SEMINARIO
LA PRIVACIDAD EN EL ÁMBITO DE LAS TECNOLOGÍAS DE LA SALUD, LA HISTORIA CLÍNICA ELECTRÓNICA

Santa Cruz de la Sierra, Bolivia
21 a 23 de octubre de 2014

LOS SERVICIOS DE CLOUD COMPUTING EN EL CAMPO DE LA SALUD

Jesús Rubí Navarrete

Adjunto al Director

Agencia Española de Protección de Datos

CLOUD COMPUTING

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

POSICIÓN JURÍDICA DE LOS INTERVINIENTES

- **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 (no se desplaza la responsabilidad)**
  - **El CCP como encargado de tratamiento**

POSICIÓN JURÍDICA DE LOS INTERVINIENTES

- **Consecuencias de la posición jurídica de los intervinientes:**
  - **Ley aplicable: La ley nacional del responsable/cliente (art. 2.1.a) LOPD)**
  - **La fragmentación y encriptación de los datos**
  - **Garantías contractuales ex art. 12 LOPD**

CAMBIO DE PARADIGMA

- **La relación tradicional responsable/encargado (art. 12 LOPD) no responde al modelo cloud computing**
  - **Instrucciones del responsable al encargado**
  - **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**

CAMBIO DE PARADIGMA: SUBCONTRATACIÓN

- **Los criterios tradicionales en la subcontratación (art. 21.2 RLOPD y STS de 15 de julio de 2010) no responden al modelo cloud computing**
  - **Especificación de los servicios a subcontratar**
  - **Indicación de las empresas subencargadas**
  - **Autorización del responsable/cliente sobre los subencargados**
  - **Contrato entre encargados y subencargados**

CAMBIO DE PARADIGMA

- **Autonomía del CCP**
- **Contratos de adhesión**
- **Selección subencargados (proceso dinámico)**
- **Oferta de medidas de seguridad**
- **Opción sobre TID**

MODULAR LA NORMATIVA APLICABLE: TRANSPARENCIA

- **Diligencia exigible al responsable:**
  - **Velar por que el encargado 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**

MODULAR LA NORMATIVA APLICABLE: TRANSPARENCIA

- **Diligencia exigible al encargado (de oficio):**
  - **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, encriptación, incidencias de seguridad<u>). Análisis funcional, no estrictamente formal</u>**
  - **Información sobre portabilidad**

MODULAR LA NORMATIVA APLICABLE: TRANSPARENCIA

- **Instrucciones del responsable:**
  - **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**

MODULAR LA NORMATIVA APLICABLE: TRANSPARENCIA

- **Medidas de seguridad:**
  - **Auditoria 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 (Notificación brechas de seguridad)**
- **Portabilidad (art. 20.3 RLOPD)**
  - **Devolución o migración a un nuevo prestador de servicios designado por el responsable**

MODULAR LA NORMATIVA APLICABLE: SUBENCARGADO

- **Autorización previa sobre empresas subencargadas**
  - **Especificación funcional de los servicios susceptibles de subcontratación (p.ej. hosting)**
  - **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 vinculante en todos los procesos de tratamiento, conforme a la ley aplicable (responsable/encargado. Encargado/subencargado)**
- **Posibilidad de actuación de la AEPD**

ESCENARIOS DE TRANSFERENCIAS INTERNACIONALES

- **NIVEL ADECUADO DE PROTECCIÓN**
  - **Establecido por Decisión de la Comisión Europea**
  - **Suiza, Argentina, Canadá, Guernsey, Isla de Man, Jersey, Andorra, Israel y Uruguay**
  - **ENTIDADES DE EEUU ADHERIDAS A PUERTO SEGURO/SAFE HARBOR**
- **TERCEROS PAÍSES (Clausulas contractuales, BCR,s)**

ADHERIDOS A PUERTO SEGURO

- **La prestación de servicios desde Estados Unidos a una empresa española supone TID.**
- **Las entidades estadounidenses adheridas a Safe Harbor tienen reconocido por la Comisión un adecuado nivel de protección (Decisión 2000/520/CE).**
- **Esta TI no requiere autorización del Director de la Agencia.**
- **Requiere un contrato de prestación de servicios (art. 12 LOPD y arts. 20-22 RLOPD, FAQ nº 10 Decisión 2000/520/CE)**
- **El contrato de prestación de servicios puede autorizar la subcontratación.**
- **El principio de transferencias ulteriores de Safe Harbor limita al prestador de servicios la subcontratación a otras entidades adheridas a Safe Harbor o mediante un contrato que exija el cumplimiento de los principios de protección de datos (encadenamiento de garantías)**

Clausulas contractuales tipo (Decisión 2010/87/UE)

- **Consulta AEPD sobre adecuación a Decisión:**
  - **Auditoria por tercero independiente**
  - **Contrato único con subencargados**
- **Conclusiones:**
  - **Son garantías adecuadas TID**
  - **No amparadas por Decisión 2010/87/UE**
  - **Auditoría (cláusula 5.f), cláusula 12.2, WP 196 apartado 4.1): Capacidad de control por responsable**
  - **Contrato único (cláusula 11,WP 176). Exclusión**
  - **Posible autorización por APD nacional (Apartado 5 Preámbulo Decisión 2010/87/UE)**

SUBCONTRATACIÓN
ENCARGADO - SUBENCARGADO

- **Decisión 2010/87 (Considerando 23)**
- **Marco contractual que comprende dos contratos**
- **Contrato responsable-encargado:**
  - **Suscrito caso a caso por el responsable/cliente**
  - **Remisión a garantías del contrato autorizado para TID**

SUBCONTRATACIÓN
ENCARGADO - SUBENCARGADO

- **Contrato responsable – encargado/exportador en UE. Garantías**
  - **Ley aplicable: Ley del responsable**
  - **Autorización para subcontratar y TID**

- **Contrato encargado/exportador – Subencargado en tercer país**
  - **Encargado del tratamiento: Exportador autorizado por AEPD**
  - **El responsable no es parte del contrato**
  - **Autoriza TID, incluidas futuras TID (Condiciones generales de contratación):**
    - **Potenciales responsables/clientes**
    - **Nueva autorización innecesaria**

SUBCONTRATACIÓN ENCARGADO - SUBENCARGADO

- **Garantías Decisión 2010/87 adaptadas:**
  - **Ley aplicable: Ley del responsable**
  - **Información sobre subencargados ulteriores**
  - **Clausula de tercero beneficiario**
  - **Cooperación con AEPD**

- **Posibilidad de autorizar condiciones generales de contratación adaptados a los modelos de negocio de cloud computing (encargado principal UE, encargado principal tercer país y subencargados en terceros paises)**

CONCLUSIONES EN LA GUIA Y DIRECTRICES SOBRE CLOUD COMPUTING

CLOUD COMPUTING

- **Introducción sobre cloud computing**

- **Tipos de cloud computing (neutralidad)**
  - **Nube pública, nube privada, otros modelos**
- **Modalidades de servicios**

  - **Software como servicio, infraestructura como servicio, plataforma como servicio**

ASPECTOS DESTACADOS

- **Portabilidad (facilidad para transferir datos y aplicaciones de un proveedor a otro)**
  - **Soluciones abiertas o cerradas**
  - **Causas:**
    - **Finalización por cliente**
    - **Finalización por prestador (cambio de política comercial o del marco regulatorio)**

- **Localización**
  - **Subcontratación**
  - **Localización de los recursos para la prestación del servicio (TID)**

ASPECTOS DESTACADOS

- **Transparencia**
  - **Oferta de información sobre donde, cuando y quien procesa datos.**

- **RIESGOS**
  - **Falta de transparencia**
  - **Falta de control**

- **GARANTÍAS CONTRACTUALES (Responsable-Encargado)**

- **ESTRATEGIA PARA EL CLIENTE**
  - **Evaluar los tratamientos y la sensibilidad de los datos:**
    - **Análisis de los tratamientos a transferir a la nube**
  - **Verificación de las condiciones de prestación del servicio (aspectos tecnológicos, económicos y legales)**
    - **Lista de control (12 preguntas)**

LO QUE DEBO CONOCER
PARA LA CONTRATACIÓN DE “CLOUD COMPUTING”

- **Antes de contratar:**
  - **Evaluar la tipología de datos y los niveles de seguridad**
  - **Información sobre los tipos de nube y de servicios (incidencia en la protección de datos personales)**
  - **Seleccionar los servicios y el prestador**

- **Responsabilidad del cliente**
  - **El cliente es responsable del tratamiento**
  - **El prestador de servicios es encargado del tratamiento**
  - **La responsabilidad no se desplaza contractualmente**

- **Legislación aplicable**
  - **Ley aplicable al responsable (LOPD)**
  - **No se modifica contractualmente**
  - **La fragmentación y encriptación no excluyen la aplicación de la ley (Dictamen 05/2012 – WP 196- sobre computación en nube. Nota a pie de página nº 27)**

- **Obligaciones en subcontratación (modulación)**
  - **Obtener información sobre subcontratistas**
  - **Dar su conformidad (al menos delimitando genéricamente los servicios)**
  - **Poder conocer a los subcontratistas (p.ej. Acceso a web)**
  - **Garantías contractuales entre el prestador y los subcontratistas**

- **Localización de los datos**
  - **UE/EEE. Cesiones de datos**
  - **Terceros países: TID**

- **Garantías para TID**
  - **Nivel adecuado de protección (enlace a países)**
  - **Acuerdo de Puerto Seguro con empresas EEUU (Para prestación de servicios, garantías contractuales)**
  - **Otras garantías contractuales (información adicional)**
  - **Diligencia para conocer si hay TID,s y con qué garantías (requerimientos de información por autoridades de terceros países)**

- **Medidas de seguridad (modulación)**
  - **Conocer los niveles de seguridad exigibles (información adicional)**
  - **Certificación de seguridad adecuada**
  - **Auditoria por tercero independiente y confiable**
  - **Diligencia para informarse sobre las medidas de seguridad que se ofrecen y sobre su cumplimiento**
  - **Conocer los incidentes de seguridad sobre los datos de los que es responsable**

- **Garantías de confidencialidad**
  - **Tratamiento de datos sólo para la prestación del servicio**
  - **Compromiso de confidencialidad del personal del prestador**

- **Garantías de portabilidad**
  - **Devolución a sus propios sistemas o migración a un nuevo proveedor**
  - **Formato que permita su utilización en plazo breve y garantizando la integridad**

- **Garantías sobre el borrado de los datos (certificación de destrucción)**

- **Garantías para el ejercicio de derechos ARCO**
  - **Información y cooperación de prestador de servicios**

- **Garantías contractuales en la contratación y subcontratación (RD Legislativo 3/2011)**
- **Solicitudes de acceso a la información por autoridades de terceros países**
- **Esquema nacional de seguridad (RD 3/2010)**
  - **Análisis y gestión de riesgos (Análisis de amenazas, controles y salvaguardas)**
  - **Profesionalidad (seguridad atendida, revisada y auditada por personal cualificado)**

- **Protección información almacenada y en transito (técnicas robustas de cifrado y copias de respaldo)**

- **Incidencias de seguridad y continuidad de la actividad**

- **Auditorias de seguridad ordinarias y extraordinarias (art. 34 ENS)**

- **Esquema Nacional de Interoperabilidad (RD 4/2010)**
  - **Portabilidad de datos entre servicios y ejercicio de derechos de los ciudadanos mediante formatos estandarizados**
    - **Estándares abiertos**
    - **Neutralidad evitando discriminación por razones de la elección tecnológica**

- **Remisión a las preguntas**
- **Responsable del contrato (Art. 52 RDL 3/2011)**
  - **Recomendable en función de la complejidad de los servicios**

Orientaciones para prestadores de servicios

- **Desequilibrio entre las partes**

- **Posición jurídica de las partes**
  - **Responsable**
  - **Encargado**
  - **Ley aplicable (LOPD)**

- **Diligencia**

- **Transparencia**
  - **Atender solicitudes de información del cliente (remisión a preguntas de la guía)**
  - **Ofrecer información “de oficio”**
  - **Valoración por AEPD**

Orientaciones para prestadores de servicios

- Garantías exigibles a los “partners”
- Modulación de las garantías tradicionales
- Portabilidad
- TID
- Ejercicio de derechos ARCO
- Administraciones públicas

- ORIENTACIONES A TENER EN CUENTA
  - Revisar sus contratos
  - Adaptarlos, en su caso, informando a sus clientes
  - Ser conscientes de que pueden ser responsables por incumplimiento

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es