

## 6. Seguridad, Privacidad y Contratación de Servicios Cloud

### 6.2. Seguridad y Privacidad en el Cloud.

Con frecuencia se dice que la seguridad es un proceso y no un producto. La gobernabilidad de la nube se rige también por esta regla. La capacidad para aplicar las reglas de gobernabilidad depende de que los desarrolladores sean conscientes de que se ha instaurado el marco de la gobernabilidad teniendo en cuenta no solo el registro y conservación de la información sino el acceso y sus permisos.

En seguridad es importante no confundir la confidencialidad de los datos con los datos personales. Estos sólo afectan al individuo. Pero puede que en nuestra empresa tengamos datos confidenciales, críticos e incluso secretos! Secuencialmente, imaginemos un plan estratégico, nuestro sistema de seguridad de acceso a las instalaciones o a la fórmula de la Coca-Cola!

Empezando por lo sencillo: La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) regula los aspectos relativos al tratamiento de los datos personales y la libre circulación de los datos. La Agencia Española de Protección de Datos (AEPD) es el órgano de control que se encarga de garantizar el cumplimiento de esta normativa dentro del territorio español.

En primer lugar, tanto la empresa contratante de servicios como la proveedora deben tener en cuenta la definición de dato personal que establece el artículo 3 de la LOPD: “un dato personal es cualquier información concerniente a personas físicas identificadas o identificables”.

Si los datos con los que se va a trabajar en la nube pertenecen a esta categoría, la empresa que los trate debe cumplir con carácter previo con el conjunto de obligaciones previstas en la LOPD: la inscripción de ficheros, deberes relacionados con la información en la recogida, el consentimiento y la calidad de los datos, garantía de los llamados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) o la adopción de medidas de seguridad.

Si los datos con los que se va a trabajar en la nube no son datos personales (son, por ejemplo, complejas operaciones matemáticas, cálculos físicos o químicos, etc.), se puede proceder sin que la LOPD señale impedimento alguno.

Además, en el caso del cloud computing es fundamental revisar las condiciones del contrato a fin de garantizar una adecuada previsión de las cuestiones relacionadas con la presencia de un encargado del tratamiento y/o una transferencia internacional de datos personales.

Lo que ocurre es que la técnica está superando cualquier previsión del legislador, y cualquier



política que no pase por los principios de gobernabilidad esenciales está condenada al fracaso.

En Europa se está llevando a cabo la redacción de la directiva de protección de datos. Ello supondrá que en lugar de veinticinco legislaciones, solo tendremos una. Y mucho antes de lo que pensamos. Probablemente en la primavera del 2014 sea una realidad. Lo que no sabemos es cuán estrictos serán las diferentes autoridades de control.

Una pista que le puede ayudar a comprender la importancia de la seguridad: entre las certificaciones habituales en el tratamiento de la seguridad de la información se encuentra la ISO 27000 y su familia. Aproximadamente tiene tres centenares de puntos de control. Cumplir con la LOPD, a nivel alto, significa cumplir unos setenta puntos de esta certificación.

Si una empresa desea conservar lo que a buen seguro será la información, seguramente deberá plantearse el hacer una auditoría de LOPD. Le ayudará a entender y conseguir, si la necesitase, una certificación 27000. Incluso tiene a su disposición herramientas que le pueden ayudar a modo de auto-auditoría, y si la cosa se complica, siempre puede contar con la colaboración de buenos profesionales.

#### Referencias:

- [Riesgos y amenazas en Cloud Computing. Págs 12-30](#)
- [Guía para empresas: seguridad y privacidad del cloud computing Págs. 40-46](#)
- [Security for Cloud Computing 10 Steps to Ensure Success. Págs. 7-30](#)