30/09/2025
ESMA65-294529287-4737

Directrices

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

Tabla de Contenidos

1 Ámbito de aplicación

¿Quién?

1. Las presentes directrices se aplican a las autoridades competentes y a i) los depositarios de fondos de inversión alternativos (FIA) a que se refieren el artículo 21, apartado 3, letra c) y el artículo 21, apartado 3, párrafo tercero, de la Directiva GFIA, cuando no sean entidades financieras a las que se aplique DORA, y ii) los depositarios de OICVM a que se refiere el artículo 23, apartado 2, letra c), de la Directiva OICVM, cuando no sean entidades financieras a las que se aplique DORA.[1]

¿Qué?

2. Las presentes directrices se aplican en relación con las siguientes disposiciones:

a) Con referencia a los depositarios de FIA: el artículo 21 de la Directiva GFIA; el artículo 98 del Reglamento Delegado (UE) 2013/231 de la Comisión;

b) Con referencia a los depositarios de OICVM: los artículos 22, 22 bis y 23, apartado 2, de la Directiva OICVM; el artículo 32 de la Directiva 2010/43/UE de la Comisión; el artículo 2, apartado 2, letra j), el artículo 3, apartado 1, el artículo 13, apartado 2 y los artículos 15, 16 y 22 del Reglamento Delegado (UE) 2016/438 de la Comisión.

¿Cuándo?

3. Las presentes directrices se aplicarán a partir de la fecha de su publicación en el sitio web de la AEVM en todas las lenguas oficiales de la UE y a todos los acuerdos de externalización en la nube celebrados, renovados o modificados a partir de esa fecha.

4. A la luz de la aplicación de DORA, las anteriores Directrices de la AEVM sobre la externalización a proveedores de servicios en la nube dejan de aplicarse a las entidades financieras sujetas a DORA a que se refiere el artículo 2 del mismo Reglamento. En el caso de los depositarios de FIA y de los depositarios de OICVM a que se refiere el apartado 1, las anteriores Directrices de la AEVM sobre la externalización a proveedores de servicios en la nube seguirán aplicándose hasta la fecha de publicación de las presentes Directrices en el sitio web de la AEVM en todas las lenguas oficiales de la UE.

[1] Con referencia a los acuerdos de externalización en la nube, las entidades financieras definidas en el artículo 2, apartados 1 y 2 del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011 (Reglamento DORA), están sujetas a las normas específicas establecidas en el Reglamento DORA y en los Reglamentos Delegados e de Ejecución de la Comisión.

2 Referencias legislativas, abreviaturas y definiciones

2.1 Referencias legislativas

Reglamento ESMA	Reglamento (UE) n.º 1095/2010 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 Valores y Mercados), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/77/CE de la Comisión[2]
Directiva GFIA	Directiva 2011/61/UE del Parlamento Europeo y del Consejo, de 8 de junio de 2011, relativa a los gestores de fondos de inversión alternativos y por la que se modifican las Directivas 2003/41/CE y 2009/65/CE y los Reglamentos (CE) n.º 1060/2009 y (UE) n.º 1095/2010[3]
Reglamento Delegado (UE) n.º 2013/231 de la Comisión	Reglamento Delegado (UE) n.º 2013/231 de la Comisión, de 19 de diciembre de 2012, por el que se complementa la Directiva 2011/61/CE del Parlamento Europeo y del Consejo en lo referente a las exenciones, las condiciones generales de ejercicio de la actividad, los depositarios, el apalancamiento, la transparencia y la supervisión[4]
Directiva OICVM	Directiva 2009/65/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, sobre la coordinación de las disposiciones legales, reglamentarias y administrativas sobre determinados organismos de inversión colectiva en valores mobiliarios (OICVM)[5]
Directiva 2010/43/UE de la Comisión	Directiva 2010/43/UE de la Comisión, de 1 de julio de 2010, por la que se establecen disposiciones de aplicación de la Directiva 2009/65/CE del Parlamento Europeo y del Consejo en lo que atañe a los requisitos de organización, los conflictos de intereses, la conducta empresarial, la gestión de riesgos y el contenido de los acuerdos celebrados entre depositarios y sociedades de gestión[6]

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

DORA	Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014, (UE) n.o 909/2014 y (UE) 2016/1011[7]
RGPD	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[8]

2.2 Abreviaturas

CSP	Proveedor de servicios en la nube
ESMA	Autoridad Europea de Valores y Mercados
UE	Unión Europea

2.3 Definiciones

función	cualesquiera procesos, servicios o actividades;
Función esencial o importante	cualquier función cuyo defecto o fallo en su ejecución afectaría considerablemente: a) al cumplimiento por parte de una empresa de las obligaciones que le incumben en virtud de la legislación aplicable; b) a los resultados financieros de una empresa; o c) a la solidez o la continuidad de los principales servicios y actividades de una empresa;
servicios en la nube	servicios prestados mediante informática en la nube;

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

informática en la nube o nube[9]	paradigma para permitir el acceso de la red a un conjunto escalable y elástico de recursos físicos o virtuales compartidos (por ejemplo, servidores, sistemas operativos, redes, programas informáticos, aplicaciones y equipos de almacenamiento) con suministro de autoservicio y administración a la carta;
proveedor de servicios en la nube	tercero que presta servicios en la nube de un acuerdo de externalización en la nube;
acuerdo de externalización en la nube	acuerdo de cualquier forma, incluidos los acuerdos de delegación, entre: (i) una empresa y un CSP por los que dicho CSP desempeñe una función que, de otro modo, sería asumida por la propia empresa; o (ii) una empresa y un CSP que no es un CSP, pero que depende significativamente de un CSP para desempeñar una función que, de otro modo, sería asumida por la propia empresa. En este caso, debe entenderse que una referencia a un «CSP» en las presentes directrices se refiere a dicho tercero.
subcontratación	situación en la que el CSP transfiere la función externalizada (o una parte de esa función) a otro proveedor de servicios en virtud de un acuerdo de externalización;
modelo de despliegue en la nube	la forma en que la nube puede organizarse sobre la base del control y la puesta en común de recursos físicos o virtuales. Los modelos de despliegue en la nube incluyen nubes comunitarias[10], híbridas[11], privadas[12] y públicas[13];

[9] La informática en la nube a menudo se abrevia como «nube». El término «nube» se utiliza en el resto del documento para facilitar la consulta.
[10] Un modelo de despliegue en la nube en el que los servicios en nube apoyen exclusivamente y sean compartidos por una colección específica de clientes de servicios en nube que tengan necesidades compartidas y una relación entre ellos, y en la que los recursos estén controlados por al menos un miembro de esta colección;
[11] Un modelo de despliegue en la nube que utiliza al menos dos modelos de despliegue en la nube distintos
[12] Un modelo de despliegue en la nube en el que los servicios en la nube son utilizados exclusivamente por un único cliente y los recursos están controlados por dicho cliente
[13] Un modelo de despliegue en la nube en el que los servicios en la nube estén potencialmente disponibles para cualquier cliente de servicios en la nube y que los recursos sean controlados por el proveedor de servicios en la nube

empresas	a) los depositarios a que se refieren el artículo 21, apartado 3, letra c), y el artículo 21, apartado 3, párrafo tercero, de la Directiva GFIA («depósitos de fondos de inversión alternativos (FIA)»); b) los depositarios a que se refiere el artículo 23, apartado 2, letra c), de la Directiva OICVM («depósitos de OICVM»).

3 Objeto

5. Las presentes directrices están basadas en el artículo 16, apartado 1, del Reglamento de la ESMA. Los objetivos de estas directrices son establecer prácticas de supervisión coherentes, eficaces y eficientes dentro del Sistema Europeo de Supervisión Financiera (SESF) y garantizar una aplicación común, uniforme y coherente de la aplicación de los requisitos mencionados en la sección 1.1 en el título «¿Qué?», cuando las empresas externalizan los CSP. En particular, estas directrices tienen por objeto ayudar a las empresas y a las autoridades competentes a identificar, abordar y supervisar los riesgos y retos derivados de los acuerdos de externalización en la nube, desde la toma de decisiones de externalización, la selección de un proveedor de servicios en la nube, el seguimiento de las actividades externalizadas y la elaboración de estrategias de salida.

4 Obligaciones de cumplimiento y de información

4.1 Categoría de las directrices

5. Con arreglo al artículo 16, apartado 3, del Reglamento de la ESMA, las autoridades competentes y las empresas harán todo lo posible por atenerse a las directrices.

6. Las autoridades competentes sujetas a la aplicación de las presentes directrices deberán darles cumplimiento mediante su incorporación a sus marcos jurídicos o de supervisión nacionales según corresponda, incluso en aquellos casos en los que determinadas directrices estén dirigidas fundamentalmente a las empresas. En tales casos, las autoridades competentes deberán garantizar mediante su supervisión que las empresas cumplan con las directrices.

4.2 Requisitos de información

7. En el plazo de dos meses a partir de la fecha de publicación de las directrices en todas las lenguas oficiales de la UE en el sitio web de la ESMA, las autoridades competentes sujetas a la aplicación de las presentes directrices deberán notificar a la ESMA si i)

cumplen, ii) no cumplen, pero tienen intención de cumplir, o iii) no cumplen y no tienen intención de cumplir las directrices.

8. En caso de incumplimiento, las autoridades competentes también deberán notificar a la ESMA, en un plazo de dos meses a partir de la fecha de publicación de las directrices en el sitio web de la ESMA en todas las lenguas oficiales de la UE, las razones por las que no cumplen las directrices. En el sitio web de la ESMA se encuentra disponible un modelo para estas notificaciones. Una vez cumplimentado el modelo, se transmitirá a la ESMA.

9. Las empresas no están obligadas a informar de si cumplen o no con lo dispuesto en las presentes directrices.

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

Directriz 1. Gobernanza, supervisión y documentación

10. Una empresa debe contar con una estrategia definida y actualizada de externalización en la nube que sea coherente con las estrategias pertinentes y las políticas y procesos internos de la empresa en relación con las tecnologías de la información y de las comunicaciones, la seguridad de la información y la gestión del riesgo operativo.

11. Una empresa debe:

    a) asignar claramente las responsabilidades relativas a la documentación, gestión y control de los acuerdos de externalización dentro de su organización;
    b) asignar recursos suficientes para garantizar el cumplimiento de las presentes directrices y de todos los requisitos legales aplicables a sus acuerdos de externalización en la nube;
    c) establecer una función de supervisión de la externalización en la nube o designar altos cargos que sean directamente responsables ante el órgano de dirección y responsables de gestionar y supervisar los riesgos de los acuerdos de externalización en la nube. Al cumplir esta directriz, las empresas deben tener en cuenta la naturaleza, relevancia y complejidad de su actividad, también en términos de riesgo para el sistema financiero, y los riesgos inherentes a las funciones externalizadas, y asegurarse de que su órgano de administración posee las competencias técnicas pertinentes para comprender los riesgos que entrañan los acuerdos de externalización en la nube. Las empresas pequeñas y menos complejas deben garantizar al menos una división clara de tareas y responsabilidades para la gestión y supervisión de los acuerdos de externalización en la nube.

12. Una empresa debe supervisar la realización de las actividades, las medidas de seguridad y el cumplimiento de los niveles de servicio acordados por sus CSP. Este seguimiento debe basarse en el riesgo, centrándose principalmente en las funciones esenciales o importantes que se hayan externalizado.

13. Una empresa debe volver a evaluar periódicamente si sus acuerdos de externalización en la nube se refieren a una función esencial o importante y siempre que el riesgo, la naturaleza o la relevancia de una función externalizada se haya modificado de manera fundamental.

14. Las empresas deben mantener un registro actualizado de información sobre todos sus acuerdos de externalización en la nube, distinguiendo entre la externalización de funciones esenciales o importantes y otros acuerdos de externalización. Al distinguir entre la externalización de funciones esenciales o importantes y otros acuerdos de externalización, debe proporcionarse un breve resumen de las razones por las que la función externalizada se considera o no esencial o importante. Teniendo en cuenta la legislación nacional, una empresa también debe mantener durante un período adecuado un registro de los acuerdos de externalización en la nube terminados.

15. Para los acuerdos de externalización en la nube relativos a funciones esenciales o importantes, el registro debe incluir, como mínimo, la siguiente información para cada acuerdo de externalización en la nube:

    a) un número de referencia;
    b) la fecha de inicio y, en su caso, la próxima fecha de renovación del contrato, la fecha de finalización y/o los plazos de preaviso para el CSP y para la empresa;
    c) una breve descripción de la función externalizada, incluidos los datos que se externalicen y si estos datos incluyen datos personales (por ejemplo, facilitando un «sí» o un «no» en un campo de datos separado);
    d) una categoría asignada por la empresa que refleje la naturaleza de la función externalizada (por ejemplo, función de tecnología de la información o función de control), que debe facilitar la identificación de los diferentes tipos de acuerdos de externalización en la nube;
    e) si la función externalizada presta apoyo a operaciones de negocio en las que el tiempo es un factor crítico;
    f) el nombre y la marca (en su caso) del CSP, su país de registro, su número de registro, su 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);
    g) la legislación aplicable al acuerdo de externalización en la nube y, en su caso, la elección de la jurisdicción;
    h) el tipo de servicios en nube y modelos de despliegue y la naturaleza específica de los datos que deben conservarse y los lugares (es decir, regiones o países) en los que pueden almacenarse dichos datos;

i) la fecha de última evaluación de la esencialidad o importancia de la función externalizada y la fecha de la próxima evaluación prevista;
j) la fecha de la evaluación de riesgos o auditoría más reciente del CSP, junto con un breve resumen de los principales resultados, y la fecha de la próxima evaluación de riesgos/auditoría prevista;
k) la persona física o el órgano responsable de la decisión de aprobar el acuerdo de externalización en la nube;
l) en su caso, los nombres de los subcontratistas a los que se subcontrate una función esencial o importante (o partes importantes de la misma), incluidos los países en los que están registrados los subcontratistas, en los que se prestará el servicio subcontratado, y los lugares (es decir, regiones o países) en los que se almacenarán los datos;
m) el presupuesto anual estimado del acuerdo de externalización en la nube.

16. Para los acuerdos de externalización en la nube relativos a funciones no esenciales o no importantes, la empresa debe definir la información que debe incluirse en el registro en función de la naturaleza, escala y complejidad de los riesgos inherentes a la función externalizada.

Directriz 2. Análisis previo a la externalización y diligencia debida

17. Antes de celebrar cualquier acuerdo de externalización en la nube, la empresa deberá:

a) evaluar si el acuerdo de externalización en la nube se refiere a una función esencial o importante;
b) identificar y evaluar todos los riesgos pertinentes del acuerdo de externalización en la nube;
c) realizar las comprobaciones adecuadas de diligencia debida sobre el CSP seleccionado;
d) identificar y evaluar cualquier conflicto de intereses que pueda causar la externalización.

18. El análisis previo a la externalización y las comprobaciones adecuadas de diligencia debida sobre el CSP seleccionado deben ser proporcionales a la naturaleza, consideración y complejidad de la función que la empresa se proponga externalizar y a los riesgos inherentes a esta función. Debe incluir, como mínimo, una evaluación del impacto potencial en los riesgos operativos, jurídicos, de cumplimiento y de reputación de la empresa del acuerdo de externalización en la nube. en

19. En caso de que el acuerdo de externalización en la nube se refiera a funciones esenciales o importantes, la empresa también deberá:

a) evaluar todos los riesgos pertinentes que puedan surgir como consecuencia del acuerdo de externalización en la nube, incluidos los riesgos relacionados con la

tecnología de la información y la comunicación, la seguridad de la información, la continuidad de la actividad, los riesgos jurídicos y de cumplimiento, los riesgos de reputación, los riesgos operativos y las posibles limitaciones de supervisión para la empresa, derivados de:

i. el servicio en la nube seleccionado y los modelos de despliegue propuestos;
ii. la migración y/o los procesos de implementación;
iii. la criticidad de la función y los datos relacionados que están siendo objeto de externalización y las medidas de seguridad que deberían adoptarse;
iv. la interoperabilidad de los sistemas y aplicaciones de la empresa y del CSP, en particular su capacidad para intercambiar información y utilizar mutuamente la información intercambiada;
v. la portabilidad de los datos de la empresa, es decir, la capacidad de transferir fácilmente los datos de la empresa de un CSP a otro o de vuelta a ella;
vi. la estabilidad política, la situación en materia de seguridad y el sistema jurídico (incluidas las disposiciones de aplicación de la ley vigentes, las disposiciones de la legislación en materia de insolvencia que se aplicarían en caso de quiebra del CSP, la legislación sobre protección de datos en vigor y si se cumplen las condiciones para la transferencia de datos personales a un tercer país en virtud del RGPD) de los países (dentro o fuera de la UE) en los que se facilitarían las funciones externalizadas y en los que se almacenarían los datos externalizados; en caso de subcontratación, los riesgos adicionales que puedan surgir si el subcontratista está situado en un tercer país o un país distinto del CSP y, en el caso de una cadena de subcontratación, cualquier riesgo adicional que pueda surgir, en particular en relación con la ausencia de un contrato directo entre la empresa y el subcontratista que desempeñe la función externalizada;
vii. posible concentración dentro de la empresa (incluido, en su caso, a nivel de grupo) causada por múltiples acuerdos de externalización en la nube con el mismo CSP, así como una posible concentración dentro del sector financiero de la UE, causada por múltiples empresas que utilizan el mismo CSP o un pequeño grupo de CSP. Al evaluar el riesgo de concentración, la empresa debe tener en cuenta todos sus acuerdos de externalización en la nube (y, en su caso, los acuerdos de externalización en la nube a nivel de su grupo) con dicho CSP;

b) tener en cuenta los beneficios y costes previstos del acuerdo de externalización en la nube, 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.

20. En caso de externalización de funciones esenciales o importantes, las comprobaciones adecuadas de diligencia debida debe incluir una evaluación de la idoneidad del CSP. Al evaluar la idoneidad del CSP, la empresa debería velar por que el proveedor tenga la reputación empresarial, las capacidades, los recursos (incluidos humanos, informáticos y financieros), la estructura organizativa y, en su caso, las autorizaciones o registros pertinentes para desempeñar la función esencial o importante de manera fiable y profesional y cumplir sus obligaciones durante el período de vigencia del acuerdo de externalización en la nube. Entre otros factores que han de considerarse en las comprobaciones adecuadas de diligencia debida respecto de un CSP se incluyen, a título ilustrativo:

    a) la gestión de la seguridad de la información y, en particular, la protección de datos personales, confidenciales y otros datos sensibles;
    b) el soporte de servicio, incluidos los planes y contactos de soporte, y los procesos de gestión de incidentes;
    c) la continuidad de la actividad y los planes de recuperación en caso de catástrofe;

21. Cuando proceda, y con el fin de apoyar las comprobaciones adecuadas de diligencia debida, las empresas también podrán utilizar certificaciones basadas en normas internacionales e informes de auditoría externa o interna.

22. Si la empresa tiene conocimiento de deficiencias significativas y/o cambios importantes en los servicios prestados o la situación del CSP, deberá revisarse o volverse a realizar sin demora. el análisis previo a la externalización y la diligencia debida del proveedor.

23. En caso de que la empresa celebre un nuevo acuerdo o renueve un acuerdo existente con un CSP que ya haya sido objeto de evaluación, la empresa deberá determinar, siguiendo un enfoque basado en los riesgos, si es necesaria una segunda realización de comprobaciones adecuadas de diligencia debida.

Directriz 3. Elementos contractuales clave

24. Los derechos y obligaciones respectivos de la empresa y de su CSP deberán establecerse claramente en un acuerdo escrito.

25. El acuerdo escrito debe permitir expresamente a la empresa rescindir el acuerdo, en caso necesario.

26. En caso de externalización de funciones esenciales o importantes, el acuerdo escrito deberá incluir, como mínimo:

    a) una descripción clara de la función externalizada;

b) la fecha de inicio y de finalización, si procede, del acuerdo y los plazos de preaviso para el CSP y para la empresa;

c) la legislación aplicable al acuerdo y, en su caso, la elección de la jurisdicción;

d) las obligaciones financieras de la empresa y del CSP;

e) si se permite la subcontratación y, en caso afirmativo, en qué condiciones, teniendo en cuenta la Directriz 7;

f) la localización o las localizaciones (es decir, países o regiones) en la que prestará la función externalizada y en las que se tratarán y almacenarán los datos, así como las condiciones que deben cumplirse, incluido el requisito de notificar a la empresa si el CSP propone cambiar la localización o las localizaciones;

g) las disposiciones relativas a la seguridad de la información y la protección de los datos personales, teniendo en cuenta la Directriz 4;

h) el derecho de la empresa a supervisar periódicamente la actuación del CSP en el marco del acuerdo de externalización en la nube, teniendo en cuenta la Directriz 6;

i) los niveles de servicio acordados, que incluirán objetivos de rendimiento cuantitativos y cualitativos 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 CSP a la empresa y, cuando proceda, las obligaciones de remitir los informes pertinentes para la función de seguridad de la empresa y las funciones principales, como los informes elaborados por la función de auditoría interna del CSP;

k) disposiciones relativas a la gestión de incidentes por parte del CSP, incluida la obligación del proveedor de informar a la empresa sin demora indebida de los incidentes que hayan afectado al funcionamiento del servicio contratado por la empresa;

l) si el CSP deberá suscribir un seguro obligatorio frente a determinados riesgos y, si procede, el nivel de cobertura requerido del mismo;

m) los requisitos para que el CSP aplique y ponga a prueba los planes de continuidad de las actividades y los planes de recuperación en caso de catástrofe;

n) el requisito de que el CSP conceda a la empresa, a sus autoridades competentes y a cualquier otra persona designada por la empresa o las autoridades competentes el derecho de acceso («derechos de acceso») e inspección («derechos de auditoría») a la información, los locales, los sistemas y los dispositivos pertinentes del CSP en la medida necesaria para supervisar la actuación del CSP en el marco del acuerdo de externalización en la nube y su

conformidad con los requisitos reglamentarios y contractuales aplicables, teniendo en cuenta la Directriz 6;

o) disposiciones para garantizar que se pueda acceder a los datos, que el CSP trata o almacena en nombre en la empresa, recuperarlos o devolverlos a la empresa, según sea necesario, teniendo en cuenta la Directriz 5.

Directriz 4. Seguridad de la información

27. Una empresa debe establecer requisitos de seguridad de la información en sus políticas y procedimientos internos y en el acuerdo escrito de externalización en la nube, y supervisar el cumplimiento de estos requisitos de forma permanente, en particular para proteger los datos confidenciales, personales u otros datos. Dichos requisitos deben ser proporcionales a la naturaleza, relevancia y complejidad de la función que la empresa se proponga externalizar al CSP y a los riesgos inherentes a esta función.

28. A tal fin, en caso de externalización de funciones esenciales o importantes, y sin perjuicio de los requisitos aplicables en virtud del RGPD, una empresa, aplicando un enfoque basado en el riesgo, debe, como mínimo:

a) *organización de la seguridad de la información:* garantizar que exista una asignación clara de funciones y responsabilidades en materia de seguridad de la información entre la empresa y el CSP respecto de la detección de amenazas, la gestión de incidentes y la gestión de soluciones, y garantizar que el CSP sea efectivamente capaz de cumplir sus funciones y responsabilidades;
b) *gestión de la identidad y el acceso*: garantizar que existen mecanismos sólidos de autenticación (por ejemplo, autenticación multifactor) y controles de acceso con el fin de evitar el acceso no autorizado a los datos de la empresa y a los recursos en la nube;
c) *cifrado y gestión de claves:* garantizar que se utilizan las tecnologías de cifrado pertinentes, cuando sea necesario, para los datos en tránsito, los datos en memoria, los datos en reposo y las copias de seguridad de los datos, en combinación con soluciones de gestión de claves adecuadas para limitar el riesgo de acceso no autorizado a las claves de cifrado; en particular, la empresa debe tener en cuenta la tecnología y los procesos más avanzados a la hora de seleccionar su solución de gestión de claves;
d) *seguridad de las operaciones y de la red:* considerar niveles apropiados de disponibilidad de la red, segregación de la red (por ejemplo, aislamiento del usuario en el entorno compartido de la nube, separación operativa en lo que respecta a la web, lógica de las aplicaciones, sistema operativo, red, Sistema de Gestión de Bases de Datos (SGBD) y capas de almacenamiento) y entornos de procesamiento (por ejemplo, pruebas de aceptación del usuario, d desarrollo o de producción)

e) *interfaz de programación de aplicaciones (API):* considerar mecanismos para la integración de los servicios en la nube en los sistemas de la empresa a fin de garantizar la seguridad de las API (por ejemplo, establecer y mantener políticas y procedimientos de seguridad de la información para las API en múltiples interfaces de sistema, jurisdicciones y funciones empresariales para impedir la divulgación, la modificación o la destrucción de datos no autorizadas);
f) *continuidad de la actividad y recuperación en caso de catástrofe*: garantizar la existencia de controles eficaces de la continuidad de la actividad y de la recuperación en caso de catástrofe (por ejemplo, estableciendo requisitos mínimos de capacidad, seleccionando opciones de alojamiento geográficamente dispersas, con capacidad de cambiar de uno a otro, o solicitando y revisando la documentación que muestre las rutas seguidas por los datos de la empresa entre los sistemas del CSP, así como considerando la posibilidad de replicar imágenes de máquinas en una ubicación de almacenamiento independiente, suficientemente aislada o desconectada);
g) *localización de datos*: adoptar un enfoque basado en los riesgos para las localizaciones del almacenamiento y el tratamiento de datos (a saber, regiones o países);
h) *cumplimiento y supervisión*: verificar que el CSP cumple las normas de seguridad de los sistemas de información reconocidas internacionalmente y ha aplicado controles de seguridad de la información adecuados (por ejemplo, pidiendo que el CSP aporte pruebas de que lleva a cabo revisiones pertinentes de seguridad de la información y mediante la realización de evaluaciones y pruebas periódicas de las medidas de seguridad de la información del CSP).

Directriz 5. Estrategias de salida

29. En caso de externalización de funciones esenciales o importantes, una empresa debe asegurarse de poder salir del acuerdo de subcontratación en la nube sin perturbar indebidamente sus actividades comerciales ni los servicios que presta a sus clientes, y sin que ello vaya en detrimento del cumplimiento de las obligaciones que le incumben en virtud de la legislación aplicable, así como de la confidencialidad, integridad y disponibilidad de sus datos. Para tal fin, una empresa debe:

a) desarrollar planes de salida que sean completos, estén documentados y estén suficientemente probados. Estos planes deben actualizarse cuando sea necesario, como en el caso de cambios en la función externalizada;
b) identificar soluciones alternativas y desarrollar planes de transición para eliminar la función y los datos externalizados del CSP y, en su caso, de cualquier subcontratista, y transferirlos al CSP alternativo indicado por la empresa o directamente a la empresa. Estas soluciones se definirán teniendo en cuenta las dificultades que puedan surgir debido a la localización de los datos, y se adoptarán

las medidas necesarias para garantizar la continuidad del negocio durante la fase de transición;

c) garantizar que el acuerdo escrito de externalización en la nube incluya la obligación de que el CSP apoye la transferencia ordenada de la función externalizada, y el correspondiente tratamiento de datos, del CSP, y de cualquier subcontratista a otro CSP indicado por la empresa o directamente a la empresa en caso de que la empresa active la estrategia de salida. La obligación de permitir la transferencia ordenada de la función externalizada y el tratamiento relacionado de los datos debe incluir, cuando proceda, la eliminación segura de los datos de los sistemas del CSP y de cualquier subcontratista.

30. Al elaborar los planes y soluciones de salida a que se refieren las letras a) y b) («estrategia de salida»), la empresa deberá tener en cuenta lo siguiente:

a) definir los objetivos de la estrategia de salida;
b) definir los eventos desencadenantes que podrían activar la estrategia de salida. Estos deben incluir al menos la terminación del acuerdo de externalización en la nube por iniciativa de la empresa o del CSP y el fallo o cualquier otra interrupción grave de la actividad comercial del CSP;
c) realizar un análisis de impacto en el negocio que sea adecuado a la función externalizada para identificar los recursos humanos y de otro tipo que serían necesarios para implementar el plan de salida;
d) asignar funciones y responsabilidades para gestionar la estrategia de salida;
e) comprobar la idoneidad de la estrategia de salida, utilizando un enfoque basado en el riesgo (por ejemplo, realizando un análisis de los posibles costes, impactos, recursos e implicaciones temporales de transferir un servicio externalizado a un proveedor alternativo);
f) la definición de los criterios de éxito de la transición.

31. Una empresa debe incluir indicadores de los acontecimientos desencadenantes de la estrategia de salida en su supervisión y vigilancia continuadas de los servicios prestados por el CSP en el marco del acuerdo de externalización en la nube.

Directriz 6. Derechos de acceso y de auditoría

32. La empresa debe garantizar que el acuerdo escrito de externalización en la nube no limite el ejercicio efectivo por parte de la empresa y la autoridad competente de los derechos de acceso y auditoría y las opciones de supervisión del CSP.

33. La empresa debe asegurarse de que el ejercicio de los derechos de acceso y auditoría (por ejemplo, la frecuencia de auditoría y los ámbitos y servicios que deben auditarse) tiene en cuenta si la externalización está relacionada con una función esencial o importante, así como la naturaleza y el alcance de los riesgos y el impacto derivados del acuerdo de externalización en la nube sobre la empresa.

34. En caso de que el ejercicio de los derechos de acceso o auditoría, o el uso de determinadas técnicas de auditoría creen un riesgo para el entorno del CSP y/u otros clientes del CSP (por ejemplo, afectando a los niveles de servicio, la confidencialidad, la integridad y la disponibilidad de los datos), el CSP debe proporcionar a la empresa una justificación clara de por qué ello crearía un riesgo y debe acordar con la empresa formas alternativas para lograr un resultado similar (por ejemplo, la inclusión de controles específicos que deben comprobarse en un informe/certificación específico elaborado por el CSP).

35. Sin perjuicio de su responsabilidad final en relación con los acuerdos de externalización en la nube, con el fin de utilizar los recursos de auditoría de forma más eficaz y reducir la carga organizativa del CSP y sus clientes, las empresas podrán utilizar:

    a) certificaciones de terceros e informes de auditoría internos o externos facilitados por el CSP;
    b) auditorías conjuntas realizadas conjuntamente con otros clientes del mismo CSP o auditorías conjuntas realizadas por un tercero auditor designado por múltiples clientes del mismo CSP.

36. En caso de externalización de funciones esenciales o importantes, la empresa debe evaluar si las certificaciones de terceros y los informes de auditoría externa o interna a que se refiere el apartado 37, letra a), son adecuados y suficientes para cumplir las obligaciones que le aplican en virtud de la legislación aplicable y deben tener como objetivo no basarse únicamente en dichas certificaciones e informes a lo largo del tiempo.

37. En caso de externalización de funciones esenciales o importantes, la empresa debería utilizar las certificaciones de terceros y los informes de auditoría externa o interna a que se refiere el apartado 37, letra a), únicamente si:

    a) considera que el alcance de las certificaciones o los informes de auditoría incluyen los principales sistemas del CSP (es decir, los procesos, aplicaciones, infraestructuras, centros de datos) y los principales controles identificados por la empresa y el cumplimiento de la normativa aplicable;
    b) evalúa en profundidad el contenido de las certificaciones o informes de auditoría de manera periódica y verifican que no estén obsoletos;
    c) garantiza que los sistemas y controles clave del CSP estarán cubiertos en las futuras versiones de las certificaciones o informes de auditoría;
    d) considera adecuada la certificadora o auditora (por ejemplo, en lo que se refiere a sus cualificaciones, conocimientos especializados, repetición o verificación de las pruebas del expediente de auditoría subyacente, así como a la rotación de la empresa certificadora o auditora);

e) está segura 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 de los principales controles establecidos;
f) tiene el derecho contractual de solicitar la extensión del alcance de las certificaciones o los informes de auditoría a otros sistemas y controles pertinentes del CSP; 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) conserva el derecho contractual de llevar a cabo auditorías individuales *in situ* de la función externalizada a su discreción.

38. La empresa debe asegurarse de que, antes de realizar una visita *in situ*, incluso por parte de un tercero designado por la empresa (por ejemplo, un auditor) se notifique previamente al CSP en un plazo razonable, a menos que no sea posible efectuar una notificación previa con tiempo suficiente debido a una situación de emergencia o de crisis o que hiciera que la auditoría deje de ser efectiva. Dicha notificación deberá incluir la ubicación, el objeto de la visita, así como el personal que participará en la misma.

39. Teniendo en cuenta que los servicios en la nube presentan un elevado nivel de complejidad técnica y plantean problemas jurisdiccionales específicos, el personal que realiza la auditoría, ya sea el auditor interno de la empresa o auditores que actúen en su nombre, debe tener las competencias y los conocimientos adecuados para evaluar adecuadamente los servicios pertinentes en la nube y llevar a cabo auditorías eficaces y pertinentes. Esto también debe ser de aplicación para el personal de las empresas que revise las certificaciones o los informes de auditoría facilitados por el CSP.

Directriz 7. Subcontratación

40. En caso de que esté permitida la subcontratación de funciones esenciales o importantes (o de partes importantes de estas), el acuerdo escrito de externalización en la nube entre la empresa y el CSP deberá:

a) especificar cualquier parte o aspecto de la función externalizada que esté excluido de la posible subcontratación;
b) indicar las condiciones que han de cumplirse en caso de subcontratación;
c) especificar que el CSP sigue siendo responsable y está obligado a supervisar los servicios que haya subcontratado para garantizar que todas las obligaciones contractuales entre el CSP y la empresa se cumplen en todo momento;
d) incluir una obligación de que el CSP notifique a la empresa cualquier subcontratación prevista, o cualquier cambio significativo de la misma, en particular cuando ello pueda afectar a la capacidad del CSP para cumplir sus obligaciones en virtud del acuerdo de externalización en la nube con la empresa. El plazo de notificación establecido en el acuerdo escrito debe permitir a la empresa disponer de tiempo suficiente para, como mínimo, llevar a cabo una

evaluación de riesgos de la subcontratación propuesta o de los cambios importantes de la misma y oponerse a ellos o aprobarlos explícitamente, como se indica en la letra e);

e) garantizar que la empresa tenga derecho a oponerse a la subcontratación prevista, o a cambios significativos de la misma, o que se requiera una aprobación explícita antes de que surtan efecto la subcontratación propuesta o los cambios significativos;

f) garantizar que la empresa tenga derecho contractual a rescindir el acuerdo de externalización en la nube con el CSP en caso de que se oponga a la subcontratación propuesta o a los cambios importantes de la misma y en caso de subcontratación indebida (por ejemplo, cuando el CSP proceda a la subcontratación sin notificarlo a la empresa o infrinja gravemente las condiciones de la subcontratación especificadas en el acuerdo de externalización).

41. La empresa debe asegurarse de que el CSP supervisa adecuadamente al subcontratista.

Directriz 8. Notificación escrita a las autoridades competentes

42. La empresa debe notificar por escrito a su autoridad competente, de manera oportuna, los acuerdos de externalización en la nube previstos que afecten a una función esencial o importante. La empresa también debe notificar por escrito y a su debido tiempo a su autoridad competente los acuerdos de externalización en la nube relativos a una función que anteriormente estaba clasificada como no esencial o no importante y que posteriormente pasó a serlo.

43. La notificación por escrito de la empresa deberá incluir, teniendo en cuenta el principio de proporcionalidad, al menos la siguiente información:

a) la fecha de inicio del acuerdo de externalización en la nube y, en su caso, la próxima fecha de renovación del contrato, la fecha de finalización y/o los plazos de preaviso para el CSP y para la empresa;

b) una breve descripción de la función externalizada;

c) un breve resumen de los motivos por los que la función externalizada se considera esencial o importante;

d) el nombre y la marca comercial (en su caso) del CSP, su país de registro, su número de registro, su 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);

e) la legislación aplicable al acuerdo de externalización en la nube y, en su caso, la elección de la jurisdicción;

f) los modelos de despliegue y la naturaleza específica de los datos que el CSP debe conservar y los lugares (es decir, regiones o países) en los que pueden almacenarse dichos datos;

g) la fecha de la última evaluación del carácter esencial o la importancia de la función externalizada;
h) la fecha de la evaluación de riesgos o auditoría más reciente del CSP, junto con un breve resumen de los principales resultados, y la fecha de la próxima evaluación de riesgos o auditoría prevista;
i) la persona física o el órgano encargado de la adopción de decisiones de la empresa que aprobó el acuerdo de externalización en la nube;
j) 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 subcontratado, y en el que se almacenarán los datos;

Directriz 9. Control de los acuerdos de externalización en la nube

44. Las autoridades competentes evaluarán los riesgos derivados de los acuerdos de externalización en la nube de las empresas como parte de su proceso de supervisión. En particular, esta evaluación debe centrarse en los acuerdos relacionados con la externalización de funciones esenciales o importantes.

45. Las autoridades competentes deberán tener la seguridad de que pueden llevar a cabo una supervisión eficaz, en particular cuando las empresas externalicen funciones esenciales o importantes que se llevan a cabo fuera de la UE.

46. Las autoridades competentes evaluarán, sobre la base de un enfoque basado en el riesgo, si las empresas:

a) disponen de la gobernanza, los recursos y los procesos operativos pertinentes para suscribir, aplicar y supervisar de manera adecuada y efectiva los acuerdos de externalización en la nube;
b) identificar y gestionar todos los riesgos pertinentes relacionados con la externalización en la nube.

47. 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 empresas que supervisan como la estabilidad del mercado financiero.