

Directrices sobre la externalización a proveedores de servicios en la nube

Índice

Introducción	3
Definiciones	4
Fecha de aplicación	4
Directriz 1 – Servicios en la nube y externalización	5
Directriz 2 – Principios generales de gobernanza para la externalización en la nube.....	5
Directriz 3 – Actualización de la política de externalización por escrito	5
Directriz 4 - Notificación por escrito a la autoridad de supervisión	6
Directriz 5 – Requisitos de documentación	7
Directriz 6 – Análisis previo a la externalización.....	8
Directriz 7 – Evaluación de las funciones o actividades operativas críticas o importantes.....	8
Directriz 8 – Evaluación de riesgos de la externalización en la nube	9
Directriz 9 – Diligencia debida del proveedor de servicios en la nube	10
Directriz 10 – Requisitos contractuales	11
Directriz 11 – Derechos de acceso y auditoría.....	12
Directriz 12 – Seguridad de los datos y los sistemas	13
Directriz 13 – Subexternalización de las funciones o actividades operativas - críticas o importantes	14
Directriz 14 – Supervisión y control de los acuerdos de externalización en la nube	15
Directriz 15 – Derechos de rescisión y estrategias de salida	15
Directriz 16 – Supervisión de los acuerdos de externalización en la nube por las autoridades de supervisión	16
Normas sobre el cumplimiento y el deber de información.....	17
Disposición final sobre revisiones.....	17

Introducción

1. De conformidad con el artículo 16 del Reglamento (UE) n.º 1094/2010¹ la AESPJ emite directrices para ofrecer orientaciones a las empresas de seguros y de reaseguros respecto a la forma en que las disposiciones sobre externalización establecidas en la Directiva 2009/138/CE² (en lo sucesivo, «Directiva Solvencia II») y en el Reglamento Delegado (UE) n.º 2015/35 de la Comisión³ (en lo sucesivo, «Reglamento Delegado») deben aplicarse en caso de externalización a proveedores de servicios en la nube.
2. Estas Directrices se basan en los artículos 13, apartado 28, 38 y 49 de la Directiva Solvencia II y en el artículo 274 del Reglamento Delegado. Estas Directrices se basan asimismo en las orientaciones de las Directrices de la AESPJ sobre el Sistema de Gobernanza (EIOPA-BoS-14/253).
3. Las presentes Directrices se dirigen a las autoridades competentes con el fin de ofrecer orientaciones sobre la forma en que las empresas de seguros y reaseguros (conjuntamente, «empresa(s)») deben aplicar los requisitos de externalización previstos en los actos jurídicos antes mencionados en el contexto de la externalización a los proveedores de servicios en la nube.
4. Las Directrices se aplican tanto a empresas individuales como a grupos *mutatis mutandis*⁴.

Las entidades sujetas a otros requisitos sectoriales, y que formen parte de un grupo, están excluidas del ámbito de aplicación de las presentes Directrices a nivel individual, ya que deben seguir los requisitos sectoriales específicos, así como las orientaciones pertinentes emitidas por la Autoridad Europea de Valores y Mercados y la Autoridad Bancaria Europea.

5. En caso de externalización intragrupo y de subexternalización a proveedores de servicios en la nube, estas Directrices deberán aplicarse junto con las disposiciones de las Directrices de la AESPJ sobre el Sistema de Gobernanza en la externalización intragrupo.
6. Al cumplir o supervisar el cumplimiento de las presentes Directrices, las empresas y las autoridades competentes deberán tener en cuenta el principio de proporcionalidad⁵ y la esencialidad o importancia del servicio externalizado a proveedores de servicios en la nube. El principio de proporcionalidad debe garantizar que los acuerdos de gobernanza, incluidos los relativos a la externalización a proveedores de servicios en la nube, sean coherentes con la naturaleza, el volumen y la complejidad de los riesgos subyacentes.
7. Las presentes Directrices deben leerse junto con (y sin perjuicio de) las Directrices de la AESPJ sobre el Sistema de Gobernanza y las obligaciones reglamentarias enumeradas en el apartado 1.

¹ Reglamento (UE) n.º 1094/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión n.º 2009/79/CE de la Comisión (DO L 331 del 15.12.2010, p. 48).

² Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio («Solvencia II»), DO L 335 de 17.12.2009, p. 1.

³ Reglamento Delegado (UE) 2015/35 de la Comisión, de 10 de octubre de 2014, por el que se completa la Directiva 2009/138/CE del Parlamento Europeo y del Consejo sobre el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II), DO L 12, 17.1.2015, p. 1.

⁴ Artículo 212, apartado 1, de la Directiva Solvencia II.

⁵ Artículo 29, apartado 3, de la Directiva Solvencia II.

Definiciones

8. Si no se definen en las presentes Directrices, los términos tienen el significado que se les atribuye en los actos jurídicos mencionados en la introducción.
9. Además, a los efectos de estas Directrices, se entenderá por:

Proveedor de servicios	Tercera parte que realiza un proceso, servicio o actividad, o partes de los mismos, con arreglo a un acuerdo de externalización.
Proveedor de servicios en la nube	Proveedor de servicios, tal y como se define más arriba, encargado de prestar servicios en la nube 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 empresa.
Nube comunitaria	Infraestructura de nube disponible para el uso exclusivo de una comunidad específica de empresas, incluido el caso de varias empresas de un mismo grupo.
Nube híbrida	Infraestructura de nube compuesta por dos o más infraestructuras de nube distintas.

Fecha de aplicación

10. Las presentes Directrices se aplicarán a partir del 1 de enero de 2021 a todos los acuerdos de externalización de servicios en la nube celebrados o modificados en dicha fecha o con posterioridad a la misma.
11. Las empresas deberán revisar y modificar en consecuencia los acuerdos de externalización en la nube existentes relativos a funciones o actividades operativas críticas o importantes con vistas a garantizar el cumplimiento de las presentes Directrices antes del 31 de diciembre de 2022.
12. Cuando la revisión de los acuerdos de externalización de funciones o actividades operativas críticas o importantes no haya finalizado antes del 31 de diciembre de 2022, la empresa deberá informar de ello a su autoridad de supervisión⁶, incluyendo las medidas previstas para completar la revisión o la posible estrategia de salida. La autoridad de supervisión podrá acordar con la empresa una prórroga del plazo para completar dicha revisión, cuando proceda.
13. La actualización (cuando sea necesaria) de las políticas y procesos internos de la empresa deberá efectuarse antes del 1 de enero de 2021, y los requisitos de documentación para los acuerdos de externalización en la nube relativos a funciones o actividades operativas críticas o importantes deberán aplicarse antes del 31 de diciembre de 2022.

⁶ Artículo 13, apartado 10, de la Directiva Solvencia II.

Directriz 1 – Servicios en la nube y externalización

14. La empresa debe determinar si un acuerdo con un proveedor de servicios en la nube está comprendido en la definición de externalización de conformidad con la Directiva Solvencia II. A la hora de realizar la evaluación, debe tomarse en consideración:
- a. si la función o actividad operativa (o una parte de las mismas) externalizada se realiza de forma recurrente o continua; y
 - b. si dicha función o actividad operativa (o una parte de las misma) normalmente estaría comprendida en el ámbito de aplicación de las funciones o actividades operativas que realizaría o podría realizar la empresa en el curso de sus actividades comerciales normales, aunque la empresa no haya desempeñado esa función o actividad operativa en el pasado.
15. Cuando un acuerdo con un proveedor de servicios abarque varias funciones o actividades operativas, la empresa debe tener en cuenta todos los aspectos del acuerdo en su evaluación.
16. En los casos en los que la empresa externalice funciones o actividades operativas a proveedores de servicios que no sean proveedores de servicios en la nube pero se basen significativamente en infraestructuras de nube para prestar sus servicios (por ejemplo, cuando el proveedor de servicios en la nube forme parte de una cadena de subexternalización), el acuerdo para tal externalización pertenece al ámbito de aplicación de las presentes Directrices.

Directriz 2 – Principios generales de gobernanza para la externalización en la nube

17. Sin perjuicio del artículo 274, apartado 3, del Reglamento Delegado, el órgano de administración, dirección o supervisión de la empresa («OADS») debe asegurarse de que cualquier decisión de externalizar funciones o actividades operativas críticas o importantes a proveedores de servicios en la nube se base en una evaluación de riesgos exhaustiva que incluya todos los riesgos pertinentes que implica el acuerdo, como las tecnologías de la información y la comunicación («TIC»), la continuidad de las actividades, la legalidad y el cumplimiento, la concentración, otros riesgos operativos y los riesgos asociados a la migración de datos y/o la fase de aplicación, cuando proceda.
18. En caso de externalización a proveedores de servicios en la nube de funciones o actividades operativas críticas o importantes, la empresa, cuando proceda, deberá reflejar en su perfil de riesgo los cambios derivados de los acuerdos de externalización en la nube en su propia evaluación interna de los riesgos y de la solvencia («EIRS»).
19. El uso de servicios en la nube debe ser coherente con las estrategias de la empresa (por ejemplo, estrategia de TIC, estrategia de seguridad de la información, estrategia de gestión de riesgos operativos) y las políticas y procesos internos, que deberán actualizarse cuando sea necesario.

Directriz 3 – Actualización de la política de externalización por escrito

20. En caso de externalización a proveedores de servicios en la nube, la empresa deberá actualizar la política de externalización por escrito (por ejemplo, revisándola, añadiendo un anexo separado o elaborando nuevas políticas específicas) y las demás políticas internas pertinentes (por ejemplo, seguridad de la información), teniendo en cuenta las particularidades de la externalización en la nube al menos en los siguientes aspectos:

- a. los roles y responsabilidades de las funciones afectadas de la empresa, en especial el OADS, y las funciones responsables de TIC, la seguridad de la información, el cumplimiento, la gestión de riesgos y la auditoría interna;
- b. los procesos y procedimientos de información necesarios para la aprobación, aplicación, supervisión, gestión y renovación, si procede, de los acuerdos de externalización en la nube relativos a funciones o actividades operativas críticas o importantes;
- c. el control de los servicios en la nube coherente con la naturaleza, el volumen y la complejidad de los riesgos inherentes a los servicios prestados, como: i) evaluación de riesgos de los acuerdos de externalización en la nube y debida diligencia de los proveedores de servicios en la nube, incluida la frecuencia de la evaluación de riesgos; ii) controles de gestión y supervisión (por ejemplo, comprobación del acuerdo de nivel de servicio); iii) normas y controles de seguridad;
- d. respecto a la externalización en la nube de funciones o actividades operativas críticas o importantes, debe hacerse referencia a los requisitos contractuales descritos en la Directriz 10;
- e. los requisitos de documentación y notificación por escrito a la autoridad de supervisión en relación con la externalización en la nube de funciones o actividades operativas críticas o importantes;
- f. respecto a cada acuerdo de externalización en la nube que abarque funciones o actividades operativas críticas o importantes, ~~un requisito de una~~ «estrategia de salida» documentado y, cuando proceda, suficientemente probado, que sea coherente con la naturaleza, el volumen y la complejidad de los riesgos inherentes a los servicios prestados. La estrategia de salida puede incluir una serie de procesos de terminación, entre otros, la interrupción, la reintegración o el traslado de los servicios incluidos en el acuerdo de externalización en la nube.

Directriz 4 - Notificación por escrito a la autoridad de supervisión

- 21. Los requisitos de notificación por escrito establecidos en el artículo 49, apartado 3, de la Directiva Solvencia II y detallados en las Directrices de la AESPJ sobre el Sistema de Gobernanza son aplicables a todas las externalizaciones de funciones o actividades operativas críticas o importantes a proveedores de servicios en la nube. En caso de que una función o actividad operativa externalizada previamente clasificada como no **esencial crítica** o no importante pase a ser **esencial crítica** o importante, la empresa deberá notificarlo a la autoridad de supervisión.
- 22. La notificación por escrito de la empresa deberá incluir, teniendo en cuenta el principio de proporcionalidad, al menos la siguiente información:
 - a. una breve descripción de la función o actividad operativa externalizada;
 - 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 en la nube y para la empresa;
 - c. el Derecho aplicable por el que se rige el acuerdo de externalización;
 - d. el nombre del proveedor de servicios en la nube, 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); en el caso de los grupos, si el proveedor de servicios en la nube forma parte del grupo;

- e. el modelo de servicios y 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) donde se almacenarán dichos datos;
- f. un breve resumen de los motivos por los que la función o actividad operativa externalizada se considera **esencial crítica** o importante;
- g. la fecha de última evaluación de ~~la esencialidad o importancia de~~ que la función o actividad operativa externalizada **es crítica o importante**.

Directriz 5 – Requisitos de documentación

23. Como parte de su sistema de gestión de riesgos y gobernanza, la empresa debe llevar un registro de sus acuerdos de externalización en la nube, por ejemplo, en forma de un registro específico que se actualice con el tiempo. La empresa debe asimismo llevar un registro de los acuerdos de externalización en la nube rescindidos durante un período de conservación adecuado sujeto a la normativa nacional.
24. En caso de externalización de funciones o actividades operativas críticas o importantes, la empresa debe registrar toda la información siguiente:
 - a. la información que debe notificarse a la autoridad de supervisión mencionada en la Directriz 4;
 - b. en el caso de los grupos, las empresas de seguros y reaseguros y demás empresas del ámbito de aplicación de la consolidación prudencial que utilizan los servicios en la nube;
 - c. la fecha de la última evaluación de riesgos efectuada y un breve resumen de los principales resultados;
 - d. la persona física o el órgano encargado de la adopción de decisiones (por ejemplo, el OADS) de la empresa que aprobó el acuerdo de externalización en la nube;
 - e. las fechas de las auditorías más recientes y de las próximas auditorías programadas, en su caso;
 - f. los nombres de los subcontratistas a los que se hayan subcontratado partes significativas de una función o actividad operativa **esencial crítica** o importante, incluido el país en el que están registrados los subcontratistas, en el que se prestará el servicio y, si procede, las localizaciones (es decir, países o regiones) en las que se almacenarán los datos;
 - g. el resultado de la evaluación de la sustituibilidad del proveedor de servicios en la nube (por ejemplo, fácil, difícil o imposible);
 - h. si la función o actividad operativa **esencial crítica** o importante externalizada **asiste se refiere** a operaciones de negocio en las que el tiempo es un factor esencial;
 - i. el presupuesto anual estimado;
 - j. si la empresa cuenta con una estrategia de salida en caso de rescisión por cualquiera de las partes o de interrupción de los servicios por parte del proveedor de servicios en la nube.

En caso de externalización de funciones o actividades operativas no ~~críticas~~ o no importantes, la empresa debe definir la información que debe registrarse en función de la naturaleza, el volumen y la complejidad de los riesgos inherentes a los servicios prestados por el proveedor de servicios en la nube.

25. La empresa debe poner a disposición de la autoridad de supervisión, previa petición, toda la información necesaria para que la autoridad de supervisión pueda llevar a cabo la supervisión de la empresa, incluida una copia del acuerdo de externalización.

Directriz 6 – Análisis previo a la externalización

26. Antes de celebrar un acuerdo con un proveedor de servicios en la nube, la empresa deberá:

- a. evaluar si el acuerdo de externalización en la nube afecta a una función o actividad operativa **esencial crítica** o importante de conformidad con la Directriz 7;
- b. identificar y evaluar todos los riesgos pertinentes del acuerdo de externalización en la nube, de conformidad con la Directriz 8;
- c. llevar a cabo las comprobaciones adecuadas de diligencia debida respecto al posible proveedor de servicios en la nube, de conformidad con la Directriz 9;
- d. identificar y evaluar los conflictos de intereses que la empresa podría causar de acuerdo con los requisitos establecidos en el artículo 274, apartado 3, letra b), del Reglamento Delegado.

Directriz 7 – Evaluación de las funciones o actividades operativas críticas o importantes

27. Antes de celebrar un acuerdo de externalización con proveedores de servicios en la nube, la empresa debe evaluar si el acuerdo se refiere a una función o actividad operativa que es **esencial crítica** o importante. Al realizar dicha evaluación, en su caso, la empresa debe tener en cuenta si el acuerdo puede pasar a ser **esencial crítica** o importante en el futuro. La empresa también debe evaluar la esencialidad o importancia de la función o actividad operativa previamente externalizada a los proveedores de servicios en la nube, si la naturaleza, el volumen y la complejidad de los riesgos inherentes al acuerdo cambian significativamente.

28. En la evaluación, la empresa debe tomar en consideración, junto con el resultado de la evaluación de riesgos, al menos los siguientes factores:

- a. el impacto potencial de cualquier interrupción significativa de la función o actividad operativa externalizada o de la incapacidad del proveedor de servicios en la nube para prestar el servicio con los niveles de servicio acordados en:
 - i. el cumplimiento continuo por parte de la empresa de sus obligaciones reglamentarias;
 - ii. la viabilidad y resiliencia financiera y de solvencia a corto y largo plazo de la empresa;
 - iii. la continuidad de sus actividades y su resiliencia operativa;
 - iv. el riesgo operativo de la empresa, incluidos los riesgos de conducta, los riesgos ligados a las tecnologías de la información y la comunicación (TIC) y los riesgos legales;
 - v. los riesgos para la reputación;
- b. el impacto potencial del acuerdo de externalización en la nube en la capacidad de la empresa para:
 - i. identificar, supervisar y gestionar todos los riesgos pertinentes;
 - ii. cumplir todos los requisitos legales y reglamentarios;

- iii. realizar las debidas auditorías en relación con la función o actividad operativa externalizada;
- c. la exposición agregada de la empresa (y/o del grupo, en su caso) al mismo proveedor de servicios en la nube y el potencial impacto acumulado de los acuerdos de externalización en la misma área de negocio;
- d. el volumen y la complejidad de las áreas de negocio de la empresa afectadas por el acuerdo de externalización en la nube;
- e. la capacidad, si fuera necesario o aconsejable, de transferir el acuerdo de externalización en la nube propuesto a otro proveedor de servicios en la nube o reintegrar los servicios («sustituibilidad»);
- f. la protección de los datos de carácter personal y no personal y el eventual impacto en la empresa, los tomadores de seguros u otros aspectos pertinentes de un incumplimiento de confidencialidad o de no garantizar la disponibilidad e integridad de los datos en función *inter alia* del Reglamento (UE) 2016/679⁷. La empresa debe tener en cuenta especialmente los datos que sean secretos comerciales y/o sensibles (por ejemplo, los datos sanitarios de los tomadores de seguros).

Directriz 8 – Evaluación de riesgos de la externalización en la nube

29. En general, la empresa debe adoptar un enfoque coherente con la naturaleza, el volumen y la complejidad de los riesgos inherentes a los servicios externalizados a los proveedores de servicios en la nube. Esto incluye evaluar los posibles efectos de cualquier externalización en la nube, en particular, sobre sus riesgos operativos y de reputación.
30. En caso de externalizar funciones o actividades operativas críticas o importantes a proveedores de servicios en la nube, la empresa debe:
- a. tener en cuenta los beneficios y costes previstos del acuerdo de externalización en la nube propuesto, incluida la ponderación de cualquier riesgo significativo que se pueda atenuar o gestionar mejor frente a cualesquiera riesgos significativos que puedan surgir como resultado del acuerdo de externalización en la nube propuesto;
 - b. evaluar, cuando proceda y sea adecuado, los riesgos, incluidos los riesgos legales, de TIC, de cumplimiento y de reputación, así como las limitaciones de **control, derivados** de:
 - i. el servicio en la nube seleccionado y los modelos de desarrollo propuestos (esto es, públicos/privados/híbridos/comunitarios);
 - ii. la migración y/o aplicación;
 - iii. las actividades y los datos y sistemas relacionados que se está considerando externalizar (o se han externalizado) y su sensibilidad y medidas de seguridad exigidas;
 - iv. la estabilidad política y la situación de seguridad de los países (dentro o fuera de la UE) en los que se prestan o pueden prestarse los servicios externalizados y en los que se almacenen o sea probable que se vayan a almacenar los datos; la evaluación debe tomar en consideración:

⁷Reglamento (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) (DO L 119 de 4.5.2016, p. 1).

1. la legislación en vigor, incluida la legislación en materia de protección de datos;
 2. las disposiciones en vigor para hacer cumplir la ley;
 3. 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 empresa;
- v. la subexternalización, incluidos los riesgos adicionales que pueden surgir si el subcontratista está situado en un tercer país o en un país diferente del país del proveedor de servicios en la nube y el riesgo de que las cadenas de subexternalización largas y complejas reduzcan la capacidad de la empresa para controlar sus funciones o actividades operativas críticas o importantes y la capacidad de las autoridades de supervisión para **supervisarlos supervisarlas** eficazmente;
- vi. el riesgo de concentración general de empresas para el mismo proveedor de servicios en la nube, incluida la externalización a un proveedor de servicios en la nube que no se pueda sustituir fácilmente o varios acuerdos de externalización con el mismo proveedor de servicios en la nube. A la hora de evaluar el riesgo de concentración, la empresa (y/o el grupo, si es el caso) debe tener en cuenta todos sus acuerdos de externalización en la nube con ese proveedor.
31. La evaluación de riesgos debe realizarse antes de llevar a cabo una externalización en la nube. En caso de que la empresa pase a tener conocimiento de deficiencias significativas y/o cambios importantes en los servicios prestados o la situación del proveedor de servicios en la nube, la evaluación de riesgos debe revisarse o volverse a realizar sin demora. En caso de renovación de un acuerdo de externalización en la nube en relación con su contenido y ámbito de aplicación (por ejemplo, ampliación del ámbito de aplicación o inclusión en este de funciones operativas críticas o importantes no incluidas previamente), la evaluación de riesgos debe volver a realizarse.

Directriz 9 – Diligencia debida del proveedor de servicios en la nube

32. En su proceso de evaluación **y selección, la empresa** debe asegurarse de que el proveedor de servicios en la nube sea adecuado de conformidad con los criterios definidos en su política escrita de externalización.
33. La diligencia debida del proveedor de servicios en la nube debe realizarse antes de externalizar cualquier función o actividad operativa. En caso de que la empresa celebre un segundo acuerdo con un proveedor de servicios en la nube que ya haya sido objeto de evaluación, la empresa deberá determinar, siguiendo un enfoque basado en los riesgos, si es necesaria una segunda diligencia debida. En caso de que la empresa pase a tener conocimiento de deficiencias significativas y/o cambios importantes en los servicios prestados o la situación del proveedor de servicios en la nube, la diligencia debida debe revisarse o volverse a realizar sin demora.
34. En caso de externalización en la nube de funciones operativas críticas o importantes, la diligencia debida deberá incluir una evaluación de la adecuación del proveedor de servicios en la nube (por ejemplo, conocimientos, infraestructura, situación financiera, situación corporativa y reglamentaria). Cuando proceda, la empresa podrá utilizar para apoyar la diligencia debida pruebas, certificados basados

en normas internacionales, informes de auditoría de terceros reconocidos o informes de auditoría interna.

Directriz 10 – Requisitos contractuales

35. Los derechos y obligaciones respectivos de la empresa y del proveedor de servicios en la nube deberán asignarse claramente y establecerse en un **acuerdo por escrito**.

36. Sin perjuicio de los requisitos definidos en el artículo 274 del Reglamento Delegado, en caso de externalización de funciones o actividades operativas críticas o importantes a un proveedor de servicios en la nube, el acuerdo por escrito entre este último y la empresa deberá contener:

- a. una descripción clara de la función externalizada que se va a prestar (servicios en la nube, incluido el tipo de servicios de apoyo);
- b. la fecha de inicio y de finalización, si procede, del acuerdo y los plazos de preaviso para el proveedor de servicios en la nube y para la empresa;
- c. la jurisdicción y la legislación por la que se rige el acuerdo;
- d. las obligaciones financieras de las partes;
- e. si la subexternalización de una función o actividad operativa ~~esencial~~ crítica o importante (o partes significativas de las mismas) está permitida y, en caso afirmativo, las condiciones a las que está sujeta la subexternalización significativa (véase la Directriz 13);
- f. la o las localizaciones (es decir, países o regiones) en los que se almacenarán y tratarán los datos pertinentes (ubicación de los centros de datos), y las condiciones que deben cumplirse, incluido el requisito de notificar a la empresa si el proveedor de servicios propone cambiar la o las localizaciones;
- g. las disposiciones relativas a la accesibilidad, disponibilidad, integridad, confidencialidad, privacidad y seguridad de los datos pertinentes, teniendo en cuenta las especificaciones de la Directriz 12;
- h. el derecho de la empresa a supervisar el rendimiento del proveedor de servicios en la nube periódicamente;
- i. los niveles de servicio acordados, que incluirán objetivos de rendimiento cuantitativos y cualitativos precisos 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 notificación del proveedor de servicios en la nube a la empresa, incluidas cuando proceda las obligaciones de remitir los informes pertinentes para la función de seguridad de la empresa y las funciones principales, como los informes de la función de auditoría interna del proveedor de servicios en la nube;
- k. si el proveedor de servicios en la nube debe 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. el requisito de que el proveedor de servicios en la nube conceda a la empresa, sus autoridades de supervisión y cualquier otra persona que nombren aquellas, lo siguiente:

- i. pleno acceso a todas las instalaciones pertinentes (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 en la nube («derechos de acceso»);
 - ii. derechos sin restricciones de inspección y auditoría en relación con el acuerdo de externalización en la nube («derechos de auditoría»), para que puedan realizar un seguimiento del acuerdo de externalización y garantizar el cumplimiento de todos los requisitos reglamentarios y contractuales aplicables;
- n. disposiciones que garanticen que la empresa pueda recuperar inmediatamente los datos de su propiedad en caso de insolvencia, resolución o cese de las operaciones del proveedor de servicios en la nube.

Directriz 11 – Derechos de acceso y auditoría

- 37. El acuerdo de externalización en la nube no debe limitar el ejercicio efectivo por parte de la empresa de los derechos de acceso y auditoría así como de las opciones de control sobre los servicios en la nube con el fin de cumplir sus obligaciones reglamentarias.
- 38. La empresa debe ejercer sus derechos de acceso y auditoría, determinar la frecuencia de las auditorías y las áreas y servicios que se van a auditar siguiendo un enfoque basado en los riesgos, de conformidad con el artículo 8 de las Directrices de la AESPJ sobre el Sistema de Gobernanza.
- 39. A la hora de determinar la frecuencia y el ámbito de aplicación del ejercicio de sus derechos de acceso y auditoría, la empresa debe tener en cuenta si la externalización en la nube está relacionada con una función o actividad operativa **esencial crítica** o importante, la naturaleza y volumen del riesgo y el impacto en la empresa de los acuerdos de externalización en la nube.
- 40. Si el ejercicio de sus derechos de acceso y auditoría o el uso de determinadas técnicas de auditoría plantea un riesgo para el entorno del proveedor de servicios en la nube y/o de otro cliente de este (por ejemplo, el impacto en los niveles de servicio, la disponibilidad de los datos o los aspectos de confidencialidad), la empresa y el proveedor de servicios en la nube deben adoptar de mutuo acuerdo formas alternativas de ofrecer un nivel similar de garantía y servicio a la empresa (por ejemplo, la inclusión de controles específicos para probarse en un informe o certificación específicos elaborados por el proveedor de servicios en la nube).
- 41. Sin perjuicio de su responsabilidad final en relación con las actividades realizadas por sus proveedores de servicios en la nube, con el fin de utilizar los recursos de auditoría de forma más eficaz y reducir la carga organizativa del proveedor de servicios en la nube y sus clientes, las empresas podrán utilizar:
 - a. certificaciones externas e informes de auditoría internos o externos facilitados por el proveedor de servicios en la nube;
 - b. auditorías compartidas (es decir, realizadas conjuntamente con otros clientes del mismo proveedor de servicios en la nube) o auditorías compartidas realizadas por un tercero nombrado por ellos.
- 42. En el caso de la externalización en la nube de funciones o actividades operativas críticas o importantes, las empresas deben utilizar el método indicado en el apartado 42, letra a) únicamente si:

- a. garantizan 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 identificados por la empresa y evalúa el cumplimiento de los requisitos reglamentarios pertinentes;
 - b. evalúan en profundidad el contenido de las nuevas certificaciones o informes de auditoría de manera periódica y verifican que no estén obsoletos;
 - c. garantizan que los sistemas y controles clave se incluyen en futuras versiones de la certificación o el informe de auditoría;
 - d. están satisfechas con la aptitud de la parte certificadora o auditora (por ejemplo, en relación con la rotación de la empresa certificadora o auditora, sus cualificaciones, conocimientos y experiencia, repetición/verificación de las pruebas del expediente de auditoría correspondiente);
 - e. están seguras de que las certificaciones se emiten y las auditorías se llevan a cabo de acuerdo con los estándares adecuados e incluyen una prueba de la eficacia operativa de los principales controles establecidos;
 - f. tienen el derecho contractual de solicitar la extensión del alcance de las certificaciones o los informes de auditoría a otros sistemas y controles pertinentes; el número y la frecuencia de tales solicitudes de modificar el alcance deberán ser razonables y legítimos desde el punto de vista de la gestión de riesgos;
 - g. conservan el derecho contractual a realizar auditorías individuales por su exclusivo criterio con respecto a la externalización en la nube de funciones o actividades operativas críticas o importantes; dicho derecho deberá ejercerse cuando las necesidades específicas no sean posibles a través de otros tipos de interacciones con el proveedor de servicios en la nube.
43. Para la externalización de funciones operativas críticas o importantes a proveedores de servicios en la nube, la empresa debe evaluar si las certificaciones externas e informes a que se refiere el apartado 42, letra a) son adecuados y suficientes para cumplir sus obligaciones reglamentarias y, con un enfoque basado en los riesgos, no deben confiar exclusivamente en estos informes y certificaciones a lo largo del tiempo.
44. Antes de realizar una visita programada presencial, la parte que va a ejercer su derecho de acceso (empresa, auditor o tercero en nombre de la o las empresas) deberá notificarlo previamente con antelación suficiente, a menos que no haya sido posible hacerlo anteriormente por una situación de emergencia o de crisis. Dicha notificación deberá incluir la ubicación y el objeto de la visita así como el personal que participará en la misma.
45. Habida cuenta del alto grado de complejidad técnica de las soluciones en la nube, la empresa 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 las auditorías o evaluaciones pertinentes.

Directriz 12 – Seguridad de los datos y los sistemas

46. La empresa deberá garantizar que los proveedores de servicios en la nube cumplen los reglamentos europeos y nacionales y las normas de seguridad de TIC pertinentes.

47. En caso de externalizar funciones o actividades operativas críticas o importantes a proveedores de servicios en la nube, la empresa deberá además definir requisitos de seguridad de la información específicos en el acuerdo de externalización y supervisar el cumplimiento de los mismos periódicamente.
48. A efectos del apartado 48, en caso de externalización de funciones o actividades operativas críticas o importantes a proveedores de servicios en la nube, la empresa, aplicando un enfoque basado en los riesgos y teniendo en cuenta sus responsabilidades y las del proveedor de servicios en la nube:
- a. acordará funciones y responsabilidades claras entre el proveedor de servicios en la nube y la empresa en relación con las funciones o actividades operativas afectadas por la externalización en la nube, que deberán desglosarse claramente;
 - b. definirá y decidirá sobre el nivel apropiado de protección de los datos confidenciales, la continuidad de las actividades externalizadas, la integridad y la trazabilidad de los datos y sistemas en el contexto de la externalización de servicios en la nube prevista;
 - c. considerará la adopción de medidas específicas cuando sean necesarias para proteger los datos en tránsito, los datos en memoria y los datos en reposo, como, por ejemplo, el uso de tecnologías de cifrado combinadas con una gestión de claves adecuada;
 - d. considerará los mecanismos de integración de los servicios en la nube con los sistemas de la empresa, por ejemplo, las interfaces de programación de aplicaciones (API) y un proceso de gestión de acceso y usuarios adecuado;
 - e. garantizará contractualmente que la disponibilidad y la capacidad prevista del tráfico de red cumplen unos requisitos de continuidad sólidos, cuando proceda y sea viable;
 - f. definirá y decidirá sobre los requisitos de continuidad adecuados a fin de garantizar unos niveles adecuados en cada eslabón de la cadena tecnológica, en su caso;
 - g. dispondrá de un proceso de gestión de incidentes sólido y bien documentado que incluya las respectivas responsabilidades, por ejemplo, definiendo un modelo de colaboración en caso de que se produzcan incidentes reales o eventuales;
 - h. adoptará un enfoque basado en los riesgos para las ubicaciones de almacenamiento y tratamiento de los datos (es decir, país o región) así como consideraciones de seguridad de la información;
 - i. supervisará el cumplimiento de los requisitos relativos a la efectividad y eficacia de los mecanismos de control aplicados por el proveedor de servicios en la nube para mitigar los riesgos relativos a los servicios prestados.

Directriz 13 – Subexternalización de las funciones o actividades operativas - críticas o importantes

49. En caso de que esté permitida la subexternalización de funciones operativas críticas o importantes (o de una parte de estas), el acuerdo de externalización en la nube entre la empresa y el proveedor de servicios en la nube deberá:
- a. especificar cualquier tipo de actividad que esté excluido de la eventual subexternalización;

- b. indicar las condiciones que deben cumplirse en caso de subexternalización (por ejemplo, que el encargado de la subexternalización cumpla también íntegramente las obligaciones pertinentes del proveedor de servicios en la nube). Estas obligaciones incluirán los derechos de auditoría y acceso y la seguridad de los datos y los sistemas;
- c. indicar que el proveedor de servicios en la nube conserva la plena responsabilidad y control de los servicios sujetos a subexternalización;
- d. incluir la obligación para el proveedor de servicios en la nube de informar a la empresa de cualquier cambio importante previsto en relación con los subcontratistas o con los servicios subcontratados que pueda afectar a la capacidad del proveedor de servicios para cumplir sus obligaciones de conformidad con el acuerdo de externalización. El período de notificación de dichos cambios deberá permitir que la empresa realice, como mínimo, una evaluación de riesgos de los efectos de los cambios propuestos antes de que se produzca efectivamente el cambio de los encargados de la subexternalización o de los servicios objeto de esta;
- e. garantizar, en caso de que el proveedor de servicios en la nube **planee cambios en** un encargado de subexternalización o en los servicios objeto de estos cambios cuyo efecto en la evaluación de riesgos de los servicios acordados sea negativo, que la empresa tenga derecho a rescindir y desistir del contrato.

Directriz 14 – Supervisión y control de los acuerdos de externalización en la nube

- 50. La empresa controlará de forma periódica el rendimiento de las actividades, las medidas de seguridad y el cumplimiento del nivel de servicio acordado por sus proveedores de servicios en la nube siguiendo un enfoque basado en los riesgos. El principal objetivo será la externalización en la nube de funciones operativas críticas e importantes.
- 51. Para ello, la empresa establecerá mecanismos de supervisión y control que deberán tener en cuenta, cuando proceda y sea viable, la existencia de subexternalización de funciones operativas críticas o importantes o de una parte de las mismas.
- 52. Se informará periódicamente al OADS sobre los riesgos identificados en la externalización en la nube de funciones o actividades operativas críticas o importantes.
- 53. Con el fin de garantizar la supervisión y el control adecuados de sus acuerdos de externalización en la nube, las empresas utilizarán recursos suficientes que cuenten con las habilidades y conocimientos necesarios para supervisar los servicios externalizados en la nube. El personal de la empresa a cargo de estas actividades deberá contar con los conocimientos comerciales y de TIC necesarios.

Directriz 15 – Derechos de rescisión y estrategias de salida

- 54. En caso de externalización en la nube de funciones o actividades operativas críticas o importantes, en el marco del acuerdo de externalización en la nube la empresa deberá contar con una cláusula sobre la estrategia de salida claramente definida que garantice que es capaz de rescindir el acuerdo cuando sea necesario. La rescisión deberá ser posible sin detrimento de la continuidad y la calidad de su prestación de servicios a los tomadores de seguros. Para lograrlo, la empresa:

- a. desarrollará planes de salida exhaustivos, basados en los servicios, documentados y suficientemente probados (por ejemplo, realizando un análisis de los posibles costes, impactos, recursos e implicaciones temporales de las distintas opciones de salida eventual);
- b. identificará soluciones alternativas y desarrollará planes de transición adecuados y viables para que la empresa pueda eliminar y transferir las actividades y los datos existentes del proveedor de servicios en la nube a proveedores de servicios alternativos o de nuevo a la empresa. Estas soluciones se definirán teniendo en cuenta las dificultades que puedan surgir debido a la ubicación de los datos, y se adoptarán las medidas necesarias para garantizar la continuidad del negocio durante la fase de transición;
- c. garantizará que el proveedor de servicios en la nube apoye adecuadamente a la empresa cuando transfiera los datos, sistemas o aplicaciones externalizados a otro proveedor de servicios o directamente a la empresa;
- d. acordará con el proveedor de servicios en la nube que una vez transferidos de nuevo a la empresa, el proveedor eliminará los datos de forma íntegra y segura en todas las regiones.

55. A la hora de desarrollar las estrategias de salida, la empresa debe considerar lo siguiente:

- a. definir los objetivos de la estrategia de salida;
- b. definir los eventos desencadenantes (por ejemplo, indicadores de riesgo clave que indiquen un nivel de servicio inaceptable) que pueden activar la estrategia de salida;
- c. realizar un análisis de impacto en el negocio que sea proporcional a las actividades externalizadas para identificar los recursos humanos y de otro tipo que serían necesarios para implementar el plan de salida, así como el tiempo necesario para dicha implementación;
- d. asignar funciones y responsabilidades para gestionar los planes de salida y las actividades de transición;
- e. definir los criterios de éxito de la transición.

Directriz 16 – Supervisión de los acuerdos de externalización en la nube por las autoridades de supervisión

56. Las autoridades de supervisión llevarán a cabo el análisis de los impactos derivados de los acuerdos de externalización en la nube de las empresas como parte de su proceso de revisión y supervisión. El análisis de los impactos se centrará, en particular, en los acuerdos relativos a la externalización de funciones o actividades operativas críticas o importantes.

57. Las autoridades de supervisión tendrán en cuenta los siguientes riesgos en la supervisión de los acuerdos de externalización en la nube de las empresas:

- a. riesgos de TIC;
- b. otros riesgos operativos (incluidos los riesgos legales y de cumplimiento, externalización y de gestión de terceros);
- c. riesgo de reputación;
- d. riesgo de concentración, a nivel de país y sectorial.

58. En su evaluación, las autoridades de supervisión incluirán los siguientes aspectos en un enfoque basado en los riesgos:

- a. adecuación y efectividad de los procesos operativos y de gobernanza de la empresa relativos a la aprobación, aplicación, supervisión, gestión y renovación de los acuerdos de externalización en la nube;
 - b. si la empresa cuenta con los recursos suficientes que tengan las habilidades y conocimientos adecuados para supervisar los servicios externalizados en la nube;
 - c. si la empresa identifica y gestiona todos los riesgos indicados en las presentes Directrices.
59. En el caso de los grupos, el supervisor del grupo se asegurará de que el impacto de la externalización en la nube de las funciones o actividades operativas o importantes se refleje en la gestión de riesgos de supervisión del grupo, teniendo en cuenta los requisitos enumerados en los apartados 58 y 59 y las características operativas y de gobernanza individuales del grupo.
60. Cuando la externalización en la nube de funciones o actividades operativas críticas o importantes implique a más de una empresa en diferentes Estados miembros y esté gestionada centralmente por la entidad matriz o por una filial del grupo (por ejemplo, una entidad o una empresa de servicios del grupo como el proveedor de TIC del grupo), el supervisor del grupo y/o las autoridades de supervisión pertinentes de las empresas implicadas en la externalización en la nube debatirán, cuando proceda, el impacto de esta en el perfil de riesgo del grupo en el Colegio de Supervisores.
61. Cuando se detecten aspectos preocupantes que lleven a la conclusión de que una empresa ya no dispone de acuerdos de gobernanza sólidos o no cumple los requisitos reglamentarios, las autoridades de supervisión adoptarán las medidas oportunas, que podrán incluir, por ejemplo, exigir a la empresa que mejore el acuerdo de gobernanza, limitando o restringiendo el alcance de las funciones externalizadas o exigiendo la salida de uno o más acuerdos de externalización. En particular, habida cuenta de la necesidad de que la empresa opere de forma continuada, podría ser necesario cancelar los contratos si no se pueden garantizar la supervisión y el cumplimiento de los requisitos reglamentarios por otros medios.

Normas sobre el cumplimiento y el deber de información

62. El presente documento contiene las Directrices emitidas en virtud del artículo 16 del Reglamento (UE) n.º 1094/2010. En virtud de lo dispuesto en el apartado 3 de dicho artículo, las autoridades competentes y las entidades financieras harán todo lo posible para atenerse a las directrices y recomendaciones.
63. Las autoridades competentes que cumplan o tengan la intención de cumplir estas Directrices deberán incorporarlas debidamente a su marco regulador o supervisor.
64. Las autoridades competentes deberán confirmar a la AESPJ si cumplen o tienen la intención de cumplir estas Directrices, junto con los motivos de incumplimiento, en el plazo de dos meses tras la publicación de las versiones traducidas.
65. A falta de respuesta antes del plazo señalado, se considerará que las autoridades competentes no cumplen y se informará sobre ellas en consecuencia.

Disposición final sobre revisiones

66. Las presentes Directrices serán objeto de una revisión por parte de la AESPJ.