EBA/REC/2017/03

28/03/2018

Recomendaciones

sobre la externalización de servicios a proveedores de servicios en la nube

1. Obligaciones de cumplimiento y de notificación

Rango jurídico de las presentes recomendaciones

1. El presente documento contiene recomendaciones 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 recomendaciones 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 definidas en el artículo 4, apartado 2, del Reglamento (UE) n.º 1093/2010 a las que sean de aplicación las recomendaciones 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 recomendaciones vayan dirigidas principalmente a las entidades.

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 28.05.2018, si cumplen o se proponen cumplir estas recomendaciones indicando, en caso negativo, los motivos para no cumplirlas. A falta de notificación en ese 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/REC/2017/03». Las notificaciones serán presentadas por personas debidamente facultadas para comunicar el cumplimiento en nombre de las respectivas autoridades competentes. Cualquier cambio en la situación de cumplimiento de las recomendaciones deberá notificarse igualmente a la ABE.

[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 y ámbito de aplicación

1. Las presentes recomendaciones especifican las condiciones para la externalización de servicios contemplada en las Directrices del CSBE sobre externalización de servicios, de 14 de diciembre de 2006, y se aplican a la externalización que realicen las entidades definidas en el artículo 4, apartado 1, punto 3, del Reglamento (UE) n.º 575/2013 a proveedores de servicios en la nube.

Destinatarios

2. Las presentes recomendaciones van dirigidas a las autoridades competentes definidas en el artículo 4, apartado 2, inciso i), del Reglamento (UE) n.º 1093/2010 y a las entidades definidas en el artículo 4, apartado 1, punto 3, del Reglamento n.º 575/2013[2].

Definiciones

3. A menos que se indique lo contrario, los términos utilizados y definidos en la Directiva 2013/36/UE[3] sobre requerimientos de capital y en las Directrices del CSBE tienen el mismo significado en las recomendaciones. Adicionalmente, a efectos de estas recomendaciones, se aplicarán las definiciones siguientes:

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.

[2] 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.

[3] 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.

Nube comunitaria	Infraestructura de nube disponible para el uso exclusivo de una comunidad específica de entidades, incluido el caso de varias entidades de un mismo grupo.
Nube híbrida	Infraestructura de nube compuesta por dos o más infraestructuras de nube distintas.

3. Aplicación

Fecha de aplicación

4. Estas recomendaciones serán de aplicación a partir del 1 de julio de 2018.

4. Recomendaciones sobre la externalización de servicios a proveedores de servicios en la nube

4.1 Evaluación de significatividad

1. Antes de externalizar sus actividades, las entidades deberán evaluar qué actividades deben considerarse significativas. Las entidades llevarán a cabo la evaluación de significatividad de sus actividades de conformidad con la Directriz 1, letra f), de las Directrices del CSBE y, en lo que respecta a la externalización a proveedores de servicios en la nube en particular, teniendo en cuenta los siguientes aspectos:

    (a) la criticidad y el perfil de riesgo inherente de las actividades que van a externalizarse, es decir, si se trata de actividades críticas para la continuidad del negocio o la viabilidad de la entidad y sus obligaciones con los clientes;

    (b) el impacto directo sobre la operativa de las interrupciones del servicio, y los riesgos jurídico y de reputación relacionados;

    (c) el impacto que cualquier interrupción de la actividad podría tener sobre las perspectivas de ingresos de la entidad;

    (d) el impacto potencial que una violación de la confidencialidad o un error en la integridad de los datos podría tener en la entidad y sus clientes.

4.2 Deber de informar adecuadamente a las autoridades supervisoras

2. Las entidades que externalizan informarán adecuadamente a las autoridades competentes de las actividades significativas que se propongan externalizar a proveedores de servicios en la nube. Para ello, tendrán en cuenta el punto 4.3 de las Directrices del CSBE y, en todo caso, pondrán a disposición de las autoridades competentes la siguiente información:

    (a) el nombre del proveedor de servicios en la nube y el nombre de su empresa matriz (si la hubiera);
    (b) una descripción de las actividades y datos que se externalizarán;
    (c) el país o los países en los que se prestará el servicio (incluida la localización de los datos);
    (d) la fecha de comienzo del servicio;
    (e) la última fecha de renovación del contrato (si procede);
    (f) la legislación aplicable por la que se rige el contrato;

(g) la fecha de vencimiento del servicio o la próxima fecha de renovación del contrato (si procede).

3. Además de la información facilitada de acuerdo con el punto anterior, la autoridad competente podrá pedir a la entidad que externaliza información adicional sobre su análisis de riesgos de las actividades significativas que van a externalizarse, como por ejemplo:

   (a) si el proveedor de servicios en la nube cuenta con un plan de continuidad de negocio apropiado para los servicios prestados a la entidad que externaliza;
   (b) si la entidad que externaliza cuenta con una estrategia de salida en caso de rescisión del contrato por cualquiera de las partes o de la interrupción de la prestación de servicios por parte del proveedor de servicios en la nube;
   (c) si la empresa que externaliza posee las habilidades y los recursos necesarios para realizar un seguimiento adecuado de las actividades externalizadas.

4. La entidad que externaliza mantendrá un registro actualizado de información sobre todas sus actividades significativas y no significativas externalizadas a proveedores de servicios en la nube, tanto a nivel de la entidad como del grupo. La entidad que externaliza pondrá a disposición de la autoridad competente, previa solicitud, una copia del acuerdo de externalización y de la información relacionada contenida en dicho registro, independientemente de que la actividad externalizada a un proveedor de servicios en la nube haya sido identificada como significativa o no en la evaluación realizada por la entidad.

5. En el registro al que se hace mención en el punto anterior, deberá incluirse la siguiente información, como mínimo:

   (a) la información indicada en el punto 2, letras a) a g), si no se ha facilitado todavía;
   (b) el tipo de externalización (modelo de servicio en la nube y modelo de despliegue en la nube; a saber, nube pública, privada, híbrida o comunitaria);
   (c) las partes beneficiarias de los servicios en la nube de conformidad con el acuerdo de externalización;
   (d) pruebas de la aprobación de la externalización por parte del órgano de administración o sus comités delegados, si procede;
   (e) los nombres de los subcontratistas, si procede;
   (f) el país en el que se encuentra registrado el proveedor de servicios en la nube o el subcontratista principal;
   (g) si la externalización se ha calificado como significativa (sí/no);
   (h) la fecha de la última evaluación que ha realizado la entidad sobre si las actividades externalizadas son significativas;
   (i) si el proveedor de servicios en la nube o los subcontratistas están soportando operaciones de negocio en las que el factor tiempo es crítico (sí/no);
   (j) una evaluación de la sustituibilidad del proveedor de servicios en la nube (fácil, difícil o imposible);
   (k) identificación de un proveedor de servicios alternativo, siempre que resulte posible;
   (l) la fecha de la última evaluación de riesgos del acuerdo de externalización o subcontratación.

4.3 Derechos de acceso y de auditoría

Para las entidades

6. En virtud de la Directriz 8, apartado 2, letra g) de las Directrices del CSBE y a efectos de la externalización de servicios en la nube, las entidades que externalizan se asegurarán de contar con un acuerdo por escrito con el proveedor de servicios en la nube por medio del cual este último se obliga a:

    (a) proporcionar a la entidad, a cualquier tercero que la entidad designe para tal efecto y al auditor legal de esta acceso pleno a las instalaciones (oficinas centrales y centros de operaciones), incluida toda la gama de dispositivos, sistemas, redes y datos utilizados para prestar los servicios externalizados (derecho de acceso);

    (b) otorgar a la entidad, a cualquier tercero que la entidad designe para tal efecto y al auditor legal de esta derechos ilimitados de inspección y auditoría en relación con los servicios externalizados (derecho de auditoría).

7. Los acuerdos contractuales no obstaculizarán ni limitarán el ejercicio efectivo de los derechos de acceso y de auditoría. Si la realización de auditorías o la utilización de ciertas técnicas de auditoría pudieran crear un riesgo para el entorno de otro cliente, deberán acordarse formas alternativas de facilitar a la entidad un nivel de aseguramiento similar.

8. La entidad que externaliza ejercerá sus derechos de auditoría y de acceso en función del riesgo. Si no utiliza sus propios recursos de auditoría, deberá plantearse el uso de al menos una de las siguientes herramientas:

    (a) Auditorías compartidas organizadas conjuntamente con otros clientes del mismo proveedor de servicios en la nube, y realizadas por dichos clientes o por un tercero que ellos designen, 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 en la nube.

    (b) Certificaciones externas e informes de auditoría internos o externos facilitados por el proveedor de servicios en la nube, siempre y cuando:

        i. La entidad que externaliza se asegure 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 que ella considera clave.
        ii. La entidad que externaliza evalúe en profundidad el contenido de las certificaciones o de los informes de auditoría de forma continua y, en particular, se asegure de que los controles clave sigan estando incluidos en versiones futuras de un informe de auditoría y verifique que la certificación o el informe de auditoría no estén obsoletos.
        iii. La entidad que externaliza esté satisfecha con la aptitud de la parte certificadora o auditora (por ejemplo, con relación a la rotación de la empresa

certificadora o auditora, su cualificación, conocimientos y experiencia, repetición/verificación de las pruebas del expediente de auditoría correspondiente).

iv. 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.

v. La entidad que externaliza disponga del derecho contractual de solicitar una ampliación del alcance de las certificaciones o informes de auditoría para que incluyan ciertos sistemas o 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.

9. Habida cuenta del alto grado de complejidad técnica de las soluciones en la nube, la entidad que externaliza comprobará que el personal que lleve a cabo la auditoría (ya sean sus auditores internos o los auditores compartidos que actúen en su nombre, o los auditores designados por el proveedor de servicios en la nube) o, según proceda, el personal que revise las certificaciones de terceros o los informes de auditoría del proveedor de servicios, hayan adquirido las habilidades y conocimientos necesarios para realizar auditorías o evaluaciones eficaces y pertinentes de las soluciones en la nube.

Para las autoridades competentes

10. En virtud de la Directriz 8, apartado 2, letra h) de las Directrices del CSBE y a efectos de la externalización de servicios en la nube, las entidades que externalizan se asegurarán de contar con un acuerdo por escrito con el proveedor de servicios en la nube por medio del cual este último se obliga a:

    (a) proporcionar a la autoridad competente encargada de supervisar a la entidad que externaliza (o a cualquier tercero designado a tal fin por esta autoridad) acceso pleno a las instalaciones del proveedor de servicios en la nube (oficinas centrales y centros de operaciones), incluida toda la gama de dispositivos, sistemas, redes y datos utilizados para prestar los servicios a la entidad que externaliza (derecho de acceso);

    (b) otorgar a la autoridad competente encargada de supervisar a la entidad que externaliza (o a cualquier tercero designado a tal fin por esta autoridad) derechos ilimitados de inspección y auditoría en relación con los servicios externalizados (derecho de auditoría).

11. La entidad que externaliza se asegurará de que los acuerdos contractuales no impidan que su autoridad competente lleve a cabo y cumpla su función y sus objetivos de supervisión.

12. La información que las autoridades competentes obtengan del ejercicio de los derechos de acceso y de auditoría estará sujeta a las obligaciones de secreto profesional y confidencialidad mencionadas en el artículo 53 y siguientes de la Directiva 2013/36/UE (DRC IV). Las autoridades competentes se abstendrán de suscribir acuerdos o declaraciones contractuales que les impidan

cumplir con las provisiones del Derecho de la Unión en materia de confidencialidad, secreto profesional e intercambio de información.

13. En función de los resultados de la auditoría, la autoridad competente abordará cualquier deficiencia identificada, si fuera necesario, mediante la imposición de medidas directamente a la entidad que externaliza.

4.4 En relación con el derecho de acceso en particular

14. El acuerdo al que se refieren los puntos 6 y 10 incluirá las siguientes estipulaciones:

(a) La parte que tenga intención de ejercer su derecho de acceso (entidad, autoridad competente, auditor o tercero que actúe en nombre de la entidad o de la autoridad competente) deberá informar con un periodo de tiempo razonable de la visita *in situ* prevista a las instalaciones pertinentes antes de su realización, a menos que no sea posible notificar la visita con antelación debido a una situación de emergencia o de crisis.

(b) El proveedor de servicios en la nube deberá cooperar plenamente con las autoridades competentes pertinentes, así como con la entidad y su auditor, en relación con la visita *in situ.*

4.5 Seguridad de los datos y sistemas

15. Como se menciona en la Directriz 8, apartado 2, letra e) de las Directrices del CSBE, el contrato de externalización obligará al proveedor de los servicios externalizados a proteger la confidencialidad de la información transmitida por la entidad financiera. De acuerdo con la Directriz 6, apartado 6, letra e), de las Directrices del CSBE, las entidades implantarán medidas para asegurar la continuidad de los servicios prestados por los proveedores de los servicios externalizados. Sobre la base de la Directriz 8, apartado 2, letra b) y de la Directriz 9 de las Directrices del CSBE, las respectivas necesidades de las entidades que externalizan con respecto a la calidad y al rendimiento se plasmarán por escrito en contratos de externalización y en acuerdos de nivel de servicio. Estos aspectos relacionados con la seguridad serán además objeto de seguimiento continuado (Directriz 7).

16. A efectos del punto anterior, la entidad llevará a cabo, antes de la externalización y a fin de que sirvan de base para la decisión pertinente, como mínimo las siguientes acciones:

(a) identificará y clasificará sus actividades, procesos y datos y sistemas relacionados en función de su sensibilidad y de las medidas de protección requeridas;

(b) realizará una selección minuciosa, en función del riesgo, de las actividades, procesos y datos y sistemas relacionados que se esté considerando externalizar a un proveedor de soluciones de computación en nube;

(c) definirá y decidirá 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 en la nube prevista. Además, las entidades considerarán 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.

17. Posteriormente, las entidades se asegurarán de disponer de un acuerdo por escrito con el proveedor de servicios en la nube en el que, entre otras, se estipulen las obligaciones de este de conformidad con el punto 16, letra c).

18. De conformidad con la Directriz 7 de las Directrices del CSBE, las entidades realizarán un seguimiento continuado del desempeño de las actividades y de las medidas de seguridad, incluidos incidentes, revisarán, según proceda, si la externalización de las actividades cumple con lo establecido en los puntos anteriores y tomarán las medidas correctoras necesarias de inmediato.

4.6 Localización de los datos y del procesamiento de datos

19. Según lo indicado en la Directriz 4, apartado 4, de las Directrices del CSBE, las entidades actuarán con especial prudencia cuando suscriban y gestionen contratos de externalización con proveedores ubicados fuera del EEE, debido a los posibles riesgos relativos a la protección de datos y a la realización de una supervisión eficaz por parte de la autoridad supervisora.

20. Cuando externalice a un entorno en la nube, la entidad que externaliza evaluará la localización de los datos y del procesamiento de datos con un enfoque basado en el riesgo. La evaluación tendrá en cuenta el impacto potencial de los riesgos, incluidos los riesgos jurídicos y de cumplimiento, y las limitaciones a la vigilancia relacionados con los países en los que se van a llevar a cabo, o es probable que se lleven a cabo, los servicios externalizados y en los que se van a almacenar, o es probable que se almacenen, los datos. La evaluación tomará en consideración la estabilidad política y en materia de seguridad de las jurisdicciones en cuestión, la legislación vigente en dichas jurisdicciones (incluidas las leyes de protección de datos), y los mecanismos para asegurar el cumplimiento de las leyes en dichas jurisdicciones, incluidas las disposiciones de la legislación de insolvencia que serían aplicables en caso de quiebra del proveedor de servicios en la nube. La entidad que externaliza se asegurará de que esos riesgos permanezcan dentro de unos límites aceptables y proporcionales a la significatividad de la actividad externalizada.

4.7 Externalización en cadena

21. Tal y como se establece en la Directriz 10 de las Directrices del CSBE, las entidades tendrán en cuenta los riesgos asociados a la externalización «en cadena» cuando el proveedor del servicio externalizado subcontrate partes del servicio a otros proveedores. La entidad que externaliza aceptará la externalización en cadena solamente si el subcontratista cumple también plenamente con las obligaciones existentes entre la entidad que externaliza y el proveedor del servicio externalizado. Además, la entidad que externaliza tomará las medidas necesarias para hacer frente al riesgo de deficiencias o fallos en la realización de las actividades subcontratadas que pudieran tener un efecto significativo en la capacidad del proveedor del servicio externalizado para cumplir sus responsabilidades de conformidad con el acuerdo de externalización.

22. El acuerdo de externalización entre la entidad que externaliza y el proveedor de servicios en la nube detallará los tipos de actividad que quedan excluidos de posibles subcontrataciones e indicará que el proveedor de servicios en la nube vigilará y será plenamente responsable de aquellos servicios que subcontrate.

23. El acuerdo de externalización también incluirá la obligación para el proveedor de servicios en la nube de informar a la entidad que externaliza de cualquier cambio importante previsto con relación a los subcontratistas o a los servicios subcontratados que figuran en el acuerdo inicial y que podría afectar a la capacidad del proveedor de servicios para cumplir con sus responsabilidades de conformidad con el acuerdo de externalización. El periodo de notificación

de dichos cambios se establecerá previamente en el acuerdo para permitir que la entidad que externaliza realice una evaluación de riesgos de los efectos de los cambios propuestos antes de que se produzca efectivamente el cambio de subcontratistas o en los servicios subcontratados.

24. En caso de que el proveedor de servicios en la nube planeara un cambio de subcontratista o cambios en los servicios subcontratados cuyo efecto en la evaluación de riesgos de los servicios acordados fuera negativo, la entidad que externaliza tendría derecho a rescindir el contrato.

25. La entidad que externaliza revisará y realizará un seguimiento de la prestación global del servicio de forma continuada, independientemente de si lo prestan el proveedor de servicios en la nube o sus subcontratistas.

4.8 Planes de contingencia y estrategias de salida

26. Tal y como se establece en la Directriz 6.1, 6, apartado 6, letra e), y en la Directriz 8, apartado 2, letra d), de las Directrices del CSBE, la entidad que externaliza planeará e implantará medidas para mantener la continuidad de su negocio en caso de que la prestación de servicios por parte de un proveedor de servicios externalizados falle o se deteriore hasta un grado inaceptable. Estas medidas incluirán un plan de contingencia y una estrategia de salida claramente definida. Asimismo, el contrato de externalización contendrá una cláusula de resolución y de gestión de salida que permita que las actividades realizadas por el proveedor de los servicios externalizados se transfieran a otro proveedor externo o vuelvan a incorporarse en la entidad que externaliza.

27. La entidad que externaliza también se asegurará de poder salir de los acuerdos de externalización de servicios en la nube, en caso necesario, sin que ello genere alteraciones excesivas en los servicios prestados, ni afecte negativamente a su cumplimiento con el régimen regulatorio, ni comprometa la continuidad y la calidad de los servicios prestados a sus clientes. A estos efectos, la entidad que externaliza deberá:

    (a) desarrollar e implementar planes de salida que sean completos, estén documentados y estén suficientemente probados, cuando proceda;

    (b) identificar soluciones alternativas y desarrollar planes de transición que le permitan retirar y transferir las actividades y datos existentes desde el proveedor de servicios en la nube a dichas soluciones de manera controlada y suficientemente probada, teniendo en cuenta la cuestión de la localización de los datos y el mantenimiento de la continuidad del negocio durante la fase de transición;

    (c) asegurarse de que el acuerdo de externalización imponga al proveedor de servicios en la nube la obligación de prestar apoyo suficiente a la entidad que externaliza para la transferencia ordenada de la actividad a otro proveedor de servicios o directamente a la propia entidad en caso de resolución del acuerdo de externalización.

28. A la hora de desarrollar las estrategias de salida, la entidad que externaliza considerará:

(a) el desarrollo de indicadores clave de riesgo para detectar un nivel de servicio inaceptable;

(b) la realización de un análisis de impacto en el negocio que sea proporcional a las actividades externalizadas para identificar los recursos humanos y materiales que serían necesarios para implementar el plan de salida, así como el tiempo necesario para dicha implementación;

(c) la asignación de funciones y responsabilidades para gestionar los planes de salida y las actividades de transición;

(d) la definición de los criterios de éxito de la transición.

29. En su seguimiento y supervisión continuos de los servicios prestados por el proveedor de servicios en la nube, la entidad que externaliza incluirá indicadores que puedan activar el plan de salida.