30/09/2025
ESMA65-294529287-4737

Orientações

relativas à subcontratação de prestadores de serviços de computação em nuvem

Índice

1 Âmbito de aplicação

Destinatários

1. As presentes orientações aplicam-se às autoridades competentes e i) aos depositários de fundos de investimento alternativos (FIA) referidos no artigo 21.o, n.o 3, alínea c), e no artigo 21.o, n.o 3, terceiro parágrafo, da DGFIA, caso não sejam entidades financeiras às quais se aplique o Regulamento DORA, e ii) aos depositários de OICVM referidos no artigo 23.o, n.o[1]2, alínea c), da Diretiva OICVM, caso não sejam entidades financeiras às quais se aplique o Regulamento DORA.

O quê?

2. As presentes orientações aplicam-se às seguintes disposições:

a) No que se refere aos depositários dos FIA: Artigo 21.o da DGFIA; Artigo 98.o do Regulamento Delegado (UE) 2013/231 da Comissão;

b) No que se refere aos depositários de OICVM: Artigos 22.o, 22.o-A e 23.o, n.o 2, da Diretiva OICVM; Artigo 32.o da Diretiva 2010/43/UE da Comissão; Artigo 2.o, n.o 2, alínea j), artigo 3.o, n.o 1, artigo 13.o, n.o 2, e artigos 15.o, 16.o e 22.o do Regulamento Delegado (UE) 2016/438 da Comissão.

Quando?

3. As presentes orientações são aplicáveis a partir da data da sua publicação no sítio Web da ESMA em todas as línguas oficiais da UE e a todos os acordos de subcontratação em nuvem celebrados, renovados ou alterados nessa data ou posteriormente.

4. À luz da aplicação do Regulamento DORA, as anteriores orientações da ESMA sobre a subcontratação a prestadores de serviços de computação em nuvem deixam de ser aplicáveis às entidades financeiras sujeitas ao Regulamento DORA referidas no artigo 2.o desse mesmo regulamento. Relativamente aos depositários de FIA e aos depositários de OICVM a que se refere o n.o 1 *supra*, as anteriores Orientações da ESMA relativas à subcontratação a prestadores de serviços de computação em nuvem continuarão a ser aplicáveis até à data de publicação das presentes orientações no sítio Web da ESMA em todas as línguas oficiais da UE.

[1] Com referência aos acordos de subcontratação de serviços de computação em nuvem, as entidades financeiras definidas no artigo 2.º, n.ºs 1 e 2 do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (Regulamento DORA), estão sujeitas às regras específicas estabelecidas no Regulamento DORA e nos respetivos regulamentos delegados e de execução da Comissão.

2 Referências legislativas, abreviaturas e definições

2.1 Referências legislativas

Regulamento ESMA	Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Valores Mobiliários e dos Mercados), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/77/CE da Comissão[2]
DGFIA	Diretiva 2011/61/UE do Parlamento Europeu e do Conselho, de 8 de junho de 2011, relativa aos gestores de fundos de investimento alternativos e que altera as Diretivas 2003/41/CE e 2009/65/CE e os Regulamentos (CE) n.º 1060/2009 e (UE) n.º 1095/2010[3]
Regulamento Delegado (UE) 2013/231 da Comissão	Regulamento Delegado (UE) n.º 231/2013 da Comissão, de 19 de dezembro de 2012, que complementa a Diretiva 2011/61/UE do Parlamento Europeu e do Conselho no que diz respeito às isenções, condições gerais de funcionamento, depositários, efeito de alavanca, transparência e supervisão[4]
Diretiva OICVM	Diretiva 2009/65/CE do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que coordena as disposições legislativas, regulamentares e administrativas respeitantes a alguns organismos de investimento coletivo em valores mobiliários (OICVM)[5]
Diretiva 2010/43/UE da Comissão	Diretiva 2010/43/CE da Comissão, de 1 de julho de 2010, que aplica a Diretiva 2009/65/CE do Parlamento Europeu e do Conselho no que diz respeito aos requisitos organizativos, aos conflitos de interesse, ao exercício da atividade, à gestão de riscos e ao conteúdo do acordo celebrado entre o depositário e a sociedade gestora[6]

[2] JO L 331 de 15.12.2010, p. 84
[3] JO L 174 de 1.7.2011, p. 1.
[4] JO L 83 de 22.3.2013, p. 1
[5] JO L 302 de 17.11.2009, p. 32
[6] JO L 176 de 10.7.2010, p. 42

DORA	Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014, (UE) n.o 909/2014 e (UE) 2016/1011[7]
RGPD	Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE[8]

2.2 Abreviaturas

PSCN	Prestador de serviços de computação em nuvem
ESMA	Autoridade Europeia dos Valores Mobiliários e dos Mercados
UE	União Europeia

2.3 Definições

Função	quaisquer processos, serviços ou atividades;
Funções essenciais ou importantes	quaisquer funções cuja falha ou insucesso no seu desempenho prejudicaria significativamente: a) o cumprimento, por parte de uma empresa, das obrigações que lhe incumbem por força da legislação aplicável; b) o desempenho financeiro de uma empresa; ou c) a solidez ou continuidade dos principais serviços e atividades de uma empresa;
Serviços de computação em nuvem	os serviços fornecidos através de computação em nuvem;

[7] *JO L 333 de 27.12.2022, p. 1.*
[8] JO L 119 de 4.5.2016, p. 1-88

Computação em nuvem ou nuvem[9]	um modelo que permite o acesso em rede a um conjunto escalável e adaptável de recursos físicos ou virtuais partilhados (por exemplo, servidores, sistemas operativos, redes, software, aplicações e equipamento de armazenamento) que podem ser utilizados e geridos autonomamente a pedido;
Prestador de serviços de computação em nuvem	uma entidade terceira que presta serviços de computação em nuvem ao abrigo de um acordo de subcontratação;
Acordo de subcontratação de serviços de computação em nuvem	qualquer acordo, incluindo acordos de delegação, entre: (i) uma empresa e um PSCN mediante os quais este último desempenha uma função que de outra forma seria assumida pela própria empresa; ou (ii) uma empresa e uma entidade terceira que não seja um PSCN, mas que dependa significativamente de um PSCN para desempenhar uma função que de outra forma seria assumida pela própria empresa. Neste caso, a referência a um «PSCN» nas presentes orientações deve ser entendida como uma referência a essa entidade terceira.
Sub-subcontratação	uma situação em que o PSCN transfere uma função subcontratada (ou parte dessa função) para outro prestador de serviços ao abrigo de um acordo de subcontratação;
Modelo de implantação da nuvem	a forma como o serviço de computação em nuvem pode ser organizado com base no controlo e partilha de recursos físicos ou virtuais. Os modelos de implantação

[9] A expressão «computação em nuvem» é frequentemente utilizada na forma abreviada de «nuvem». O termo «nuvem» é utilizado em todo o resto do documento para facilitar a referência.

da nuvem incluem nuvens comunitárias[10], híbridas[11], privadas[12] e públicas[13];

Empresas

a) depositários referidos no artigo 21.o, n.o 3, alínea c), e no artigo 21.o, n.o 3, terceiro parágrafo, da DGFIA («depositários de fundos de investimento alternativos (FIA)»);

b) depositários referidos no artigo 23.o, n.o 2, alínea c), da Diretiva OICVM («depositários de OICVM»).

3 Finalidade

5. As presentes orientações baseiam-se no artigo 16.º, n.º 1, do Regulamento ESMA. As presentes orientações têm por objetivo estabelecer práticas de supervisão coerentes, eficientes e eficazes no âmbito do Sistema Europeu de Supervisão Financeira (SESF) e garantir uma aplicação comum, uniforme e coerente dos requisitos mencionados na Secção 1.1 do título «O quê?» sempre que as empresas subcontratarem funções a PSCN. As presentes orientações visam, em especial, ajudar as empresas e as autoridades competentes a identificar, abordar e acompanhar os riscos e desafios decorrentes dos acordos de subcontratação de serviços de computação em nuvem, desde a decisão de subcontratar, a seleção de um prestador de serviços em nuvem, o acompanhamento das atividades subcontratadas até à definição de estratégias de saída.

4 Obrigações em matéria de cumprimento e notificação

4.1 Natureza jurídica das presentes orientações

6. Em conformidade com o disposto no artigo 16.º, n.º 3, do Regulamento ESMA, as autoridades competentes e as empresas devem desenvolver todos os esforços para dar cumprimento às presentes orientações.

7. As autoridades competentes às quais as presentes orientações se destinam devem assegurar o seu cumprimento através da incorporação das mesmas nos respetivos quadros nacionais jurídicos e/ou de supervisão, consoante os casos, incluindo nos

[10] Um modelo de implantação de nuvem em que os serviços de computação em nuvem oferecem exclusivamente suporte e são partilhados por um grupo específico de clientes de serviços em nuvem que possuem requisitos partilhados e uma mantêm uma relação entre si, e em que os recursos são controlados por, pelo menos, um membro desse grupo;
[11] Um modelo de implantação de nuvem que utiliza, pelo menos, dois modelos diferentes de implantação de nuvem
[12] Um modelo de implantação de nuvem em que os serviços de computação em nuvem são utilizados exclusivamente por um único cliente de serviço de computação em nuvem e os recursos são controlados por esse cliente
[13] Um modelo de implantação de nuvem em que os serviços de computação em nuvem podem ser disponibilizados a qualquer cliente de serviço em nuvem e os recursos são controlados pelo prestador de serviços de computação em nuvem

casos em que determinadas orientações se destinem sobretudo às empresas. Neste caso, as autoridades competentes devem assegurar, através da sua supervisão, que as empresas cumprem as orientações.

4.2 Obrigações de prestação de informações

8. No prazo de dois meses a contar da data de publicação das orientações no sítio Web da ESMA, em todas as línguas oficiais da UE, as autoridades competentes destinatárias das presentes orientações devem comunicar à ESMA se i) cumprem, ii) não cumprem, mas pretendem cumprir ou iii) não cumprem, nem pretendem cumprir as orientações.

9. Em caso de não cumprimento, as autoridades competentes devem também comunicar à ESMA, no prazo de dois meses a contar da data de publicação das orientações no sítio Web da ESMA em todas as línguas oficiais da UE, as razões pelas quais não cumprem estas orientações. No sítio Web da ESMA encontra-se disponível um modelo para as notificações. O modelo deve ser transmitido à ESMA, assim que estiver preenchido.

10. As empresas não estão obrigadas a informar se dão cumprimento às presentes orientações.

5 Orientações relativas à subcontratação a prestadores de serviços de computação em nuvem

Orientação 1. Governação, supervisão e documentação

11. As empresas devem dispor de uma estratégia de subcontratação de serviços de computação em nuvem definida e atualizada que seja coerente com as estratégias e as políticas e processos internos relevantes da empresa, incluindo no que diz respeito às tecnologias da informação e comunicação, à segurança da informação e à gestão do risco operacional.

12. As empresas devem:

    a) atribuir claramente, dentro da sua organização, as responsabilidades pela documentação, pela gestão e pelo controlo dos acordos de subcontratação de serviços de computação em nuvem;
    b) atribuir recursos suficientes para garantir o cumprimento das presentes orientações e de todos os requisitos legais aplicáveis aos seus acordos de subcontratação de serviços de computação em nuvem;
    c) estabelecer uma função de supervisão da subcontratação de serviços de computação em nuvem ou designar funcionários superiores que respondam

diretamente perante o órgão de administração e sejam responsáveis pela gestão e supervisão dos riscos inerentes aos acordos de subcontratação de serviços de computação em nuvem. Ao cumprirem a presente orientação, as empresas devem ter em conta a natureza, a escala e a complexidade das suas atividades, nomeadamente em termos de risco para o sistema financeiro, e os riscos inerentes às funções subcontratadas, bem como assegurar que o seu órgão de administração possui as competências técnicas necessárias para compreender os riscos envolvidos nos acordos de subcontratação de serviços de computação em nuvem. As empresas pequenas e menos complexas devem, no mínimo, assegurar uma clara divisão de tarefas e responsabilidades na gestão e supervisão dos acordos de subcontratação de serviços de computação em nuvem.

13. As empresas devem controlar o desempenho das suas atividades, as medidas de segurança e o cumprimento dos níveis de serviço acordados pelos seus PSCN. Este controlo deve basear-se no risco, com especial incidência nas funções essenciais ou importantes subcontratadas.

14. As empresas devem reavaliar se os seus acordos de subcontratação de serviços de computação em nuvem dizem respeito a uma função essencial ou importante. Essa reavaliação deve ser realizada periodicamente e sempre que o risco, a natureza ou a escala de uma função subcontratada tenham sido alterados de forma significativa.

15. As empresas devem manter um registo atualizado de informações sobre todos os seus acordos de subcontratação de serviços de computação em nuvem, distinguindo entre a subcontratação de funções essenciais ou importantes e outros acordos de subcontratação. Ao estabelecer a distinção entre a subcontratação de funções essenciais ou importantes e outros acordos de subcontratação, devem apresentar um breve resumo das razões pelas quais as funções subcontratadas são ou não consideradas essenciais ou importantes. Sem prejuízo da legislação nacional, as empresas devem igualmente conservar, durante um período apropriado, um registo dos acordos de subcontratação de serviços de computação em nuvem que já tenham cessado.

16. No caso dos acordos de subcontratação de serviços de computação em nuvem respeitantes a funções essenciais ou importantes, o registo deve incluir, pelo menos, as seguintes informações para cada acordo:

    a) um número de referência;
    b) a data de início e, se for caso disso, a data da próxima renovação do acordo, a data do termo do acordo e/ou os períodos de pré-aviso aplicáveis ao PSCN e à empresa;
    c) uma breve descrição da função subcontratada, incluindo os dados que são objeto de subcontratação e se foram ou não transferidos dados pessoais (por exemplo, indicando «sim» ou «não» num campo de dados separado);

d) uma categoria atribuída pela empresa que reflita a natureza da função subcontratada (por exemplo, a função de tecnologia da informação, a função de controlo), que deverá facilitar a identificação dos diferentes tipos de acordos de subcontratação de serviços de computação em nuvem;
e) se a função subcontratada apoia operações de negócio que sejam urgentes;
f) o nome e a marca (se for caso disso) do PSCN, o seu país de registo, o número de registo da sociedade, o seu identificador de entidade jurídica (se existir), a morada da sede social, os dados de contacto pertinentes e o nome da sua empresa-mãe (se for caso disso);
g) o direito que rege o acordo de subcontratação de serviços de computação em nuvem e, se for caso disso, a escolha da jurisdição;
h) o tipo de serviços em nuvem e os modelos de implantação, assim como a natureza específica dos dados a conservar e os locais (a saber, regiões ou países) onde esses dados podem ser armazenados;
i) a data da avaliação mais recente do caráter essencial ou da importância da função subcontratada e a data da próxima avaliação programada;
j) a data da mais recente avaliação/auditoria de riscos associados ao PSCN e um breve resumo dos principais resultados, assim como a data da próxima avaliação/auditoria de riscos programada;
k) o órgão individual ou decisório da empresa que aprovou o acordo de subcontratação de serviços de computação em nuvem;
l) se for caso disso, os nomes de subcontratantes aos quais seja subcontratada uma função essencial ou importante (ou partes significativas da mesma), incluindo o país onde os subcontratantes estão registados, o país onde o serviço subcontratado será prestado e os locais (a saber, as regiões ou os países) onde os dados serão armazenados;
m) o custo anual orçamentado estimado do acordo de subcontratação de serviços de computação em nuvem.

17. No caso da subcontratação de serviços de computação em nuvem respeitantes a funções não essenciais ou não importantes, as empresas devem definir as informações a incluir no registo com base na natureza, escala e complexidade dos riscos inerentes à função subcontratada.

Orientação 2. Análise prévia à subcontratação e devida diligência

18. Antes de celebrar qualquer acordo de subcontratação de serviços de computação em nuvem, as empresas devem:

a) avaliar se o acordo de subcontratação de serviços de computação em nuvem diz respeito a uma função essencial ou importante;
b) identificar e avaliar todos os riscos relevantes do acordo de subcontratação de serviços de computação em nuvem;
c) proceder à devida diligência em relação ao potencial PSCN;

d) identificar e avaliar qualquer conflito de interesses que a subcontratação possa implicar.

19. A análise prévia à subcontratação e a devida diligência em relação ao potencial PSCN devem ser proporcionais à natureza, escala e complexidade da função que a empresa tenciona subcontratar e aos riscos inerentes a essa função. Deverá incluir, pelo menos, uma avaliação do potencial impacto do acordo de subcontratação de serviços de computação em nuvem nos riscos operacionais, jurídicos, de conformidade e de reputação da empresa.

20. No caso da subcontratação de serviços de computação em nuvem respeitantes a funções essenciais ou importantes, a empresa deve igualmente:

a) avaliar todos os riscos relevantes que possam resultar do acordo de subcontratação de serviços de computação em nuvem, incluindo os riscos das tecnologias da informação e comunicação, de segurança da informação, de continuidade das atividades, os riscos jurídicos e de conformidade, os riscos reputacionais, os riscos operacionais e as eventuais limitações de supervisão para a empresa, relacionados com:
   i. o serviço de computação em nuvem selecionado e os modelos de implantação propostos;
   ii. os processos de migração e/ou implementação;
   iii. o caráter sensível da função e dos dados implicados que são objeto da subcontratação, assim como as medidas de segurança necessárias;
   iv. a interoperabilidade dos sistemas e aplicações da empresa e do PSCN, a saber, a sua capacidade de intercâmbio de informações e de utilização mútua das informações intercambiadas;
   v. a portabilidade dos dados da empresa, a saber, a capacidade de transferir facilmente os dados da empresa de um PSCN para outro ou de os transferir novamente para a empresa;
   vi. a estabilidade política, a situação de segurança e o sistema jurídico (incluindo as disposições em vigor em matéria de aplicação das leis, as disposições em matéria de insolvência que seriam aplicáveis em caso de falência do PSCN, a legislação em vigor sobre proteção de dados e o preenchimento ou não das condições previstas no RGPD para a transferência de dados pessoais para um país terceiro) dos países (pertencentes ou não pertencentes à UE) onde os serviços subcontratados seriam prestados e onde os dados objeto da subcontratação seriam armazenados; no caso da sub-subcontratação, os riscos adicionais que podem surgir se o sub-subcontratante estiver localizado num país terceiro ou num país diferente do PSCN e, no caso de uma sub-subcontratação em cadeia, qualquer risco adicional que possa surgir, incluindo em relação à ausência de um contrato direto entre a empresa e o sub-subcontratante que exerce a função subcontratada;

vii. o risco de concentração na empresa (incluindo, se for o caso, ao nível do seu grupo), decorrente da celebração de múltiplos acordos de subcontratação de serviços de computação em nuvem com o mesmo PSCN, assim como o risco de concentração no setor financeiro da UE, decorrente do facto de várias empresas recorrerem ao mesmo PSCN ou a um grupo restrito de PSCN. Ao avaliar o risco de concentração, a empresa deve ter em conta todos os seus acordos de subcontratação de serviços de computação em nuvem (e, quando aplicável, os acordos de subcontratação ao nível do seu grupo) com esse PSCN;

b) ter em conta os benefícios e custos esperados do acordo de subcontratação de serviços de computação em nuvem, incluindo a ponderação de riscos significativos que possam ser reduzidos ou mais bem geridos face a riscos significativos que possam resultar do acordo de subcontratação.

21. Em caso de subcontratação de funções essenciais ou importantes, a devida diligência deverá incluir uma avaliação da adequação do PSCN. Ao avaliar a adequação do PSCN, a empresa deve assegurar que este possui a reputação comercial, as competências adequadas, os recursos (incluindo humanos, informáticos e financeiros), a estrutura organizativa e, se for caso disso, a(s) autorização(ões) ou registo(s) relevantes para desempenhar as funções essenciais ou importantes de uma forma fiável e profissional e cumprir as suas obrigações durante o período de vigência do acordo de subcontratação de serviços de computação em nuvem. Os fatores adicionais a ter em conta na devida diligência em relação ao PSCN devem incluir, entre outros:

    a) a gestão da segurança da informação e, em particular, a proteção de dados pessoais, confidenciais ou que sejam sensíveis por outras razões;
    b) o apoio ao serviço, incluindo planos e contactos de apoio, assim como os procedimentos de gestão de incidentes;
    c) os planos de continuidade das atividades e de recuperação em caso de catástrofe;

22. Sempre que adequado e a fim de apoiar o exercício de devida diligência, as empresas podem também utilizar certificações baseadas em normas internacionais e relatórios de auditoria externa ou interna.

23. Sempre que as empresas tiverem conhecimento de deficiências significativas e/ou alterações significativas nos serviços prestados ou na situação do PSCN, a análise prévia à subcontratação e a devida diligência em relação ao PSCN devem ser imediatamente revistas ou, se necessário, voltar a ser realizadas.

24. Caso uma empresa celebre um novo acordo ou renove um acordo em vigor com um PSCN que já tenha sido avaliado, deve determinar, em função do risco, se é necessário cumprir um novo dever de diligência.

Orientação 3. Requisitos contratuais

25. Os direitos e obrigações da empresa e do seu PSCN devem ser claramente definidos num acordo escrito.

26. O acordo escrito deve permitir expressamente à empresa rescindir o contrato, se necessário.

27. No caso da subcontratação de funções essenciais ou importantes, o acordo escrito deve incluir, pelo menos:

    a) uma descrição clara da função subcontratada;

    b) a data de início e a data de termo, se for caso disso, do acordo e os períodos de pré-aviso aplicáveis ao PSCN e à empresa;

    c) o direito que rege o acordo e, se for caso disso, a escolha da jurisdição;

    d) as obrigações financeiras da empresa e do PSCN;

    e) se é permitida a sub-subcontratação e, em caso afirmativo, em que condições, tendo em conta a Orientação 7;

    f) o(s) local(ais) (a saber, regiões ou países) onde será desempenhada a função subcontratada e onde os dados serão tratados e armazenados, bem como as condições a cumprir, incluindo a obrigação de notificar a empresa caso o PSCN pretenda alterar o(s) local(ais);

    g) disposições relativas à segurança da informação e à proteção dos dados pessoais, tendo em conta a Orientação 4;

    h) o direito de a empresa acompanhar regularmente o desempenho do PSCN ao abrigo do acordo de subcontratação de serviços de computação em nuvem, tendo em conta a Orientação 6;

    i) os níveis de serviço acordados, que devem incluir objetivos de desempenho quantitativos e qualitativos, a fim de permitir o acompanhamento em tempo útil e a adoção sem demora de medidas corretivas adequadas, caso os níveis de serviço acordados não sejam cumpridos;

    j) as obrigações de reporte do PSCN à empresa e, se for caso disso, as obrigações de apresentação de relatórios relevantes para a função de segurança da empresa e para as principais funções, tais como relatórios elaborados pela função de auditoria interna do PSCN;

    k) disposições relativas à gestão de incidentes pelo PSCN, incluindo a obrigação de o PSCN notificar à empresa sem demora incidentes que tenham afetado o desempenho do serviço contratado pela empresa;

l) se o PSCN deve subscrever um seguro obrigatório contra determinados riscos e, se for caso disso, o nível de cobertura exigido;

m) os requisitos de implementação e teste, por parte do PSCN, de planos de continuidade das atividades e de planos de recuperação em caso de catástrofe;

n) a obrigação de o PSCN conceder à empresa, às suas autoridades competentes e a qualquer outra pessoa designada pela empresa ou pelas autoridades competentes o direito de aceder («direitos de acesso») e inspecionar («direitos de auditoria») as informações, instalações, sistemas e dispositivos relevantes do PSCN, na medida do necessário para acompanhar o desempenho do PSCN no âmbito do acordo de subcontratação de serviços de computação em nuvem e o cumprimento dos requisitos regulamentares e contratuais aplicáveis, tendo em conta a Orientação 6;

o) disposições destinadas a assegurar que os dados tratados ou armazenados pelo PSCN em nome da empresa possam ser acedidos, recuperados e devolvidos à empresa, se necessário, tendo em conta a Orientação 5.

Orientação 4. Segurança da informação

28. As empresas devem estabelecer requisitos de segurança da informação nas suas políticas e procedimentos internos, assim como no seu acordo de subcontratação de serviços de computação em nuvem e controlar regularmente o cumprimento desses requisitos, incluindo proteger os dados confidenciais, pessoais ou que sejam sensíveis por outras razões. Estes requisitos devem ser proporcionais à natureza, escala e complexidade da função subcontratada pela empresa ao PSCN e aos riscos inerentes a essa função.

29. Para o efeito, na subcontratação de funções essenciais ou importantes, e sem prejuízo dos requisitos aplicáveis do RGPD, ao aplicar uma abordagem baseada no risco, as empresas devem, no mínimo:

a) *organização da segurança da informação:* assegurar uma clara repartição das funções e responsabilidades em matéria de segurança da informação entre a empresa e o PSCN, nomeadamente no que se refere à deteção de ameaças, à gestão de incidentes e de medidas corretivas, e garantir que o PSCN possa cumprir de forma eficiente as suas funções e responsabilidades;
b) *gestão de identidades e acessos*: assegurar a existência de mecanismos de autenticação fortes (por exemplo, autenticação multifatores) e de controlos de acesso, a fim de impedir o acesso não autorizado aos dados da empresa e aos recursos de retaguarda em nuvem;
c) *encriptação e gestão de chaves:* assegurar que sejam utilizadas, sempre que necessário, tecnologias de encriptação relevantes para os dados em trânsito, os dados em memória, os dados inativos e dados armazenados, em conjugação com

uma arquitetura de gestão de chaves adequada para limitar o risco de acesso não autorizado às chaves de cifragem; em particular, as empresas devem considerar os mais avançados processos e tecnologias ao selecionar as suas soluções de gestão de chaves;

d) *segurança de operações e de redes:* considerar níveis adequados de disponibilidade da rede, separação da rede (por exemplo, separação dos utilizadores no ambiente partilhado em nuvem, separação operacional no que diz respeito à Web, lógica de aplicação, sistema operativo, rede, Sistema de Gestão da Base de Dados – DBMS – e camadas de armazenamento) e ambientes de processamento (por exemplo, teste, teste de aceitação do utilizador, desenvolvimento, produção);
e) *interface de programação de aplicações (API):* considerar mecanismos para a integração dos serviços em nuvem com os sistemas da empresa, a fim de garantir a segurança das API (por exemplo, estabelecendo e mantendo políticas e procedimentos de segurança da informação para as API em várias interfaces de sistemas, jurisdições e funções comerciais, a fim de impedir a divulgação, modificação ou destruição não autorizadas de dados);
f) *continuidade das atividades e recuperação em caso de catástrofe*: assegurar a existência de controlos eficazes para garantir a continuidade das atividades e a recuperação em caso de catástrofe (por exemplo, estabelecendo requisitos mínimos de capacidade, selecionando opções de alojamento geograficamente dispersas, com capacidade de alternância entre as mesmas, ou solicitando e revendo documentação que permita visualizar os fluxos dos dados da empresa entre os sistemas do PSCN, assim como considerar a possibilidade de replicar imagens automatizadas para um local de armazenamento independente, que esteja suficientemente isolado da rede e possa ser retirado de linha);
g) *local de armazenamento de dados*: adotar uma abordagem baseada no risco para o(s) local(ais) de armazenamento e de processamento de dados (a saber, regiões ou países);
h) *conformidade e monitorização*: verificar se o PSCN cumpre as normas internacionalmente reconhecidas em matéria de segurança da informação e implementou controlos adequados em matéria de segurança da informação (por exemplo, solicitando ao PSCN que apresente provas de que procede a análises relevantes em matéria de segurança da informação e realizando avaliações e testes regulares dos sistemas e procedimentos do PSCN para garantir a segurança da informação).

Orientação 5. Estratégias de saída

30. Na subcontratação de funções essenciais ou importantes, as empresas devem assegurar que estão em condições de pôr termo ao acordo de subcontratação de serviços de computação em nuvem sem causar perturbações indevidas às suas atividades e serviços comerciais para os seus clientes, sem prejuízo do cumprimento

das suas obrigações nos termos da legislação aplicável e sem prejuízo também da confidencialidade, integridade e disponibilidade dos seus dados. Para o efeito, as empresas devem:

a) elaborar planos de saída abrangentes, documentados e suficientemente testados. Estes planos devem ser atualizados sempre que necessário, incluindo nos casos em que forem realizadas alterações na função subcontratada;
b) identificar soluções alternativas e elaborar planos de transição para eliminar a função e os dados subcontratados ao PSCN e, se for o caso, a qualquer sub-subcontratante, e transferi-los para o PSCN alternativo indicado pela empresa ou para a própria empresa. Estas soluções devem ser definidas tendo em conta os desafios que possam surgir devido à localização dos dados e adotando as medidas necessárias para garantir a continuidade da atividade durante a fase de transição;
c) assegurar que o acordo escrito de subcontratação de serviços de computação em nuvem inclua a obrigação de o PSCN apoiar a transferência ordenada da função subcontratada, assim como o tratamento dos respetivos dados, do PSCN e de qualquer sub-subcontratante para outro PSCN indicado pela empresa ou para a própria empresa quando a empresa ativar a estratégia de saída. A obrigação de apoiar a transferência ordenada da função subcontratada e o tratamento dos respetivos dados deve incluir, sempre que necessário, a eliminação segura dos dados contidos nos sistemas do PSCN e de qualquer sub-subcontratante.

31. Ao elaborar os planos e soluções de saída referidos nas alíneas a) e b) anteriores («estratégia de saída»), as empresas devem:

a) definir os objetivos da estratégia de saída;
b) definir os fatores que deverão desencadear a estratégia de saída. Estes fatores devem contemplar, pelo menos, a rescisão do acordo de subcontratação de serviços de computação em nuvem por iniciativa da empresa ou do PSCN e a incapacidade do PSCN em desempenhar a sua atividade ou outra situação que implique uma grave interrupção dessa atividade;
c) realizar uma análise do impacto das atividades que seja proporcional às atividades subcontratadas, a fim de identificar os recursos humanos e materiais que seriam necessários para implementar a estratégia de saída;
d) atribuir funções e responsabilidades para gerir a estratégia de saída;
e) testar a adequação da estratégia de saída, utilizando uma abordagem baseada no risco (por exemplo, realizando uma análise dos potenciais custos, do impacto, dos recursos e do tempo necessário para transferir um serviço subcontratado a outro prestador de serviços);
f) definir critérios de sucesso para a transição.

32. As empresas devem incluir indicadores para os fatores desencadeadores da estratégia de saída na sua ação de acompanhamento e supervisão permanentes dos serviços

prestados pelo PSCN no âmbito do acordo de subcontratação de serviços de computação em nuvem.

Orientação 6. Direitos de acesso e de auditoria

33. As empresas devem assegurar que o acordo escrito de subcontratação de serviços de computação em nuvem não limita o exercício efetivo, por parte da empresa e da autoridade competente, dos direitos de acesso e de auditoria, bem como as opções de controlo sobre o PSCN.

34. No exercício dos direitos de acesso e de auditoria (por exemplo, a frequência das auditorias e os domínios e serviços a auditar), as empresas devem considerar se a subcontratação está relacionada com uma função essencial ou importante e ter em conta a natureza e a dimensão dos riscos e do impacto que o acordo de subcontratação de serviços de computação em nuvem representa para a empresa.

35. Se o exercício dos direitos de acesso ou de auditoria, ou a utilização de determinados métodos de auditoria criarem riscos para o ambiente do PSCN e/ou de outro cliente do PSCN (por exemplo, afetando os níveis de serviço, a confidencialidade, a integridade e a disponibilidade dos dados), o PSCN deve apresentar à empresa uma justificação clara para esses riscos. Além disso, o PSCN deve acordar com a empresa formas alternativas de fornecer um nível de garantia e de serviço semelhante (por exemplo, a inclusão de controlos específicos a testar num relatório/certificação específico elaborado pelo PSCN).

36. Sem prejuízo da sua responsabilidade final no que se refere aos acordos de subcontratação de serviços de computação em nuvem e a fim de utilizar os recursos de auditoria de forma mais eficiente e diminuir os encargos administrativos para o PSCN e os seus clientes, as empresas podem utilizar:

    a) certificações de terceiros e relatórios de auditoria interna ou externa disponibilizados pelo PSCN;
    b) auditorias comuns realizadas conjuntamente com outros clientes do mesmo PSCN ou realizadas por uma entidade terceira designada por vários clientes do mesmo PSCN.

37. No caso da subcontratação de funções essenciais ou importantes, a empresa deve avaliar se as certificações de terceiros e os relatórios de auditoria externa ou interna referidos na alínea a) do ponto 37 são adequados e suficientes para cumprir as suas obrigações nos termos da legislação aplicável e não devem recorrer exclusivamente a essas certificações e relatórios ao longo do tempo.

38. No caso da subcontratação de funções essenciais ou importantes, a empresa só deverá recorrer às certificações de terceiros e aos relatórios de auditoria externa ou interna referidos na alínea a) do ponto 37 se:

    a) tiver confirmado que o âmbito das certificações ou dos relatórios de auditoria abrange os principais sistemas do PSCN (por exemplo, os processos, aplicações, infraestruturas, centros de dados), os principais controlos identificados pela empresa e permitir avaliar a conformidade com a legislação aplicável;
    b) efetuar uma avaliação exaustiva e regular do conteúdo das certificações ou dos relatórios de auditoria e verificar se os relatórios ou as certificações não são obsoletos;
    c) assegurar que os sistemas e controlos fundamentais do PSCN são incluídos em futuras versões das certificações ou dos relatórios de auditoria;
    d) tiver confirmado a aptidão da entidade de certificação ou de auditoria (por exemplo, no que diz respeito às suas qualificações, competências especializadas, repetição/verificação das provas constantes do processo de auditoria subjacente, bem como à rotatividade da empresa de certificação ou de auditoria);
    e) tiver confirmado que as certificações são emitidas e as auditorias são realizadas de acordo com as normas relevantes e incluem um teste da eficácia dos controlos fundamentais existentes;
    f) tiver o direito contratual de solicitar a extensão do âmbito das certificações ou dos relatórios de auditoria a outros sistemas e controlos relevantes do PSCN; o número e a frequência desses pedidos de alteração do âmbito devem ser razoáveis e legítimos do ponto de vista da gestão dos riscos;
    g) mantiver o direito contratual de realizar auditorias individuais no local, por sua livre iniciativa, em relação à função subcontratada.

39. As empresas devem assegurar que, antes de uma visita no local, incluindo por uma entidade terceira designada pela empresa (por exemplo, um auditor), seja enviada ao PSCN uma notificação prévia num prazo razoável, a menos que tal não seja possível devido a uma situação de emergência ou de crise ou que a notificação prévia comprometa a eficácia da auditoria. Nessa notificação prévia, devem ser indicados a localização e o objetivo da visita, assim como o pessoal que participará na mesma.

40. Tendo em conta que os serviços de computação em nuvem têm um elevado nível de complexidade técnica e suscitam desafios jurisdicionais específicos, as pessoas que realizam a auditoria (sejam os auditores internos da empresa ou auditores que atuam em seu nome) deverão possuir as competências e os conhecimentos apropriados para avaliar adequadamente os serviços de computação em nuvem relevantes e realizar auditorias eficazes e relevantes. O mesmo se aplica ao pessoal das empresas que fiscalizam as certificações ou os relatórios de auditoria apresentados pelo PSCN.

Orientação 7. Sub-subcontratação

41. Se a sub-subcontratação de funções essenciais ou importantes (ou partes significativas das mesmas) for autorizada, o acordo escrito de subcontratação de serviços de computação em nuvem entre a empresa e o PSCN deverá:

    a) especificar todas as partes ou aspetos da função subcontratada que são excluídos de uma potencial sub-subcontratação;
    b) indicar as condições a respeitar em caso de sub-subcontratação;
    c) especificar que o PSCN continua a ser responsável e é obrigado a supervisionar os serviços que sub-subcontratou para garantir que todas as obrigações contratuais entre o PSCN e a empresa devem ser permanentemente cumpridas;
    d) incluir a obrigação de o PSCN informar a empresa de qualquer sub-subcontratação prevista ou de quaisquer alterações significativas nessa sub-subcontratação, em especial, quando tal possa afetar a capacidade do PSCN para cumprir as obrigações que lhe incumbem por força do acordo de subcontratação de serviços de computação em nuvem com a empresa. O prazo de notificação estabelecido no acordo escrito deve permitir que a empresa disponha de tempo suficiente para realizar, pelo menos, uma avaliação dos riscos de uma proposta de sub-subcontratação proposta ou de propostas de alterações significativas numa sub-subcontratação e opor-se ou aprovar explicitamente tal proposta de sub-subcontratação, conforme indicado na alínea e) abaixo;
    e) assegurar que a empresa tem o direito de se opor a uma proposta de sub-subcontratação ou a alterações significativas numa sub-subcontratação, ou que qualquer proposta de sub-subcontratação ou alteração a uma sub-subcontratação seja sujeita a uma aprovação explícita antes de ser implementada;
    f) assegurar que a empresa tem o direito contratual de pôr termo ao acordo de subcontratação de serviços de computação em nuvem com o PSCN caso se oponha a uma sub-subcontratação ou a alterações significativas de uma sub-subcontratação e em caso de sub-subcontratação indevida (por exemplo, quando o PSCN sub-subcontrata um serviço ou função a outra entidade sem notificar a empresa ou viola gravemente as condições de sub-subcontratação especificadas no acordo de subcontratação).

42. A empresa deve assegurar que o PSCN supervisiona adequadamente o sub-subcontratante.

Orientação 8. Notificação por escrito às autoridades competentes

43. As empresas devem notificar por escrito a sua autoridade competente, em tempo útil, de qualquer acordo de subcontratação de serviços de computação em nuvem que tencionem celebrar em relação a uma função essencial ou importante. As empresas devem igualmente notificar, em tempo útil e por escrito, a sua autoridade competente de qualquer acordo de subcontratação de serviços de computação em nuvem

relacionado com uma função anteriormente classificada como não essencial ou não importante e que tenha posteriormente passado a ser considerada como essencial ou importante.

44. A notificação por escrito por parte das empresas deve incluir, tendo em conta o princípio da proporcionalidade, pelo menos as seguintes informações:

    a) a data de início do acordo de subcontratação de serviços de computação em nuvem e, se for caso disso, a data da próxima renovação do contrato, a data do termo do contrato e/ou os períodos de pré-aviso aplicáveis ao prestador de serviços de computação em nuvem e à empresa;
    b) uma breve descrição da função subcontratada;
    c) um breve resumo das razões pelas quais a função subcontratada é considerada essencial ou importante;
    d) o nome e a marca (se for caso disso) do PSCN, o seu país de registo, o número de registo da sociedade, o seu identificador de entidade jurídica (se existir), a morada da sede social, os dados de contacto pertinentes e o nome da sua empresa-mãe (se for caso disso);
    e) o direito que rege o acordo de subcontratação de serviços de computação em nuvem e, se for caso disso, a escolha da jurisdição;
    f) os modelos de implantação da nuvem, assim como a natureza específica dos dados a conservar pelo PSCN e os locais (a saber, regiões ou países) onde esses dados irão ser armazenados;
    g) a data da avaliação mais recente do caráter essencial ou da importância da função subcontratada;
    h) a data da mais recente avaliação ou auditoria de riscos associados ao PSCN e um breve resumo dos principais resultados, assim como a data da próxima avaliação ou auditoria de riscos programada;
    i) o órgão individual ou decisório da empresa que aprovou o acordo de subcontratação de serviços de computação em nuvem;
    j) se for caso disso, os nomes dos sub-subcontratantes aos quais sejam sub-subcontratadas partes significativas de uma função essencial ou importante, incluindo o país ou região onde os sub-subcontratantes estão registados, o país ou região onde será realizado o serviço sub-subcontratado e o local onde os dados serão armazenados;

Orientação 9. Supervisão dos acordos de subcontratação de serviços de computação em nuvem

45. As autoridades competentes deverão avaliar os riscos decorrentes dos acordos de subcontratação de serviços de computação em nuvem celebrados pelas empresas no âmbito do seu processo de supervisão. Esta avaliação deve incidir, em particular, nos acordos relacionados com a subcontratação de funções essenciais ou importantes.

46. As autoridades competentes devem certificar-se de que têm condições para exercer uma supervisão efetiva, em especial, quando as empresas subcontratam funções essenciais ou importantes que são desempenhadas fora da UE.

47. As autoridades competentes devem avaliar, usando uma abordagem baseada no risco, se as empresas:

    a) dispõem dos relevantes meios de governação, recursos e processos operacionais para celebrar, implementar e supervisionar de forma adequada e eficaz acordos de subcontratação de serviços de computação em nuvem;
    b) identificam e gerem todos os riscos relevantes relacionados com a subcontratação de serviços de computação em nuvem.

48. Sempre que sejam identificados riscos de concentração, as autoridades competentes devem acompanhar a evolução desses riscos e avaliar quer o seu potencial impacto noutras empresas por si supervisionadas, quer a estabilidade do mercado financeiro.