



Cloud Computing y Protección de Datos de Carácter Personal

Febrero 2012

José María de las Heras Montes
Vocal Junta Directiva

Como se puso de manifiesto en la 4ª sesión anual abierta de la AEPD celebrada el pasado 27 de enero, la seguridad en las arquitecturas de computación en nube se ha convertido en uno de los factores más críticos para la aceptación y desarrollo de estas nuevas arquitecturas en las organizaciones privadas y públicas. Para la Ingeniería en Informática el estudio de las soluciones de seguridad en estas nuevas arquitecturas ha de pasar a un primer plano para poder aprovechar, con confianza, las múltiples ventajas derivadas de este nuevo modelo de computación.

A. Resumen de los temas tratados en 4ª Sesión Anual Abierta de la AEPD

El pasado 27 de enero de 2012 se celebró, en los Teatros del Canal de Madrid, la 4ª Sesión Anual Abierta de la AEPD - Agencia Española de protección de Datos. La sesión se llevó a cabo en dos partes y estuvo llena de buenas noticias y novedades que fueron expuestas por su Director, D. José Luís Rodríguez Álvarez, en su intervención de apertura en la que destacó:

- La creciente concienciación ciudadana sobre la protección de sus datos y puso de manifiesto que las denuncias y reclamaciones de tutela recibidas en 2011 crecieron en torno a un 50% y un 34%, respectivamente, respecto a 2010.
- El nuevo marco de protección de datos en la UE presentado el 25/1/2012:
 - o nuevo reglamento; revisión de la Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995; integración del tercer pilar con una regulación específica.
 - o Se armoniza el régimen sancionados para toda la UE.
 - o Se reconocerá expresamente el derecho al olvido en Internet, *“algo que desde la AEPD hemos venido defendiendo e intentando materializar de forma continuada en los últimos años”*.
 - o Se exigirá que determinadas entidades dispongan de un responsable de protección de datos (DPO).
- Que ante las cuestiones que plantea el Cloud Computing para la protección de los datos, la AEPD está desarrollando iniciativas como la consulta pública abierta para conocer las necesidades de prestadores y usuarios en España.

Bajo el epígrafe "**Cloud Computing: Sujetos que intervienen, ley aplicable, garantías. Transferencias Internacionales de Datos**", la AEPD dedicó la primera parte de la sesión a dar su visión y recomendaciones para el cumplimiento de la LOPD y RLOPD en las nuevas "Arquitecturas de computación en Nube" o "Cloud Computing", y que por su mayor incidencia en la Ingeniería en Informática comentamos con mas detalle en el apartado (B) del presente resumen.

Antes de iniciar la segunda parte de la sesión, D. José Luís Rodríguez Álvarez hizo la entrega de los premios 2011 en protección de datos, destacando la gran labor de divulgación y promoción del derecho fundamental a la protección de datos, que a través de sus obras han realizado todos los premiados, así como la calidad de las candidaturas presentadas en esta edición, 19 candidaturas en el apartado de comunicación y 27 en el apartado de investigación.

La segunda parte de la sesión estuvo dedicada a presentar y comentar las "**Principales novedades y desarrollos en materia de protección de datos**":

D. Agustín Puente Escobar, Abogado del Estado Jefe del Gabinete Jurídico, comentó los **informes y sentencias relevantes** entre las que destacó:

- La sentencia del Tribunal de Justicia de la Unión Europea que resuelve las cuestiones prejudiciales planteadas por el Tribunal Supremo sobre la interpretación del artículo 7.f) de la Directiva Europea de Protección de Datos. Dicha sentencia proclama que el citado artículo tiene efecto directo en España y precisa el alcance del citado artículo, haciendo hincapié en la necesidad de ponderar caso a caso los derechos e intereses en conflicto
- La sentencia del Tribunal Supremo de 2 de diciembre de 2011, que si bien no cuestiona la sujeción de los órganos judiciales a la LOPD, establece que la competencia en este ámbito no corresponde a la Agencia sino al CGPJ, tanto en lo que respecta a los ficheros jurisdiccionales como a los no jurisdiccionales o gubernativos.

D. José López Calvo, Subdirector General de Inspección de Datos, comentó las **principales resoluciones y el nuevo régimen sancionador**:

- En 2011 la entrada de denuncias y reclamaciones de tutela creció frente a 2010 en aproximadamente un 50% y un 34,5 %, respectivamente.
- Durante los primeros meses de aplicación del nuevo régimen sancionador de la LOPD, entre el 3 de marzo y el 31 de diciembre de 2011, tras la entrada en vigor en marzo de 2011 de la Ley de economía sostenible, que introdujo la figura del apercibimiento, se dictaron 394 resoluciones sancionadoras y 284 apercibimientos, es decir, que el 42 % de los asuntos en los que se aprecia una infracción acabaron en apercibimiento, sin imposición de sanciones, atendiendo a los criterios para la aplicación de esta figura contenidos en la Ley.

D^a María José Blanco Antón, Subdirectora General del Registro de la AEPD, comentó el **régimen de transferencias internacionales de datos a encargados de tratamiento**. En su intervención comentó con gran detalle:

- Los requisitos del procedimiento de autorización.
- La flexibilidad del procedimiento de autorización:
 - o Decisión 2010/87/UE: la autoridad nacional puede adecuar las cláusulas contractuales para no desfavorecer a encargados del EEE.
 - o Partiendo de que los responsables de ficheros -clientes outsourcing- autorizan al encargado de tratamiento en España -prestador de servicios outsourcing- para que realice las transferencias internacionales de datos.
 - o La AEPD ha elaborado un nuevo modelo de cláusulas contractuales Encargado – Subencargado.
- Los requisitos de la solicitud de transferencias internacionales por el encargado.

D. Rafael García Gozalo, Coordinador del Área Internacional de la AEPD, informó de los importantes **Desarrollos internacionales**. Anunció que ya se había finalizado la propuesta del nuevo marco normativo europeo presentado por la Comisión Europea y que la opción final ha sido la reforma integral que incluye **Reglamento General sobre Protección de Datos y Directiva sobre materias policiales y judiciales**:

- El instrumento principal es un Reglamento, directamente aplicable en todos los estados miembro que aportará un marco uniforme para toda la UE, limitando el margen de desarrollo de los propios EEMM e incorporando muchas novedades que dan respuestas a las nuevas necesidades planteadas:

- incluye el nuevo criterio de tratamientos relacionados con oferta de bienes o servicios a ciudadanos de la UE o destinados a monitorizar su conducta para responsables sin establecimiento en la UE.
 - Clarificación de consentimiento
 - Nueva previsión sobre derecho al olvido
 - Principio de responsabilidad
 - Protección de datos “by design”
 - Inclusión de DPO
 - Inclusión de notificación de quebras de seguridad a APD e interesados.
 - Refuerzo de independencia de APD
 - Mecanismo de consistencia en actuación de APD
 - Armonización de poderes de APD, incluida potestad sancionadora
- Inicio del procedimiento legislativo ordinario
 - Modernización de la Convención 108

Ampliar información¹: **“The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age”**

Viviane Reding

Vice-President of the European Commission, EU Justice Commissioner

Al finalizar la segunda sesión se dio respuesta a las preguntas formuladas por escrito por los asistentes en la solicitud de inscripción.

La AEPD ha incluido en su sitio web² un apartado dedicado a la sesión³, en el que incluye: programa, informe de conclusiones, presentaciones de los ponentes y respuestas a las preguntas formuladas.

B. Cloud Computing: Sujetos que intervienen, ley aplicable, garantías. Transferencias Internacionales de Datos

Como se ha comentado en el apartado (A) D. José Luís Rodríguez Álvarez en su intervención de apertura comentó que ante las cuestiones que plantea el Cloud Computing para la protección de los datos, la AEPD está desarrollando iniciativas como la consulta pública abierta para conocer las necesidades de prestadores y usuarios en España. Esta consulta requiere dar a conocer los conceptos y definiciones fundamentales relacionadas con cloud computing, que la propia AEPD expone en sus formularios de consulta.

¹ <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26>

² <http://www.agpd.es>

³ http://www.agpd.es/portalwebAGPD/jornadas/4_sesion_abierta_2011/index-ides-idphp.php

B1. Definición operativa de "Cloud computing" - Computación en nube -

Existen muchas posibles definiciones de "cloud computing" que suelen coincidir en la mayor parte de las características que destacan. Aquí, y con el único propósito de establecer los términos de partida de esta consulta, se ha escogido la que proporciona el National Institute of Standards and Technology (NIST)⁴. Según esta definición, la computación en nube es un "modelo que permite, de forma práctica y desde cualquier ubicación, el acceso bajo demanda a una serie de recursos informáticos configurables compartidos (redes, servidores, sistemas de almacenamiento, aplicaciones y servicios), que pueden ser rápidamente dotados y puestos en funcionamiento con un mínimo esfuerzo de gestión e interacción con el proveedor de servicios".

Las principales características de la computación en nube serían, por tanto: Autoservicio bajo demanda; Acceso a través de la red; Agrupación de recursos; Flexibilidad; Servicio sujeto a medida; Pago por servicio.

Modelos de computación en nube

La prestación de servicios nube puede desplegarse según varios modelos. Los estudios al respecto difieren muy ligeramente entre sí. Una clasificación general, aceptada generalmente, puede ser la siguiente:

- **Nube pública:** es aquel tipo de cloud en el cual la infraestructura y los recursos lógicos están bajo el control del proveedor de servicios que la aloja, opera y gestiona, estando disponible para el público en general.
- **Nube privada:** de uso exclusivo para una organización, se crea generalmente con recursos propios de la empresa que lo implanta, que puede recibir ayuda de empresas especializadas.
- **Nube comunitaria:** un cloud comunitario se da cuando dos o más organizaciones integran una comunidad que comparte intereses e implementan una infraestructura cloud común, que se gestiona por una de ellas o por una tercera parte en su nombre.
- **Nube híbrida:** la infraestructura es el resultado de la combinación de varias de las anteriores, incluyendo los medios para la conexión y la portabilidad de la información entre las diferentes estructuras.

De igual modo, los servicios que pueden prestarse en nube son también variados, pudiendo agruparse en tres grandes tipos:

- **Software como servicio (SaaS),** donde el cliente utiliza las aplicaciones diseñadas por el proveedor del servicio sin tener capacidad para gestionar la infraestructura subyacente.
- **Plataforma como servicio (PaaS),** en la que el cliente utiliza aplicaciones diseñadas por él mismo o por un tercero utilizando la infraestructura de programación que pone a su disposición el proveedor, también sin una capacidad plena para gestionar la infraestructura.
- **Infraestructura como servicio (IaaS),** caso en el que el cliente dispone de recursos básicos de infraestructura gestionados por el proveedor sobre los que puede desplegar

⁴ <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

y utilizar recursos lógicos de nivel superior, incluidos sistemas operativos y aplicaciones.

Responsabilidades de los diferentes actores

Responsable del fichero: De acuerdo con la normativa española de protección de datos, el cliente que contrata servicios de cloud computing para el tratamiento de datos de carácter personal (fuera de la excepción de actividades personales o domésticas) asume las obligaciones inherentes al responsable de fichero.

Encargado del tratamiento: Por su parte, el proveedor del servicio, en la medida en que efectúa el tratamiento por cuenta del responsable, desempeñaría el rol de encargado del tratamiento.

No obstante, las posiciones relativas de cliente y prestador de servicios de computación en nube presentan unas características peculiares. ***Dependiendo del tipo de servicio en nube que se contrate y de los perfiles del cliente y del proveedor variará sensiblemente la posibilidad de que el cliente-responsable pueda impartir al prestador las instrucciones sobre el modo de tratar los datos a que se refiere la legislación.***

Ley aplicable

La legislación española establece que la ley aplicable a un tratamiento de datos será la española cuando el tratamiento se produzca en el marco de las actividades de un establecimiento del responsable situado en España o cuando el responsable no esté establecido en la Unión Europea pero utilice medios en territorio español. Por ello, la ley aplicable a la prestación de servicios de cloud computing sería, en principio, la española, cuando el cliente (responsable del tratamiento) esté situado en España. ***Sin embargo, una de las características esenciales de los servicios de computación en nube es que se prestan usualmente de forma descentralizada, con servidores y otros recursos situados en una pluralidad de países.***

Garantías

Según la normativa española de protección de datos, las relaciones entre el cliente-responsable y el prestador-encargado deben materializarse en un contrato de prestación de servicios. De acuerdo con la ley, es el responsable el que determina el contenido, especialmente en materia de medidas de seguridad. ***Sin embargo, las características de la prestación de servicios en un modelo de cloud hacen que varios de los elementos característicos de estos contratos de servicios deban ser tratados de forma diferente a como sucede habitualmente.***

La normativa española prevé que el responsable conocerá y autorizará, en uno u otro momento, todas las subcontrataciones y, en todo caso, que conocerá quiénes son las entidades con las que se subcontrata la prestación. ***En el modelo de computación en nube, puede ser muy frecuente no sólo que el primer prestador ignore qué entidades van a participar en cada momento en el tratamiento sino, también, que esas entidades varíen con gran frecuencia, de forma que no sea posible notificar al responsable todos los cambios en los tiempos que marca la normativa.***

Transferencias internacionales

El tratamiento de datos mediante el uso de servicios en nube implicará, con mucha frecuencia y por la propia naturaleza de este modo de prestación, la existencia de transferencias internacionales con origen en territorio español. La normativa española de protección de datos prevé que puedan realizarse transferencias internacionales a países que ofrezcan un nivel adecuado de protección.

Cuando el país destinatario no ofrezca ese nivel adecuado, las transferencias podrán autorizarse si:

- Concurre alguna de las excepciones legalmente previstas (consentimiento del interesado, transferencia necesaria para la ejecución de un contrato, etc.) o
- El responsable ofrece garantías adecuadas. El responsable podrá aportar esas garantías mediante la presentación de un contrato (especialmente si el mismo incluye las cláusulas tipo aprobadas por la Comisión Europea) o, en los casos en que las transferencias se produzcan en el seno de grupos multinacionales, de normas corporativas vinculantes (BCR) que hayan sido adoptadas por esos grupos.

Estos mecanismos están básicamente diseñados para transferencias que siguen un esquema clásico, en el que se conoce el país o países a los que se van a exportar los datos y la entidad o entidades que los van a recibir. Las últimas cláusulas contractuales tipo aprobadas por la Comisión Europea y las BCR son un intento de responder a la indeterminación que sobre algunos de estos elementos ha propiciado la evolución de los flujos internacionales de datos, ofreciendo instrumentos que permiten gestionar transferencias a una pluralidad de destinatarios siempre que se encuentren en un mismo grupo y estén ligados por unas reglas comunes de protección de datos y subcontrataciones no previstas en el momento en que se autorizó la primera transferencia.

El modelo de cloud computing, por su propia naturaleza, implica en muchos casos el desconocimiento del país preciso en que los datos van a ser tratados y de las entidades (subcontratadas) que van a intervenir en ese tratamiento. Más importante aún, la flexibilidad del modelo supone que países y entidades pueden variar constantemente de forma no predecible en el momento en que se produce la contratación del servicio y debe decidirse la utilización del instrumento jurídico más adecuado al tipo de transferencia que se va a producir.

B2. Consideraciones sobre la seguridad en modelos de computación en nube

Como es lógico la AEPD no se plantea, en el ámbito de sus competencias, pronunciarse a este respecto. Así podemos observar en los párrafos precedentes cómo sus primeros análisis se dirigen a analizar, a la luz de la de la legislación española y de la UE los posibles criterios para poder cumplir con dicha legislación:

- LOPD, RLOPD, Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, Binding Corporate Rules basadas en WP 153, WP154, WP155, WP108, WP107, WP74 del Grupo de Autoridades Europeas de Protección de Datos art. 29, etc.

Hay aspectos, expuestos por la propia AEPD ya comentados en (B1) que ponen de manifiesto la mayor dificultad de cumplimiento/aplicación de las medidas de seguridad exigibles por la LOPD en los modelos cloud computing, o incluso la imposibilidad de cumplirlas en algunos de los posibles. En el siguiente apartado (B3) se resume lo expuesto por la AEPD a este respecto.

No es objeto de este documento entrar en los detalles de requisitos y especificaciones de seguridad, pero si constatar que las leyes deberían tenerlos en cuenta en los modelos de cloud computing que sean utilizados para el tratamiento de datos de carácter personal. Son diversas las alternativas al respecto que podrían pasar:

- Por una legislación específica aplicable a las nuevas figuras que representan las nuevas organizaciones proveedores de servicios cloud computing y en cuyo marco se contemplen las exigencias de seguridad. Hemos de ser conscientes que en el modelo cloud computing la seguridad también es un servicio.
- Una definición precisa de las medidas de seguridad suplementarias que pudieran ser exigibles a los modelos de cloud computing cuando sean utilizados para tratar datos de carácter personal que podrían recogerse en el RLOPD
- Definición de estándares internacionales para el modelo cloud computing como podrían ser: Código de buenas prácticas en cloud computing, auditorías, certificaciones de cumplimiento, etc. Es en esta última opción en la que actualmente más se está trabajando. Así en Reino Unido el **Cloud Industry Forum** ha desarrollado un Código de buenas prácticas para Proveedores de Servicios Cloud⁵ y en la UE se va a crear una Alianza Europea de Cloud Computing⁶ que impondrá unos requisitos comunes para la adquisición de las ofertas cloud, además de llegar a estándares que garanticen la seguridad y la competencia Así mismo la organización **Cloud Security Alliance**⁷ puede considerarse como la organización internacional más destacada en el desarrollo de buenas prácticas de seguridad y cumplimiento en cloud computing. Los trabajos que está desarrollando son de mayor alcance e incluyen: formación, investigación, estudios, publicaciones, certificaciones, foros, convenciones, etc. Su capítulo en España ha publicado el documento "**Cloud Compliance Report**"⁸ que aborda con detalle el tema que estamos tratando.

Dar solución a estas necesidades está estrechamente relacionado con el propio desarrollo y aceptación de cloud computing por las organizaciones privadas y públicas como muestran los estudios realizados al respecto. Por la estrecha relación entre virtualización y cloud computing podemos citar el estudio independiente encargado por CA Technologies:

Security – an essential prerequisite for successful virtualization⁹

© KuppingerCole, IT Analysts, 2010 - Author: Martin Kuppinger

⁵ <http://www.cloudindustryforum.org/code-of-practice-for-cloud-service-providers>

⁶ <http://www.idg.es/computerworld/La-nueva-estrategia-cloud-de-la-Union-Europea-conv/seccion-actualidad/articulo-205596>

⁷ <https://cloudsecurityalliance.org/csa-news/csa-issues-first-cloud-compliance-report-for-spain/>

⁸ http://www.bdigital.org/Documents/Cloud_Compliance_Report_CSA-ES.pdf

⁹ http://www.kuppingercole.com/report/ca_study_virtualization2010

Estudio comentado en los medios de comunicación: ***“La gestión inadecuada de la seguridad pone en riesgo los entornos virtuales”***¹⁰.

Como se señala en el informe, el modelo cloud computing se basa en la virtualización y los primeros problemas de seguridad a resolver los encontramos en la virtualización. Estos problemas se amplifican al pasar al modelo cloud computing. En el informe al que hacemos referencia las organizaciones privadas y públicas así lo manifiestan:

- Las tecnologías y políticas de seguridad de la virtualización aplicadas actualmente en las organizaciones no están tratando suficientemente los privilegios del hipervisor y la dispersión de los datos. El 81 por ciento de los encuestados considera esta última como una amenaza "muy importante" o "importante", ya que encierra el riesgo de que la información viaje sin control por los entornos virtualizados y pueda terminar en entornos menos seguros.
- Al 73 por ciento de las empresas le preocupan los amplios privilegios de los administradores de los hipervisores, puesto que podrían dar lugar a errores o abusos por parte de esos usuarios privilegiados. Y es que la cuenta de administración del hipervisor tiene amplios privilegios de acceso con muy pocas limitaciones o controles de seguridad.
- El estudio también revela que existen demasiadas actividades de seguridad que siguen dependiendo de procesos manuales que se llevan a cabo sin el apoyo de la tecnología, lo cual pone en riesgo la seguridad de la organización.
- Si bien el principal motor de la virtualización es la mejora de la eficiencia operativa de las TI, citada por el 91 por ciento de los encuestados, la seguridad es también una preocupación importante de cara a su adopción; hasta tal punto que el 39 por ciento de las organizaciones cree que los entornos virtuales son más difíciles de asegurar que los físicos.
- La mitad de las organizaciones consultadas ha implementado o está implementando la integración entre gestión de cambios y configuraciones y gestión de la seguridad TI. Sin embargo, la tasa de implementación de otros elementos importantes en los tres ámbitos fundamentales ("integración de la seguridad de la virtualización con gestión de incidentes y problemas", "niveles de servicio en la gestión de la seguridad de la virtualización" y "gestión del rendimiento de los servicios de seguridad",) está por debajo del 50 por ciento de forma general. "Esta integración es un reto importante para las infraestructuras de TI ágiles y debe ser uno de los criterios de decisión clave en la elección de los proveedores de TI, tanto en los segmentos de gestión TI como de gestión de la seguridad".

Y los problemas de seguridad ponen freno a las nubes privadas

- Se preguntó a los participantes sobre sus planes para evolucionar desde su entorno virtual a una nube privada. En este caso, los principales inhibidores para avanzar a una

¹⁰ <http://www.boletindintel.es/BoletinesAVS/Publico/PresentaContenido.php?Fase=1%20%&%20Referencia=1473>

estrategia de cloud privada fueron “los aspectos relacionados con las normas de cumplimiento y privacidad en la nube” y “los aspectos relativos a la seguridad cloud”, citadas por cerca del 85 por ciento.

- En un tono más positivo, el estudio muestra la concienciación en la organización de que la seguridad, y en particular la gestión de identidades y accesos, así como la gobernanza, riesgo y cumplimiento, son requisitos previos para una exitosa estrategia de cloud computing

La Ingeniería en Informática, junto con las organizaciones y centros de investigación especializados en cloud computing, debe asumir la responsabilidad de dar respuestas y soluciones a las necesidades integrales de seguridad en los modelos de cloud computing y analizar los requisitos de seguridad y limitaciones a tener en cuenta para que cuando las organizaciones públicas o privadas decidan utilizarlos, lo puedan hacer de forma segura y con garantías de cumplimiento de la legislación vigente, en particular LOPD, RLOPD y además el Esquema Nacional de Seguridad – ENS en las organizaciones públicas.

El modelo cloud computing, es en la actualidad uno de los centros de atención más importante que impulsa la investigación y desarrollo de nuevas tecnologías informáticas. Aprovechar sus grandes ventajas pasa, obligatoriamente, por hacerle un modelo de computación seguro.

B3. CLOUD COMPUTING: Sujetos que intervienen, Ley aplicable, Garantías

D. Jesús Rubí Navarrete, Adjunto al Director, expuso, forma muy brillante, los criterios que bajo las exigencias de la LOPD y el RLOPD debemos considerar al optar por el nuevo modelo:

- Las modalidades de computación en nube (Privada, Pública, Híbrida, Comunitaria y las modalidades de servicios: Infraestructura como servicio (IAAS), Plataforma como servicio (PAAS), Software como servicio (SAAS) condicionan la aplicación de la LOPD.
- Formular reflexiones generales que han de adaptarse a dichas modalidades.

Posición jurídica:

El cliente como responsable del tratamiento:

- Decisión sobre la finalidad, contenido y uso del tratamiento (Art. 3.d) LOPD)
 - Decisión sobre optar por la computación en nube (total o parcial)
 - Decisión sobre la modalidad de computación en nube (en particular sobre TID)
 - Decisión sobre las modalidades de servicios de computación en nube
- Responsabilidad sobre el tratamiento de los datos Personales
- El Proveedor de Cloud Computing CCP como encargado de tratamiento

Consecuencias de la posición jurídica de los intervinientes:

- Ley aplicable: La ley nacional del responsable/cliente (art. 2.1.a) LOPD) (Salvo medidas de seguridad en otro Estado miembro de la UE)
- Inexistencia de obligación de informar a los interesados

- Garantías contractuales ex art. 12 LOPD

Cambio de paradigma:

- La relación tradicional responsable/encargado (art. 12 LOPD)
 - Instrucciones del responsable (Cliente) al encargado (CCP)
 - No comunicación a terceros ni siquiera para su conservación
 - Estipulación de las medidas de seguridad a implementar por el encargado
 - Destrucción o devolución de datos al término de la prestación.

El contrato entre el Cliente y el CCP debe recoger con el mayor detalle las instrucciones, es decir el Cliente es el responsable de realizar un análisis de los requisitos de seguridad teniendo en cuenta el modelo de cloud computing que va a contratar y recogerlas en el contrato.

- Los criterios tradicionales en la subcontratación (art. 21.2 RLOPD y STS de 15 de julio de 2010)
 - Especificación de los servicios a subcontratar
 - Indicación de las empresas subencargadas
 - Autorización del responsable/cliente sobre los subencargados
 - Contrato entre encargados y subencargados
- Autonomía del CCP
- Contratos de adhesión (propuestos por el CCP)
- Selección subencargados (proceso dinámico)
- Oferta de medidas de seguridad (propuestas por el CCP)
- Opción sobre transferencias internacionales de datos TID

Modular la normativa aplicable: Transparencia

Diligencia exigible al responsable (mayor intensidad):

- Velar por que el encargado (CCP) reúna las garantías exigibles (art. 20.2 RLOPD)
 - Obtener información sobre las garantías del contrato conforme al art. 12 LOPD
 - Ejercer diligentemente su posición de responsable sobre el tratamiento de los datos de los interesados
- Ejercicio de derechos ARCO (debe estar estipulado en el contrato)
- Responsabilidad por daños (el contrato también deberá tenerlos en cuenta)
- Deberes de diligencia de oficio exigible al encargado y que el CCP informe al cliente.
 - Información detallada sobre la tipología de computación en nube y de servicios que ofrece (tipología de nube, tipología de servicios, participantes en la prestación de servicios, TID).
 - Información sobre medidas de seguridad (niveles de seguridad, auditoría, cifrado, incidencias de seguridad).

- La literalidad de las medidas de seguridad pasa a la funcionalidad (análisis funcional de la seguridad y no estrictamente formal, tener en cuenta los estándares internacionales disponibles sobre seguridad).
- Información sobre portabilidad

Instrucciones del responsable (cliente) teniendo en cuenta:

- Selección del tipo de computación en nube y de los servicios a contratar.
- Decisión sobre los tratamientos que no se contratan al CCP (naturaleza de la información, posible pérdida de control,...).
- Decisión sobre la información solicitada y/o ofrecida por el CCP.

Medidas de seguridad:

- Auditoría externa e independiente (incluso cuando no se exijan medidas de seguridad de nivel medio).
- Comunicación de las incidencias de seguridad que afecten al cliente/responsable

Portabilidad (art. 20.3 RLOPD)

- Devolución o migración a un nuevo prestador de servicios designado por el responsable

Modular la normativa aplicable: Subencargado del tratamiento

- Autorización previa sobre empresas subencargadas
 - Especificación funcional de los servicios susceptibles de subcontratación
 - Especificación de los niveles de calidad exigibles
 - Relación actualizada de entidades subencargadas (p.ej. Accesible en sitio web con indicación de países en que opera)
 - Tipología de garantías a exigir (incluidas TID)
- Contratos jurídicamente vinculantes en todos los procesos de tratamiento, conforme a la ley aplicable (responsable/encargado. Encargado/subencargado).
- Posibilidad de actuación de la AEPD.

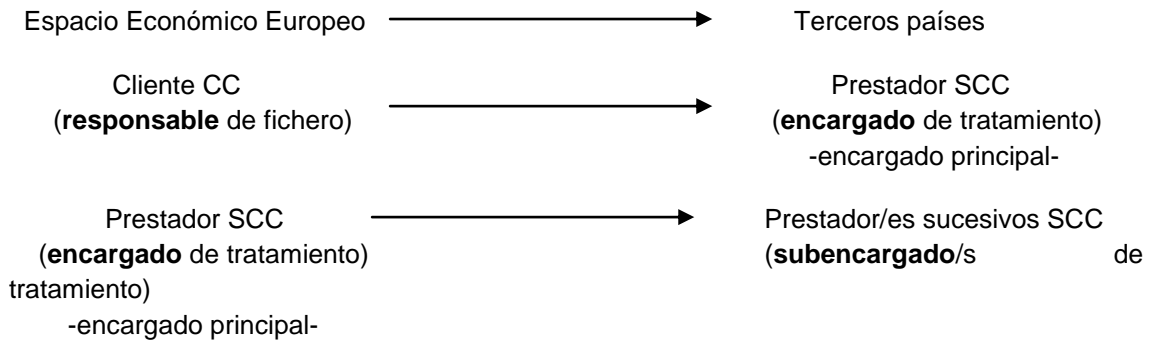
CLOUD COMPUTING: Transferencias Internacionales de Datos (TID)

D^a María José Blanco Antón, Subdirectora General del Registro General de Protección de Datos, profundizó en la problemática que plantea el cloud computing en las TID así como en los criterios a tener en cuenta.

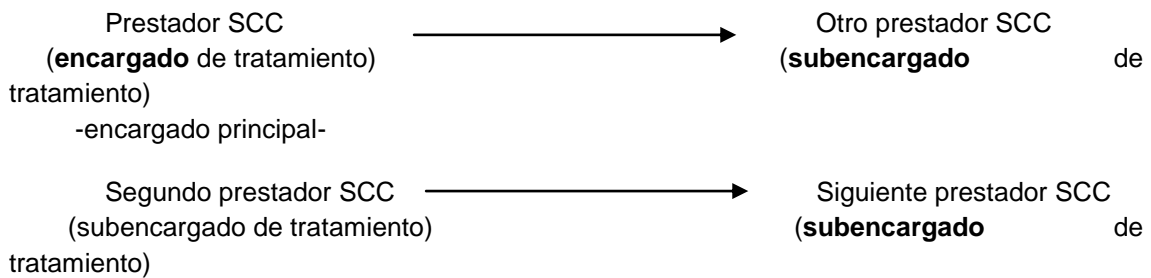
Ubicuidad: una de las características de cloud computing es la ubicuidad de los recursos informáticos: acceso desde cualquier lugar, almacenamiento y tratamiento en cualquier lugar.

Transferencia internacional de datos: *“tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo” para “la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español” - art. 5.1.s) RLOPD.*

Los supuestos de TID en cloud computing podemos esquematizarlos:



También hemos de tener en cuenta las TIC entre SSCs ubicados en terceros países



En el escenario de las TID el nivel adecuado de protección está establecido por Decisión de la Comisión Europea. Este nivel adecuado también alcanza a los países: Suiza, Argentina, Canadá, Guernsey, Isla de Man, Islas Feroe, Jersey, Andorra e Israel y entidades de EEUU adheridas a Puerto Seguro/Safe Harbor. Para Terceros países, distintos a los indicados, se requiere de la autorización de la AEPD.

El nivel adecuado de protección se plasma mediante los modelos de garantías a aplicar:

- Contrato de prestación de servicios (art.12 LOPD, arts. 20-22 RLOPD entre el responsable (cliente CC) y el encargado (prestador SCC)
 - Garantías de protección de datos.
 - En caso de subcontratación se requiere del encadenamiento de garantías de protección de datos y de la autorización y/o conocimiento de la subcontratación por parte del Responsable.

- En cloud computing es necesario obtener información sobre los posibles destinatarios de transferencias ulteriores, o disponer de acceso a dicha información. El prestador SCC puede mantener actualizada y disponible la relación de los mismos.

Las autorizaciones de TID a terceros países deben ser autorizadas por la AEPD y se tramitan según el RLOPD, en un periodo tres meses según:

Las solicitudes de autorización del Director de la Agencia requieren:

- Contrato cláusulas contractuales tipo – Decisión 2010/87/UE
- Ofrecer garantías en la transferencia de EEE al tercer país
- Cláusula 11, subcontratación del encargado – importador
 - Encadenamiento de garantías de protección de datos.
 - Autorización y conocimiento de la subcontratación por parte del Responsable.
 - Información de los subencargados disponible para la AEPD.

Hasta la fecha la AEPD ha autorizado todas las solicitudes recibidas según los requisitos indicados.

Para corporaciones multinacionales con necesidades de transferencias internacionales de datos entre empresas del Grupo, y cuyos responsables son las mismas empresas el modelo de garantías a aplicar esta recogido en - Binding Corporate Rules (BCRs) - **Reglas corporativas vinculantes**, basadas en WP 153, WP154, WP155, WP108, WP107, WP74 del Grupo de Autoridades Europeas de Protección de Datos art. 29. Este **modelo permite a las corporaciones desarrollar sus nubes privadas de Grupo**.

Tomando como referencia la experiencia de las BCRs el pasado 10 de Enero de 2012 el Grupo de Autoridades Europeas de Protección de Datos art. 29 ha constituido un subgrupo para desarrollar **las Binding Processor Rules – BPRs** (equivalente WP153 BCR) que crearan un marco general de garantías aplicables en cloud computing:

- Principios de privacidad en las BPRs
- Fórmula de autorización de subcontrataciones
- Sistema de gestión de reclamaciones de interesados
- Acceso a las auditorías de las BPRs por parte del responsable

Conclusiones:

Cloud Computing es el modelo de computación en el que se basarán la mayoría de servicios de la Sociedad de la Información. De hecho ya se están ofreciendo muchos servicios con este modelo. Puesto que cloud computing utiliza y optimiza los recursos y capacidades disponibles en Internet, su seguridad no se plantea en un contexto local sino global. Como se ha intentado presentar en este documento los principales actores, desde los ángulos legal, de proveedores de servicios y proveedores de tecnológicos ya están trabajando intensamente para permitir el desarrollo de un cloud computing seguro. **Felicitar a la AEPD que en la 4ª sesión anual abierta y con las iniciativas que está llevando a cabo, nos ha mostrado ser uno de los principales actores legales europeos decidido a desarrollar un cloud computing seguro.**