

# Computación en la Nube: Enfoques de regulación y supervisión

A2ii – IAIS Llamada de Consulta

28 de noviembre de 2019

# Oradores



**Denise Garcia Ocampo**  
FSI, Senior Advisor



**Lázaro Cuesta Barbera**  
Senior Expert,  
European and Occupational  
Pensions Authority (EIOPA)

## IAIS representative



**Alessandro Nardi**  
International  
Association of  
Insurance Supervisors  
(IAIS)



**Regina Simoes**  
Iniciativa de Acceso a los Seguros  
(A2ii)

Financial Stability Institute



## Computación en la nube: Enfoques de regulación y supervisión

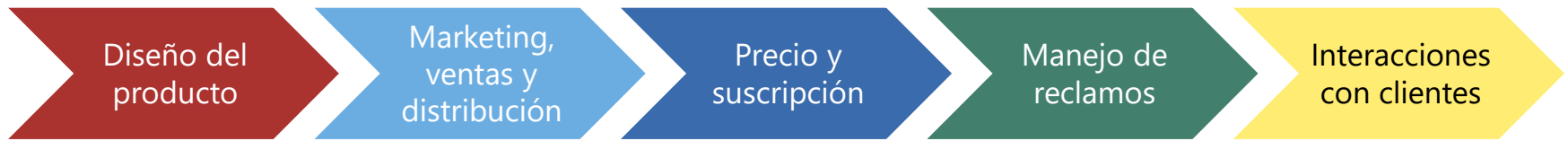
Llamada de Consulta de la A2ii - IAIS

28 de noviembre de 2019

Denise Garcia Ocampo, Asesora Principal, FSI \*

*\*Las opiniones expresadas en esta presentación son del presentador y no las del BIS o de los comités con sede en Basilea.  
Las opiniones y el contenido de esta presentación se utilizarán para los fines de esta reunión y no deben ser citados o difundidos públicamente sin la autorización del presentador.*

# Digitalización del negocio asegurador



(Interfaz de programación de aplicaciones) Application Programming Interface (API)

Artificial Intelligence (AI)  
(Inteligencia Artificial)

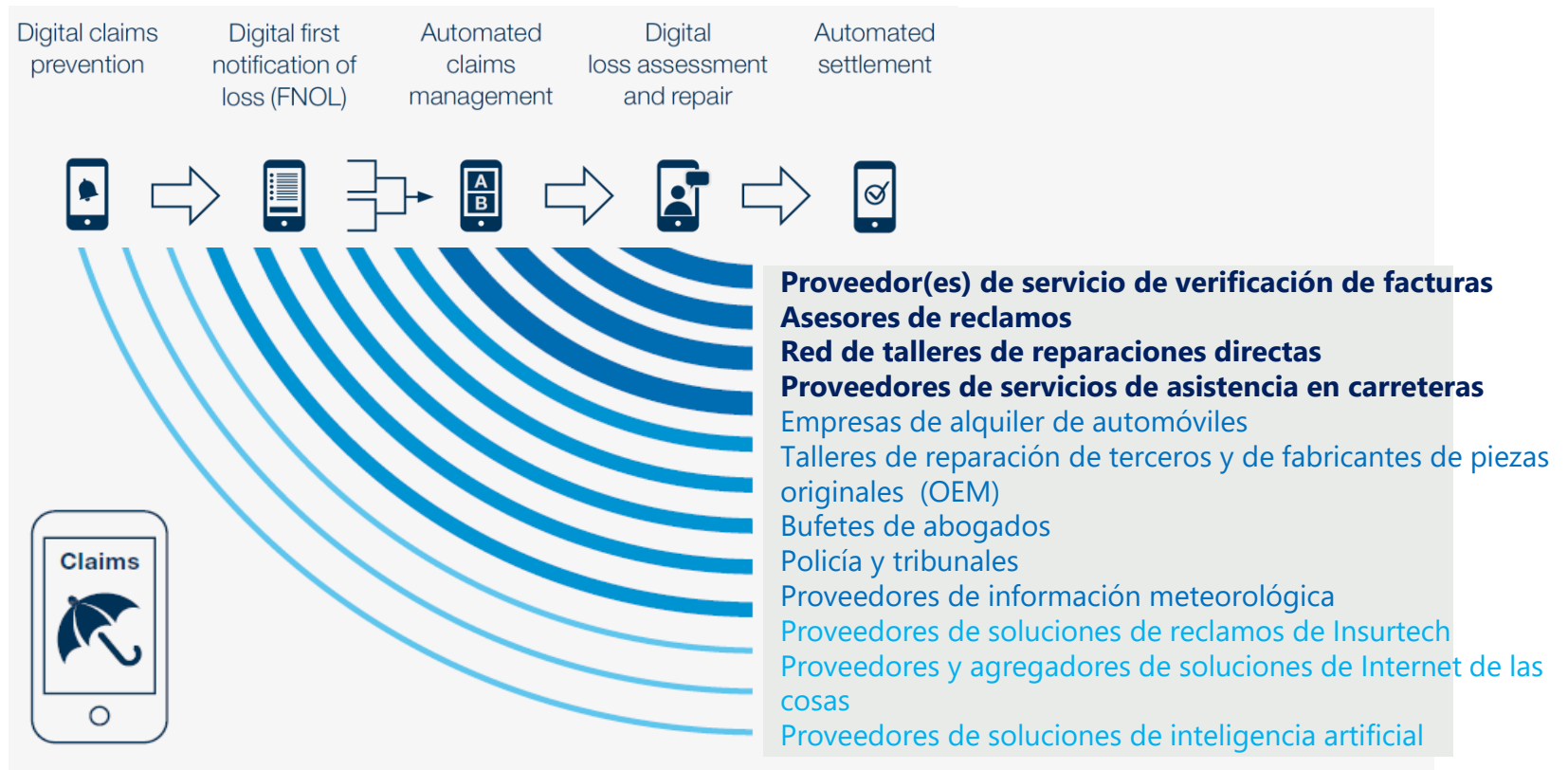
Biometrics  
(Biométrica)

Distributed Ledger Technology (DLT)  
(Tecnología de contabilidad distribuida)

Internet of Things (IoT)  
(Internet de las cosas)

Machine Learning (ML)  
(Aprendizaje de máquinas)

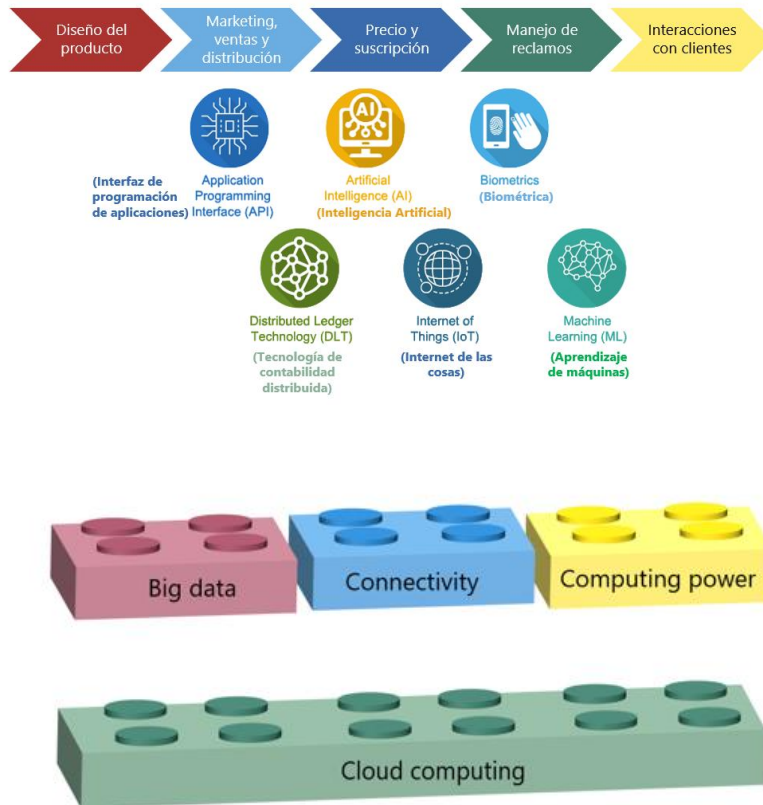
# Digitalización y proveedores de servicios tecnológicos de terceros – ejemplo



Source: Digital insurance in 2018: Driving real impact with digital and analytics, McKinsey & Company

Digital Claims - Prevención de reclamos digitales  
 FNOL - Primera notificación digital de pérdida  
 Automated claims management - Gestión automatizada de reclamos  
 Digital assessment and repair - Evaluación digital de pérdidas y reparaciones  
 Automated resettlement - Liquidación automatizada

# Computación en la nube como habilitadora de la innovación



## 5 Características de la nube:

- Autoservicio bajo demanda
- Servicio de amplio acceso a la red
- Recursos compartidos (multi-arrendamiento)
- Elasticidad rápida
- Servicio administrado

## 4 Modelos de implementación

- Nube pública
- Nube híbrida
- Nube comunitaria
- Nube privada

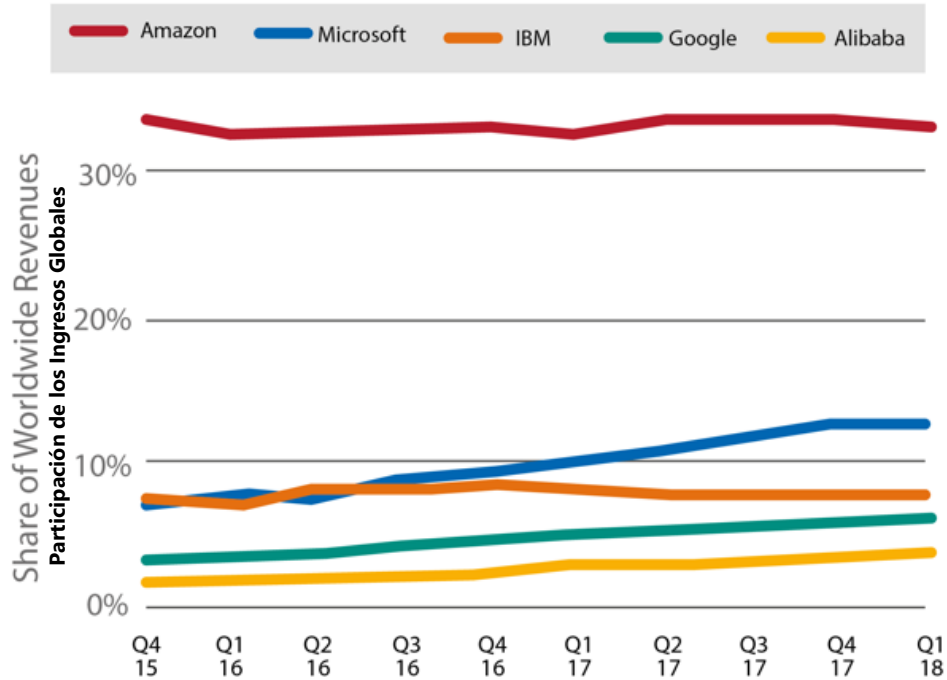
## 3 Modelos de Servicio

- Infraestructura como un servicio
- Plataforma como servicio
- Software como servicio

# Proveedores de servicios en la nube

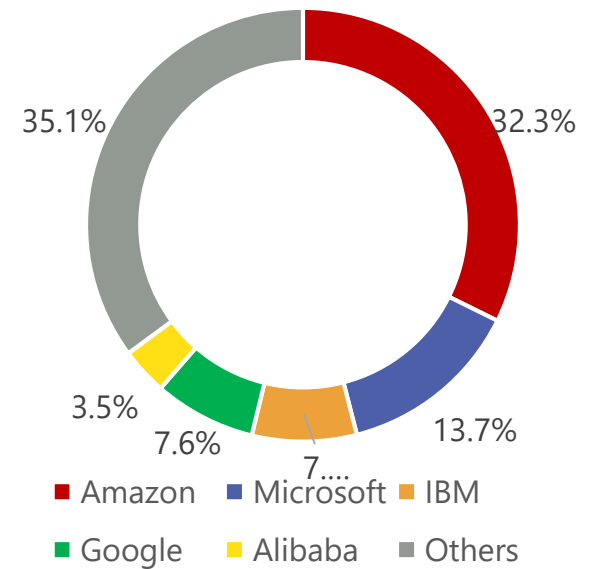
Market share trend of cloud infrastructure services (IaaS, PaaS & Hosted Private Cloud)

Tendencia de participación de mercado de la infraestructura de los servicios en la nube (IaaS, PaaS y Nube Privada Alojada)



Source: Synergy Research Group

Participación de Mercado, Q1 18



# ¿Donde está la nube?





## Beneficios y riesgos potenciales de la nube



- Costo efectiva
  - Eficiencia aumentada
  - Flexibilidad
  - Escalabilidad
  - Tiempo de comercialización más rápido –  
habilitadora de innovación
  - Seguridad mejorada para pequeñas  
empresas
- Ciberseguridad y protección de datos
  - Gobernanza
  - Legales y cumplimiento
  - Concentración
  - Lock-in del proveedor y sustituibilidad
  - Continuidad comercial

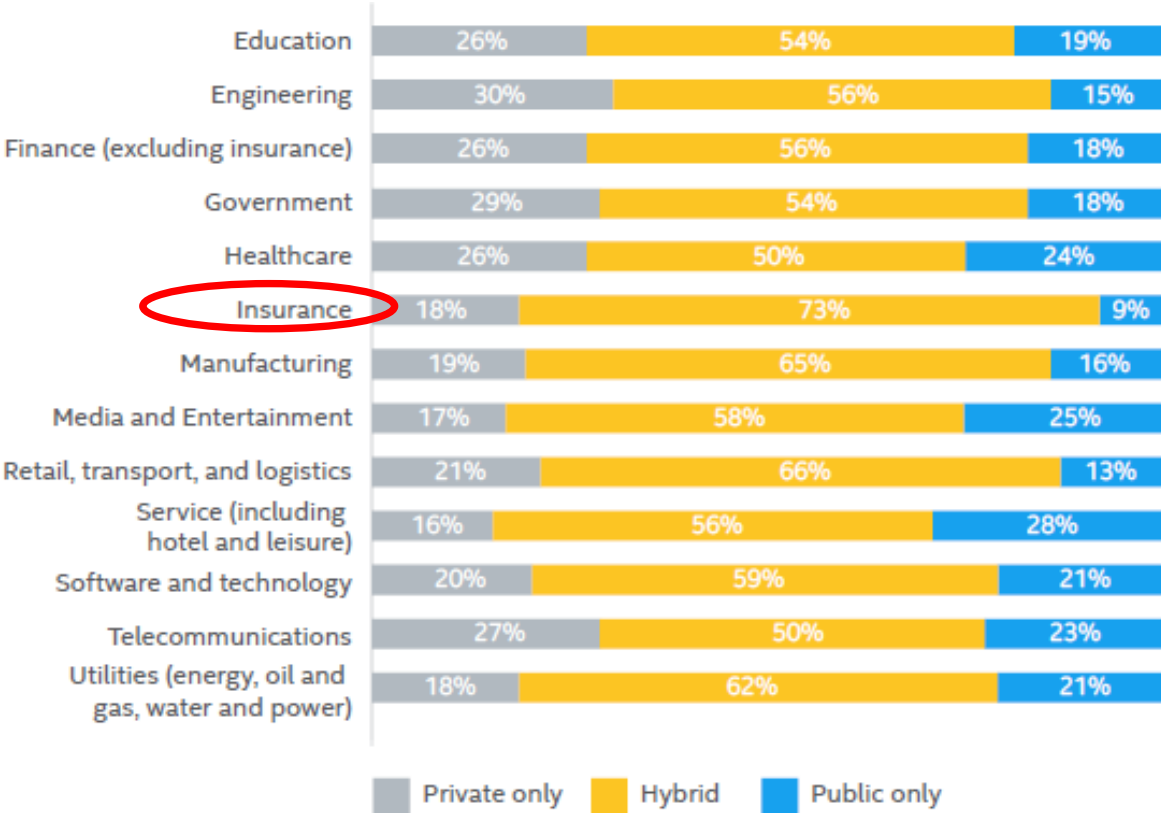
# Uso de la nube en el sector de seguros

La **adopción** de la CN observa un **crecimiento** sostenido en todos los sectores de la economía.

En general, la CN se utiliza en el sector de **seguros**:

- Ampliamente por los **recién llegados** y por un **nicho** de mercado para funciones **críticas**.
- Utilizado principalmente por **las instituciones más grandes** para **funciones no críticas**.

Arquitectura de la nube por industria, 2017



Source: Building trust in a Cloud Sky, Cloud Security Alliance

## Documento sobre observaciones del FSI sobre la computación en la nube *por Juan Carlos Crisanto, Conor Donaldson, Denise Garcia y Jermy Prenio*



Basado en la información pública y las entrevistas a 14 autoridades ubicadas en Asia, Europa y América del Norte, este documento presenta **observaciones** clave sobre el emergente **tratamiento prudencial** de la computación en la nube que surge en la industria **aseguradora**.

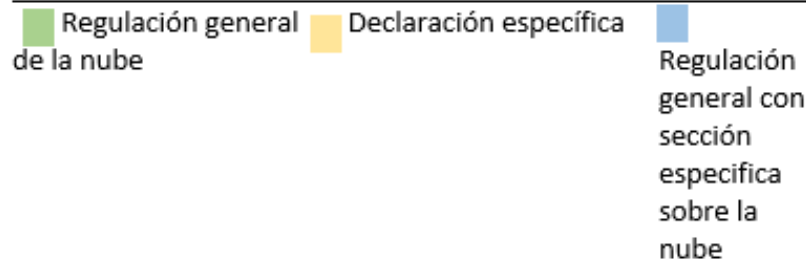
[www.bis.org](http://www.bis.org)

# Enfoques regulatorios

Regulaciones y declaraciones de la autoridad de supervisión que se aplican a la subcontratación en la nube

Marcos	Subcontratación		Gobernanza y Gestión del riesgo		Seguridad de la información	
	Generales	Específicos de la nube	Generales	Específicos de la nube	Generales	Específicos de la nube
APRA	Regulación general	Declaración específica	Regulación general		Regulación general *	
OSFI	Regulación general	Declaración específica			Regulación general	
EIOPA			Regulación general			
ACPR			Regulación general	Declaración específica		
BaFin			Regulación general	Declaración específica	Regulación general *	
HKIA	Regulación general		Regulación general			
IRDAI			Regulación general			Regulación general con sección específica sobre la nube
DNB			Regulación general	Declaración específica		
SAMA	Regulación general					Regulación general con sección específica sobre la nube
MAS <sup>37</sup>			Regulación general con sección específica sobre la nube			Regulación general con sección específica sobre la nube
FINMA	Regulación general		Regulación general			
FCA	Regulación general	Declaración específica				
PRA			Regulación general			
NAIC			Regulación general		Regulación general	

\*Actualmente en proceso de consulta



## Requisitos regulatorios para la computación en la nube

1. Valoración de materialidad, criticalidad o importancia
2. **Gobernanza**
3. Debida diligencia
4. **Evaluación de riesgos**
5. **Protección de datos y seguridad de la información**
6. Ubicación
7. Subcontratación
8. **Continuidad del negocio y estrategia de salida**
9. Monitorear y controlar
10. Auditoría y derecho de acceso

# Gobernanza



## Específicos de la nube

La Junta, y la alta gerencia deben:

- Definir la **estrategia tecnológica** y **los objetivos corporativos** incluyendo la subcontratación **sustancial** en la nube
- para la gestión de los riesgos de la computación en la nube:
  - asignar **responsabilidad**
  - definir la **estructura organizacional** y **operacional**
  - Garantizar **personal** con suficientes **habilidades** y **recursos**

## Evaluación de riesgos



Específicos de la nube

La evaluación de riesgos en **cuestiones relacionadas con los datos** debe tomar en cuenta:

- La **identificación, clasificación e importancia** de los datos almacenados y procesados en la nube
- Identificación de los **riesgos** relacionados con la **confidencialidad, disponibilidad y seguridad** de estos datos
- Evaluación de los **impactos** causados por las **violaciones** de datos

APRA recomienda el uso **de análisis de escenarios** en eventos que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos almacenados en la nube.

## Protección de datos y seguridad de la información



### Específicos de la nube

Las aseguradoras deben comprender la **naturaleza** y **fortaleza** de **los controles de del proveedor de servicios en la nube** (seguridad física de los centros de datos, medidas de ciberseguridad, etc.).

APRA, ACPR, IRDAI, SAMA y MAS recomiendan que los acuerdos de subcontratación incluyan políticas y procedimientos sobre la **clasificación, segregación, seguridad, retención prevención de pérdidas, notificación** de incidentes, **recuperación y destrucción** de los datos.

APRA hace hincapié sobre la importancia de **asignar responsabilidades**.

OSFI recomienda contar con procedimientos que garanticen la **notificación oportuna de incidentes cibernéticos**, y la protección y la seguridad de la información.



## Continuidad del negocio y estrategia de salida



### Específicos de la nube

El acuerdo de subcontratación debe incluir la **duración máxima del tiempo de inactividad** y la **máxima pérdida de datos permitida**.

Dos **elementos** clave de la **estrategia de salida** para los arreglos en la nube son:

- **Remoción y eliminación** completa de datos de todos los sitios donde se almacenan, gestionan o procesan;
- Definir la habilidad de la institución supervisada para **reabsorber** la actividad subcontratada.

Las condiciones de **reversibilidad** deben definirse al suscribir el acuerdo de subcontratación, incluyendo el formato de los datos devueltos y su destrucción.

## Comunicación del plan de computación en la nube

	Notificación	Consulta o Aprobación
APRA	Sí, para arreglos de subcontratación que impliquen bajos riesgos inherentes a la nube.	Consulta, para arreglos de subcontratación que involucren actividades sustanciales que impliquen deslocalización y arreglos que involucren riesgos inherentes a la nube extremos o potenciados, haya o no deslocalización.
OSFI	No	No
EIOPA	Sí, para arreglos de subcontratación que involucren funciones críticas o importantes	No
ACPR	Sí, para arreglos de subcontratación que involucren funciones críticas o importantes	No
BAFIN	Sí, para arreglos de subcontratación que involucren funciones críticas o importantes	No
HKIA	Sí, para arreglos de subcontrataciones sustanciales	No
IRDAI	No	Aprobación para todos los arreglos de subcontratación que involucren funciones principales
DNB	Sí, para arreglos de subcontrataciones sustanciales	No
SAMA	No	Aprobación para la subcontratación sustancial y para cualquier arreglo de servicio en la nube
MAS	No	No
FINMA	No	Aprobación para arreglos de subcontratación que involucren funciones significativas o de control relevantes para el plan de negocios
FCA	Sí, para arreglos de subcontrataciones sustanciales	No
PRA	Sí, para arreglos de subcontratación que involucren funciones críticas o importantes	No
NAIC	No	No

## Prácticas de supervisión Supervisory practices

- Supervisión bajo **riesgo operacional** siguiendo un enfoque **basado en el riesgo**
- Las inspecciones *in situ* incluyen la revisión de:
  - **Documentación** de respaldo del acuerdo de subcontratación (por ejemplo, debida diligencia, evaluación de riesgos de la actividad que se subcontratará)
  - Evaluación de los **procesos** de la aseguradora relacionados con la gestión de la ciberseguridad, los informes de monitoreo y controles, los planes de continuidad comercial
- Las revisiones realizadas fuera del sitio se centran en la evaluación de la gobernanza y las prácticas de gestión de riesgos de la aseguradora
  - Archivo de **notificación o aprobación**
  - Información **pública** (por ejemplo, certificaciones e informes de garantía de CSP)
  - **Informes** reglamentarios (por ejemplo, póliza de subcontratación, ORSA, informes de subcontratación)
  - **Solicitudes** específicas (por ejemplo, revisiones temáticas, cuestionarios)

## Hallazgos clave

- Vale la pena **aclarar las expectativas regulatorias** con el fin de:
  - Abordar los **riesgos específicos** potenciales asociados con la computación en la nube,
  - Proporcionar un nivel razonable de **certeza regulatoria** con respecto al uso de los servicios en la nube
  - **Apoyar** a los participantes del mercado en la **adopción responsable** de tecnología
- Consideraciones para los marcos regulatorios: **basados en principios, tecnológicamente neutrales, consistentes** entre sectores financieros y aplicados de manera **proporcional**.
- **La cooperación internacional** entre las autoridades de origen y de destino, en particular mediante el **intercambio** de informaciones relevantes sobre **CSP** es especialmente importante cuando se trata de garantizar una **supervisión** efectiva de las actividades de computación en la nube.



**eiopa**  
EUROPEAN INSURANCE  
AND OCCUPATIONAL PENSIONS AUTHORITY

# Externalización en la nube

**Lazaro Cuesta**

A2ii IAIS Llamada de consulta  
28 Noviembre 2019

---

# Externalización en Solvencia II EIOPA

**Externalización:** *cualquier tipo de acuerdo entre una empresa de (rea)seguros y un proveedor de servicios, ya sea o no una entidad sujeta a supervisión, en virtud del cual ese proveedor de servicios, directamente o por sub-externalización, realice un proceso, una prestación de servicios o una actividad que, en otras circunstancias, hubiese realizado la propia empresa de (rea)seguros (Artículo 13 (28) Directiva de Solvencia II)*

## Externalización en Solvencia II

Artículo 49 Directiva de Solvencia II

Artículo 274 Reglamento de Solvencia II

Directrices de EIOPA sobre el Sistema de gobernanza

## Normas generales sobre externalización

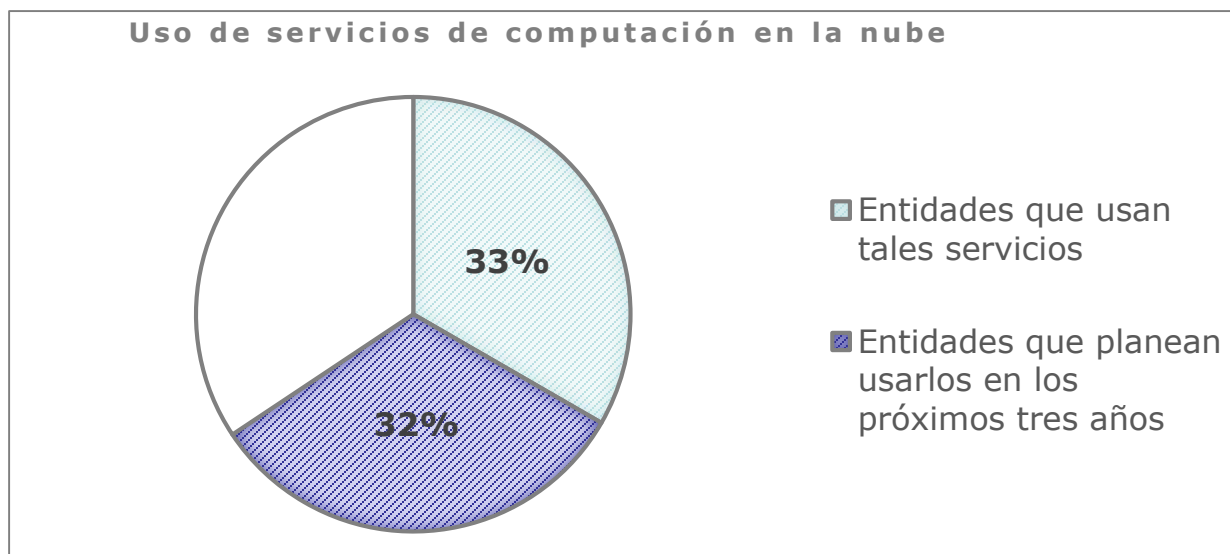
- Responsabilidad de las entidades aseguradoras por las funciones o actividades externalizadas
- Política escrita

# Externalización en Solvencia II EIOPA

## Externalización de funciones o de actividades operativas críticas o importantes

- **Límites** – no podrá realizarse de forma que pueda:
  - perjudicar sensiblemente la calidad del sistema de gobernanza de la empresa considerada;
  - aumentar indebidamente el riesgo operacional;
  - menoscabar la capacidad de las autoridades de supervisión para comprobar que la empresa cumple con sus obligaciones;
  - afectar a la prestación de un servicio continuo y satisfactorio a los tomadores.
- **Información al supervisor:** previa y de cualquier cambio significativo
- Elección del proveedor de servicios
- Contenido del contrato
- Control y gestión de riesgos de las actividades externalizadas

- Uso extensivo de externalización en la nube por nuevos participantes y por ciertos nichos de mercado (optimización de gastos, innovación)
- Parte de la estrategia de transformación digital de los mayores grupos aseguradores europeos
- Nivel de uso no homogéneo entre países de la UE





## Áreas a clarificar

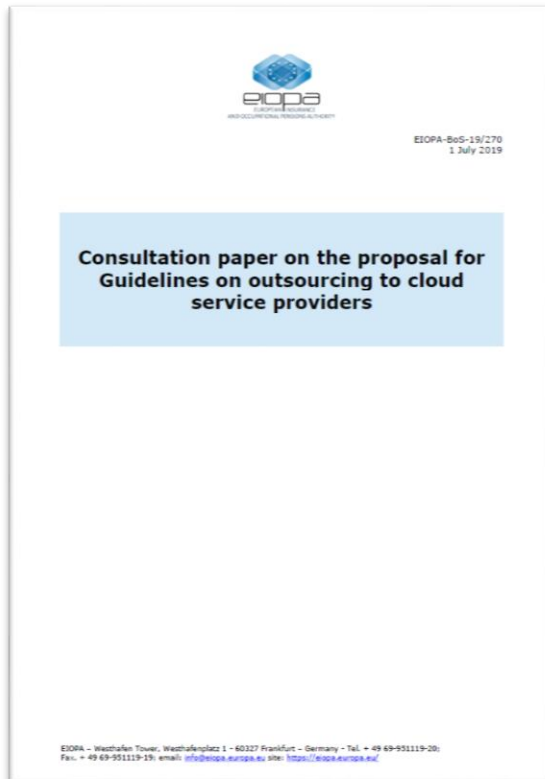
- aplicación de la **definición legal de “externalización”** a la compra de servicios en la nube;
- evaluación de riesgos y **notificación a las autoridades** competentes antes de entrar en un acuerdo de externalización en la nube;
- **gestión de riesgos** específicos asociados al uso de servicios de computación en la nube (por ejemplo: seguridad de datos y sistemas, confidencialidad, riesgo legal y reputacional, riesgo de concentración);
- aplicación de los requisitos de **auditoría y acceso** a los acuerdos;
- supervisión de los acuerdos de externalización en la nube

## Consulta pública sobre una propuesta de directrices de EIOPA sobre externalización a proveedores de servicios en la nube

- Fecha límite de la consulta: 30 Septiembre 2019
- Aprobación: principios de 2020
- Entrada en vigor: 01 Julio 2020 – 1 Julio 2022

### Antecedentes;

- Respuesta de EIOPA al Plan de Acción de la Comisión Europea sobre Fintech (Marzo 2019)
- Recomendaciones de EBA (European Banking Authority) sobre externalización a proveedores de servicios en la nube



## **Propuesta de directrices**

1. Servicios en la nube y externalización
2. Principios generales de gobernanza para externalización
3. Política escrita sobre la externalización
4. Notificación a la autoridad supervisora
5. Requisitos de documentación
6. Análisis previo
7. Evaluación de materialidad
8. Evaluación de riesgos

## **Propuesta de directrices**

9. "Due diligence" del proveedor de servicios en la nube
10. Requisitos contractuales
11. Derechos de acceso y auditoría
12. Seguridad de datos y sistemas
13. Subcontratación
14. Control y supervisión de los acuerdos
15. Derechos de rescisión y estrategias de salida
16. Supervisión de los acuerdos de externalización en la nube por las autoridades supervisoras

## Supervisión de los acuerdos de externalización en la nube

- Enfoque basado en riesgo
- **Valoración supervisora:**
  - ✓ Gobernanza de los acuerdos
  - ✓ Recursos, habilidades y conocimientos
  - ✓ Gestión de riesgos
- **Inspecciones in-situ** a los proveedores de servicios en la nube
- Posibles **medidas:**
  - Mejora de la gobernanza, restricción del ámbito de la externalización, salida de los acuerdos



# Muchas gracias

Lázaro Cuesta Barberá

EIOPA

European Insurance and Occupational Pensions Authority

WesthafenTower | Westhafenplatz 1

60327 Frankfurt am Main | Germany

Tel: +49 69 9511 19-381

Email: [lazaro.cuesta@eiopa.europa.eu](mailto:lazaro.cuesta@eiopa.europa.eu)

# Gracias

Follow us on Twitter [@a2ii\\_org](#), Youtube and LinkedIn