Directrices sobre la externalización a proveedores de servicios en la nube. Boletín Internacional de marzo de 2021.

La creciente importancia de los proveedores de servicios en la nube (en adelante, CSPs por sus siglas en inglés –*cloud service providers*–) revela los beneficios aportados a las empresas y, a su vez, a los inversores mediante la reducción de costes así como una mayor eficiencia y flexibilidad operativa. No obstante, su uso plantea una serie de desafíos en términos de ubicación y protección de datos, además de suscitar posibles problemas de seguridad y riesgos de concentración que, si no son tratados adecuadamente, pudieran amenazar la protección de inversores, la integridad del mercado y la estabilidad financiera.A este respecto, ESMA publicó el 3 de junio de 2020 un documento a consulta (en adelante, CP por sus siglas en inglés –*consultation paper*–) con su propuesta de directrices. Posteriormente, el 18 de diciembre de 2020 publicó el Informe final de las directrices, cuya aplicación será efectiva para los nuevos acuerdos, o los anteriores a esta fecha que sean objeto de modificación o renovación, a partir del 31 de julio de 2021 –los previos deberán ajustarse a lo dispuesto en estas directrices antes del 31 de diciembre de 2022–.
Las directrices propuestas tienen como objetivo ayudar a las entidades y las autoridades competentes a identificar, abordar y realizar un seguimiento de los riesgos y desafíos que surgen durante el proceso que tiene lugar al suscribir acuerdos con los CSPs.

En cuanto a su ámbito de aplicación, se concreta que las directrices competen tanto a las autoridades pertinentes como a instituciones del ámbito de la inversión colectiva (sociedades gestoras de fondos de inversión alternativos y los depositarios de estos fondos, instituciones de inversión colectiva en valores negociables (UCITS) así como las sociedades gestoras y los depositarios de estos fondos o las compañías de inversión (*investment companies*) cuando no se haya designado una sociedad gestora), entidades de contrapartida central (incluyendo a las de nivel 2 de terceros países), depositarios centrales de valores, registros de operaciones (*trade repositaries*), empresas de servicios de inversión y entidades de crédito que presten servicios de inversión, agencias de calificación crediticia, operadores de mercado de los centros de negociación, proveedores de servicios de suministros de datos, administradores de índices de referencia críticos y los registros de titulización (securitisation repositaries).

El propósito de estas directrices es establecer prácticas de supervisión coherentes, eficientes y efectivas dentro del Sistema Europeo de Supervisión Financiera (SESF) y garantizar la aplicación común, uniforme y coherente de los requisitos. Para ello se introduce una definición clave en relación con la externalización que es lo que debe entenderse por función crítica o importante externalizada, siendo esta cualquier función cuyo defecto o fallo en su desempeño perjudique materialmente el cumplimiento de obligaciones legales exigibles a la entidad, tenga un impacto en su actividad financiera de esta o afecte a la solidez o la continuidad de sus principales servicios y actividades.

A continuación se expone una descripción de cada directriz incluida en el Informe final acompañada de una observación sobre su tratamiento en el proceso de consulta:
Directriz 1. Gobernanza, supervisión y documentación

La **directriz 1** prevé que las entidades deberán contar con una estrategia de externalización en la nube precisa y actualizada, además de coherente con la estrategia, políticas y procedimientos internos de la entidad.
Se resalta que deberán ser definidas las responsabilidades de documentación, gestión y control, además de destinar recursos suficientes para garantizar su cumplimiento. Por otro lado, las entidades deberán o bien establecer una función de supervisión o designar a personal *senior* a quienes se encomendará la gestión y el seguimiento de los riesgos derivados de los acuerdos de externalización en la nube, los cuales, a su vez, deberán reportar directamente al órgano de administración (*management body*) –en particular cuando se trate de funciones críticas o importantes que deberán ser reevaluadas de forma periódica y cuando tengan lugar cambios sustanciales–. En cualquier caso, las entidades deberán tener en cuenta en este diseño la naturaleza, escala y

complejidad de su negocio, incluso en términos de riesgo para el sistema financiero. En cuanto a las entidades pequeñas y menos complejas, esta directriz señala que, al menos, se deberá garantizar una división clara de tareas y responsabilidades para la gestión y supervisión de estos acuerdos.Por otro lado, la entidad deberá mantener un registro actualizado de los acuerdos de externalización con el CSP y distinguirá entre funciones críticas y otros acuerdos. En esta cuestión, las respuestas al CP mostraron un acuerdo general con el enfoque de ESMA basado en el riesgo y centrado en las funciones críticas. No obstante, se recibieron comentarios solicitando mayor orientación sobre las definiciones y apuntando la necesidad de garantizar la coherencia con las directrices de EBA[1] en esta cuestión, dadas las posibles interacciones entre ambos desarrollos normativos que puedan afectar a entidades dentro su alcance. En respuesta, ESMA indica que dada la diversidad de empresas dentro de su ámbito de aplicación, no cree que sea útil ser más prescriptivo en el texto puesto que las directrices proporcionan ya definiciones coherentes con el marco de MIFID y sus desarrollos. Finalmente, también resalta que ESMA garantiza la coherencia con las directrices no solo de EBA sino también con las emitidas por EIOPA[2]. Además, ESMA ha tenido en cuenta en su desarrollo la propuesta del Reglamento sobre resiliencia operativa digital de la Comisión Europea (DORA)[3] y la consulta de IOSCO sobre nuevos principios en relación con la externalización[4].

Directriz 2. Análisis previo a la externalización y diligencia debida

La **directriz 2** atiende a la evaluación del posible proveedor y marco de actuación anterior a la firma de cualquier acuerdo de externalización en la nube. En concreto, obliga a la entidad a evaluar si se van a externalizar funciones críticas, identificar los riesgos que puedan derivarse de la externalización en la nube, aplicar un procedimiento de diligencia debida a la hora de evaluar al futuro CSP así como identificar y valorar los posibles conflictos de interés que puedan surgir del acuerdo. No obstante, se invoca de nuevo en esta directriz el principio de proporcionalidad al señalar que tanto el análisis previo como el procedimiento de diligencia debida deberán ser proporcionales a la naturaleza, escala y complejidad de la función que la empresa pretende externalizar así como a los riesgos inherentes que puedan derivarse de esta externalización. Aunque sí que precisa que, al menos, deberá incluir una evaluación del impacto potencial del acuerdo respecto de los riesgos operativos, legales, de cumplimiento y de reputación de la entidad.Específicamente, cuando se trate de funciones críticas, la entidad deberá evaluar por su parte todos los riesgos relevantes que puedan surgir como resultado del acuerdo de la externalización en la nube, incluyendo los relacionados con la tecnología de la información y comunicaciones, la seguridad de la información, la continuidad del negocio, los riesgos legales, de cumplimiento y reputacionales, los riesgos operativos y las posibles limitaciones de supervisión al CSP. En este sentido, la evaluación observará ciertas cuestiones a tener en cuenta en relación con los riesgos mencionados, como por ejemplo: el servicio en la nube seleccionado; los procesos de migración y/o implementación; la sensibilidad y medidas de seguridad exigidas; la interoperabilidad entre los sistemas de la entidad y el CSP así como la portabilidad de datos de la entidad al CSP. Por último, se tendrá en cuenta la estabilidad política, la seguridad y el sistema legal (incluyendo el régimen jurídico sobre insolvencias aplicable al CSP y el de protección de datos) de los países donde sean almacenados los datos y externalizadas las funciones.

Cuando se externalicen funciones críticas el procedimiento de diligencia debida incluirá una evaluación de la idoneidad del proveedor que contemple, a su vez, que goza de reputación profesional, que cuenta con las capacidades y recursos (humanos, técnicos y financieros), su estructura organizativa y, si procede, su autorización o registro preceptivo para el desarrollo de la función crítica. Adicionalmente, se pueden incluir consideraciones sobre los siguientes factores adicionales: la gestión de la seguridad de la información, el soporte del servicio y los planes de continuidad del negocio.

Este marco será de aplicación al suscribirse un nuevo acuerdo o si al renovar un acuerdo existente con el proveedor se determina como necesario un nuevo análisis de diligencia debida.

En las respuestas al CP se observa el acuerdo generalizado sobre el enfoque propuesto por ESMA, si bien muchos estimaron que podría ser aventurado solicitar a las entidades una evaluación tan exhaustiva del proveedor, incluyendo el riesgo de concentración del sector. Por su parte ESMA cree que las directrices proporcionan el nivel adecuado de orientación a este respecto y concreta que las entidades deben considerar la posición dominante de ciertos CSPs ya que dificultaría su sustitución.

Directriz 3. Elementos contractuales clave

La **directriz 3** contempla que los derechos y obligaciones acordados entre la entidad y el CSP deben fijarse claramente en acuerdo escrito que permita, entre otros, la posibilidad de resolución cuando proceda. En caso de externalización de funciones críticas, el acuerdo escrito debe incluir, al menos, lo siguiente: descripción clara de la función externalizada; fechas relevantes y preavisos; leyes aplicables al acuerdo; obligaciones financieras de ambas partes; posible subcontratación (*sub-outsourcing*) y condiciones; ubicación de la función externalizada (incluido donde se procesarán y almacenarán los datos); seguridad de la información y protección de datos

personales; derecho por parte de la entidad a la supervisión del servicio; niveles de servicio acordados (rendimiento cuantitativos y cualitativos); disposiciones relacionadas con la gestión de incidentes; cobertura vía seguro de ciertos riesgos; planes de continuidad del negocio y recuperación de desastres del CSP y, por último, derechos de acceso y de auditoría sobre la información, instalaciones, sistemas y dispositivos oportunos del CSP para la supervisión de su actuación cuando así proceda.En las respuestas al CP se ha destacado que los CSPs normalmente ofrecen contratos estandarizados que dificultan la negociación de los términos contractuales. También se muestra preocupación sobre la cuestión de la ubicación de los datos y alertan de posibles solapamientos con el Reglamento General de Protección de Datos (en adelante, GDPR por su acrónimo en inglés)[5]. Por último, instan a ESMA, junto con EBA e EIOPA, al desarrollo de cláusulas contractuales estándar para su adopción voluntaria. Por su parte, ESMA considera que esta directriz es un instrumento para negociar los términos contractuales con los CSPs. Asimismo, reitera la importancia de la previsión en el contrato sobre la ubicación de los datos. Por último, ESMA coincide con que estandarizar las clausulas puede resultar beneficioso y espera con interés los avances de los trabajos que la Comisión ha iniciado sobre esta cuestión[6].

Directriz 4. Seguridad de la información

La **directriz 4** establece que las entidades deberán fijar en sus políticas y procedimientos internos requisitos de seguridad de la información concretos que, a su vez, se incluirán en los contratos formalizados con los CSPs y respecto de los que deberán realizar un seguimiento sobre su cumplimiento de manera continua. No obstante, permite, nuevamente, que estos requisitos sean proporcionales a la naturaleza, escala y complejidad de la función externalizada así como a los riesgos que puedan derivarse de la misma.En este sentido, cuando la función sea considerada crítica los requisitos incluirán, al menos, las siguientes cuestiones: organización de seguridad de la información; gestión de la identidad y el acceso; cifrado y gestión de claves; seguridad de la red y de las operaciones; interfaz de programación de aplicaciones; continuidad del negocio y recuperación de desastres; ubicación de datos y, por último, cumplimiento y seguimiento de los estándares y controles de la seguridad de la información.

En las respuestas al CP las opiniones recogidas indican que la redacción es demasiado prescriptiva y no refleja los diferentes tipos de modelos de externalización en la nube y acaban por sugerir un enfoque más basado en principios. Por último, también se solicita una mayor alineación con otras iniciativas (Directiva de ciberseguridad[7], GDPR y las directrices EBA sobre externalización). Por su parte, ESMA entiende que el enfoque es equilibrado y la redacción considera los estándares previstos en otros documentos análogos. No obstante, declara que los ejemplos proporcionados no pretenden ser exhaustivos e invoca nuevamente el principio de proporcionalidad a la hora de establecer los requisitos.

Directriz 5. Estrategias de salida

La **directriz 5** prevé que las entidades que resuelvan el acuerdo con su CSP puedan continuar su actividad sin interrumpir los servicios que prestan y sin incurrir en el incumplimiento de sus obligaciones legales a la vez que sin vulnerar la confidencialidad, integridad y disponibilidad de sus datos. A tal efecto, la entidad debe desarrollar planes de salida adecuados, identificar soluciones alternativas a la vez que desarrollar planes de transición y asegurar formalmente el respaldo del CSP saliente para una transferencia ordenada.En este sentido, se concreta que al desarrollar los planes de salida las entidades deben definir los objetivos de la estrategia de salida y los eventos desencadenantes que la activarían. Asimismo, se prevé que realicen un análisis de impacto acorde con la función externalizada para identificar qué recursos serían necesarios y la asignación de roles y responsabilidades para su gestión. Por último, se contempla que el plan conlleve pruebas de idoneidad, aspecto que fue contestado en la CP, de la propia estrategia utilizando un enfoque basado en el riesgo.

Las respuestas al CP coinciden en la necesidad de contar con una estrategia de salida claramente definida que evite interrupciones de los servicios y perjuicios en el cumplimiento de las obligaciones previstas. No obstante, se cuestiona el carácter práctico de las pruebas de idoneidad previstas en las estrategias de salida y presentan dudas sobre su plena implementación. Respecto a la transferencia y/o eliminación de datos se destacó que la entidad, y no el proveedor, debería tener el control de ello. ESMA ha recogido en su documento final los comentarios sobre las prueba de la estrategia de salida. Asimismo, se incorporan disposiciones relacionadas con el respaldo a la transferencia ordenada, junto con lo relativo al procesamiento y eliminación de datos.

Directriz 6. Derechos de acceso y auditoría

La **directriz 6** establece que el contrato subscrito con el CSP no debe limitar el ejercicio de los derechos de acceso y auditoría por parte de la entidad y las autoridades competentes (ni tampoco la posibilidad de su supervisión). Además, la entidad deberá garantizar el ejercicio efectivo de estos derechos en caso de externalización de una función crítica o importante. A este respecto, se prevé que para utilizar los recursos de auditoría de manera más eficiente, y así reducir la carga, se puedan utilizar certificaciones de terceros e informes de auditoría externa o

interna del CSP. Además, podrán realizarse auditorías compartidas conjuntamente con otros clientes del mismo CSP, pudiendo estas ser realizadas por un tercero nombrado por ellos.Los comentarios al CP recibidos estaban principalmente relacionados, en primer lugar, con la carencia de poder de negociación necesario para imponer amplios derechos de acceso al CSP (por ejemplo, normalmente las inspecciones *in-situ* quedan restringidas) y, en segundo lugar, acerca de cuestiones prácticas sobre el uso de certificaciones e informes de auditoría de terceros. En respuesta, ESMA vuelve a hacer una llamada a la proporcionalidad y recalca la importancia de esta cuestión para una adecuada gestión riesgos.

Directriz 7. Subcontratación de la externalización

La **directriz 7** establece que, en caso de subcontratación a terceros de funciones críticas ya externalizadas, el acuerdo escrito inicial de externalización entre la entidad y el CSP deberá prever si existe un perímetro de exclusión para la subcontratación de ciertas funciones críticas a estos terceros. En cualquier caso, para los supuestos en los que se incluya esta subcontratación, el acuerdo escrito entre la entidad y el CSP comprenderá indicaciones sobre las condiciones a cumplir además de concretar específicamente la continua responsabilidad del CSP, al igual que su obligación de hacer un seguimiento sobre el cumplimiento de las condiciones pactadas entre el CSP y la entidad respecto de las funciones subcontratadas o de notificar a la entidad cualquier subcontratación o modificación. Por último, el acuerdo entre la entidad y el CSP deberá garantizar el derecho de oposición y el derecho contractual a resolver cuando la primera no esté de acuerdo con la subcontratación, implique cambios materiales o pueda considerarse indebida.Las cuestiones planteadas por esta directriz suscitaron múltiples comentarios al CP inicial, llegando a considerarse como desproporcionado y desafiante en determinados aspectos como, por ejemplo, en cuestiones relacionadas con la delimitación, la responsabilidad y la notificación. Concretamente, se plantean dudas sobre si la directriz pretende captar la subcontratación de áreas no materiales de funciones críticas y sobre la capacidad de las entidades para asegurar que sus CSPs supervisan eficazmente las funciones subcontratadas. En respuesta, ESMA ha aclarado en su versión final estas cuestiones planteadas, si bien sigue haciendo hincapié en la ineludible responsabilidad de los CSPs y entidades ante estas situaciones. Asimismo, resalta la importancia de los deberes de notificación y derechos de oposición como salvaguardas de importancia.

Directriz 8. Notificación por escrito a las autoridades competentes

La **directriz 8** precisa que la entidad deberá notificar por escrito a su autoridad competente de manera oportuna los acuerdos de externalización en la nube planificados que se relacionen con una función crítica así como, cuando proceda, notificar aquellas funciones subcontratadas que hayan pasado de categoría no crítica a crítica. La notificación deberá incluir básicamente, y respetando el criterio de proporcionalidad, la información definida en la directriz 1, referente al contenido del registro de la entidad sobre acuerdos de externalización y acompañada de una motivación sobre la criticidad de la función.Las respuestas recibidas al CP indicaban la necesidad de aclaraciones sobre el proceso de notificación y destacaban algunos solapamientos con otras disposiciones de notificación existentes a nivel sectorial. En réplica, ESMA cree en la precisa redacción de esta directriz, si bien ha modificado su redacción inicial para guardar coherencia con la directriz 1. Respecto a posibles solapamientos, ESMA manifiesta que las directrices han de ser asumidas sin perjuicio de los requisitos, directrices o prácticas aplicables a determinados sectores (como por ejemplo, el de agencias de calificación crediticia), que por ser más estrictas pudieran ya satisfacer implícitamente su cumplimiento[8].

Directriz 9. Supervisión de los acuerdos de subcontratación en la nube

La **directriz 9** especifica que las autoridades competentes evaluarán los riesgos derivados de los acuerdos de externalización en la nube de las entidades, particularmente en lo referente a funciones críticas o importantes. Se pondrá especial foco cuando las funciones externalizadas se realicen fuera de la Unión Europea y, de forma general, cuando se identifiquen riesgos de concentración que requieran de un seguimiento especial del posible impacto en el sector y, en general, sobre la estabilidad del mercado financiero.Las autoridades competentes deberán evaluar, mediante un enfoque basado en el riesgo, si las entidades cuentan con la gobernanza, los recursos y los procesos operativos necesarios para celebrar, implementar y supervisar de manera adecuada y eficaz sus acuerdos con los CSPs. Con el mismo enfoque, deberán identificar y gestionar todos los riesgos oportunos relacionados con tal externalización.

Las respuestas al CP recibidas muestran acuerdo con el enfoque propuesto, es más, se aprecian medidas como esta que fomentan una mayor convergencia supervisora, además de considerar valiosa cualquier información sobre los riesgos de concentración que pudiera facilitarse desde las autoridades competentes. ESMA toma nota sobre lo indicado en las respuestas y, a su vez, hace referencia a que en el marco de DORA se podrá profundizar en las cuestiones de armonización.

Para concluir ESMA ha manifestado que, entre los beneficios vinculados a su publicación, estas servirán de apoyo a las entidades en sus procesos de transición a la nube aportando un marco coherente entre los distintos sectores así como que su impacto general será bajo en términos de costes de implementación. Igualmente, considera que

con su implementación se mitigarán los riesgos de arbitraje y de elusión de normas mediante una mayor convergencia normativa y supervisora. En otras palabras, la adopción de estas directrices reduce aún más el riesgo de interpretaciones divergentes que podrían dar lugar a discrepancias en la aplicación y supervisión de las disposiciones pertinentes en los Estados miembros. Para terminar, ESMA señala que ha tratado de garantizar la coherencia con las directrices de EBA y EIOPA.

[1] EBA/GL/2019/02 – European Banking Authority Guidelines on outsourcing arrangements
[2] EIOPA-BoS-20-002 – European Insurance and Occupational Pensions Authority Guidelines on outsourcing to cloud service providers
[3] COM(2020) 595 final – 2020/0266(COD) Propuesta de Reglamento sobre la resiliencia operativa digital del sector financiero
[4] CR01/2020 – IOSCO Principles on Outsourcing Consultation Report
[5] 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
[6] Cloud Service Providers consultation meeting on standard contractual clauses for cloud use by financial institutions y Consultation meeting for Financial Institutions on standard contractual clauses for cloud use in the financial sector
[7] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
[8] Por ejemplo, apartado 36 de las directrices para la presentación de informes periódicos a ESMA por parte de las agencias de calificación crediticia

---

Enlaces de interés:

Directrices sobre la externalización a proveedores de servicios en la nube

Documento de consulta sobre el borrador de las directrices sobre la externalización a proveedores de servicios en la nube