BANCO DE ESPAÑA
Eurosistema

Directrices sobre externalización

(EBA/GL/2019/02)

Estas Directrices de la Autoridad Bancaria Europea ("EBA", por sus siglas en inglés) están dirigidas a las autoridades competentes según se definen en el artículo 4, apartado 1, punto 40, del Reglamento (UE) n.º 575/2013, incluido el Banco Central Europeo para los asuntos relacionados con las tareas que le encomienda el Reglamento (UE) n.º 1024/2013, a las entidades definidas en el artículo 4, apartado 1, punto 3, del Reglamento (UE) n.º 575/2013, a las entidades de pago definidas en el artículo 4, apartado 4, de la Directiva (UE) 2015/2366 y a las entidades de dinero electrónico en el sentido del artículo 2, apartado 1, de la Directiva 2009/110/CE. Los proveedores de servicios de información sobre cuentas que solo prestan el servicio contemplado en el punto 8 del anexo I de la Directiva (UE) 2015/2366 no se incluyen en el ámbito de aplicación de las presentes directrices, de conformidad con el artículo 33 de dicha Directiva.

Las Directrices especifican los sistemas de gobierno interno, incluida la adecuada gestión de los riesgos, que las entidades de crédito, las entidades de pago y las entidades de dinero electrónico deben aplicar cuando externalicen funciones, en particular, en relación con la externalización de las denominadas funciones esenciales o importantes. Estas Directrices, para cuya aplicación ha de tenerse en cuenta el principio de proporcionalidad, derogan las Guías del Comité de Supervisores Bancarios Europeos sobre externalización de servicios, de 14 de diciembre de 2006 y las Recomendaciones de la EBA sobre la externalización de servicios a proveedores de servicios en la nube de 20 de diciembre de 2017 (versión en español de 28 de marzo de 2018), con efectos a partir del 30 de septiembre de 2019.

Las Directrices se distribuyen en cinco títulos, relativos al principio de proporcionalidad y la aplicación de las Directrices respecto de grupos y entidades que forman parte de un sistema institucional de protección, la evaluación de los acuerdos de externalización, el marco de gobernanza, el proceso de externalización y las directrices destinadas a las autoridades competentes.

Estas Directrices han sido desarrolladas por la EBA de acuerdo con lo señalado en el artículo 16 del Reglamento (UE) n.º 1093/2010. La EBA publicó la versión en inglés

de estas Directrices el 25 de febrero de 2019 y la versión en español el 5 de junio de 2019. Se aplicarán a partir del 30 de septiembre de 2019, si bien se incluyen determinados periodos transitorios en relación con la aplicación de determinadas directrices.

La Comisión Ejecutiva del Banco de España, en su calidad de autoridad competente de la supervisión directa de las entidades de crédito menos significativas, entidades de pago y entidades de dinero electrónico, adoptó estas Directrices como propias el día 29 de julio de 2019, con excepción de lo previsto en las directrices 62 y 63, en lo que se refiere a la externalización de actividades reservadas a las entidades de crédito, y 62, en relación con la externalización de funciones relativas a los servicios de pago cuya realización requiera autorización o registro, que únicamente será posible cuando el proveedor de servicios en el que se realiza dicha externalización esté autorizado o registrado por una autoridad competente para llevar a cabo dichos servicios de pago (directriz 62 a.)

EBA/GL/2019/02

25 de febrero de 2019

Directrices

sobre externalización

1. Obligaciones de cumplimiento y de notificación

Rango jurídico de las presentes directrices

1. El presente documento contiene directrices emitidas en virtud del artículo 16 del Reglamento (UE) n.º 1093/2010[1]. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) n.º 1093/2010, las autoridades competentes y las entidades financieras harán todo lo posible para atenerse a ellas.

2. En las directrices se expone el punto de vista de la ABE sobre las prácticas de supervisión más adecuadas en el marco del Sistema Europeo de Supervisión Financiera o sobre cómo debería aplicarse el Derecho de la Unión en un determinado ámbito. Las autoridades competentes, según se definen en el artículo 4, apartado 2, del Reglamento (UE) n.º 1093/2010, a las que sean de aplicación las directrices deberían cumplirlas incorporándolas a sus prácticas de la forma más apropiada (modificando, por ejemplo, su marco jurídico o sus procedimientos de supervisión), incluso en aquellos casos en los que las directrices vayan dirigidas principalmente a las entidades y las entidades de pago.

Requisitos de notificación

3. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) n.º 1093/2010, las autoridades competentes deberán notificar a la ABE, a más tardar el [(dd.mm.aaaa]), si cumplen o se proponen cumplir estas directrices indicando, en caso negativo, los motivos para no cumplirlas. A falta de notificación en dicho plazo, la ABE considerará que las autoridades competentes no las cumplen. Las notificaciones se presentarán remitiendo el modelo que se encuentra disponible en el sitio web de la ABE a compliance@eba.europa.eu, con la referencia «EBA/GL/2019/02». Las notificaciones serán remitidas por personas debidamente facultadas para comunicar el cumplimiento en nombre de las respectivas autoridades competentes. Cualquier cambio en la situación de cumplimiento de las directrices deberá notificarse igualmente a la ABE.

4. Las notificaciones se publicarán en el sitio web de la ABE, tal como contempla el artículo 16, apartado 3.

[1] Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión n.º 2009/78/CE de la Comisión (DO L 331 de 15.12.2010, p. 12).

2. Objeto, ámbito de aplicación y definiciones

Objeto

5. Las presentes directrices especifican los sistemas de gobierno interno, incluida la adecuada gestión de los riesgos, que las entidades, las entidades de pago y las entidades de dinero electrónico deberían aplicar cuando externalicen funciones, en particular en relación con la externalización de funciones esenciales o importantes.

6. Las directrices especifican el modo en que las autoridades competentes deberían revisar y supervisar los sistemas referidos en el párrafo anterior, en el contexto del artículo 97 de la Directiva 2013/36/UE[2] (proceso de revisión y evaluación supervisora, PRES), el artículo 9, apartado 3, de la Directiva (UE) 2015/2366[3] y el artículo 5, apartado 5, de la Directiva 2009/110/CE[4], cumpliendo su obligación de vigilar el cumplimiento continuo de las condiciones de autorización por parte de las entidades a las que se dirigen las presentes directrices.

Destinatarios

7. Las presentes directrices están dirigidas a las autoridades competentes según se definen en el artículo 4, apartado 1, punto 40, del Reglamento (UE) n.º 575/2013[5], incluido el Banco Central Europeo para los asuntos relacionados con las tareas que le encomienda el Reglamento (UE) n.º 1024/2013[6], a las entidades definidas en el artículo 4, apartado 1, punto 3, del Reglamento (UE) n.º 575/2013, a las entidades de pago definidas en el artículo 4, apartado 4, de la Directiva (UE) 2015/2366 y a las entidades de dinero electrónico en el sentido del artículo 2, apartado 1, de la Directiva 2009/110/CE. Los proveedores de servicios de información sobre cuentas que solo prestan el servicio contemplado en el punto 8 del anexo I de la Directiva (UE) 2015/2366 no se incluyen en el ámbito de aplicación de las presentes directrices, de conformidad con el artículo 33 de dicha Directiva.

---

[2] Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE.

[3] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/CE y el Reglamento (UE) n.° 1093/2010 y se deroga la Directiva 2007/64/CE.

[4] Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE.

[5] Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 176 de 27.6.2013, p. 1).

[6] Reglamento (UE) n.° 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito.

8. A efectos de las presentes directrices, toda referencia a «entidades de pago» comprende las «entidades de dinero electrónico», y toda referencia a «servicios de pago» incluye la «emisión de dinero electrónico».

Ámbito de aplicación

9. Sin perjuicio de lo dispuesto en la Directiva 2014/65/UE[7] y el Reglamento Delegado (UE) 2017/565 de la Comisión[8] (que contiene los requisitos relativos a la externalización por parte de las entidades que prestan servicios de inversión y realizan actividades de inversión, así como las directrices al respecto emitidas por la Autoridad Europea de Valores y Mercados en relación con los servicios y actividades de inversión), las entidades definidas en el artículo 3, apartado 1, punto 3, de la Directiva 2013/36/UE deberían cumplir las presentes directrices en base individual, subconsolidada y consolidada. Las autoridades competentes podrían renunciar a la aplicación a nivel individual con arreglo al artículo 21 de la Directiva 2013/36/UE o al artículo 109, apartado 1, de la Directiva 2013/36/UE, conjuntamente con el artículo 7 del Reglamento (UE) n.º 575/2013. Las entidades sujetas a la Directiva 2013/36/UE deberían cumplir esta Directiva y las presentes directrices en base consolidada y subconsolidada, conforme a lo dispuesto en los artículos 21 y 108 a 110 de la Directiva 2013/36/UE.

10. Sin perjuicio de lo dispuesto en el artículo 8, apartado 3, de la Directiva (UE) 2015/2366 y en el artículo 5, apartado 7, de la Directiva 2009/110/CE, las entidades de pago y las entidades de dinero electrónico deberían cumplir las presentes directrices en base individual.

11. Las autoridades competentes responsables de la supervisión de las entidades, de las entidades de pago y de las entidades de dinero electrónico deberían cumplir las presentes directrices.

Definiciones

12. A menos que se indique lo contrario, los términos utilizados y definidos en la Directiva 2013/36/UE, el Reglamento (UE) n.º 575/2013, la Directiva 2009/110/CE, la Directiva (UE) 2015/2366 y las Directrices de la ABE sobre gobierno interno[9] tienen el mismo significado en las presentes directrices. Adicionalmente, a efectos de estas directrices se aplicarán las definiciones siguientes:

Externalización	Acuerdo de cualquier forma entre una entidad, una entidad de pago o una entidad de dinero electrónico y un proveedor de servicios por el

[7] Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE (DO L 173 de 12.6.2014, p. 349).

[8] Reglamento Delegado (UE) 2017/565 de la Comisión, de 25 de abril de 2016, por el que se completa la Directiva 2014/65/UE del Parlamento Europeo y del Consejo en lo relativo a los requisitos organizativos y las condiciones de funcionamiento de las empresas de servicios de inversión y términos definidos a efectos de dicha Directiva (DO L 87 de 31.3.2017, p. 1).

[9] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

	que dicho proveedor realiza un proceso, un servicio o una actividad que, de otro modo, serían realizados por la propia entidad, entidad de pago o entidad de dinero electrónico.
Función	Cualesquiera procesos, servicios o actividades.
Función esencial o importante[10]	Toda función que se considere esencial o importante según se establece en el apartado 4 de estas directrices.
Subcontratación	Situación en la que el proveedor de servicios bajo un acuerdo de externalización transfiere una función externalizada a otro proveedor de servicios[11] .
Proveedor de servicios	Tercera parte que realiza un proceso, servicio o actividad que se ha externalizado, o partes de los mismos, con arreglo a un acuerdo de externalización.
Servicios en la nube	Servicios prestados usando computación en la nube, es decir, un modelo que permite el acceso de red ubicuo, conveniente y bajo demanda, a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden suministrar y desplegar rápidamente, requiriendo un esfuerzo de gestión o una interacción con el proveedor del servicio mínimos.
Nube pública	Infraestructura de nube disponible para el uso abierto del público en general.
Nube privada	Infraestructura de nube disponible para el uso exclusivo de una sola entidad o entidad de pago.
Nube comunitaria	Infraestructura de nube disponible para el uso exclusivo de una comunidad específica de entidades o de entidades de pago, incluido el caso de varias entidades de un mismo grupo.
Nube híbrida	Infraestructura de nube compuesta por dos o más infraestructuras de nube distintas.
Órgano de administración	Órgano u órganos de una entidad o entidad de pago, designados de conformidad con el derecho nacional, que están facultados para fijar la estrategia, los objetivos y la dirección general de la entidad o la entidad de pago, y que se ocupan de la vigilancia y el control del proceso

[10] La expresión «función esencial o importante» se basa en la terminología utilizada en la Directiva 2014/65/UE (MiFID II) y el Reglamento Delegado (UE) 2017/565 de la Comisión por el que se completa la MiFID II y se utiliza únicamente a efectos de la externalización; no está relacionada con la definición de «funciones esenciales» a los efectos del marco de recuperación y resolución que se define en el artículo 2, apartado 1, punto 35, de la Directiva 2014/59/UE (DRRB).

[11] Para la evaluación se aplican las disposiciones de la Sección 3; la subcontratación también se ha denominado «cadena de externalización» o «externalización en cadena» en otros documentos de la ABE.

	de adopción de decisiones de gestión e incluyen a quienes dirigen de forma efectiva la actividad de la entidad o la entidad de pago, así como a los administradores y las personas responsables de la gestión de la entidad de pago.

3. Aplicación

Fecha de aplicación

13. Con la excepción del apartado 63, letra b), estas directrices serán de aplicación a partir del 30 de septiembre de 2019 a todos los acuerdos de externalización celebrados, revisados o modificados en esa fecha o con posterioridad. El apartado 63, letra b), es aplicable a partir del 31 de diciembre de 2021.

14. Las entidades y las entidades de pago deberían revisar y modificar en consecuencia los acuerdos de externalización existentes, con el fin de asegurarse de que estos cumplan con lo dispuesto en las presentes directrices.

15. Cuando la revisión de los acuerdos de externalización de funciones esenciales o importantes no haya finalizado antes del 31 de diciembre de 2021, las entidades y las entidades de pago deberían informar de ello a su autoridad competente, incluyendo las medidas previstas para completar la revisión o la posible estrategia de salida.

Disposiciones transitorias

16. Las entidades y las entidades de pago deberían finalizar la documentación de todos los acuerdos de externalización existentes, distintos de los de externalización a proveedores de servicios en la nube, en línea con las presentes directrices tras la primera fecha de renovación de cada acuerdo de externalización existente, pero no más tarde del 31 de diciembre de 2021.

Derogación

17. Las Directrices del Comité de Supervisores Bancarios Europeos (CSBE) sobre externalización de servicios, de 14 de diciembre de 2006, y las Recomendaciones de la ABE sobre la externalización de servicios a proveedores de servicios en la nube[12] quedan derogadas con efecto a partir del 30 de septiembre de 2019.

[12] Recomendaciones sobre la externalización de servicios a proveedores de servicios en la nube (EBA/REC/2017/03).

4. Directrices sobre externalización

Título I – Proporcionalidad: aplicación a nivel de grupos y de sistemas institucionales de protección

1 Proporcionalidad

18. Las entidades, las entidades de pago y las autoridades competentes, a la hora de cumplir o supervisar el cumplimiento de las presentes Directrices, deberían tener en cuenta el principio de proporcionalidad. El principio de proporcionalidad tiene por objeto garantizar que los sistemas de gobierno, en particular los relacionados con la externalización, sean coherentes con el perfil de riesgo individual, la naturaleza y el modelo de negocio de la entidad o la entidad de pago, y con la escala y complejidad de sus actividades, de manera que se alcancen eficazmente los objetivos de los requisitos regulatorios.

19. Cuando apliquen los requisitos establecidos en las presentes Directrices, las entidades y las entidades de pago deberían tener en cuenta la complejidad de las funciones externalizadas, los riesgos derivados del acuerdo de externalización, la esencialidad o importancia de la función externalizada y el posible impacto de la externalización sobre la continuidad de sus actividades.

20. Para aplicar el principio de proporcionalidad, las entidades, las entidades de pago[13] y las autoridades competentes deberían tener en cuenta los criterios especificados en el título I de las Directrices de la ABE sobre gobierno interno, en línea con el artículo 74, apartado 2, de la Directiva 2013/36/UE.

2 Externalización por parte de grupos y entidades que forman parte de un sistema institucional de protección

21. Con arreglo al artículo 109, apartado 2, de la Directiva 2013/36/UE, las presentes Directrices deberían aplicarse asimismo en base consolidada y subconsolidada, teniendo en cuenta el ámbito de aplicación de la consolidación prudencial[14] . A estos efectos, las entidades matrices de la UE o la entidad matriz de un Estado miembro deberían asegurarse de que los sistemas, procedimientos y mecanismos de gobierno interno de sus filiales, incluidas las entidades de pago, sean coherentes, estén bien integrados y sean adecuados para poder aplicar efectivamente las presentes Directrices a todos los niveles oportunos.

[13] Las entidades de pago deberían remitirse también a las Directrices de la ABE emitidas con arreglo a la Directiva PSD2 sobre la información que debe facilitarse para la autorización de entidades de pago y de entidades de dinero electrónico y para el registro de proveedores de servicios de información sobre cuentas, disponibles a través del siguiente enlace en el sitio web de la ABE : https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-authorisation-and-registration-under-psd2

[14] Véase el artículo 4, apartado 1, puntos 47 y 48, del Reglamento (UE) n.º 575/2013 en relación con el ámbito de aplicación de la consolidación.

22. Las entidades y las entidades de pago, conforme al apartado 21, y las entidades que, formando parte de un sistema institucional de protección, utilicen sistemas de gobierno proporcionados de forma centralizada, deberían cumplir las siguientes condiciones:

    a. cuando dichas entidades o entidades de pago hayan suscrito acuerdos de externalización con proveedores de servicios que pertenezcan al grupo o formen parte del sistema institucional de protección [15], el órgano de administración de dichas entidades o entidades de pago sigue siendo plenamente responsable, también en relación con estos acuerdos de externalización, del cumplimiento de todos los requisitos regulatorios y de la aplicación efectiva de las presentes Directrices,;

    b. cuando dichas entidades o entidades de pago externalicen las tareas operativas de las funciones de control interno a un proveedor de servicios que pertenezca al grupo o forme parte del sistema institucional de protección, a efectos del seguimiento y la auditoría de los acuerdos de externalización, las entidades se asegurarán, también en relación con estos acuerdos de externalización, de que dichas tareas operativas se llevan a cabo de manera efectiva, incluyendo a través de la recepción de los informes oportunos.

23. Además del apartado 22, las entidades y las entidades de pago pertenecientes a un grupo a las que no se haya concedido una excepción sobre la base del artículo 109 de la Directiva 2013/36/UE y el artículo 7 del Reglamento (UE) n.º 575/2013, las entidades que sean un organismo central o estén afiliadas permanentemente a un organismo central y a las que no se hayan concedido excepciones sobre la base del artículo 21 de la Directiva 2013/36/UE, o las entidades que formen parte de un sistema institucional de protección, deberían tener en cuenta lo siguiente:

    a. cuando el seguimiento operativo de la externalización esté centralizado (por ejemplo, como parte de un acuerdo marco para el seguimiento de los acuerdos de externalización), las entidades y las entidades de pago deberían asegurarse de que, al menos para las funciones esenciales o importantes externalizadas, sea posible tanto un seguimiento independiente del proveedor de servicios como una supervisión adecuada por parte de cada entidad o entidad de pago, incluyendo la recepción, como mínimo anualmente y previa petición por parte de la función de seguimiento centralizada, de informes que contengan, por lo menos, un resumen de la evaluación de riesgos y la supervisión del desempeño. Además, las entidades y las entidades de pago deberían recibir de la función de seguimiento centralizada un resumen de los informes de auditoría relevantes de las externalizaciones esenciales o importantes y, previa petición, el informe de auditoría completo;

[15] De conformidad con el artículo 113, apartado 7, del RRC, por «sistema institucional de protección» se entiende un acuerdo de responsabilidad contractual o legal que protege a las entidades que participan en el sistema y, en particular, garantiza su liquidez y solvencia, a fin de evitar la quiebra, cuando resulte necesario.

b. las entidades y las entidades de pago deberían asegurarse de que su órgano de administración sea debidamente informado de los cambios significativos previstos en relación con los proveedores de servicios controlados de forma centralizada y del impacto potencial de estos cambios sobre las funciones esenciales o importantes que se realicen, incluyendo un resumen del análisis de riesgos, que incluya los riesgos legales, el cumplimiento de los requisitos regulatorios y el impacto sobre niveles de servicio, a fin de que puedan valorar el impacto de estos cambios;

c. cuando las entidades y las entidades de pago pertenecientes a un grupo, las entidades afiliadas a un organismo central o las entidades que formen parte de un sistema institucional de protección recurran a una evaluación centralizada de los acuerdos de externalización previa a la externalización, de acuerdo con la sección 12, cada entidad y entidad de pago debería recibir un resumen de la evaluación y asegurarse de que tenga en cuenta su estructura y sus riesgos específicos dentro del proceso de toma de decisiones;

d. cuando el registro de todos los acuerdos de externalización existentes al que se refiere la sección 11 se establezca y se mantenga de forma centralizada en un grupo o en un sistema institucional de protección, las autoridades competentes, todas las entidades y las entidades de pago deberían poder obtener su registro individual sin demoras injustificadas. Este registro debería incluir todos los acuerdos de externalización, incluidos los acuerdos de externalización con proveedores de servicios pertenecientes a dichos grupo o sistema institucional de protección;

e. cuando dichas entidades y entidades de pago recurran a un plan de salida en relación con una función esencial o importante que se haya establecido a nivel del grupo, dentro del sistema institucional de protección o por el organismo central, todas las entidades y entidades de pago deberían recibir un resumen del plan y quedar satisfechas de que este se puede ejecutar efectivamente.

24. Cuando se hayan concedido excepciones en virtud del artículo 21 de la Directiva 2013/36/UE o del artículo 109, apartado 1, de la Directiva 2013/36/UE, conjuntamente con el artículo 7 del Reglamento (UE) n.º 575/2013, las disposiciones incluidas en las presentes Directrices deberían ser aplicadas por la entidad matriz en un Estado miembro para sí misma y sus filiales, o por el organismo central y sus afiliadas en conjunto.

25. Las entidades y las entidades de pago que sean filiales de una entidad matriz de la UE o de una entidad matriz de un Estado miembro a las que no se hayan concedido excepciones sobre la base del artículo 21 de la Directiva 2013/36/UE o del artículo 109, apartado 1, de la Directiva 2013/36/UE conjuntamente con el artículo 7 del Reglamento (UE) n.º 575/2013 deberían asegurarse de cumplir las presentes Directrices a nivel individual.

Título II – Evaluación de los acuerdos de externalización

3 Externalización

26. Las entidades y las entidades de pago deberían determinar si un acuerdo con un tercero se ajusta a la definición de externalización. Dentro de esta evaluación, deberían considerar si la función (o parte de la misma) que se externaliza a un proveedor de servicios es realizada por este de manera recurrente o continua y si dicha función (o parte de la misma) se incluiría normalmente entre las funciones que desempeñarían o podrían desempeñar de forma realista las entidades o las entidades de pago, aunque la propia entidad o entidad de pago no haya llevado a cabo dicha función anteriormente.

27. Cuando el acuerdo con un proveedor de servicios abarque múltiples funciones, las entidades y las entidades de pago deberían considerar en su evaluación todos los aspectos del acuerdo; por ejemplo, si el servicio prestado incluye el suministro de hardware para el almacenamiento de datos y la copia de seguridad de los datos, ambos aspectos deberían analizarse conjuntamente.

28. Como principio general, las entidades y las entidades de pago no deberían considerar como externalización lo siguiente:

    a. una función que legalmente debe realizarse por un proveedor de servicios, p. ej., una auditoría legal;

    b. los servicios de información de mercado (p. ej., el suministro de datos por parte de Bloomberg, Moody's, Standard & Poor's, Fitch);

    c. las infraestructuras de red globales (p. ej., Visa, Mastercard);

    d. los acuerdos de compensación y liquidación entre cámaras de compensación, entidades de contrapartida central y entidades de liquidación y sus miembros;

    e. las infraestructuras de mensajería financiera globales sujetas a la vigilancia de las autoridades pertinentes;

    f. los servicios de corresponsalía bancaria; y

    g. la adquisición de servicios que no serían asumidos de otro modo por la entidad o la entidad de pago (p. ej., asesoramiento de un arquitecto, emisión de dictamen jurídico y representación ante órganos judiciales y administrativos, limpieza, jardinería y mantenimiento de las instalaciones de la entidad o la entidad de pago, servicios médicos, mantenimiento de coches de empresa, servicios de restauración, servicios de máquinas expendedoras, servicios administrativos, servicios de viaje, servicios de correo, recepcionistas, personal de secretaría y operadores de centralita), bienes (p.

ej., tarjetas de plástico, lectores de tarjetas, material de oficina, ordenadores personales, mobiliario) o de suministros básicos (p. ej., electricidad, gas, agua, línea telefónica).

4 Funciones esenciales o importantes

29. Las entidades y las entidades de pago deberían considerar siempre que una función es esencial o importante en las siguientes situaciones[16]:

    a. si una anomalía o fallo en su ejecución afectase considerablemente:

        i. al cumplimiento continuado de sus condiciones de autorización o a sus otras obligaciones en virtud de la Directiva 2013/36/UE, el Reglamento (UE) n.º 575/2013, la Directiva 2014/65/UE, la Directiva (UE) 2015/2366 y la Directiva 2009/110/CE y sus obligaciones regulatorias;

        ii. a sus resultados financieros; o

        iii. a la solidez o la continuidad de sus actividades bancarias y servicios de pago;

    b. cuando se externalicen tareas operativas de las funciones de control interno, a menos que la evaluación determine que un fallo en la realización de la función externalizada o la realización inadecuada de la función externalizada no repercutiría negativamente en la eficacia de la función de control interno;

    c. cuando pretendan externalizar funciones relativas a actividades bancarias o servicios de pago en la medida que requeriría la autorización[17] de una autoridad competente, a tenor de lo indicado en la sección 12.1.

30. En el caso de las entidades, debería prestarse especial atención a la evaluación de la esencialidad o la importancia de las funciones si la externalización se refiere a funciones relacionadas con ramas de actividad principales y con funciones esenciales, tal como se definen en el artículo 2, apartado 1, puntos 35 y 36, de la Directiva 2014/59/UE[18], e identificadas por las entidades utilizando los criterios establecidos en los artículos 6 y 7 del Reglamento Delegado (UE) 2016/778 de la Comisión[19]. Las funciones que resulten necesarias para desempeñar

[16] Véase asimismo el artículo 30 del Reglamento Delegado (UE) 2017/565 de la Comisión, de 25 de abril de 2016, por el que se completa la Directiva 2014/65/UE del Parlamento Europeo y del Consejo en lo relativo a los requisitos organizativos y las condiciones de funcionamiento de las empresas de servicios de inversión y términos definidos a efectos de dicha Directiva.

[17] Véanse las actividades enumeradas en el anexo I de la Directiva 2013/36/UE.

[18] Directiva 2014/59/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, por la que se establece un marco para la reestructuración y la resolución de entidades de crédito y empresas de servicios de inversión, y por la que se modifican la Directiva 82/891/CEE del Consejo, y las Directivas 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE y 2013/36/UE, y los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 648/2012 del Parlamento Europeo y del Consejo (DO L 173 de 12.6.2014, p. 190).

[19] Reglamento Delegado (UE) 2016/778 de la Comisión, de 2 de febrero de 2016, por el que se complementa la Directiva 2014/59/UE del Parlamento Europeo y del Consejo en lo que respecta a las circunstancias y condiciones en que el pago

actividades de las ramas de actividad principales o las funciones esenciales deberían considerarse funciones esenciales o importantes a efectos de las presentes Directrices, a menos que la evaluación de la entidad determine que un fallo en la realización de la función externalizada o su realización inadecuada no repercutirían negativamente en la continuidad operativa de la rama de actividad principal o la función esencial.

31. Al evaluar si un acuerdo de externalización afecta a una función esencial o importante, las entidades y las entidades de pago deberían tener en cuenta, además de los resultados de la evaluación de riesgos detallada en la sección 12.2, al menos los siguientes factores:

    a. si el acuerdo de externalización está directamente relacionado con la prestación de actividades bancarias o servicios de pago[20] para los que están autorizadas;

    b. el impacto potencial de cualquier interrupción de la función externalizada o la incapacidad del prestador de servicios para prestar el servicio con los niveles de servicio acordados y de forma continuada, sobre:

        i. su resiliencia y viabilidad financieras a corto y a largo plazo, incluidos, en su caso, sus activos, capital, costes, financiación, liquidez, beneficios y pérdidas;

        ii. la continuidad de sus actividades y su resiliencia operativa;

        iii. su riesgo operacional, incluidos los riesgos de conducta, los riesgos ligados a las tecnologías de la información y la comunicación (TIC) y los riesgos legales;

        iv. sus riesgos reputacionales;

        v. cuando proceda, sus planes de recuperación y resolución, su resolubilidad y la continuidad de sus actividades en una situación de actuación temprana, recuperación o resolución;

    c. el impacto potencial del acuerdo de externalización sobre su capacidad para:

        i. identificar, supervisar y gestionar todos los riesgos;

        ii. cumplir todos los requisitos legales y regulatorios;

        iii. llevar a cabo auditorías adecuadas de la función externalizada;

    d. el impacto potencial sobre los servicios prestados a sus clientes;

    e. todos los acuerdos de externalización, la exposición agregada de la entidad o la entidad de pago frente al mismo proveedor de servicios y el potencial impacto acumulado de los acuerdos de externalización en la misma área de negocio;

de contribuciones extraordinarias *ex post* puede ser aplazado parcial o totalmente, y sobre los criterios de determinación de las actividades, los servicios y las operaciones en relación con las funciones esenciales, así como de las ramas de actividad y servicios asociados con respecto a las ramas de actividad principales (DO L 131 de 20.5.2016, p. 41).

[20] Véanse las actividades enumeradas en el anexo I de la Directiva 2013/36/UE.

f. el tamaño y la complejidad de cualquier área de negocio afectada;

g. la posibilidad de que pudiera ampliarse el acuerdo de externalización propuesto sin sustituir o revisar el contrato subyacente;

h. la capacidad para transferir el acuerdo de externalización propuesto a otro proveedor de servicios, si fuera necesario o deseable, tanto desde el punto de vista contractual como en la práctica, incluidos los riesgos estimados, los impedimentos que afectan a la continuidad de las actividades, los costes y el plazo para dicha transferencia («sustituibilidad»);

i. la capacidad para reincorporar la función externalizada en la entidad o la entidad de pago, en caso de que fuera necesario o deseable;

j. la protección de datos y el impacto potencial de una vulneración de la confidencialidad o de la incapacidad para garantizar la disponibilidad e integridad de los datos sobre la entidad o la entidad de pago y sus clientes, incluyendo, sin carácter limitativo, el cumplimiento del Reglamento (UE) 2016/679[21].

[21] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Título III – Marco de gobernanza

5 Sistemas de gobierno adecuados y riesgo de terceros

32. Como parte del marco general de control interno[22], incluidos los mecanismos de control interno,[23] las entidades y las entidades de pago deberían disponer de un marco global de gestión de riesgos que abarque todas las ramas de actividad y las unidades internas. En virtud de dicho marco, las entidades y las entidades de pago deberían identificar y gestionar todos sus riesgos, incluyendo los riesgos derivados de acuerdos con terceros. El marco de gestión de riesgos también debería permitir a las entidades y a las entidades de pago tomar decisiones bien fundamentadas sobre la asunción de riesgos y asegurar la correcta aplicación de las medidas de gestión de riesgos, en particular los ciberriesgos[24].

33. Teniendo en cuenta el principio de proporcionalidad señalado en la sección 1, las entidades y las entidades de pago deberían identificar, evaluar, controlar y gestionar todos los riesgos derivados de los acuerdos con terceros a los que estén o puedan estar expuestas, independientemente de que dichos acuerdos sean o no acuerdos de externalización. Los riesgos, en particular los riesgos operacionales, de todos los acuerdos con terceros, incluidos los mencionados en los apartados 26 y 28, deberían evaluarse en línea con la sección 12.2.

34. Las entidades y las entidades de pago deberían asegurarse del cumplimiento de todos los requisitos contemplados en el Reglamento (UE) 2016/679, incluso en lo que respecta a sus acuerdos con terceros y sus acuerdos de externalización.

6 Sistemas de gobierno adecuados y externalización

35. La externalización de funciones no puede dar lugar a la delegación de las responsabilidades del órgano de administración. Las entidades y las entidades de pago son plenamente responsables y responden del cumplimiento de todas sus obligaciones regulatorias, incluida la capacidad para supervisar la externalización de funciones esenciales o importantes.

36. El órgano de administración es plenamente responsable y responde en todo momento, como mínimo, de lo siguiente:

    a. asegurarse de que la entidad o la entidad de pago cumple permanentemente las condiciones necesarias para mantener su autorización, incluidas las condiciones impuestas por la autoridad competente;

---

[22] Las entidades deberán remitirse al título V de las Directrices de la ABE sobre gobierno interno.

[23] Véase asimismo el artículo 11 de la Directiva 2015/2366 (PSD2).

[24] Véanse asimismo las Directrices de la ABE sobre la gestión de riesgos de seguridad y de TIC (https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management) y los elementos fundamentales del G7 para la gestión de riesgos cibernéticos de terceros en el sector financiero (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

b. la organización interna de la entidad o la entidad de pago;

c. la identificación, evaluación y gestión de los conflictos de interés;

d. el establecimiento de las estrategias y las políticas de la entidad o la entidad de pago (p. ej., el modelo de negocio, el apetito de riesgo y el marco de gestión de riesgos);

e. la supervisión de la gestión diaria de la entidad o la entidad de pago, incluida la gestión de todos los riesgos asociados a la externalización; y

f. el papel supervisor del órgano de administración en su función de supervisión, incluida la vigilancia y el seguimiento de los procesos de toma de decisión.

37. La externalización no debería reducir los requisitos de idoneidad aplicados a los miembros del órgano de administración de una entidad, los administradores y las personas responsables de la gestión de la entidad de pago y los titulares de funciones clave. Las entidades y las entidades de pago deberían contar con competencias adecuadas y con recursos suficientes y debidamente cualificados para garantizar la gestión y supervisión apropiadas de los acuerdos de externalización.

38. Las entidades y las entidades de pago deberían:

a. asignar claramente las responsabilidades relativas a la documentación, gestión y control de los acuerdos de externalización;

b. destinar recursos suficientes para garantizar el cumplimiento de todos los requisitos legales y regulatorios, incluidas las presentes Directrices, y la documentación y seguimiento de todos los acuerdos de externalización;

c. teniendo en cuenta la sección 1 de las presentes Directrices, crear una función de externalización o nombrar a un miembro del personal directivo que asumirá la responsabilidad ante el órgano de administración (p. ej., un titular de funciones clave de una función de control) y será responsable de gestionar y supervisar los riesgos de los acuerdos de externalización como parte del marco de control interno de la entidad y de supervisar la documentación de dichos acuerdos. Las entidades o las entidades de pago pequeñas y menos complejas deberían garantizar como mínimo una división clara entre las tareas y responsabilidades de gestión y control de los acuerdos de externalización y podrán asignar la función de externalización a un miembro del órgano de administración de la entidad o de la entidad de pago.

39. Las entidades y las entidades de pago deberían tener suficiente sustancia en todo momento y no convertirse en «estructuras vacías de contenido» («*empty shells*») o «entidades ficticias» («*letter box entities*»). A este fin, deberían:

a. cumplir en todo momento todas las condiciones[25] de su autorización, en particular que el órgano de administración desempeñe de manera efectiva sus responsabilidades, tal como establece el apartado 36 de las presentes Directrices;

b. mantener un marco organizativo claro y transparente y una estructura que les permita garantizar el cumplimiento de los requisitos legales y regulatorios;

c. cuando se externalicen tareas operativas de funciones de control interno (p. ej., en el caso de externalización dentro del grupo o en sistemas institucionales de protección), ejercer una supervisión apropiada y ser capaces de gestionar los riesgos generados por la externalización de funciones esenciales o importantes; y

d. contar con recursos y capacidades suficientes para garantizar el cumplimiento de lo establecido en las letras a) a c).

40. Cuando externalicen servicios, las entidades y las entidades de pago deberían asegurarse, como mínimo, de que:

a. pueden tomar y aplicar decisiones relativas a sus actividades y a funciones esenciales o importantes, incluidas aquellas que se han externalizado;

b. mantienen la ordenada conducta en el desempeño sus actividades y de los servicios bancarios y de pago que prestan;

c. se identifican, evalúan, gestionan y mitigan adecuadamente los riesgos asociados a los acuerdos de externalización vigentes y planificados, en particular los riesgos vinculados a las TIC y a las innovaciones financieras de base tecnológica (fintech);

d. se han establecido los acuerdos de confidencialidad apropiados en relación con los datos y otra información;

e. se mantiene un flujo adecuado de información pertinente con los proveedores de servicios;

f. por lo que respecta a la externalización de funciones esenciales o importantes, están en condiciones de tomar al menos una de las siguientes medidas dentro de un plazo apropiado:

[25] Véanse asimismo las normas técnicas de regulación en virtud del artículo 8, apartado 2, de la Directiva 2013/36/UE sobre la información que habrá de proporcionarse para la autorización de entidades de crédito, y las normas técnicas de aplicación en virtud del artículo 8, apartado 3, de la Directiva 2013/36/UE sobre modelos de formularios, plantillas y procedimientos para la remisión de la información necesaria para la autorización de entidades de crédito (https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions).

En el caso de las entidades de pago, véanse las Directrices de la ABE emitidas con arreglo a la Directiva (UE) 2015/2366 (PSD2) sobre la información que debe facilitarse para la autorización de entidades de pago y de entidades de dinero electrónico y para el registro de proveedores de servicios de información sobre cuentas (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

i. transferir la función a proveedores de servicios alternativos;

ii. reincorporar la función; o

iii. interrumpir las actividades de negocio que dependen de la función.

g. cuando los datos personales sean tratados por proveedores de servicios ubicados en la UE o en terceros países, se aplican las medidas apropiadas y el tratamiento de los datos es acorde con el Reglamento (UE) 2016/679.

7 Política de externalización

41. El órgano de administración de una entidad o una entidad de pago[26] que tenga acuerdos de externalización en vigor o planee celebrarlos debería aprobar, revisar periódicamente y actualizar una política escrita de externalización y garantizar que se aplica, cuando proceda, a nivel individual, subconsolidado y consolidado. En el caso de las entidades, la política de externalización debería ajustarse a lo dispuesto en la sección 8 de las Directrices de la ABE sobre gobierno interno y, en particular, debería tener en cuenta los requisitos establecidos en la sección 18 («Nuevos productos y cambios significativos») de dichas Directrices. Las entidades de pago también podrán ajustar sus políticas a las secciones 8 y 18 de las Directrices de la ABE sobre gobierno interno.

42. La política debería incluir las principales fases del ciclo de vida de los acuerdos de externalización y definir los principios, las responsabilidades y los procesos en relación con la externalización. En concreto, la política debería abarcar al menos:

a. las responsabilidades del órgano de administración en línea con el apartado 36, incluida su involucración, cuando proceda, en la toma de decisiones sobre la externalización de funciones esenciales o importantes;

b. la participación de las líneas de negocio, las funciones de control interno y otras personas en relación con los acuerdos de externalización;

c. la planificación de los acuerdos de externalización, incluyendo:

i. la definición de los requisitos de negocio en relación con los acuerdos de externalización;

ii. los criterios, incluidos los mencionados en la sección 4, y los procesos para identificar las funciones esenciales o importantes;

[26] Véanse asimismo las Directrices de la ABE sobre las medidas de seguridad para los riesgos operativos y de seguridad asociados a los servicios de pago en virtud de la Directiva PSD2, disponibles en: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

iii. la identificación, evaluación y gestión de riesgos con arreglo a la sección 12.2.;

iv. las comprobaciones de diligencia debida respecto de posibles proveedores de servicios, incluidas las medidas requeridas en la sección 12.3;

v. los procedimientos para identificar, evaluar, gestionar y mitigar posibles conflictos de interés, de acuerdo con la sección 8;

vi. un plan de continuidad de negocio de conformidad con la sección 9;

vii. el proceso de aprobación de nuevos acuerdos de externalización;

d. la ejecución, el seguimiento y la gestión de los acuerdos de externalización, incluidos:

i. la supervisión continua del desempeño del proveedor de servicios en consonancia con la sección 14;

ii. los procedimientos para recibir notificaciones y responder a los cambios en un acuerdo de externalización o en un proveedor de servicios (p. ej., en su posición financiera, su estructura organizativa o de propiedad, subcontratación);

iii. la revisión independiente y la auditoría del cumplimiento de las políticas y requisitos legales y regulatorios;

iv. los procesos de renovación

e. la documentación y mantenimiento del registro, teniendo en cuenta los requisitos en la sección 11;

f. las estrategias de salida y los procesos de resolución, incluida la obligación de contar con un plan de salida documentado para cada función esencial o importante que se vaya a externalizar cuando dicha salida se considere posible teniendo en cuenta posibles interrupciones del servicio o la resolución imprevista de un acuerdo de externalización.

43. La política de externalización debería diferenciar entre lo siguiente:

a. externalización de funciones esenciales o importantes y otros acuerdos de externalización;

b. externalización a proveedores de servicios que están autorizados por una autoridad competente y a aquellos que no lo están;

c. acuerdos de externalización dentro de un grupo, acuerdos de externalización dentro del mismo sistema institucional de protección (incluidas entidades participadas al 100%, ya sea a nivel individual o colectivo, por entidades integradas en el sistema

institucional de protección) y externalización a entidades no pertenecientes al grupo; y

d. externalización a proveedores de servicios ubicados en un Estado miembro y en terceros países.

44. Las entidades y las entidades de pago deberían asegurarse de que la política comprenda la identificación de los siguientes efectos potenciales de los acuerdos de externalización de funciones esenciales o importantes y de que estos efectos se tengan en cuenta en el proceso de toma de decisiones:

a. el perfil de riesgo de la entidad;

b. la capacidad para supervisar al proveedor de servicios y gestionar los riesgos;

c. las medidas de continuidad de negocio; y

d. la realización de sus actividades.

8 Conflictos de interés

45. Las entidades, en consonancia con el título IV, sección 11, de las Directrices de la ABE sobre gobierno interno [27], y las entidades de pago deberían identificar, evaluar y gestionar los conflictos de interés relacionados con sus acuerdos de externalización.

46. Cuando la externalización cree conflictos de interés importantes, incluyendo entre entidades del mismo grupo o pertenecientes a un sistema institucional de protección, las entidades y las entidades de pago deberían adoptar medidas adecuadas para gestionar dichos conflictos.

47. Cuando las funciones sean realizadas por un proveedor de servicios que forma parte de un grupo o de un sistema institucional de protección o que es propiedad de la entidad, la entidad de pago, el grupo o entidades participantes en un sistema institucional de protección, las condiciones, incluidas las condiciones financieras, aplicables al servicio externalizado se fijarán en condiciones de mercado. Sin embargo, en relación con el precio de los servicios podrán considerarse las sinergias derivadas de prestar el mismo servicio o servicios similares a varias entidades de un grupo o sistema institucional de protección, siempre y cuando el proveedor de servicios siga siendo viable de manera independiente; dentro de un grupo, esto será aplicable con independencia de la quiebra de cualquier otra entidad del grupo.

9 Planes de continuidad de negocio

[27] Las entidades de pago también podrán ajustar sus políticas a dichas Directrices.

48. Las entidades, en línea con los requisitos establecidos en el artículo 85, apartado 2, de la Directiva 2013/36/UE y en el título VI de las Directrices de la ABE sobre gobierno interno[28], y las entidades de pago deberían establecer, mantener y probar periódicamente planes de continuidad de negocio apropiados con respecto a las funciones esenciales o importantes externalizadas. Las entidades y las entidades de pago pertenecientes a un grupo o que formen parte de un sistema institucional de protección podrán recurrir a planes de continuidad de negocio establecidos de forma centralizada en relación con sus funciones externalizadas.

49. Los planes de continuidad de negocio deberían tener en cuenta el posible escenario en el que la calidad del servicio relativo a la función esencial o importante externalizada se deteriore hasta llegar a niveles inaceptables o falle. Estos planes también deberían tener en cuenta el posible impacto de la insolvencia u otros incumplimientos por parte de los proveedores de servicios y, en su caso, los riesgos políticos en la jurisdicción del proveedor de servicios.

10 Función de auditoría interna

50. Las actividades de la función de auditoría interna[29] deberían abarcar, siguiendo un enfoque basado en el riesgo, la revisión independiente de las actividades externalizadas. El programa y el plan de auditoría[30] deberían incluir, en particular, los acuerdos de externalización de funciones esenciales o importantes.

51. En relación con el proceso de externalización, la función de auditoría interna debería confirmar al menos:

    a. que el marco de externalización de la entidad o de la entidad de pago, incluida la política de externalización, se aplica correcta y eficazmente y se ajusta a la normativa aplicable, a la estrategia de riesgo y a las decisiones del órgano de administración;

    b. la idoneidad, calidad y eficacia de la evaluación de la esencialidad o importancia de las funciones;

    c. la idoneidad, calidad y eficacia de la evaluación de riesgos de los acuerdos de externalización y la coherencia continuada de los riesgos con la estrategia de riesgo de la entidad;

[28] Disponibles en: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-

[29] Respecto de las responsabilidades de la función de auditoría interna, las entidades deberán remitirse a la sección 22 de las Directrices de la ABE sobre gobierno interno (https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-) y las entidades de pago deberán remitirse a la Directriz 5 de las Directrices de la ABE sobre la autorización de entidades de pago (https://eba.europa.eu/documents/10180/1904583/Final+Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29.pdf).

[30] Véanse asimismo las Directrices de la ABE sobre el proceso de revisión y evaluación supervisora: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing.

d. la involucración apropiada de los órganos de gobierno; y

e. el seguimiento y gestión adecuados de los acuerdos de externalización.

11 Requisitos de documentación

52. Como parte de su marco de gestión de riesgos, las entidades y las entidades de pago deberían mantener un registro actualizado de información sobre todos sus acuerdos de externalización y, cuando proceda, a nivel subconsolidado y consolidado, tal como se establece en la sección 2, y deberían documentar convenientemente todos los acuerdos de externalización en vigor, diferenciando entre la externalización de funciones esenciales o importantes y otros acuerdos de externalización. Teniendo en cuenta la legislación nacional, las entidades deberían conservar en el registro la documentación de los acuerdos de externalización ya finalizados y los documentos justificativos durante un plazo apropiado.

53. Teniendo en cuenta el título I de las presentes Directrices, y con arreglo a las condiciones contempladas en el apartado 23, letra d), en el caso de entidades y entidades de pago pertenecientes a un grupo, entidades afiliadas de forma permanente a un organismo central o entidades que formen parte de un mismo sistema institucional de protección, el registro podrá mantenerse centralizado.

54. El registro debería incluir, al menos, la siguiente información para todos los acuerdos de externalización existentes:

    a. un número de referencia para cada acuerdo de externalización;

    b. la fecha de entrada en vigor y, en su caso, la próxima fecha de renovación del contrato, la fecha de finalización y/o los plazos de preaviso para el proveedor de servicios y para la entidad o entidad de pago;

    c. una breve descripción de la función externalizada, incluidos los datos que se externalizan y si se han transferido o no datos personales (p. ej., indicando «sí» o «no» en un campo de datos independiente) o si su tratamiento se ha externalizado a un proveedor de servicios;

    d. una categoría asignada por la entidad o la entidad de pago que refleje la naturaleza de la función tal como se describe en la letra c) (p. ej., tecnologías de la información, función de control) y que debería facilitar la identificación de los distintos tipos de acuerdos;

    e. el nombre del proveedor de servicios, su número de registro, el identificador de entidad jurídica (cuando se disponga de él), el domicilio social y otra información de contacto pertinente, así como el nombre de su entidad matriz (en su caso);

f. el país o los países en los que se prestará el servicio, incluida la localización (es decir, país o región) de los datos;

g. si la función externalizada se considera esencial o importante o no (sí/no), incluido, cuando proceda, un breve resumen de las razones por las que la función externalizada se considera esencial o importante;

h. en el caso de externalización a un proveedor de servicios en la nube, el modelo de servicio en la nube y el modelo de despliegue en la nube, es decir, nube pública/privada/híbrida/comunitaria, y la naturaleza específica de los datos que se alojarán y las localizaciones (es decir, países o regiones) en que se almacenarán dichos datos;

i. la fecha de última evaluación de la esencialidad o importancia de la función externalizada.

55. Para la externalización de funciones esenciales o importantes, el registro debería incluir, como mínimo, la siguiente información adicional:

a. las entidades, entidades de pago y otras empresas incluidas en el ámbito de aplicación de la consolidación prudencial o que formen parte del sistema institucional de protección, cuando proceda, que hacen uso de la externalización;

b. si el proveedor de servicios o subcontratista forma parte del grupo o del sistema institucional de protección o es propiedad de entidades o entidades de pago incluidas en el grupo o que forman parte del sistema institucional de protección, o no;

c. la fecha de la última evaluación de riesgos efectuada y un breve resumen de los principales resultados;

d. la persona u órgano decisorio (p. ej., el órgano de administración) de la entidad o entidad de pago que aprobó el acuerdo de externalización;

e. el Derecho aplicable por el que se rige el acuerdo de externalización;

f. las fechas de las auditorías más recientes y de las próximas auditorías programadas, en su caso;

g. cuando proceda, los nombres de los subcontratistas a los que se hayan subcontratado partes significativas de una función esencial o importante, incluido el país en que están registrados los subcontratistas, en el que se prestará el servicio y, si procede, la localización (es decir, país o región) en la que se almacenarán los datos;

h. el resultado de la evaluación de la sustituibilidad del proveedor de servicios (fácil, difícil o imposible), la posibilidad de reincorporar una función esencial o importante en la entidad o la entidad de pago, o el impacto de interrumpir la función esencial o importante;

i. identificación de proveedores de servicios alternativos en consonancia con la letra h);

j. si la función esencial o importante externalizada asiste a operaciones de negocio en las que el tiempo es un factor crítico;

k. el presupuesto anual estimado.

56. Las entidades y las entidades de pago deberían poner a disposición de la autoridad competente, previa solicitud, el registro completo de todos los acuerdos de externalización existentes[31] o secciones específicas del mismo, como la información sobre todos los acuerdos de externalización comprendidos en una de las categorías referidas en el apartado 54, letra d), de las presentes Directrices (por ejemplo, todos los acuerdos de externalización de tecnologías de la información). Las entidades y las entidades de pago deberían facilitar esta información en un formato electrónico procesable (p. ej., un formato de base de datos de uso común, valores separados por comas).

57. Las entidades y las entidades de pago deberían poner a disposición de la autoridad competente, previa solicitud, toda la información necesaria para que la autoridad competente pueda llevar a cabo la supervisión efectiva de la entidad o la entidad de pago, incluida, cuando se requiera, una copia del acuerdo de externalización.

58. Las entidades y las entidades de pago, sin perjuicio de lo dispuesto en el artículo 19, apartado 6, de la Directiva (UE) 2015/2366, deberían informar adecuada y diligentemente a las autoridades competentes o entablar con ellas un diálogo supervisor sobre la externalización prevista de funciones esenciales o importantes o cuando una función externalizada se hubiese convertido en esencial o importante y deberían facilitar como mínimo la información especificada en el apartado 54.

59. Las entidades y las entidades de pago[32] deberían informar diligentemente a las autoridades competentes de cualquier cambio significativo y/o acontecimiento grave en relación con sus acuerdos de externalización que pudiera afectar significativamente a la continuidad de sus actividades.

60. Las entidades y las entidades de pago deberían documentar adecuadamente las evaluaciones realizadas en virtud del título IV y los resultados de su seguimiento continuado (p. ej., desempeño del proveedor de servicios, cumplimiento de los niveles de servicio acordados, otros requisitos contractuales y regulatorios, actualizaciones de la evaluación de riesgos).

Título IV – Proceso de externalización

[31] Véanse asimismo las Directrices de la ABE sobre el proceso de revisión y evaluación supervisora, disponibles en: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[32] Véanse asimismo las Directrices de la ABE sobre la notificación de incidentes graves de conformidad con la Directiva PSD2, disponibles en: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2

12 Análisis previo a la externalización

61. Antes de celebrar cualquier acuerdo de externalización, las entidades y las entidades de pago deberían:

    a. evaluar si el acuerdo de externalización se refiere a una función esencial o importante, tal como se establece en el título II;

    b. evaluar si se cumplen las condiciones supervisoras para la externalización establecidas en la sección 12.1;

    c. identificar y evaluar todos los riesgos pertinentes del acuerdo de externalización, de conformidad con la sección 12.2.;

    d. llevar a cabo las comprobaciones adecuadas de diligencia debida respecto del posible proveedor de servicios, de conformidad con la sección 12.3;

    e. identificar y evaluar los conflictos de interés que la externalización pueda causar, en línea con la sección 8.

12.1 Condiciones supervisoras para la externalización

62. Las entidades y las entidades de pago deberían asegurarse de que las funciones relativas a las actividades bancarias[33] o los servicios de pago, en la medida en que su realización requiera autorización o registro por parte de una autoridad competente en el Estado miembro en el que están autorizadas, se externalicen a un proveedor de servicios ubicado en el mismo o en otro Estado miembro exclusivamente si se cumple una de las siguientes condiciones:

    a. el proveedor de servicios está autorizado o registrado por una autoridad competente para llevar a cabo dichas actividades bancarias o servicios de pago; o

    b. el proveedor de servicios está habilitado de otro modo para llevar cabo dichas actividades bancarias o servicios de pago con arreglo al marco jurídico nacional que corresponda.

63. Las entidades y las entidades de pago deberían asegurarse de que las funciones relativas a las actividades bancarias o servicios de pago, en la medida en que su realización requiera autorización o registro por parte de una autoridad competente en el Estado miembro en el que están autorizadas, se externalicen a un proveedor de servicios ubicado en un tercer país exclusivamente si se cumplen las siguientes condiciones:

    a. el proveedor de servicios está autorizado o registrado para realizar dicha actividad bancaria o servicio de pago en el tercer país y es supervisado por la autoridad

[33] Véase el artículo 9 de la DRC en relación con la prohibición de que la actividad de recepción de depósitos u otros fondos reembolsables procedentes de particulares pueda realizarse por personas o empresas que no sean entidades de crédito.

competente correspondiente en dicho tercer país (denominada «autoridad de supervisión»);

b. existe un acuerdo de cooperación apropiado, p. ej., en forma de memorando de entendimiento o acuerdo entre colegio de supervisores, entre las autoridades competentes responsables de la supervisión de la entidad y las autoridades de supervisión responsables de la supervisión del proveedor de servicios; y

c. el acuerdo de cooperación a que se refiere la letra b) debería garantizar que las autoridades competentes puedan, por lo menos:

i. obtener, previa petición, la información necesaria para llevar a cabo sus tareas de supervisión en virtud de la Directiva 2013/36/UE, el Reglamento (UE) n.º 575/2013, la Directiva (UE) 2015/2366 y la Directiva 2009/110/CE;

ii. obtener acceso apropiado a cualesquiera datos, documentos, instalaciones o personal del tercer país que sean relevantes para desempeñar sus poderes de supervisión;

iii. recibir, lo antes posible, información de la autoridad de supervisión del tercer país para investigar supuestos incumplimientos de los requisitos de la Directiva 2013/36/UE, el Reglamento (UE) n.º 575/2013, la Directiva (UE) 2015/2366 y la Directiva 2009/110/CE; y

iv. cooperar con las autoridades de supervisión pertinentes del tercer país en relación con la aplicación de medidas en caso de incumplimiento de los requisitos regulatorios y el Derecho nacional aplicables en el Estado miembro. La cooperación incluirá, pero no se limitará necesariamente a ello, la recepción de información sobre posibles incumplimientos de los requisitos regulatorios aplicables de las autoridades de supervisión en el tercer país lo antes posible.

12.2 Evaluación de riesgos de los acuerdos de externalización

64. Las entidades y las entidades de pago deberían evaluar el impacto potencial de los acuerdos de externalización en relación con su riesgo operacional, deberían tener en cuenta los resultados de la evaluación en el momento de decidir si la función se debe externalizar a un proveedor de servicios, y deberían tomar las medidas oportunas para evitar riesgos operacionales adicionales indebidos antes de suscribir dichos acuerdos de externalización.

65. La evaluación debería incluir, cuando proceda, escenarios de posibles situaciones de riesgo, incluidas las situaciones de conlleven riesgos operacionales de severidad alta. En el marco del análisis de escenarios, las entidades y las entidades de pago evaluarán el impacto potencial de que los servicios no sean adecuados o fallen, incluidos los riesgos causados por procesos, sistemas, personas o eventos externos. Las entidades y las entidades de pago, teniendo en cuenta el principio de proporcionalidad referido en la sección 1, deberían documentar el

análisis realizado y sus resultados, y deberían estimar en qué medida el acuerdo de externalización incrementaría o reduciría su riesgo operacional. Teniendo en cuenta el título I, las entidades y entidades de pago pequeñas y no complejas pueden recurrir a enfoques cualitativos en su evaluación de riesgos, mientras que las entidades grandes o complejas deberían aplicar un enfoque más sofisticado, incluido, cuando esté disponible, el uso de bases de datos internas y externas de pérdidas operacionales para conformar el análisis de escenarios.

66. Dentro de la evaluación de riesgos, las entidades y las entidades de pago deberían tener asimismo en cuenta los beneficios y costes esperados del acuerdo de externalización propuesto, incluyendo la ponderación de cualesquiera riesgos que puedan reducirse o gestionarse mejor frente a los riesgos que pueden derivarse del acuerdo de externalización en cuestión, considerando por lo menos:

    a. los riesgos de concentración, incluso los derivados de:

        i. la externalización a un proveedor de servicios dominante que no es fácilmente sustituible; y

        ii. múltiples acuerdos de externalización con el mismo proveedor de servicios o proveedores de servicios estrechamente vinculados;

    b. los riesgos agregados derivados de externalizar varias funciones de la entidad o la entidad de pago y, en el caso de grupos de entidades o sistemas institucionales de protección, los riesgos agregados a nivel consolidado o a nivel del sistema institucional de protección;

    c. en el caso de entidades significativas, el riesgo de *step-in*, es decir, el riesgo que pueda derivarse de la necesidad de proporcionar apoyo financiero a un proveedor de servicios en una situación de estrés financiero o de asumir sus operaciones de negocio; y

    d. las medidas aplicadas por la entidad o la entidad de pago y por el proveedor de servicios para gestionar y mitigar los riesgos.

67. Cuando el acuerdo de externalización contemple la posibilidad de que el proveedor de servicios subcontrate funciones esenciales o importantes a otros proveedores de servicios, las entidades y las entidades de pago deberían tener en cuenta:

    a. los riesgos asociados a la subcontratación, incluidos los riesgos adicionales que podrían surgir si el subcontratista está ubicado en un tercer país o en un país distinto que el proveedor de servicios;

    b. el riesgo de que las cadenas de subcontratación largas y complejas reduzcan tanto la capacidad de las entidades o entidades de pago para supervisar la función esencial o

importante externalizada como la capacidad de las autoridades competentes para supervisarlas eficazmente.

68. Cuando realicen la evaluación de riesgos previa a la externalización y durante el seguimiento continuado del desempeño del proveedor de servicios, las entidades y las entidades de pago deberían, como mínimo:

    a. identificar y clasificar las funciones pertinentes y los datos y sistemas relacionados en función de su sensibilidad y de las medidas de seguridad necesarias;

    b. llevar a cabo un análisis exhaustivo basado en el riesgo de las funciones y los datos y sistemas asociados cuya externalización se está considerando o que ya se han externalizado y abordar los riesgos potenciales, en particular los riesgos operacionales, incluidos los riesgos legales, de TIC, de cumplimiento y de reputación, y las limitaciones de la supervisión en los países en que se presten o puedan prestarse los servicios externalizados y en que se almacenen o probablemente se almacenen los datos;

    c. considerar las consecuencias del lugar en que se ubica el proveedor de servicios (dentro o fuera de la UE);

    d. considerar la estabilidad política y la situación de seguridad de las jurisdicciones en cuestión, incluyendo:

        i. la legislación en vigor, incluida la legislación en materia de protección de datos;

        ii. las disposiciones en vigor para hacer cumplir la ley; y

        iii. las disposiciones de la legislación concursal que se aplicarían en caso de quiebra del proveedor de servicios y las posibles limitaciones que se plantearían para recuperar con urgencia los datos de la entidad o entidad de pago en particular;

    e. definir y decidir el nivel apropiado de protección de la confidencialidad de la información, la continuidad de las actividades externalizadas, así como la integridad y trazabilidad de los datos y sistemas en el contexto de la externalización de servicios prevista. Además, las entidades y las entidades de pago deberían considerar la adopción de medidas específicas cuando sean necesarias para proteger los datos en tránsito, los datos en memoria y los datos en reposo, como el uso de tecnologías de cifrado combinadas con una arquitectura de gestión de claves adecuada;

    f. considerar si el proveedor de servicios es una filial o la matriz de la entidad, si está incluido en el perímetro de consolidación contable o forma parte de un sistema institucional de protección o es propiedad de una entidad miembro de un sistema institucional de protección y, en ese caso, en qué medida la entidad lo controla o tiene capacidad para influir en sus acciones en línea con la sección 2.

12.3 Diligencia debida

69. Antes de celebrar un acuerdo de externalización y considerar los riesgos operacionales relacionados con la función que se va a externalizar, las entidades y las entidades de pago deberían asegurarse de la idoneidad del proveedor de servicios en su proceso de selección y evaluación.

70. En relación con las funciones esenciales o importantes, las entidades y las entidades de pago deberían asegurarse de que el proveedor de servicios goza de buena reputación profesional y cuenta con capacidades apropiadas y suficientes, y con los conocimientos técnicos, la competencia, los recursos (p. ej., humanos, tecnológicos y financieros), la estructura organizativa y, si procede, la(s) autorización(es) o registro(s) preceptivos que sean necesarios para desempeñar la función esencial o importante de manera fiable y profesional cumpliendo sus obligaciones durante toda la duración del futuro contrato.

71. Los factores adicionales que han de considerarse a la hora de llevar a cabo la diligencia debida respecto de un posible proveedor de servicios incluyen, a título ilustrativo:

    a. su modelo de negocio, naturaleza, escala, complejidad, situación financiera, estructura de propiedad y estructura del grupo;

    b. las relaciones a largo plazo con proveedores de servicios que ya han sido evaluados y prestan servicios a la entidad o la entidad de pago;

    c. si el proveedor de servicios es una empresa matriz o filial de la entidad o la entidad de pago, forma parte del perímetro de la consolidación contable de la entidad o de un sistema institucional de protección o es propiedad de una entidad que pertenece al mismo sistema institucional de protección que la entidad;

    d. si el proveedor de servicios es supervisado o no por autoridades competentes.

72. Cuando la externalización conlleve el tratamiento de datos personales o confidenciales, las entidades y las entidades de pago deberían estar satisfechas de que el proveedor de servicios aplica medidas técnicas y organizativas adecuadas para proteger los datos.

73. Las entidades y las entidades de pago deberían adoptar las medidas oportunas para garantizar que la actuación del proveedor de servicios se ajusta a sus valores y código de conducta. En particular, por lo que respecta a los proveedores de servicios ubicados en terceros países y, en su caso, a sus subcontratistas, las entidades y las entidades de pago deberían estar satisfechas de que el proveedor de servicios actúa de manera ética y con responsabilidad social y respeta las normas internacionales sobre derechos humanos (p. ej., el Convenio Europeo de Derechos Humanos), protección del medio ambiente y condiciones de trabajo apropiadas, incluida la prohibición del trabajo infantil.

13 Fase contractual

74. Los derechos y las obligaciones de la entidad, la entidad de pago y el proveedor de servicios deberían estar claramente asignados y establecidos en un acuerdo escrito.

75. El acuerdo de externalización de funciones esenciales o importantes debería establecer, como mínimo:

    a. una descripción clara de la función externalizada a desempeñar;

    b. la fecha de inicio y de finalización, si procede, del acuerdo y los plazos de preaviso para el proveedor de servicios y para la entidad o la entidad de pago;

    c. el Derecho aplicable por el que se rige el acuerdo;

    d. las obligaciones financieras de las partes;

    e. si se permite la subcontratación de una función esencial o importante, o de partes significativas de la misma y, de ser así, las condiciones especificadas en la sección 13.1 a las que está sujeta la subcontratación;

    f. la localización o localizaciones (es decir, regiones o países) en las que se realizará la función esencial o importante o en las que se conservarán y tratarán los datos pertinentes, incluida la posible localización del almacenamiento, y las condiciones que han de cumplirse, incluida la obligación de notificar a la entidad o la entidad de pago en caso de que el proveedor del servicio proponga cambiar la localización o localizaciones;

    g. en su caso, disposiciones relativas a la accesibilidad, disponibilidad, integridad, privacidad y seguridad de los datos pertinentes, a tenor de lo especificado en la sección 13.2;

    h. el derecho de la entidad o de la entidad de pago a realizar un seguimiento continuado del desempeño del proveedor de servicios;

    i. los niveles de servicio acordados, que incluirán objetivos de rendimiento cuantitativos y cualitativos precisos para la función externalizada que permitan realizar un seguimiento oportuno, de modo que se puedan tomar medidas correctoras apropiadas sin demoras indebidas en caso de que no se respeten los niveles de servicio acordados;

    j. las obligaciones de información del proveedor de servicios a la entidad o la entidad de pago, incluida la comunicación por parte del proveedor de servicios de cualquier circunstancia que pueda repercutir de forma significativa en su capacidad para desempeñar con eficacia la función esencial o importante con arreglo a los niveles de servicio acordados y de conformidad con la normativa aplicable y, en su caso, las

obligaciones de presentación de informes de la función de control interno del proveedor de servicios;

k. si el proveedor de servicios debería suscribir un seguro obligatorio frente a determinados riesgos y, si procede, el nivel de cobertura requerido;

l. el requisito de establecer y probar los planes de contingencia del negocio;

m. disposiciones que garanticen la accesibilidad de los datos propiedad de la entidad o de la entidad de pago en caso de insolvencia, resolución o cese de las operaciones del proveedor de servicios;

n. la obligación del proveedor de servicios de cooperar con las autoridades competentes y las autoridades de resolución de la entidad o la entidad de pago, incluidas otras personas designadas por estas;

o. en el caso de las entidades, una referencia clara a las competencias de la autoridad nacional de resolución, en especial a los artículos 68 y 71 de la Directiva 2014/59/UE (DRRB), y en particular una descripción de las «obligaciones sustantivas» del contrato en el sentido del artículo 68 de dicha Directiva;

p. el derecho ilimitado de las entidades, entidades de pago y autoridades competentes de inspeccionar y auditar al proveedor de servicios por lo que respecta, en particular, a la función esencial o importante externalizada, tal como se especifica en la sección 13.3;

q. los derechos de resolución, tal como se especifica en la sección 13.4.

13.1 Subcontratación de funciones esenciales o importantes

76. El acuerdo de externalización debería especificar si se permite la subcontratación de funciones esenciales o importantes, o partes significativas de ellas.

77. Si se permite la subcontratación de funciones esenciales o importantes, las entidades y las entidades de pago deberían determinar si la parte de la función que se va a subcontratar es, como tal, esencial o importante (es decir, una parte significativa de la función esencial o importante) y, en caso de serlo, introducirlo en el registro.

78. Si se permite la subcontratación de funciones esenciales o importantes, el acuerdo escrito debería:

a. especificar cualquier tipo de actividad que esté excluido de la subcontratación;

b. especificar las condiciones que han de cumplirse en caso de subcontratación;

c. especificar que el proveedor de servicios está obligado a supervisar los servicios que haya subcontratado para garantizar que todas las obligaciones contractuales entre el proveedor de servicios y la entidad o entidad de pago se cumplen en todo momento;

d. obligar al proveedor de servicios a obtener la autorización previa por escrito, específica o general, de la entidad o la entidad de pago antes de la subcontratación del tratamiento de datos[34];

e. incluir la obligación de que el proveedor de servicios informe a la entidad o la entidad de pago de cualquier subcontratación prevista o cambio significativo en la misma, en particular cuando pueda afectar a la capacidad del proveedor de servicios para cumplir sus responsabilidades en virtud del acuerdo de externalización. Esto incluye los cambios significativos previstos de subcontratistas y del periodo de notificación; en concreto, el periodo de notificación que se fije debe permitir que la entidad o entidad de pago que externaliza lleve a cabo, como mínimo, una evaluación de riesgo de los cambios propuestos y se oponga a ellos antes de que se hagan efectivos la subcontratación prevista o los cambios significativos en la misma;

f. garantizar, en su caso, que la entidad o la entidad de pago tiene derecho a oponerse a la subcontratación prevista, o a los cambios significativos en la misma, o que es necesaria la autorización expresa;

g. garantizar que la entidad o la entidad de pago tiene el derecho contractual de resolver el acuerdo en caso de subcontratación indebida, por ejemplo, cuando la subcontratación incremente significativamente los riesgos para la entidad o la entidad de pago o cuando el proveedor de servicios subcontrate sin notificarlo a la entidad o entidad de pago.

79. Las entidades y las entidades de pago solo deberían aceptar la subcontratación cuando el subcontratista se comprometa a:

a. cumplir todas las leyes, requisitos regulatorios y obligaciones contractuales aplicables; y

b. conceder a la entidad, entidad de pago y autoridad competente los mismos derechos contractuales de acceso y auditoría que los concedidos por el proveedor de servicios.

80. Las entidades y las entidades de pago deberían asegurarse de que el proveedor de servicios supervise adecuadamente a los subcontratistas, en línea con la política definida por la entidad o la entidad de pago. Si la subcontratación propuesta pudiera tener efectos negativos significativos sobre el acuerdo de externalización de una función esencial o importante o conllevar un incremento significativo del riesgo, incluido el caso de que no se cumpliesen las condiciones establecidas en el apartado 79, la entidad o la entidad de pago debería ejercer su

[34] Véase el artículo 28 del Reglamento (UE) 2016/679.

derecho a oponerse a la subcontratación, si se hubiese acordado tal derecho, y/o resolver el contrato.

13.2 Seguridad de los datos y sistemas

81. Las entidades y las entidades de pago deberían asegurarse de que los proveedores de servicios, en su caso, cumplen los estándares de seguridad informática oportunos.

82. Cuando proceda (p. ej., en el contexto de servicios en la nube u otras externalizaciones TIC), las entidades y las entidades de pago deberían definir los requisitos de seguridad de los datos y sistemas dentro del acuerdo de externalización y realizar un seguimiento continuado del cumplimiento de estos requisitos.

83. En el caso de externalización a proveedores de servicios en la nube y otros acuerdos de externalización que impliquen el tratamiento o la transferencia de datos personales o confidenciales, las entidades y las entidades de pago deberían adoptar un enfoque basado en el riesgo en relación con las localizaciones del almacenamiento y el procesamiento de los datos (es decir, país o región) y con las cuestiones relativas a la seguridad de la información.

84. Sin perjuicio de los requisitos contemplados en el Reglamento (UE) 2016/679, las entidades y las entidades de pago, cuando externalicen (en particular a terceros países), deberían tener en cuenta las diferencias en las disposiciones nacionales en materia de protección de datos. Las entidades y las entidades de pago deberían asegurarse de que el acuerdo de externalización incluya la obligación de que el proveedor de servicios proteja la información confidencial, personal o cualquier otro tipo de información delicada y cumpla todos los requisitos legales en relación con la protección de datos aplicables a la entidad o la entidad de pago (p. ej., que, en su caso, se cumplen las normas sobre la protección de los datos personales y el secreto bancario u obligaciones de confidencialidad similares que establezca la ley con respecto a la información de los clientes).

13.3 Derechos de acceso, información y auditoría

85. Las entidades y las entidades de pago deberían asegurarse en el acuerdo escrito de externalización de que la función de auditoría interna sea capaz de revisar la función externalizada utilizando un enfoque basado en el riesgo.

86. Independientemente de la esencialidad o la importancia de la función externalizada, los acuerdos de externalización escritos entre las entidades y los proveedores de servicios deberían referirse a las facultades de recogida de información de las autoridades competentes y las autoridades de resolución en virtud del artículo 63, apartado 1, letra a), de la Directiva 2014/59/UE y del artículo 65, apartado 3, de la Directiva 2013/36/UE por lo que respecta a los proveedores de servicios ubicados en un Estado miembro, y deberían garantizar igualmente dichos derechos en relación con los proveedores de servicios ubicados en terceros países.

87. En relación con la externalización de funciones esenciales o importantes, las entidades y las entidades de pago deberían asegurarse, en el acuerdo de externalización escrito, de que el proveedor de servicios les conceda a ellas y a sus autoridades competentes, incluidas las

autoridades de resolución, y a cualquier otra persona nombrada por ellas o las autoridades competentes, lo siguiente:

a. pleno acceso a todas las instalaciones pertinentes (p. ej., oficinas centrales y centros de operaciones), incluida toda la gama de dispositivos, sistemas, redes, información y datos utilizados para llevar a cabo la función externalizada, incluida la información financiera relacionada, el personal y los auditores externos del proveedor de servicios («derechos de acceso e información»); y

b. derechos sin restricciones de inspección y auditoría en relación con el acuerdo de externalización («derechos de auditoría»), para que puedan realizar un seguimiento del acuerdo de externalización y garantizar el cumplimiento de todos los requisitos regulatorios y contractuales aplicables.

88. En el caso de la externalización de funciones que no sean esenciales o importantes, las entidades y las entidades de pago deberían garantizar los derechos de acceso y de auditoría establecidos en el apartado 87, letras a) y b), y en la sección 13.3 mediante un enfoque basado en el riesgo, considerando la naturaleza de la función externalizada y los riesgos operacionales y de reputación asociados, su escalabilidad, el posible impacto en el desempeño continuo de sus actividades y el periodo contractual. Las entidades y las entidades de pago deberían tener en cuenta que las funciones pueden convertirse en esenciales o importantes con el transcurso del tiempo.

89. Las entidades y las entidades de pago deberían asegurarse de que el acuerdo de externalización o cualquier otro acuerdo contractual no obstaculice ni limite el ejercicio efectivo de los derechos de acceso y auditoría por parte de ellas, de las autoridades competentes o de terceros nombrados por ellas para ejercer tales derechos.

90. Las entidades y las entidades de pago deberían ejercer sus derechos de acceso y de auditoría, determinar la frecuencia de las auditorías y las áreas que se van a auditar mediante un enfoque basado en el riesgo y ajustarse a las normas de auditoría nacionales e internacionales comúnmente aceptadas[35].

91. Sin perjuicio de su responsabilidad última en relación con los acuerdos de externalización, las entidades y las entidades de pago podrán utilizar:

a. auditorías compartidas organizadas conjuntamente con otros clientes del mismo proveedor de servicios, y realizadas por ellas y dichos clientes o por un tercero designado por ellos, con el fin de utilizar los recursos de auditoría de una manera más eficaz y de reducir la carga organizativa que suponen para los clientes y para el proveedor de servicios;

[35] En el caso de las entidades, véase la sección 22 de las Directrices de la ABE sobre gobierno interno. https://eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29_ES.pdf/de7783ac-51b3-4c6f-8314-be75c2e2b85e

b. certificaciones externas e informes de auditoría internos o externos facilitados por el proveedor de servicios.

92. Para la externalización de funciones esenciales o importantes, las entidades y las entidades de pago deberían evaluar si las certificaciones externas e informes a que se refiere el apartado 91, letra b) son adecuados y suficientes para cumplir sus obligaciones regulatorias, pero no deberían confiar exclusivamente en estos informes a lo largo del tiempo.

93. Las entidades y las entidades de pago deberían utilizar el método referido en el apartado 91, letra b), únicamente cuando:

a. estén satisfechas con el plan de auditoría para la función externalizada;

b. se aseguren de que el alcance de la certificación o del informe de auditoría incluye los sistemas (es decir, los procesos, aplicaciones, infraestructuras, centros de datos, etc.) y los controles clave identificados por la entidad o la entidad de pago y el cumplimiento de los requisitos regulatorios pertinentes;

c. evalúen en profundidad el contenido de las certificaciones o los informes de auditoría de manera continua y verifiquen que no estén obsoletos;

d. se aseguren de que los sistemas y controles clave se incluyan en futuras versiones de la certificación o el informe de auditoría;

e. estén satisfechas con la aptitud de la parte certificadora o auditora (por ejemplo, con relación a la rotación de la empresa certificadora o auditora, sus cualificaciones, conocimientos y experiencia, repetición/verificación de las pruebas del expediente de auditoría correspondiente);

f. estén satisfechas de que las certificaciones se emitan y las auditorías se lleven a cabo de acuerdo con los estándares generalmente aceptados e incluyan una prueba de la eficacia operativa de los controles clave establecidos;

g. dispongan del derecho contractual de solicitar una ampliación del alcance de las certificaciones o los informes de auditoría para que incluyan otros sistemas y controles que sean relevantes; el número y la frecuencia de dichas solicitudes de modificación del alcance serán razonables y lícitos desde una perspectiva de gestión de riesgos; y

h. conserven el derecho contractual de llevar a cabo auditorías individuales a su discreción respecto a la externalización de funciones esenciales o importantes.

94. En línea con las Directrices de la ABE sobre la evaluación del riesgo de TIC en el marco del proceso de revisión y evaluación supervisora (PRES), las entidades deberían asegurarse, cuando proceda, de que pueden realizar pruebas de penetración de seguridad para evaluar la eficacia de las medidas y procesos de ciberseguridad y de seguridad tecnológica interna

implementados[36]. Teniendo en cuenta el título I, las entidades de pago también deberían contar con controles tecnológicos internos, incluidas medidas de control y mitigación de seguridad tecnológica.

95. Antes de efectuar una visita in situ planificada, las entidades, entidades de pago, autoridades competentes y auditores o terceros que actúen en nombre de la entidad, la entidad de pago o las autoridades competentes deberían avisar al proveedor de servicios con una antelación razonable, a menos que no sea posible por una situación de emergencia o de crisis o porque provocaría una situación en la que la auditoría dejaría de ser eficaz.

96. Cuando se realicen auditorías en entornos multicliente, deberían tomarse precauciones para evitar o mitigar los riesgos para el entorno de otro cliente (p. ej., impacto en los niveles de servicio, disponibilidad de los datos, aspectos de confidencialidad).

97. Cuando el acuerdo de externalización conlleve un nivel elevado de complejidad técnica, por ejemplo, en el caso de externalización de servicios en la nube, la entidad o la entidad de pago debería verificar que quien realiza la auditoría —ya sean sus auditores internos, los auditores que realizan la auditoría compartida o auditores externos que actúan en su nombre— cuenta con capacidades y conocimientos apropiados y pertinentes para llevar eficazmente a cabo las auditorías o evaluaciones pertinentes. Esto es igualmente aplicable a todo el personal de la entidad o la entidad de pago que revise las certificaciones externas o auditorías realizadas por proveedores de servicios.

13.4 Derechos de resolución

98. El acuerdo de externalización debería contemplar expresamente la posibilidad de que la entidad o la entidad de pago resuelva el acuerdo, de conformidad con la legislación aplicable, incluyendo en las siguientes situaciones:

    a. cuando el proveedor de las funciones externalizadas esté infringiendo las disposiciones legales, regulatorias o contractuales aplicables;

    b. cuando se detecten obstáculos que puedan alterar el desempeño de la función externalizada;

    c. cuando se produzcan cambios significativos que afecten al acuerdo de externalización o al proveedor de servicios (p. ej., subcontratación o cambios en los subcontratistas);

    d. cuando existan deficiencias en relación con la gestión y la seguridad de datos o información confidenciales, personales o cualquier otro tipo de información o dato delicado ; y

[36] Véanse asimismo las Directrices de la ABE sobre el riesgo de TIC: https://eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_ES.pdf/0d081451-67d1-4f53-854e-f1b74d5b8e9e

e. cuando la autoridad competente de la entidad o la entidad de pago así lo establezca, por ejemplo, en caso de que la autoridad competente, como consecuencia del acuerdo de externalización, ya no esté en posición de supervisar eficazmente a la entidad o la entidad de pago.

99. El acuerdo de externalización debería facilitar la transferencia de la función externalizada a otro proveedor de servicios o su reincorporación a la entidad o la entidad de pago. A este fin, el acuerdo de externalización escrito debería:

a. estipular claramente las obligaciones del proveedor de servicios existente, en caso de transferencia de la función externalizada a otro proveedor de servicios o de que se reincorpore a la entidad o la entidad de pago, incluido el tratamiento de datos;

b. fijar un periodo de transición apropiado, durante el cual el proveedor de servicios, una vez resuelto el acuerdo de externalización, continuaría realizando la función externalizada para reducir el riesgo de interrupciones; e

c. incluir la obligación de que el proveedor de servicios preste apoyo a la entidad o la entidad de pago en la transferencia ordenada de la función en caso de que se resuelva el acuerdo de externalización.

14 Supervisión de las funciones externalizadas

100. Las entidades y entidades de pago deberían realizar un seguimiento continuado del desempeño de los proveedores de servicios en lo que respecta a todos los acuerdos de externalización aplicando un enfoque basado en el riesgo y centrándose principalmente en la externalización de funciones esenciales o importantes, vigilando, en particular, que se garantiza la disponibilidad, integridad y seguridad de los datos y la información. Cuando el riesgo, la naturaleza o la escala de una función externalizada hayan cambiado significativamente, las entidades y las entidades de pago deberían volver a evaluar la esencialidad o importancia de dicha función en consonancia con la sección 4.

101. Las entidades y las entidades de pago deberían aplicar la capacidad, la prudencia y la diligencia debidos en el seguimiento y la gestión de los acuerdos de externalización.

102. Las entidades deberían actualizar regularmente su evaluación de riesgos de acuerdo con la sección 12.2 y comunicar periódicamente al órgano de administración los riesgos identificados en relación con la externalización de funciones esenciales o importantes.

103. Las entidades y las entidades de pago deberían controlar y gestionar los riesgos de concentración internos provocados por los acuerdos de externalización, teniendo en cuenta la sección 12.2 de las presentes Directrices.

104. Las entidades y las entidades de pago deberían asegurarse permanentemente de que los acuerdos de externalización, y en especial en relación con las funciones esenciales o

importantes externalizadas, cumplan unos niveles de rendimiento y calidad apropiados en línea con sus políticas:

a. asegurándose de recibir los informes oportunos de los proveedores de servicios;

b. evaluando el desempeño de los proveedores de servicios utilizando herramientas tales como indicadores clave de desempeño, indicadores clave de control, informes de servicios prestados, autocertificación y exámenes independientes; y

c. revisando cualquier otra información pertinente recibida por el proveedor de servicios, incluidos informes sobre las medidas de continuidad de negocio y controles.

105. Las entidades deberían adoptar las medidas oportunas si detectan deficiencias en la realización de la función externalizada. En concreto, las entidades y las entidades de pago deberían efectuar un seguimiento de cualquier indicio de que los proveedores de servicios puedan no estar realizando la función esencial o importante externalizada de manera eficaz o de conformidad con las leyes y requisitos regulatorios aplicables. En caso de que se detecten deficiencias, las entidades y las entidades de pago deberían adoptar las medidas correctoras o reparadoras adecuadas. De ser necesario, dichas medidas podrán incluir la resolución del acuerdo de externalización con efecto inmediato.

15 Estrategias de salida

106. Las entidades y las entidades de pago deberían contar con una estrategia de salida documentada cuando externalicen funciones esenciales o importantes que esté en línea con su política de externalización y con los planes de continuidad de negocio[37], teniendo en cuenta como mínimo la posibilidad de:

a. resolución de los acuerdos de externalización;

b. insolvencia del proveedor de servicios;

c. deterioro de la calidad de la función externalizada e interrupciones reales o potenciales en la actividad debido a que la función no se realiza o se realiza de forma inadecuada;

d. riesgos significativos para el ejercicio apropiado y continuo de la función.

107. Las entidades y las entidades de pago deberían asegurarse de que pueden desvincularse de los acuerdos de externalización sin que ello genere interrupciones indebidas en sus actividades, ni limite su cumplimiento de los requisitos regulatorios, ni comprometa la continuidad y la calidad de los servicios prestados a sus clientes. Para ello, deberían:

[37] Las entidades, en línea con los requisitos contemplados en el artículo 85, apartado 2, de la Directiva 2013/36/UE y el título VI de las Directrices de la ABE sobre gobierno interno, y las entidades de pago deberán disponer de planes de continuidad de negocio apropiados en relación con la externalización de funciones esenciales o importantes.

a. elaborar e implementar planes de salida que sean exhaustivos, estén documentados y, en su caso, estén suficientemente probados (p. ej., realizando un análisis de los posibles costes, impactos, recursos e implicaciones temporales de transferir un servicio externalizado a un proveedor alternativo); e

b. identificar soluciones alternativas y elaborar planes de transición para que la entidad o la entidad de pago pueda recuperar las funciones y datos externalizados del proveedor de servicios y transferirlos a proveedores alternativos o reincorporarlos a la entidad o la entidad de pago, o adoptar otras medidas que garanticen la realización continuada de la actividad o de la función esencial o importante de una manera controlada y suficientemente probada, teniendo en cuenta las dificultades que puedan surgir debido a la localización de los datos y adoptando las medidas necesarias para asegurar la continuidad del negocio durante la fase de transición.

108. A la hora de elaborar las estrategias de salida, las entidades y las entidades de pago deberían:

a. definir los objetivos de la estrategia de salida;

b. realizar un análisis de impacto en el negocio que sea proporcional al riesgo de los procesos, servicios o actividades externalizados, a fin de identificar los recursos humanos y financieros que serían necesarios para implementar el plan de salida, así como el tiempo requerido para dicha implementación;

c. asignar funciones, responsabilidades y recursos suficientes para gestionar los planes de salida y la transición de las actividades;

d. definir criterios de éxito para la transición de las funciones y datos externalizados; y

e. definir los indicadores que se emplearán para el seguimiento del acuerdo de externalización (tal como se señala en la sección 14), incluidos indicadores basados en niveles de prestación del servicio inaceptables que activarían la salida.

Título V – Directrices sobre externalización destinadas a autoridades competentes

109. A la hora de establecer métodos apropiados para controlar el cumplimiento por parte de las entidades y las entidades de pago de las condiciones de la autorización inicial, las autoridades competentes deberían intentar identificar si los acuerdos de externalización suponen un cambio significativo en las condiciones y obligaciones de la autorización inicial de las entidades y entidades de pago.

110. Las autoridades competentes deberían estar satisfechas de que pueden supervisar eficazmente a las entidades y a las entidades de pago, incluyendo que las entidades y entidades de pago se han asegurado a través del acuerdo de externalización de que los proveedores de

servicios tienen la obligación de conceder derechos de acceso y de auditoría a la autoridad competente y a la entidad, en línea con la sección 13.3.

111. El análisis de los riesgos de externalización de las entidades debería llevarse a cabo como mínimo en el marco del PRES o, respecto de las entidades de pago, como parte de otros procesos de supervisión, incluidas solicitudes ad hoc, o durante inspecciones in situ.

112. Además de la información incluida en el registro a que se refiere la sección 11, las autoridades competentes podrán solicitar información adicional a las entidades y entidades de pago, en particular cuando se trate de acuerdos de externalización de funciones esenciales o importantes, a saber:

a. el análisis de riesgos detallado;

b. si el proveedor de servicios cuenta con un plan de continuidad de negocio apropiado para los servicios prestados a la entidad o entidad de pago que externaliza;

c. la estrategia de salida que se seguirá si cualquiera de las partes resuelve el acuerdo de externalización o se interrumpe la prestación de los servicios; y

d. los recursos y las medidas disponibles para controlar adecuadamente las actividades externalizadas.

113. Además de la información requerida en virtud de la sección 11, las autoridades competentes podrán exigir a las entidades y entidades de pago que faciliten información detallada sobre cualquier acuerdo de externalización, aunque la función de que se trate no se considere esencial o importante.

114. Las autoridades competentes deberían evaluar, aplicando un enfoque basado en riesgos, lo siguiente:

a. si las entidades y las entidades de pago gestionan y realizan un seguimiento adecuado, en particular, de los acuerdos de externalización de funciones esenciales o importantes;

b. si las entidades y las entidades de pago cuentan con recursos suficientes para gestionar y realizar un seguimiento de los acuerdos de externalización;

c. si las entidades y las entidades de pago identifican y gestionan todos los riesgos relevantes; y

d. si las entidades y las entidades de pago identifican, evalúan y gestionan adecuadamente los conflictos de interés en relación con los acuerdos de externalización, como por ejemplo en caso de externalización dentro de un grupo o del mismo sistema institucional de protección.

115. Las autoridades competentes deberían velar por que las entidades y las entidades de pago de la UE o el EEE no operen como «estructuras vacías de contenido», incluidas las situaciones en que las entidades se valen de operaciones espejo (*back-to-back*) o intragrupo para transferir una parte del riesgo de mercado y de crédito a una entidad no perteneciente a la UE o al EEE, y deberían asegurarse de que disponen de sistemas de gobierno y de gestión de riesgos apropiados para identificar y gestionar sus riesgos.

116. En su evaluación, las autoridades competentes deberían tener en cuenta todos los riesgos, en particular[38]:

a. los riesgos operacionales[39] que plantea el acuerdo de externalización;

b. los riesgos de reputación;

c. el riesgo de *step-in* que podría requerir que la entidad prestase apoyo financiero a un proveedor de servicios, en el caso de entidades significativas;

d. los riesgos de concentración dentro de la entidad, también en base consolidada, causados por la existencia de múltiples acuerdos de externalización con un único proveedor de servicios o proveedores de servicios estrechamente vinculados o de múltiples acuerdos de externalización en la misma área de negocio;

e. los riesgos de concentración a nivel sectorial, por ejemplo, cuando múltiples entidades o entidades de pago utilizan un único proveedor de servicios o un grupo reducido de proveedores de servicios;

f. la medida en que la entidad o entidad de pago que externaliza controla al proveedor de servicios o tiene capacidad para influir en sus acciones, la reducción de riesgos que podría derivarse de un nivel mayor de control, y si el proveedor de servicios está incluido en la supervisión consolidada del grupo; y

g. los conflictos de interés entre la entidad y el proveedor de servicios.

117. Cuando se detecten riesgos de concentración, las autoridades competentes deberían realizar un seguimiento de la evolución de dichos riesgos y deberían evaluar tanto su posible impacto sobre otras entidades y entidades de pago como sobre la estabilidad del mercado financiero; las autoridades competentes deberían informar, cuando proceda, a la autoridad de resolución sobre las nuevas funciones potencialmente esenciales[40] que se hayan identificado durante esta evaluación.

---

[38] En el caso de las entidades sujetas a la Directiva 2013/36/UE, véanse también las Directrices de la ABE sobre el PRES: https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2

[39] Véanse asimismo las Directrices de la ABE sobre el riesgo de TIC: https://eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_ES.pdf/0d081451-67d1-4f53-854e-f1b74d5b8e9e

[40] Tal como se define en el artículo 2, apartado 1, punto 35, de la DRRB.

118. Cuando se detecten aspectos preocupantes que lleven a la conclusión de que una entidad o una entidad de pago ya no dispone de sistemas de gobierno sólidos o no cumple los requisitos regulatorios, las autoridades competentes deberían tomar las medidas oportunas, que podrán incluir limitar o restringir el alcance de las funciones externalizadas o exigir la salida de uno o más acuerdos de externalización. En particular, habida cuenta de la necesidad de que la entidad o la entidad de pago opere de forma continuada, podría ser necesario cancelar los contratos si no se pueden garantizar la supervisión y el cumplimiento de los requisitos regulatorios por otros medios.

119. Las autoridades competentes deberían estar satisfechas de que pueden llevar a cabo una supervisión eficaz, en particular cuando las entidades y las entidades de pago externalicen funciones esenciales o importantes que se desarrollan fuera de la UE o del EEE.