. As instituições devem ainda considerar medidas específicas, quando necessário, para dados em trânsito, dados em memória e dados em repouso, tais como a utilização de tecnologias de cifragem, em conjugação com uma arquitetura de gestão de chaves adequada.

17. Subsequentemente, as instituições devem garantir que se encontra em vigor um acordo por escrito com o prestador de serviços de computação em nuvem onde, entre outros aspetos, são definidas as obrigações deste último, nos termos do número 16, alínea c).

18. As instituições devem monitorizar a execução de atividades e de medidas de segurança de acordo com a orientação 7 das orientações do CEBS, incluindo incidentes, de forma contínua e supervisionar de forma apropriada se a respetiva subcontratação externa de atividades está em conformidade com os números anteriores; as instituições devem tomar prontamente quaisquer medidas corretivas necessárias.

4.6 Localização dos dados e do processamento de dados

19. Conforme referido na orientação 4, n.º 4, das orientações do CEBS, as instituições devem ter especial cuidado na celebração e gestão de acordos de subcontratação externa para fora do EEE devido a possíveis riscos de proteção de dados e riscos à supervisão eficaz por parte da autoridade supervisora.

20. A instituição que procede à subcontratação externa deve adotar uma abordagem baseada no risco em relação aos dados e a considerações relativas ao local de processamento de dados aquando da subcontratação externa para um ambiente de computação em nuvem. A avaliação deve endereçar os potenciais impactos de risco, incluindo riscos legais e questões de conformidade, e as limitações de supervisão relacionadas com os países onde se encontram os serviços subcontratados externamente ou onde for provável que sejam fornecidos e onde os dados se encontram ou seja provável que estejam armazenados. A avaliação deve incluir considerações sobre a estabilidade mais alargada a nível político e de segurança das jurisdições em questão; as leis em vigor nessas jurisdições (incluindo leis sobre proteção de dados); e as disposições de aplicação da lei em vigor nessas jurisdições, incluindo disposições legislativas em matéria de insolvência que seriam aplicáveis em caso de incumprimento do prestador de serviços de computação em nuvem. A instituição que procede à subcontratação externa deve garantir que esses riscos são mantidos dentro de limites aceitáveis compatíveis com a materialidade da atividade subcontratada externamente.

4.7 Subcontratação externa em cadeia

21. Conforme referido na orientação 10 das orientações do CEBS, as instituições devem ter em conta os riscos associados à subcontratação externa em «cadeia», em que o prestador de serviços de computação em nuvem subcontrata elementos do serviço a outros prestadores. A instituição que procede à subcontratação externa apenas deve concordar com a subcontratação externa em cadeia se o subcontratante também cumprir plenamente as obrigações existentes entre a instituição que procede à subcontratação externa e o prestador de serviços de subcontratação externa. Além disso, a instituição que procede à subcontratação externa deve tomar as medidas adequadas para fazer face ao risco de qualquer fragilidade ou incumprimento no fornecimento das atividades subcontratadas que possa ter um efeito significativo na capacidade do prestador de serviços de subcontratação externa cumprir as suas responsabilidades ao abrigo do acordo de subcontratação externa.

22. O acordo de subcontratação externa entre a instituição que procede à subcontratação externa e o prestador de serviços de computação em nuvem deve especificar quaisquer tipos de atividades que estejam excluídas da potencial subcontratação e indicar que o prestador de serviços de computação em nuvem mantém a plena responsabilidade e supervisão dos serviços subcontratados.

23. O acordo de subcontratação externa deve ainda incluir uma obrigação para que o prestador de serviços de computação na nuvem informe a instituição que procede à subcontratação externa

de quaisquer alterações significativas planeadas aos subcontratantes ou aos serviços subcontratados referidos no acordo inicial que possam afetar a capacidade do prestador de serviços de subcontratação externa de cumprir as suas responsabilidades ao abrigo do acordo de subcontratação externa. O período de notificação dessas alterações deve ser contratualmente pré-acordado para permitir que a instituição que procede à subcontratação externa efetue uma avaliação do risco dos efeitos das alterações propostas antes da alteração efetiva dos subcontratantes ou serviços subcontratados entrar em vigor.

24. Caso um prestador de serviço de computação em nuvem planeie recorrer a um subcontratante ou a serviços subcontratados que teriam um efeito negativo na avaliação do risco dos serviços acordados, a instituição que procede à subcontratação externa deve ter o direito de resolver o contrato.

25. A instituição que procede à subcontratação externa deve rever e monitorizar a execução do serviço global de forma contínua, independentemente de ser fornecido pelo prestador de serviço de computação em nuvem ou pelos respetivos subcontratantes.

4.8 Planos de contingência e estratégias de saída

26. Tal como estabelecido nas orientações 6.1, 6, n.º 6, alínea e), e 8, n.º 2, alínea d), das orientações do CEBS, a instituição que procede à subcontratação externa deve planear e implementar acordos para manter a continuidade da sua atividade, em caso de falha ou deterioração do fornecimento dos serviços por parte do prestador de serviços de subcontratação externa para um grau inaceitável. Tais acordos devem incluir planos de contingência e uma estratégia de saída claramente definida. Além do mais, o contrato de subcontratação externa deve incluir uma cláusula de resolução e de gestão da saída que permita que as atividades prestadas pelo prestador de serviços de subcontratação externa sejam transferidas para outro prestador de serviços de subcontratação externa ou sejam reintegradas na instituição que procede à subcontratação externa.

27. Uma instituição que procede à subcontratação externa também deve garantir que consegue pôr termo aos acordos de subcontratação externa na nuvem, se necessário, sem a interrupção do fornecimento dos serviços ou efeitos negativos no cumprimento do regime regulamentar e sem que tal se processe em detrimento da continuidade e da qualidade do fornecimento de serviços aos clientes. Para tal, a instituição que procede à subcontratação externa deve:

    (a) desenvolver e implementar planos de saída abrangentes, documentados e suficientemente testados, quando adequado;

    (b) identificar soluções alternativas e desenvolver planos de transição para que seja possível remover e transferir as atividades e dados existentes do prestador de serviços de computação em nuvem para estas soluções de forma controlada e suficientemente testada, tendo em consideração questões relativas à localização dos dados e manutenção da continuidade das atividades durante a fase de transição;

(c) garantir que o acordo de subcontratação externa inclui uma obrigação do prestador de serviços de computação em nuvem apoiar adequadamente a instituição que procede à subcontratação externa na transferência organizada da atividade para outro prestador de serviços de computação em nuvem ou para a gestão direta da instituição que procede à subcontratação externa em caso de resolução do acordo de subcontratação externa.

28. Aquando do desenvolvimento de estratégias de saída, uma instituição que procede à subcontratação externa deve considerar o seguinte:

(a) desenvolver indicadores de risco chave para identificar um nível de risco inaceitável;

(b) realizar uma análise de impacto das atividades proporcional às atividades subcontratadas externamente para identificar os recursos humanos e materiais que seriam necessários para implementar o plano de saída e quanto tempo demoraria;

(c) atribuir funções e responsabilidades para a gestão de planos de saída e de atividades de transição.

(d) definir critérios de sucesso da transição.

29. A instituição que procede à subcontratação externa deve incluir indicadores capazes de ativar o plano de saída no âmbito da monitorização contínua dos serviços e da supervisão dos serviços fornecidos pelo prestador de serviços de computação em nuvem.