

# SEMINARIO SOCINFO: COMPARTICIÓN DE RECURSOS Y CLOUD COMPUTING

Madrid, 11 de enero de 2011

## CLOUD COMPUTING Y PROTECCIÓN DE DATOS PERSONALES

María José Blanco Antón  
Subdirectora General del Registro  
General de Protección de Datos



AGENCIA  
ESPAÑOLA DE  
PROTECCIÓN  
DE DATOS



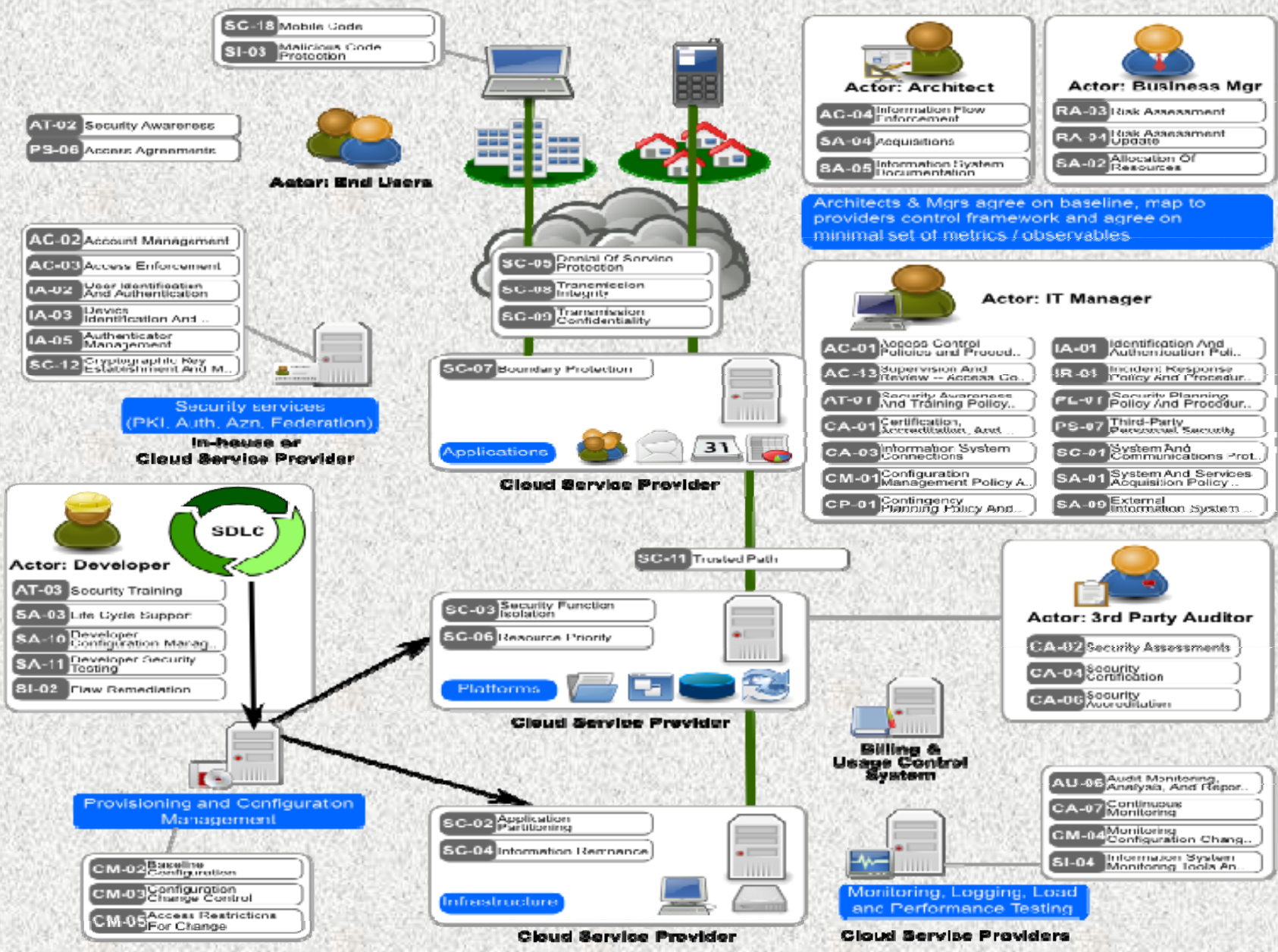
## **CLOUD COMPUTING. Definición:**

**La nube es un modelo a la carta para la asignación y el consumo de computación. La nube describe el uso de una serie de servicios, aplicaciones, información e infraestructura compuesta por reservas de recursos de computación, redes, información y almacenamiento. Estos componentes pueden orquestarse, abastecerse, implementarse y desmantelarse rápidamente, y escalarse en función de las dimensiones para ofrecer unos servicios de tipo utilidad.**

**Seguridad en la Nube – Guía de la Cloud Security Alliance (CSA)**

## **CLOUD COMPUTING. Características y servicios:**

- **Servicios a la carta o bajo demanda del consumidor.**
- **Amplio acceso a la red (PC, móvil, PDA).**
- **Compartición de recursos para el usuario con independencia de su localización.**
- **Rapidez y elasticidad en la provisión de servicios.**
- **Supervisión y control.**
- **Software (SaaS), Plataforma (PaaS), Infraestructura (IaaS).**
- **Nubes: Públicas, Privadas, Comunitarias, Híbridas.**



08\_02 Pattern 011 18 Cloud Computing.svg  
 OSA is licensed according to Creative Commons Share-Alike.  
 Please see: <http://www.opensecurityarchitecture.org/cms/community/license-terms>.

## Aspectos a tener en cuenta

- La decisión de “irse a la nube” debe tener en cuenta multitud de aspectos:
  - Técnicos.
  - Económicos.
  - Modelo de gestión.
  - JURÍDICOS.

## Aspectos jurídicos. Protección de datos



- Si la contratación de Cloud Computing afecta a datos personales:
  - Se trata de derechos fundamentales.
  - Deben atenderse necesariamente las cuestiones de cumplimiento normativo.
  - Todo el entorno, sin excepción debe ser privacy compliance.
- En cualquier caso, cuando un responsable de fichero o tratamiento en España contrata servicios de Cloud Computing aplicará los principios y obligaciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. LOPD y RLOPD
- Privacy Impact Assessment.
- Privacy by Design.

# Cloud computing y protección de datos



- El proveedor de servicios de Cloud Computing ¿es un **encargado de tratamiento**?
  - Diligencia en la elección
- ¿En qué país se encuentra la nube? **Transferencias internacionales de datos**
- Garantía de los **derechos ARCO**
- Medidas de **seguridad**

## El proveedor de servicios de Cloud Computing

¿es un **encargado del tratamiento**?

## Encargado de tratamiento



- **Encargado del tratamiento:** La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

## Diligencia en la elección



**El responsable del tratamiento deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en el RLOPD.**

- ¿Está en condiciones de garantizar la seguridad? ¿dispone de alguna certificación o emplea alguna métrica que podamos verificar? ¿ISO 27001?
- ¿Se somete a auditorías? Y si lo hace, ¿en el proceso de auditoría, garantiza la protección de mis datos?, ¿exhibe documentación acreditativa y fiable?
- ¿Se ha realizado un mínimo análisis de riesgos? ¿disponemos de información fiable?
- ¿Subcontrata? ¿qué requisitos y obligaciones impone al subcontratista?
- ¿Informa sobre la ubicación física/territorial de sus activos? ¿podemos decidir las ubicaciones?

## Diligencia en la elección



- ¿Reúne el software los requisitos de la Disp. Ad. Primera del RLOPD?
- Las aplicaciones ¿son propias o las provee un tercero? ¿puede acceder a datos el tercero?
- ¿Cómo se contrata? ¿Condiciones generales de la contratación? ¿esta dispuesto a aceptar las exigencias dimanantes de la legislación española? ¿Reúne el contrato las condiciones del artículo. 12 LOPD?
- ¿Está en condiciones de cumplir con las exigencias normativas que debe garantizar el responsable del fichero?

# Subcontrataciones



- **Prohibición de subcontratación sin autorización expresa del responsable salvo que:**
  - Se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.
  - Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.
  - Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
  - Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato del art. 12 LOPD.
  - Si se da una subcontratación sobrevenida total o parcial no prevista en el contrato: debe someterse al responsable.

# Conservación, devolución, destrucción



- El encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto
- Regla general: destrucción o devolución de los datos personales al responsable una vez cumplida la prestación contractual.
- Devolución a otro encargado que hubiese designado el responsable.
- No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
- Bloqueo. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

**¿En qué país de la nube  
se encuentran los datos?**

# Tres escenarios



- 1. Los recursos se encuentran en España. Se aplica LOPD cuando:**
  - el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento
  - le sea de aplicación al responsable la legislación española en aplicación de normas de Derecho Internacional público
  - el responsable del tratamiento no este establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.
- Los recursos se encuentran en un EM: disposiciones nacionales si el tratamiento es efectuado por un establecimiento en el EM. Si hay varios establecimientos tienen que cumplir todos.
- Los recursos se encuentran en territorio del Espacio Económico Europeo: rigen los principios generales del artículo 12 LOPD.

# Transferencias internacionales de datos personales



- Los recursos se encuentran en un tercer país:
  1. Con un nivel de protección inferior al de España, se aplica el régimen general.
  2. Con un nivel de protección equiparable (Jersey, Isla de Man, Gernsey, Argentina, Canadá, Suiza, Islas Faroe, Andorra, Safe Harbor EEUU\*), se aplica el régimen general.
  3. Sin un nivel de protección equiparable.

\* La lista de entidades estadounidenses adheridas a los principios de “Puerto Seguro” está disponible en [www.export.gov/safeharbor](http://www.export.gov/safeharbor)

## Recursos situados en países terceros sin nivel adecuado



- Decisión 2001/497/CE, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país.
- Decisión 2004/915/CE, de 27 de diciembre de 2004 , por la que se modifica la Decisión 2001/497/CE, de 15 de junio de 2001.
- VERSIÓN CONSOLIDADA de la Decisión 2001/497/CE, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país
- Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010 , relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo

## Recursos situados en países terceros sin nivel adecuado



- **Binding Corporate Rules:** se autorizan transferencias internacionales de datos entre sociedades de un mismo grupo multinacional de empresas, cuando hubieran sido adoptadas normas o reglas internas vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español. **EN ESTUDIO RESPECTO DE ENCARGADOS**
  - WP 155 - Preguntas más frecuentes sobre BCRs.
  - WP 154 - Cuadro que establece la estructura de las BCRs.
  - WP 153 - Cuadro que establece la relación de los elementos y principios que deben contener las BCRs.
  - WP 108 - Modelo de solicitud de autorización de transferencia internacional basada en BCRs en el ámbito del procedimiento coordinado.
  - WP 107 - Documento sobre la competencia de las Autoridades de Control europeas en el procedimiento coordinado de aprobación las BCRs.
  - WP- 74 - Documento sobre la aplicación del artículo 26.2 de la Directiva 95/46/CE a las BCRs.

# Garantía de los derechos ARCO



- **Forman parte del núcleo esencial del derecho a la protección de datos.**
- **En ningún caso, las dificultades que puedan derivar del funcionamiento de los sistemas de Cloud Computing pueden justificar la no satisfacción de estos derechos.**

## Especial cautela en las **medidas de seguridad**

## **Las medidas que se imponen al encargado deben ser precisas**



### **Artículo 82. Encargado del tratamiento.**

#### **1. (...)**

**Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.**

**2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.**

**3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.**

## Especial atención



- Documentación formal del encargo en el documento de seguridad.
- Los niveles establecen un mínimo: **nada impide un plus de exigencia.**
- Existen elementos realmente críticos:
  - Formación de los usuarios del encargado.
  - Copias de seguridad.
  - Protección de los accesos a través de redes.
  - Protocolos de gestión y respuesta ante incidencias.
  - Controles de acceso y protección frente accesos indebidos de otros clientes y terceros proveedores.
  - Localización de los recursos.
  - Identificación y autenticación.
- Si es una Administración Pública: cumplimiento del esquema nacional de seguridad.

AGENCIA  
ESPAÑOLA DE  
PROTECCIÓN  
DE DATOS

