



6. Seguridad, Privacidad y Contratación de Servicios Cloud

6.4.1 Contratación de Servicios Cloud (I).

Cuando hablamos de cloud computing lo asociamos de inmediato a SaaS(Software As A Service), pero como sabemos existen otros dos tipos principales aunque menos conocidos PaaS e IaaS, que es el negocio de Amazon Web Services y GoGrid, por poner dos ejemplos de los más conocidos.

Estos servicios se prestan conforme a unos niveles de servicio (SLA), ya que por el momento no son lo suficientemente estables como para garantizar una fiabilidad del 100%, por lo que se establecen unos límites que determinan el funcionamiento normal, contemplando para ello unos umbrales de “fallo normal”, que en términos absolutos son ínfimos, suelen establecerse en el 0,05%.

La Semana Santa de 2013, mientras en España estábamos pendientes del tiempo y los pasos, en los Estados Unidos hubo algunas empresas que estaban viviendo su particular “via crucis” a causa del cloud computing, y particularmente, por los servicios IaaS.

Estos fueron los casos de varias empresas de ocio, viajes, reservas, etcétera, que estuvieron sin servicio por los errores que estaban sufriendo los servidores cloud de Amazon. El compromiso del contrato a nivel de servicio de Amazon EC2 es de una disponibilidad del 99,95% en cada Región de Amazon EC2.

Ese 0,05% del tiempo indisponible puede ser insignificante según qué tipo de servicio, ya que puede representar minutos para restablecer el servicio en una región diferente pero en otros, unos minutos sin servicio puede causar daños irreparables en la imagen de marca, un ejemplo puede ser las páginas de reservas y de viajes.

En la actualidad no es difícil leer noticias acerca de la nube informándonos de las oportunidades y desventajas que presenta, pero lo que es evidente que si uno se plantea contratar este tipo de servicios, hay que tener muy claro cuales son las condiciones del servicio y cómo puede afectar al “core” de nuestro negocio.

Y aún más... cómo plantearse una política de continuidad de negocio.

A ver, debemos, lo primero determinar cuán críticos son nuestros servicios con respecto a las tecnologías de la información, y cuanto dependen del tiempo, o pueden aguantar fuera de uso o de plena accesibilidad. También qué servicios de la empresa tienen esa criticidad.

No es lo mismo un comercio que un banco, una central de reservas que una central de



alarmas, ni un sistema de gestión de entradas de un cine que de “slots” de vuelo.

A partir de ahí deberemos determinar qué servicios debemos tener redundantes, para que entre un sistema suplente si falla el principal.

Además cuales debemos diseñarlos “resilientes”... bonito término... que tengan capacidad de soportar y recuperarse ante desastres y perturbaciones. Esto es, cuales además debemos prevenir que van a “atacarlos” reiteradamente, y desde distintos puntos y con diferentes estrategias.

Lo extraordinario del “cloud” es que podemos replicar un sistema por un coste bajísimo, ya que como el proceso y las aplicaciones se diseñan una sola vez, la replicación es solo cuestión de “hardware” (y de políticas de seguridad.... Piense en que tengan alguna pequeña diferencia)

Referencias:

- [Cloud Competency Programme Workshop 4](#)