



Documento a consulta de ESMA acerca del proyecto de Directrices de externalización de servicios en la nube. (*Consultation paper on draft Guidelines on outsourcing to Cloud Services Providers*)

[Enlace al document: Consultation paper on draft Guidelines on outsourcing to Cloud Services Providers](#)

1.- A quién va dirigido (potenciales interesados):

Esta consulta va dirigida a Autoridades Nacionales Competentes (ANC) y participantes en los mercados financieros y, en particular, a aquellos que utilicen servicios de almacenamiento en la nube prestados por terceros proveedores:

- Gestores y Depositarios de Fondos de Inversión Alternativos.
- Gestores y Depositarios de Organismos de Inversión Colectiva en Valores Mobiliarios (OICVM)
- Entidades de Contrapartida Central (ECC)
- Registros de Operaciones
- Empresas de Servicios de Inversión
- Entidades de Crédito que prestan servicios de inversión
- Proveedores de servicios de suministro de datos
- Operadores de Centros de Negociación
- Depositarios Centrales de Valores
- Agencias de Calificación Crediticia
- Registros de titulaciones
- Administradores de índices

La consulta es también de interés para los proveedores de servicios de almacenamiento en la nube con quienes contratan las firmas anteriores dichos servicios.

La CNMV agradecería a todos los potenciales interesados arriba mencionados que le remitieran una copia de sus respuestas a la consulta a la dirección que se indica a continuación: Documentosinternacional@cnmv.es

2.- Nota Informativa

ESMA ha publicado, con fecha 3 de Junio, una consulta acerca del proyecto de directrices sobre de externalización de servicios en la nube.

Este proyecto tiene como objetivo asegurar que los riesgos que puedan surgir del uso por los participantes en el mercado financiero de servicios en la nube prestados son adecuadamente identificados y abordados. Las directrices pretenden ser una guía para

ayudar a las empresas a identificar, abordar y vigilar los riesgos que pueden surgir de sus acuerdos de externalización de los servicios en la nube (adoptar la decisión de externalizar, seleccionar un proveedor de servicios en la nube, vigilar las actividades contratadas y proporcionar estrategias de salida).

ESMA identificó la necesidad de emitir estas directrices después del plan de acción FinTech de la Comisión Europea y, dado que los riesgos asociados a la externalización del servicio de almacenamiento en la nube son similares en los distintos sectores, ESMA ha tenido en cuenta las directrices publicadas recientemente por EBA y EIOPA.

La estructura del documento a consulta es la siguiente:

.- La sección 2 contiene los antecedentes de las directrices:

Las entidades están utilizando de forma creciente los servicios en la nube. Aunque estos servicios pueden ofrecer beneficios e incluso una reducción de costes y mejora de la eficiencia y flexibilidad operacional, presentan numerosos desafíos en términos de protección de datos y seguridad de la información. El riesgo de concentración por el uso del mismo servicio de n la nube por muchas entidades puede tener consecuencias negativas para la estabilidad financiera.

Si bien a este tipo de externalización se le aplican los principios generales sobre controles efectivos para la externalización, ESMA reconoce que ciertas características son específicas de los servicios en la nube: tienden a ser más estandarizados y se prestan a los clientes de manera altamente automatizada y a gran escala.

Es responsabilidad de cada entidad identificar e implementar formas efectivas de gestión de los riesgos en relación con el uso de servicios en la nube.

.- La sección 3 contiene las directrices propuestas que incluyen las preguntas de la consulta:

Directriz 1: Gobierno, vigilancia y documentación

La externalización de este servicio debe ser resultado de una estrategia adoptada por la alta dirección y no ser considerada solamente un asunto IT. Además, la vigilancia de la externalización de servicios en la nube debe estar basada en el *risk-based approach*. Cada entidad mantendrá un registro de información sobre los acuerdos de externalización distinguiendo si se externalizan funciones críticas o importantes, o no.

Las directrices aplican el principio de proporcionalidad al distinguir las obligaciones de las entidades según la externalización en la nube afecte a funciones críticas o importantes, o afecte a otro tipo de funciones.

Directriz 2: Análisis previo y diligencia debida

Antes de firmar un acuerdo con un proveedor de servicios en la nube, la entidad debe valorar si el acuerdo concierne a una función crítica o importante, identificar los potenciales riesgos y las posibles limitaciones de supervisión así como los potenciales conflictos de interés. En el caso de externalización de funciones críticas o importantes, la diligencia debida incluye una evaluación de idoneidad del proveedor de servicios en la nube. En caso de cambios en el proveedor o en la criticidad de la función afectada, la entidad puede volver a evaluar tanto el análisis previo como la diligencia debida.

Directriz 3: Requisitos contractuales

Los derechos y obligaciones de la entidad y del proveedor de servicios en la nube deben constar en un acuerdo escrito con un contenido mínimo, entre los que se encuentran aspectos como la ley aplicable, jurisdicción, países donde los datos se almacenan o el derecho a vigilar de forma periódica la actuación del proveedor.

Directriz 4: Seguridad de la información

Cada entidad debe establecer un conjunto de requisitos para la seguridad de la información tanto en sus procedimientos internos como en el acuerdo escrito para la externalización y cumplir de forma continua los mismos, incluyendo la protección de datos personales, confidenciales o sensibles. En el caso de externalización de funciones críticas o importantes, la entidad debería, entre otros: utilizar sistemas de encriptación, considerar la segregación de redes, considerar la integración con sus APIs, contar con planes de continuidad del negocio y de recuperación en caso de desastre y conocer la localización del lugar del almacenamiento y procesamiento de sus datos.

Directriz 5: Estrategias de salida

En caso de funciones críticas, las entidades deben asegurarse que pueden finalizar el contrato de externalización del servicio en la nube sin que ello suponga detrimento al cumplimiento normativa o a la confidencialidad, integridad y disponibilidad de los datos y sin que se produzca la interrupción de la actividad.

Para ello, las entidades deben definir los objetivos de la estrategia de salida y los acontecimientos que permiten activar dicha estrategia de salida.

Directriz 6: Acceso y derecho de auditoría

Las entidades deben asegurarse de que el acuerdo firmado con el tercero proveedor de servicios en la nube no restringe de forma inadecuada el derecho de acceso y de auditoría de los servicios. Las entidades deben valorar si las auditorías internas o externas son adecuadas y suficientes para cumplir con sus obligaciones.

Directriz 7: Subcontratación

Si la subcontratación de funciones críticas se permite, las condiciones acordadas entre el proveedor y el subcontratado deben formar parte del acuerdo escrito entre la entidad y el proveedor. Las entidades deben asegurarse de que el proveedor vigila adecuadamente al subcontratado.

Directriz 8: Notificación por escrito a las autoridades competentes

Si una entidad decide externalizar funciones importantes o críticas, debe notificarlo a su autoridad competente. La notificación deberá incluir, entre otros, una descripción de la función a externalizar y las razones por las que se considera crítica, la identificación del proveedor, la ley aplicable y la jurisdicción elegida o el modelo de desarrollo de la nube.

Directriz 9: Supervisión de los acuerdos de externalización del almacenamiento en la nube

Las autoridades competentes deben evaluar los riesgos derivados de los acuerdos de externalización de servicios de almacenamiento en la nube como parte de su actividad de supervisión. En particular, esta evaluación debe centrarse en los acuerdos de externalización de funciones críticas o importantes. Las autoridades competentes deben poder realizar una supervisión efectiva, en particular cuando el proveedor de servicios está fuera de la UE.

Las autoridades competentes deberán evaluar con un *risk-based approach* si las entidades cuentan con la organización, recursos y procesos operativos necesarios para externalizar este servicio e identificar los riesgos relevantes. Cuando se identifiquen riesgos de concentración, las autoridades competentes deben vigilar su potencial impacto en otras entidades así como la estabilidad del mercado financiero.

.- El *anexo 1* contiene todas las preguntas de la consulta y el *anexo 2* un análisis coste/beneficio preliminar de la propuesta.

ESMA analizará las respuestas recibidas a la consulta en Q 3 2020 y espera publicar el informe final con las directrices en Q 4 2020/Q 1 2021.

Estas directrices son de aplicación a partir del 30 de junio de 2021 a todos los acuerdos de externalización de servicios en la nube suscritos, novados o modificados en esta fecha o después. Las empresas deben revisar y modificar en consecuencia los acuerdos de externalización existentes con el fin de garantizar que tengan en cuenta estas directrices antes del 31 de diciembre de 2022. Cuando la revisión de los acuerdos de externalización de funciones críticas o importantes no haya finalizado el 31 de diciembre de 2022, las empresas deben informar su autoridad competente sobre este hecho, incluidas las medidas previstas para completar la revisión o la posible estrategia de salida.

3.- Solicitud de comentarios

El período de consultas finaliza el **1 de septiembre de 2020**.

Las observaciones deben enviarse contestando al formulario de respuesta en línea que encontrará en el enlace siguiente: <https://www.esma.europa.eu/press-news/consultations/draft-guidelines-outsourcing-cloud-service-providers#registration-form>

Asimismo, como ya se ha indicado arriba, la CNMV agradecería a las partes interesadas que le remitieran una copia de sus respuestas a la consulta a la dirección que se indica a continuación: Documentosinternacional@cnmv.es

CNMV
Dirección de Asuntos Internacionales
c/ Edison 4
28006 Madrid