EBA/GL/2019/02

25 de febrero de 2019

Informe final sobre

Directrices de la EBA sobre acuerdos de subcontratación

**Resumen ejecutivo**

La confianza en la confiabilidad del sistema financiero es fundamental para su correcto funcionamiento y es un requisito previo para contribuir a la economía en su conjunto. Los acuerdos de gobernanza interna eficaces son fundamentales para que las instituciones, individualmente, y el sistema financiero que forman en su conjunto, funcionen bien.

En los últimos años, las instituciones financieras se han interesado cada vez más en la subcontratación de actividades comerciales también con el fin de reducir costos y mejorar su flexibilidad y eficiencia. En el contexto de la digitalización y la creciente importancia de los proveedores de nuevas tecnologías financieras (fintech), las instituciones financieras están adaptando sus modelos de negocio para adoptar dichas tecnologías. Algunos tienen intensificaron el uso de soluciones fintech y lanzaron proyectos para mejorar su rentabilidad también en respuesta a los márgenes de intermediación del modelo de negocio bancario tradicional que se ven presionados por el entorno de tipos de interés bajos. La subcontratación es una forma de obtener un acceso relativamente fácil a las nuevas tecnologías y lograr economías de escala.

La Directiva 2013/36 / EU (Directiva sobre requisitos de capital; CRD) refuerza los requisitos de gobernanza para las entidades y el artículo 74, apartado 3, de la CRD otorga a la EBA el mandato de desarrollar directrices sobre los mecanismos de gobernanza de las entidades. La subcontratación es uno de los aspectos específicos de los arreglos de gobernanza de las instituciones. La Directiva 2014/65 / EU (Directiva de Mercados de Instrumentos Financieros; MiFID II) contiene disposiciones explícitas sobre la subcontratación de funciones en el ámbito de los servicios y actividades de inversión. La Directiva 2015/2366 / EU (Directiva de servicios de pago revisada; PSD2) establece requisitos para la subcontratación de funciones por parte de las entidades de pago.

La EBA está actualizando las directrices del Comité de Supervisores Bancarios Europeos (CEBS) sobre subcontratación emitidas en 2006, que se aplicaban exclusivamente a las entidades de crédito; el objetivo es establecer un marco más armonizado para todas las instituciones financieras que están dentro del alcance del mandato de la EBA, a saber, las instituciones de crédito y las empresas de inversión sujetas a la CRD, así como las instituciones de pago y de dinero electrónico. Las directrices establecen disposiciones específicas para los marcos de gobernanza de estas instituciones financieras con respecto a sus acuerdos de subcontratación y las expectativas y procesos de supervisión relacionados. La recomendación sobre la subcontratación a proveedores de servicios en la nube, publicada en diciembre de 2017, se ha integrado en las directrices.

El órgano de administración de cada institución financiera sigue siendo responsable de esa institución y de todas sus actividades, en todo momento; Con este fin, el órgano de administración debe asegurarse de que se dispone de recursos suficientes para respaldar y garantizar adecuadamente el desempeño de esas responsabilidades, incluida la supervisión de todos los riesgos y la gestión de los acuerdos de subcontratación. La subcontratación no debe conducir a una situación en la que una institución se convierta en un "caparazón vacío" que carece de la sustancia para permanecer autorizada.

Con respecto a la subcontratación a proveedores de servicios ubicados en terceros países, se espera que las instituciones financieras presten especial atención al cumplimiento de la legislación y los requisitos reglamentarios de la EU. (por ejemplo, el secreto profesional, el acceso a la información y los datos, la protección de los datos personales) y que la autoridad competente pueda supervisar eficazmente a las instituciones financieras, en particular en lo que respecta a funciones críticas o importantes subcontratadas a proveedores de servicios.

Las directrices establecen qué acuerdos con terceros deben considerarse subcontratación y proporcionan criterios para la identificación de funciones críticas o importantes que tienen un fuerte impacto en el perfil de riesgo de la institución financiera o en su marco de control interno. Si se subcontratan estas funciones críticas o importantes, se aplican requisitos más estrictos a estos acuerdos de subcontratación que a otros acuerdos de subcontratación.

Se requiere que las autoridades competentes supervisen eficazmente los acuerdos de subcontratación de las instituciones financieras, incluida la identificación y el seguimiento de las concentraciones de riesgo en los proveedores de servicios individuales y la evaluación de si tales concentraciones podrían representar un riesgo para la estabilidad del sistema financiero. Para identificar tales concentraciones de riesgo, las autoridades competentes deben poder confiar en la documentación completa sobre los acuerdos de subcontratación compilados por las instituciones financieras.

**Próximos pasos**

Las directrices entrarán en vigor el 30 de septiembre de 2019. Las directrices de 2006 sobre subcontratación y la recomendación de la EBA sobre subcontratación a proveedores de servicios en la nube serán derogadas al mismo tiempo.

**Antecedentes**

1. La confianza en la fiabilidad del sistema financiero es fundamental para su correcto funcionamiento y es un requisito previo para contribuir a la economía en su conjunto. Los mecanismos de gobernanza interna eficaces son fundamentales si las entidades de crédito y las empresas de inversión sujetas a la Directiva 2013/36/EU [[1]](#footnote-1)(CRD) (ambas denominadas ``entidades''), las entidades de pago y las entidades de dinero electrónico (ambas denominadas ``entidades de pago'') el sistema financiero ellos forman parte de son para funcionar bien.

2. En los últimos años, las instituciones y las instituciones de pago han tendido cada vez más a subcontratar actividades también con el fin de reducir costes y mejorar la flexibilidad y la eficiencia. En el contexto de la digitalización y la creciente importancia de las tecnologías de la información (IT) y las tecnologías financieras (fintech), las instituciones y las instituciones de pago están adaptando sus modelos de negocio, procesos y sistemas para adoptar dichas tecnologías. La IT se ha convertido en una de las actividades más comúnmente subcontratadas. A pesar de sus beneficios, la subcontratación de servicios de datos y IT plantea problemas de seguridad y desafíos para el marco de gobierno de las instituciones y las instituciones de pago, en particular para los controles internos, así como para la gestión y protección de datos.

3. Algunas instituciones e instituciones de pago han intensificado el uso de soluciones informáticas y fintech y han puesto en marcha proyectos para mejorar su rentabilidad también en respuesta a los márgenes de intermediación del modelo de crédito bancario tradicional que se ve sometido a presión por el entorno de tipos de interés bajos. La subcontratación es una forma de obtener un acceso relativamente fácil a las nuevas tecnologías y lograr economías de escala, p. Ej. Centralizando funciones dentro de un grupo o esquema de protección institucional.

4. La importancia de la subcontratación de funciones para los proveedores de servicios en la nube ha aumentado rápidamente en muchas industrias. En 2017, la EBA abordó las especificidades de la subcontratación a la nube mediante el desarrollo de recomendaciones sobre la subcontratación a proveedores de servicios en la nube,[[2]](#footnote-2) que se basaron en las directrices de subcontratación del CEBS de 2006. Las recomendaciones encaminadas a superar el alto nivel de incertidumbre con respecto a las expectativas de los supervisores sobre subcontratación a proveedores de servicios en la nube y en la eliminación de las barreras que esta incertidumbre provocó para las instituciones que procedían a utilizar los servicios en la nube. Las recomendaciones se han integrado en las presentes directrices y serán derogadas cuando las directrices entren en vigor.

5. La subcontratación de funciones importantes o críticas, en particular cuando el proveedor de servicios se encuentra fuera de la EU, crea riesgos específicos tanto para las entidades y las entidades de pago como para sus autoridades competentes y debe estar sujeta a la supervisión adecuada. Cualquier subcontratación que suponga la delegación por parte del órgano de administración de su responsabilidad, alterando la relación y obligaciones de la entidad o entidad de pago con sus clientes, menoscabando las condiciones de su autorización o suprimiendo o modificando alguna de las condiciones a las que la entidad o se otorgó la autorización de la entidad de pago, no debe ser permitido. Los acuerdos de subcontratación no deben crear riesgos operativos indebidos ni menoscabar la calidad e independencia de los controles internos de las entidades y las entidades de pago ni la capacidad de dichas entidades y entidades de pago y de las autoridades competentes para supervisar y supervisar el cumplimiento de los requisitos reglamentarios.

6. La responsabilidad del órgano de administración de las instituciones y las instituciones de pago para la institución o la institución de pago y todas sus actividades nunca podrá subcontratarse.

7. La subcontratación también es pertinente en el contexto de obtener o mantener el acceso al mercado financiero de la EU. Las instituciones de terceros países y las instituciones de pago pueden desear establecer filiales o sucursales en la EU para obtener o mantener el acceso a las infraestructuras y los mercados financieros de la EU. En este contexto, las instituciones de terceros países y las instituciones de pago pueden intentar minimizar la transferencia del desempeño efectivo de las actividades comerciales a sus filiales y sucursales ubicadas en la EU, p. confiando en la subcontratación de funciones a la institución matriz del tercer país u otras entidades del grupo de terceros países.

8. La subcontratación no debe dar lugar a una situación en la que una entidad o una entidad de pago se convierta en un "caparazón vacío" que carece de la sustancia para permanecer autorizada. Con este fin, el órgano de administración debe asegurarse de que se dispone de recursos suficientes para respaldar y garantizar de manera adecuada el desempeño de sus responsabilidades, incluida la supervisión de los riesgos y la gestión de los acuerdos de subcontratación

9. Las funciones que se consideran críticas desde la perspectiva de la resolución también pueden subcontratarse. Los acuerdos de subcontratación no deben crear impedimentos para la resolubilidad de la institución.

10. Las autoridades competentes deben conceder la autorización en pleno cumplimiento de la legislación de la Unión. Debe establecer un marco estricto, en consonancia con estas directrices, sobre la subcontratación por parte de las instituciones y el pago instituciones de la UE a entidades de terceros países; y debe garantizar una supervisión coherente y eficaz. Las autoridades competentes también deben garantizar que las entidades y las entidades de pago cuenten con políticas y procedimientos para cumplir con el marco pertinente en todo momento.

11. Las instituciones y las instituciones de pago deben poder controlar y cuestionar de manera efectiva la calidad y el desempeño de las funciones subcontratadas y poder llevar a cabo su propia evaluación de riesgos y monitoreo continuo. No es suficiente que las instituciones y las instituciones de pago lleven a cabo únicamente evaluaciones formales de si las funciones subcontratadas cumplen o no con los requisitos reglamentarios.

12. Las directrices deben leerse junto con, pero sin perjuicio de, las Directrices de la EBA sobre gobernanza interna (que ya incluyen requisitos sobre la subcontratación de entidades políticas), las Directrices de la EBA sobre procedimientos y metodologías comunes para el proceso de revisión y evaluación supervisora ​​(SREP) y las Directrices de la EBA sobre evaluación de riesgos de tecnologías de la información y la comunicación (TIC) en el marco del SREP

12. Las directrices deben leerse junto con, pero sin perjuicio de, las Directrices de la ABE sobre gobernanza interna (que ya incluyen requisitos sobre las políticas de subcontratación de las entidades), las Directrices de la ABE sobre procedimientos y metodologías comunes para el proceso de revisión y evaluación supervisora ​​(SREP) y las Directrices de la ABE sobre evaluación de riesgos de tecnologías de la información y la comunicación (ICT) en el marco del SREP

13. Para las entidades de pago, estas directrices deben leerse junto con las Directrices de la ABE sobre la información que debe facilitarse para la autorización de las entidades de pago en virtud de la Directiva 2015/2366 / UE[[3]](#footnote-3) (PSD2), las Directrices de la ABE sobre medidas de seguridad para riesgos operativos y de seguridad. Según la PSD2[[4]](#footnote-4) y las Directrices de la EBA sobre notificación de incidentes importantes según la PSD2.[[5]](#footnote-5)

14.Todos los requisitos establecidos en estas directrices están sujetos al principio de proporcionalidad; Deben aplicarse de manera adecuada, teniendo en cuenta, en particular, el tamaño y la organización interna de la entidad o entidad de pago y la naturaleza, alcance y complejidad de sus actividades.

**Justificación y objetivo de las directrices**

15. La ABE está actualizando las directrices del CEBS sobre subcontratación emitidas en 2006, que se aplicaban exclusivamente a las entidades de crédito, con el objetivo de establecer un marco más armonizado para los acuerdos de subcontratación de las entidades financieras. El ámbito de aplicación de estas directrices abarca no solo las entidades de crédito y las empresas de inversión sujetas a la CRD (denominadas "instituciones"), sino también las instituciones de pago y de dinero electrónico (denominadas "entidades de pago"). Las directrices no están dirigidas directamente a los intermediarios de crédito y acreedores no bancarios sujetos a la Directiva 2014/17 / EU[[6]](#footnote-6) ni a los proveedores de servicios de información de cuentas que solo están registrados para la prestación del servicio 8 del anexo I de la PSD2. Los acuerdos de subcontratación entre instituciones, instituciones de pago y dichas entidades están dentro del alcance de las directrices cuando dichas entidades actúan como proveedores de servicios de subcontratación.

16. La actualización de las directrices tiene en cuenta y es coherente con los requisitos actuales de la CRD, la Directiva 2014/65 / EU[[7]](#footnote-7) (MiFID II), la Directiva 2009/110 / EC[[8]](#footnote-8) (Directiva de dinero electrónico; EMD), la PSD2 y la Directiva. 2014/59 / EU[[9]](#footnote-9) (Directiva de Recuperación y Resolución Bancaria; BRRD) y las respectivas regulaciones delegadas adoptadas por la Comisión Europea. Además, se han tenido en cuenta los desarrollos internacionales en esta área, como los principios revisados ​​de gobierno corporativo para bancos y las directrices sobre riesgo de paso publicadas por el Comité de Supervisión Bancaria de Basilea (BCBS).

17 De conformidad con el artículo 16 del Reglamento (EU) n.o 1093/2010[[10]](#footnote-10) (el Reglamento de la EBA), la EBA está obligada a emitir directrices y recomendaciones dirigidas a las autoridades competentes y las instituciones financieras con el fin de establecer prácticas de supervisión coherentes, eficientes y eficaces y garantizar la aplicación común, uniforme y coherente del Derecho de la Unión. En particular, las condiciones para la subcontratación de funciones de las actividades bancarias por parte de las instituciones no están armonizadas en la misma medida que para las instituciones e instituciones de pago sujetas a MiFID II y PSD2.

18. Los enfoques regulatorios divergentes conllevan el riesgo de arbitraje regulatorio, que puede exponer a la EU a riesgos para la estabilidad financiera. Estos riesgos son especialmente graves en relación con la subcontratación de funciones por parte de entidades y entidades de pago a terceros países, donde las autoridades de supervisión pueden carecer de los poderes y herramientas necesarios para supervisar de forma adecuada y eficaz a los proveedores de servicios que proporcionan funciones críticas o importantes a las entidades de la EU y las entidades de pago. .

19. Es necesario dar una definición clara de lo que se considera subcontratación. La definición proporcionada en las directrices está en consonancia con el Reglamento Delegado (EU) 2017/565[[11]](#footnote-11) de la Comisión relacionado que complementa MiFID II.

20. El uso del término "funciones críticas o importantes" se basa en la redacción de MiFID II y el Reglamento Delegado (EU) 2017/565 de la Comisión que complementa MiFID II. Se utiliza únicamente con el fin de identificar "funciones críticas o importantes" en los acuerdos de subcontratación a los que se aplica un conjunto específico de requisitos. El Reglamento Delegado (EU) 2017/565 de la Comisión específica, en virtud del artículo 30, que `` una función operativa se considerará crítica o importante cuando un defecto o falla en su desempeño pudiera perjudicar sustancialmente el cumplimiento continuo por una empresa de servicios de inversión de las condiciones y obligaciones ''. De su autorización o de sus otras obligaciones en virtud de la Directiva 2014/65 / EU, o de su rendimiento financiero, o de la solidez o la continuidad de sus servicios y actividades de inversión ». El mismo enfoque existe en virtud de la Directiva 2009/138 /EC[[12]](#footnote-12) (Solvencia II), mientras que, en el contexto de la subcontratación, la PSD2 utiliza "función importante" con el fin de identificar funciones en los acuerdos de subcontratación para las que se aplican requisitos específicos. Por lo tanto, para adoptar toda la legislación existente y garantizar la igualdad de condiciones para las instituciones de crédito, empresas de inversión, instituciones de pago e instituciones de dinero electrónico, en las directrices se utiliza la redacción utilizada en MiFID II. Cabe señalar que la definición de "función crítica o importante" a los efectos de la subcontratación utilizada en estas directrices es diferente de la definición de "funciones críticas" del artículo 2 (1) (35) de la BRRD.

21 El artículo 109, apartado 2, de la DRC exige que las empresas matrices y las filiales sujetas a la presente Directiva cumplan los requisitos de gobernanza no solo de forma individual, sino también consolidada o subconsolidada, a menos que se hayan concedido exenciones para la solicitud individual en virtud de Artículo 21 de la DRC o artículo 109, apartado 1, de la DRC en conjunción con el artículo 7 del Reglamento (UE) n.o 575/2013 (Reglamento de requisitos de capital; CRR).[[13]](#footnote-13) Debe garantizarse que las empresas matrices y las filiales sujetas a la CRD implementen tales acuerdos, procesos y mecanismos en sus filiales no sujetas a la presente Directiva (por ejemplo, instituciones de pago e instituciones de dinero electrónico, así como empresas sujeto a la Directiva 2011/61 / EU[[14]](#footnote-14) y la Directiva 2009/65 / EC1).[[15]](#footnote-15) Los arreglos, procesos y mecanismos de gobierno deben ser consistentes y estar bien integrados, y aquellas subsidiarias que no estén sujetas al CRD también deben poder producir cualquier dato e información relevante para el propósito de supervisión.

**Gobernanza de los acuerdos de subcontratación**

22. De conformidad con el artículo 74 de la DRC, las entidades y las instituciones de pago (de conformidad con el artículo 11 de la PSD2) deben contar con mecanismos de gobernanza interna sólidos que incluyan una estructura organizativa clara. Los acuerdos de subcontratación son un aspecto de la estructura organizativa de las instituciones y las instituciones de pago. Las pautas incluyen requisitos que tienen como objetivo garantizar que:

1. Existe una gestión diaria eficaz por parte de la alta dirección o del órgano de dirección;[[16]](#footnote-16)
2. Existe una supervisión eficaz por parte del órgano de dirección;
3. Existe una política de subcontratación sólida y procesos de subcontratación sólidos;
4. Las instituciones y las instituciones de pago cuentan con un marco de control interno eficaz y eficiente, incluso con respecto a sus funciones subcontratadas;
5. Todos los riesgos asociados con la subcontratación de funciones críticas o importantes se identifican, evalúan, monitorean, gestionan, informan y, según corresponda, mitigan;
6. Existen planes adecuados para la salida de los acuerdos de subcontratación de funciones críticas o importantes, p. ej. migrando a otro proveedor de servicios o reintegrando las funciones críticas o importantes subcontratadas; y
7. Las autoridades competentes siguen siendo capaces de supervisar eficazmente las instituciones y las instituciones de pago, incluidas las funciones que se han subcontratado.

23. Las instituciones y las instituciones de pago deben determinar si la función que se subcontratará se considera crítica o importante. Las directrices proporcionan criterios para asegurar que la evaluación de la criticidad o importancia de las funciones esté más armonizada. La subcontratación de funciones críticas e importantes puede tener un fuerte impacto en el perfil de riesgo de la institución o de la institución de pago. Con este fin, se aplican requisitos adicionales a la subcontratación de funciones críticas o importantes, cuyo objetivo es garantizar la solidez de sus mecanismos de gobernanza y que las autoridades competentes puedan ejercer una supervisión eficaz.

24 Si bien las directrices se centran en la subcontratación de funciones críticas o importantes, las instituciones y las instituciones de pago deben considerar que recibir servicios, incluidos los servicios de TI, de terceros crea riesgos, incluso cuando esos acuerdos no se consideran acuerdos de subcontratación o cuando el Los acuerdos de subcontratación se referirían a funciones que no son críticas o importantes. Para gestionar todos los riesgos, las entidades y las entidades de pago deben evaluar los riesgos que resultan o pueden resultar de esos acuerdos, en particular el riesgo operativo y reputacional.

25 Los riesgos a considerar incluyen los asociados con la relación de la entidad o la entidad de pago con el proveedor de servicios, el riesgo causado por permitir la subcontratación, el riesgo de concentración que plantean múltiples subcontrataciones al mismo proveedor de servicios y / o el riesgo de concentración planteado. Subcontratando funciones críticas o importantes a un número limitado de proveedores de servicios. La concentración de la subcontratación en un número limitado de proveedores de servicios es especialmente relevante para las autoridades competentes a la hora de supervisar el impacto de la subcontratación en la estabilidad del mercado financiero. Además, es probable que la dependencia excesiva de la subcontratación de funciones críticas o importantes afecte a las condiciones de autorización y aumente tanto los riesgos de concentración como el riesgo de crear "cáscaras vacías" que carecerían de la sustancia para seguir autorizadas.

26 De manera similar, los acuerdos de subcontratación con cadenas operativas largas o complejas y / o con un gran número de partes involucradas probablemente den lugar a desafíos adicionales tanto para las instituciones como para las empresas entidades de pago y autoridades competentes.

27. Cada forma de subcontratación tiene sus riesgos y ventajas específicos. Sin perjuicio de las exenciones incluidas en los artículos 21 de la CRD que puedan concederse cuando se cumplan las condiciones previstas en el artículo 10 de la CRR

y las exenciones con arreglo al artículo 109, apartado 1, de la DRC que se aplican cuando las autoridades competentes han concedido la excepción con arreglo al artículo 7 del RRC, la subcontratación intragrupo está sujeta al mismo marco regulador que la subcontratación a proveedores de servicios fuera del grupo. La subcontratación intragrupo no es necesariamente menos riesgosa que la subcontratación a una entidad fuera del grupo. En particular, con respecto a la subcontratación intragrupo, las instituciones y las instituciones de pago deben tener en cuenta los conflictos de intereses que pueden ser causados ​​por acuerdos de subcontratación, p. Ej. Entre diferentes entidades dentro del perímetro de consolidación.

28. Cuando las entidades e instituciones de pago pretendan subcontratar funciones importantes o críticas a entidades dentro del mismo grupo, deben asegurarse de que la selección de una entidad del grupo se base en razones objetivas y que las condiciones del acuerdo de subcontratación se establezcan en condiciones de mercado y Abordar explícitamente los conflictos de intereses que pueda entrañar dicho acuerdo de subcontratación. Las instituciones y las instituciones de pago deben identificar claramente todos los riesgos relevantes y detallar las medidas de mitigación y los controles implementados para garantizar que los acuerdos de subcontratación con entidades afiliadas no perjudiquen la capacidad de la institución o de la institución de pago para cumplir con el marco regulatorio relevante. Sin embargo, al subcontratar dentro del mismo grupo, las entidades y las entidades de pago pueden tener un mayor nivel de control sobre la función subcontratada, que podrían tener en cuenta en su evaluación de riesgos.

29. Los mismos aspectos que son relevantes para la subcontratación dentro de un grupo son válidos cuando las instituciones que son miembros de un esquema de protección institucional subcontratan funciones a un proveedor central de servicios.

30. La subcontratación de funciones críticas o importantes a proveedores de servicios ubicados en terceros países debe estar sujeta a salvaguardias adicionales que garanticen que esta subcontratación no da lugar a un aumento indebido del riesgo o no menoscaba la capacidad de las autoridades competentes para supervisar eficazmente las entidades y las entidades de pago.

31. Las instituciones también deben contar con mecanismos de gobernanza sólidos para los acuerdos de subcontratación que no se consideren críticos o importantes. Por lo tanto, las directrices proporcionan algunos requisitos que se aplican a todos los acuerdos de subcontratación y, de manera más general, a todos los acuerdos con terceros, teniendo en cuenta la aplicación del principio de proporcionalidad.

32. La externalización no reduce la obligación de las instituciones y las instituciones de pago de cumplir con los requisitos reglamentarios y los valores corporativos internos, p. Ej. Los establecidos en un código de conducta. Al seleccionar proveedores de servicios, las instituciones y las instituciones de pago deben prestar especial atención a los derechos humanos y tener en cuenta el impacto de su subcontratación en todas las partes interesadas; esto incluye tener en cuenta sus responsabilidades sociales y ambientales. Estos aspectos son de especial relevancia cuando los proveedores de servicios están ubicados en terceros países.

33. Las instituciones y las instituciones de pago deben gestionar la relación contractual; esto incluye evaluar y monitorear la capacidad del proveedor de servicios para cumplir con las condiciones incluidas en el contrato de subcontratación por escrito. De hecho, una mayor dependencia del proveedor de servicios con respecto a las funciones subcontratadas, en particular con respecto a las funciones críticas o importantes, puede tener un impacto en la capacidad de las entidades y las entidades de pago para gestionar sus riesgos, como los riesgos operativos, incluidos los riesgos de cumplimiento y de reputación. .

34. Se proporciona orientación específica sobre la relación entre las instituciones, las instituciones de pago y los proveedores de servicios, incluidos sus derechos y obligaciones. La directriz especifica un conjunto de aspectos que deben incluirse en el contrato de subcontratación por escrito.

35. Los arreglos de contratación externa también deben considerarse en el contexto de la planificación de la recuperación y la planificación de la resolución de las instituciones; la continuidad operativa de las funciones críticas debe garantizarse incluso cuando se encuentran en dificultades financieras o durante la reestructuración o resolución financiera. La decisión empresarial de subcontratar una función no debe impedir en modo alguno la resolubilidad de la institución.

36. Las instituciones, las instituciones de pago y las autoridades competentes, incluidas las autoridades de resolución, el derecho a las inspecciones y el acceso a la información, las cuentas y los locales deben estar garantizados en el contrato de subcontratación por escrito. El derecho a auditar es clave para proporcionar la garantía adecuada de que al menos las funciones críticas o importantes subcontratadas, así como las funciones que pueden llegar a ser críticas o importantes en el futuro, se brindan según lo acordado contractualmente y de acuerdo con los requisitos reglamentarios. Sin embargo, los derechos de auditoría y acceso de las autoridades competentes deben garantizarse para todos los acuerdos de subcontratación para garantizar que las instituciones pueden ser supervisadas de manera eficaz. Se proporciona más orientación sobre cómo las instituciones y las instituciones de pago pueden ejercer sus derechos de auditoría de una manera basada en el riesgo, teniendo en cuenta preocupaciones con respecto a la carga organizativa tanto para la institución de subcontratación o la institución de pago como para el proveedor de servicios, así como preocupaciones prácticas, de seguridad y confidencialidad con respecto al acceso físico a ciertos tipos de instalaciones comerciales y el acceso a los datos en entornos de múltiples inquilinos.

**Subcontratación de IT, incluida la tecnología financiera y la subcontratación a proveedores de servicios en la nube**

37. Las instituciones y las instituciones de pago deben asegurarse de que los datos personales estén adecuadamente protegidos y se mantengan confidenciales. Las instituciones y entidades de pago están dentro del ámbito de aplicación del Reglamento (EU) 2016/679[[17]](#footnote-17) (Reglamento general de protección de datos; RGPD) y deben cumplirlo. Al subcontratar servicios de datos o IT, es imperativo que la continuidad del negocio y los datos la protección se considera apropiadamente. Estas consideraciones no se limitan a la subcontratación de IT, sino que se aplican en general. Las instituciones y las instituciones de pago deben asegurarse de que cumplen con los estándares de seguridad de la información aceptados internacionalmente y esto también se aplica a las infraestructuras y servicios de IT subcontratados

38. Las instituciones y las instituciones de pago deben contar con acuerdos de contingencia y continuidad del negocio para garantizar que sus actividades comerciales importantes se puedan realizar de forma continua. Por lo tanto, algunos proveedores de servicios también requieren tales arreglos, en particular en lo que respecta a las funciones subcontratadas que son críticas o importantes.[[18]](#footnote-18)

39 La EBA identificó diferencias en los marcos regulatorios y de supervisión nacionales para la subcontratación en la nube, p. Ej. En cuanto a los requisitos de información que debían cumplir las instituciones y, por ello, en 2017 emitieron recomendaciones para la subcontratación a proveedores de servicios en la nube. Las recomendaciones se diseñaron para incorporar estas directrices revisadas para garantizar que las instituciones tengan un marco único para todos sus acuerdos de subcontratación. De hecho, varios aspectos de las recomendaciones se aplican en general y son relevantes más allá de la subcontratación a proveedores de servicios en la nube, y esos aspectos generales se reflejan en estas directrices. Sin embargo, cuando sea apropiado y relevante, algunos requisitos específicos son aplicables exclusivamente a la subcontratación en la nube.

40. El rendimiento y la calidad de la prestación de servicios del proveedor de servicios en la nube y el nivel de riesgo operativo que puede causar a la institución de subcontratación o de pago están determinados en gran medida por la capacidad del proveedor de servicios en la nube para proteger adecuadamente la confidencialidad, integridad y disponibilidad de datos (en tránsito o en reposo) y de los sistemas y procesos que se utilizan para procesar, transferir o almacenar esos datos. Los mecanismos de trazabilidad adecuados destinados a mantener registros de las operaciones técnicas y comerciales también son clave para detectar intentos maliciosos de violar la seguridad de los datos y los sistemas. Las expectativas de seguridad deben tener en cuenta la necesidad, con un enfoque basado en el riesgo, de proteger los datos y los sistemas.

41. Los proveedores de servicios en la nube a menudo operan una infraestructura informática geográficamente dispersa que implica la distribución regional y / o global del almacenamiento y procesamiento de datos; por lo tanto, la seguridad y privacidad de los datos y su procesamiento requieren una atención especial. Sin perjuicio de los requisitos incluidos en estas directrices, se aplican las leyes de la Unión y nacionales a este respecto y, en particular con respecto a las obligaciones o derechos contractuales mencionados en estas directrices, se debe prestar atención a las normas de protección de datos y los requisitos de secreto profesional.

42. Con respecto a la subcontratación, la subcontratación en la nube es de naturaleza más dinámica que la subcontratación tradicional. Es necesaria una mayor certeza sobre las condiciones en las que puede tener lugar la subcontratación, en particular en el caso de la subcontratación en la nube.

43. Las directrices especifican que la subcontratación requiere notificación previa a las instituciones y las instituciones de pago en el caso de la subcontratación de funciones críticas o importantes. Las instituciones y las entidades de pago siempre deben tener derecho a rescindir el contrato si los cambios planificados en los servicios, incluidos los cambios provocados por la subcontratación, tuvieran un efecto adverso en la evaluación de riesgos de los servicios subcontratados.

**Riesgos de supervisión y concentración**

44. Es de particular importancia que las autoridades competentes tengan una visión general completa de los acuerdos de subcontratación de las instituciones y las instituciones de pago, ya que esto les permite ejercer sus poderes de supervisión. Por tanto, las instituciones y las entidades de pago deben documentar todos sus acuerdos de subcontratación. Además, las entidades y las entidades de pago deben informar a las autoridades competentes o entablar un diálogo con las autoridades competentes sobre los acuerdos de subcontratación previstos, en particular con respecto a funciones críticas o importantes. La responsabilidad final de la subcontratación siempre recae en la entidad o entidad de pago. Con este fin, las directrices establecen requisitos de documentación específicos para las instituciones y los acuerdos de subcontratación de las instituciones de pago.

45. Las autoridades competentes deben identificar las concentraciones de acuerdos de subcontratación en los proveedores de servicios. La concentración de acuerdos de subcontratación en los proveedores de servicios y en lo que respecta a funciones críticas o importantes en particular puede, si falla la prestación del servicio, provocar la interrupción de la prestación de servicios financieros por parte de múltiples instituciones. Si los proveedores de servicios, p.ej. en el área de IT o fintech, fallan o ya no pueden brindar sus servicios, incluso en el caso de una interrupción severa del negocio causada por eventos externos, esto puede causar riesgos sistémicos para el mercado financiero.

46. La necesidad de monitorear y administrar el riesgo de concentración es particularmente relevante para ciertas formas de subcontratación de IT, incluida la subcontratación en la nube, que está dominada por un pequeño número de empresas altamente proveedores de servicios dominantes. Por ejemplo, en comparación con las formas más tradicionales de subcontratación que ofrecen soluciones a medida para los clientes, los servicios de subcontratación en la nube están mucho más estandarizados, lo que permite que los servicios se presten a un mayor número de clientes diferentes de una manera mucho más automatizada y en un mayor escala. Si bien los servicios en la nube pueden ofrecer una serie de ventajas, como economías de escala, flexibilidad, eficiencia operativa y rentabilidad, también plantean desafíos en términos de protección y ubicación de datos, problemas de seguridad y riesgo de concentración, no solo desde el punto de vista del individuo. Instituciones, sino también a nivel de la industria, ya que los grandes proveedores de servicios de IT y en la nube pueden convertirse en un único punto de falla cuando muchas instituciones confían en ellos. Asimismo, el desarrollo y mayor uso de proveedores de tecnología financiera requiere una atención específica.

1. Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC. [↑](#footnote-ref-1)
2. 2 The recommendation is available on the EBA’s website under the following link: <https://www.eba.europa.eu/regulationand-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers> [↑](#footnote-ref-2)
3. Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in theinternal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. [↑](#footnote-ref-3)
4. <https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measuresfor-operational-and-security-risks-under-the-psd2> [↑](#footnote-ref-4)
5. <https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidentsreporting-under-psd2> [↑](#footnote-ref-5)
6. Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010. [↑](#footnote-ref-6)
7. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349) [↑](#footnote-ref-7)
8. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. [↑](#footnote-ref-8)
9. Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (OJ L 173, 12.6.2014, p. 190). [↑](#footnote-ref-9)
10. Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12). [↑](#footnote-ref-10)
11. Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive. [↑](#footnote-ref-11)
12. Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance [↑](#footnote-ref-12)
13. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1). [↑](#footnote-ref-13)
14. Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 [↑](#footnote-ref-14)
15. Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) [↑](#footnote-ref-15)
16. Payment institutions should refer to the definition of a ‘management body’ and ‘senior management’ under the guidelines on the security measures for operational and security risks of payment services under PSD2 published in December 2017 on the EBA’s website: <https://www.eba.europa.eu/-/eba-publishes-final-guidelines-on-security-measures-under-psd2> [↑](#footnote-ref-16)
17. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. [↑](#footnote-ref-17)
18. The term ‘critical or important’ is used in line with MiFID II and PSD2 and replaces the term ‘material’ that was used in the previous guidelines. [↑](#footnote-ref-18)