Comité de la Comunidad Valenciana

itSMF ESPAÑA

ISACA Sistemas de información fiables y valiosos

Valencia Chapter

Cloud vs. ISO20K & 27K "sin llegar a las manos"

21 de Junio de 2012

"Algunos aspectos jurídico-internacionales del Cloud Computing"

Héctor Guzmán Rodríguez

Abogado en TI

itSMF

A efectos prácticos… ¿por qué nos interesan los aspectos jurídicos del Cloud Computing?

¿Las empresas deben preocuparse de este tema?

¿Por qué debemos considerarlo relevante?

SEGURIDAD DE LA INFORMACIÓN

TRATAMIENTO DE DATOS PERSONALES

Reglamento de la Ley Federal de Datos Personales de Posesión de los Particulares (México)

Para fines de dicho Reglamento, por cómputo en la nube se entenderá:

El modelo de provisión externa de servicios de cómputo bajo demanda,
que implica el suministro de
infraestructura,
plataforma o
software,
que se distribuyen de modo flexible,
mediante procedimientos de virtualización,
en recursos compartidos dinámicamente.

Tratamiento de datos personales en el denominado cómputo en la nube

Artículo 52. *Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor* cumpla con determinadas condiciones y cuente con determinados "mecanismos".

Condiciones que, al menos, debe cumplir el proveedor:

- Contar con políticas de protección de datos, afines a la LFPD y su Reglamento,
- Que exista transparencia de las subcontraciones relacionadas con el servicio,
- Que no existan disposiciones contractuales que le permitan asumir la titularidad de la información, y
- Deber de confidencialidad respecto de los datos tratados.

El proveedor debe contar con mecanismos, al menos, para:

- ❑ Comunicar cambios en su PP y condiciones del servicio,
- ❑ Permitir al responsable limitar el tipo de tratamiento,
- ❑ Establecer y mantener medidas de seguridad “adecuadas”,
- ❑ Garantizar la supresión y recuperación de los datos, e
- ❑ Impedir el acceso no autorizado a los datos (o **informar** si el acceso se otorga con motivo de solicitud de autoridad competente).

International Working Group on Data Protection in Telecommunications

Grupo de Berlín

Grupo de Trabajo fundado en 1983 en el marco de la Conferencia Internacional de Protección de Datos y Privacidad, por iniciativa del Comisario de Protección de Datos de Berlín, que desde entonces ha presidido el Grupo.

Documento de Trabajo sobre Cloud Computing – Aspectos de privacidad y protección de datos

(*Working Paper on Cloud Computing - Privacy and data protection issues*) "Memorándum Sopol"

Sopot, Polonia, 24 de abril de 2012

Algunos aspectos jurídico-internacionales del Cloud Computing

El Memorándum Sopot adopta como un (excelente) punto de partida para la investigación y uso del Cloud Computing (CC) la definición emitida en septiembre de 2011 por el Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de los EEUU (*National Institute of Standards and Technology* (NIST)):

> "*El Cloud Computing es un modelo que permite el acceso a una red de forma ubicua, conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que puede ser suministrado de forma rápida y lanzado con un mínimo esfuerzo de administración o de interacción por parte del proveedor del servicio.*"(1)

(1) National Institute of Standards and Technology (NIST), Special Publication 800-145, "*The NIST Definition of Cloud Computing*", Septiembre 2011, Página 3 (La traducción es nuestra).

¿Por qué es recomendable consultar el Memorándum Sopot?

- Examina específicamente al tratamiento de datos personales en entornos de cloud computing.

- No se refiere a situaciones en las que todos los usuarios finales, el responsable, el encargado y todos sus subcontratistas están sujetos a la misma legislación de protección de datos, se encuentran físicamente localizados en la misma jurisdicción y todo el tratamiento y almacenamiento de datos se lleva a cabo dentro de dicha jurisdicción.

- El documento de trabajo sólo se refiere a la utilización de servicios en la nube por empresas y autoridades públicas que mueven sus procedimientos existentes "hacia la nube", no se refiere al uso de estos servicios por personas físicas.

Algunos aspectos jurídico-internacionales del Cloud Computing

En el documento de trabajo, se reconoce que "*existe incertidumbre en relación con el CC, sobre todo cuando se trata de la privacidad, la protección de datos y otras cuestiones legales*." A partir de este reconocimiento, se proponen ciertas recomendaciones para "ayudar a reducir esa incertidumbre."

A efectos prácticos, a todo lo largo del documento se considera al cliente de la nube como el responsable del tratamiento y al proveedor del servicio como el encargado del tratamiento.

Algunos aspectos jurídico-internacionales del Cloud Computing

En el Memorándum se reconoce que la evolución del CC ha puesto de relieve una serie de cuestiones importantes, entre ellas:

a) Aún no existe un acuerdo internacional sobre terminología común;

b) El tratamiento de datos se ha convertido en global;

c) Falta transparencia en relación con los procesos, procedimientos y prácticas de los proveedores del servicio en la nube, incluyendo información sobre si estos proveedores subcontrata cualquiera aspecto del tratamiento y, de ser así cuáles son los procesos, procedimientos y prácticas de los subcontratistas;

Algunos aspectos jurídico-internacionales del Cloud Computing

d) Esta falta de transparencia dificulta la realización de una adecuada evaluación del riesgo;

e) También dificulta el cumplimiento de la normativa relativa a protección de datos;

f) Los clientes (responsables) están presionados para reducir costes, incluidos los relacionados con el tratamiento de datos, y

g) Para mantener los precios bajos, los proveedores son más propensos a ofrecer (imponer) condiciones generales de contratación (*standard terms and conditions*).

Algunos aspectos jurídico-internacionales del Cloud Computing

Estas circunstancias pueden llevar a un mayor riesgo de:

A. Violaciones a la seguridad de la información, inadvertidas por el responsable;

B. Transferencias de datos hacia jurisdicciones que no proporcionan un nivel adecuado de protección;

C. Actuaciones en violación de las leyes y principios sobre protección de la privacidad y de datos personales;

D. Aceptación de condiciones generales que otorguen al proveedor demasiado margen de acción, incluyendo la posibilidad de que éste pueda procesar los datos en contravención a las instrucciones del responsable;

Algunos aspectos jurídico-internacionales del Cloud Computing

E. Uso de los datos por parte del proveedor o de sus subcontratistas, para sus propios fines, sin conocimiento o consentimiento de los responsables;

F. Desvanecimiento o desaparición de la responsabilidad legal dentro de una cadena de subcontratistas, y

G. Obstaculización a las autoridades de protección de datos para supervisar adecuadamente el tratamiento de los datos por parte del responsable y el proveedor del servicio en la nube, y

Algunos aspectos jurídico-internacionales del Cloud Computing

Tras el análisis anterior, el Grupo de Berlín desarrolla una serie de **recomendaciones** "*destinadas a ayudar a reducir los riesgos asociados con el uso de servicios de Cloud Computing y a promover la responsabilidad y la gobernanza adecuadas, de modo que los beneficios de la utilización de CC se puede alcanzar,* ***pero no a expensas de los derechos de las personas***."

En el Memorándum Sopot se desarrollan:

- 6 recomendaciones generales,
- 9 recomendaciones adicionales sobre buenas prácticas,
- 11 buenas prácticas a cargo del responsable,
- 5 buenas prácticas a cargo del prestador de servicios en la nube, y
- 1 recomendación para auditores.

Recomendaciones generales:

- El uso del CC no debe conducir a una disminución de los niveles de protección de datos, en comparación con el procesamiento de datos convencional.

- Que los responsables del tratamiento lleven a cabo las evaluaciones de impacto en la privacidad y de riesgo que sean necesarias (si es necesario, mediante el uso de terceros de confianza) antes de embarcarse en proyectos de CC.

- Que los proveedores de servicios Cloud mejoren sus prácticas con el fin de ofrecer una mayor transparencia, seguridad, responsabilidad (accountability) y confianza en las soluciones de CC; en particular con respecto al uso de cláusulas contractuales más equilibradas que promuevan la portabilidad de los datos y el control de éstos por los usuarios de la nube.

Buenas prácticas adicionales:

- La implementación del CC debe llevarse a cabo a través de pasos cuidadosamente ponderados, comenzando con información no sensible y no confidencial.

- El tratamiento de datos sensibles a través del CC plantea problemas adicionales. Por lo tanto, y sin prejuicio de ninguna ley nacional, dicho tratamiento requerirá de medidas de seguridad adicionales.

- Se deben poner a disposición de los responsables y de las autoridades de control registros de auditoría sobre la ubicación (*location audit trails*). Los registros de auditoría deben grabarse de forma automática y mostrar las ubicaciones físicas donde los datos personales han sido guardados, tratados y en qué momento.

Buenas prácticas adicionales (cont.):

- Se deberán establecer registros de auditoría sobre copias y supresiones de datos (*copying and deletion audit trail*), que deberán mostrar claramente las copias de los datos personales que han sido creadas y suprimidas por el encargado del tratamiento (y sus subcontratistas).

- Se deberá asegurar la existencia de copias de seguridad de los registros de auditoría de referencia.

- Es preciso garantizar que los datos personales en reposo y en tránsito sean cifrados. Podrían evaluarse opciones que permitan al responsable, de forma rápida y efectiva, impedir que el encargado continúe con el descifrado de datos (*emergency brake*).

- Registros de acceso.

Buenas prácticas del responsable:

- Asegurar el cumplimiento del **principio de transparencia de ubicación**, mediante la obtención de información por anticipado sobre todas las ubicaciones físicas en que los datos serán tratados, incluyendo las copias de respaldo.

- Acordar que el proveedor del servicio, bajo ningún concepto, podrá transferir los datos hacia ubicaciones distintas a las que previamente fueron pactadas.

- Asegurar el **principio de cumplimiento de las instrucciones del responsable**, evitando cláusulas ambiguas o que den lugar a diversas interpretaciones.

Buenas prácticas del responsable (cont.):

- Acordar el derecho a permitir que un tercero de confianza pueda monitorizar, total o parcialmente, el tratamiento de datos personales por el proveedor del servicio.

- Antes del uso del CC, el responsable debe realizar una **evaluación de riesgos** basada en el conocimiento de las condiciones y circunstancias específicas en que los datos personales serán tratados por el proveedor de servicio y sus subcontratistas, si los hubiere.

- **Evitar la dependencia**, asegurando la participación activa del prestador del servicio en la transferencia de los datos, si ésta fuera necesaria.

- Considerar la conveniencia de asegurar el acceso a una copia útil de los datos, fuera del control del proveedor del servicio.

Buenas prácticas del encargado:

- Cumplimiento del **principio de transparencia de ubicación**.

- Transparencia sobre la existencia de subcontrataciones y de los servicios (tratamientos) específicamente subcontratados.

- Garantizar la transparencia contractual, absteniéndose de ofrecer el servicio mediante términos y condiciones que permitan cambios unilaterales en la prestación del servicio.

- Se recomienda que las condiciones generales de contratación ofrecidas a ciertos segmentos del mercado (por ejemplo, pymes), sean redactadas de forma tal que se garantice el respeto a la privacidad y el cumplimiento de garantías para el tratamiento de los datos.

CONCLUSIONES

- Desactualización de la normativa sobre protección de datos frente al CC.
- No prejuzgar ni menospreciar la posición del cliente (ellos o nosotros).
- Explorar alternativas.
- Involucrar a los abogados en la revisión y **negociación** del contrato.
- ¿Quién debe adaptarse? ¿La nube ó ISO20K & 27K?
- ¿Ceder para ganar?

OTROS TEMAS DE INTERÉS

Política de Geolocalización (*Geolocation Policy*)

Why Every Company Needs a Geolocation Policy
http://bit.ly/NltXTM

The Importance of Knowing Where in the World Cloud Data is Stored
http://bit.ly/OAS4P3

CLOUD DATA GOVERNANCE de Cloud Security Alliance (CSA)

Proyecto que persigue, entre otros objetivos, la adaptación de las prácticas actuales de "la industria del Cloud" a las regulaciones de Gobierno, Riesgo y Cumplimiento (GRC).
https://cloudsecurityalliance.org/research/cdg/#_overview

Comité de la Comunidad Valenciana itSMF ESPAÑA

ISACA Sistemas de información fiables y valiosos Valencia Chapter

ENLACES

Ley Federal de Protección de Datos en Posesión de los Particulares
http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Reglamento de la Ley Federal de Protección de Datos en Posesión de los Particulares
http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

Working Paper on Cloud Computing - Privacy and data protection issues
http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf?1339501499

The NIST Definition of Cloud Computing (SP800-145)
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

"Algunos aspectos jurídico-internacionales del Cloud Computing"

Héctor Guzmán Rodríguez

Abogado en TI

Twitter: @HectorGuzmanMx

LinkedIn: http://es.linkedin.com/in/hectorguzman

MUCHAS GRACIAS