

# Cómo migrar con éxito a la ‘Nube’

## Clouds privadas vs. públicas - Qué pedir a los proveedores - Los SLA como factor clave.

Los servicios TI basados en Cloud Computing generan hoy 12.800 millones de euros a nivel mundial, cifra que ascenderá a 32.300 millones en 2013. Estos datos de IDC muestran la ascensión de una tendencia que, sacando partido del auge de la virtualización y de propuestas como Utility Computing, Grid Computing y On-Demand, está transformando el modelo de adquisición y entrega de recursos hardware y software.

Pero el propio auge de Cloud Computing puede llevar a muchas organizaciones a tomar la decisión equivocada a la hora de adoptar la tecnología. Suele ocurrir con todas aquellas tendencias que acaparan en poco tiempo la atención mayoritaria del mercado. En tales casos, firmas de investigación, proveedores y medios especializados comienzan a generar y cruzar mensajes sobre sus beneficios y desventajas que en muchas ocasiones llegan al usuario con demasiada confusión y sin el análisis crítico exigible. Cuando el negocio está en juego, no es recomendable tomar decisiones sin enfocar la cuestión con la prudencia necesaria y la seguridad que añade contar con un proveedor de garantía.

### VENTAJAS E INCONVENIENTES.

Las ventajas de Cloud Computing son claras. No sólo permiten un rápido lanzamiento de nuevas empresas o nuevos proyectos en organizaciones ya establecidas sin gastos de capital (CAPEX), si no que además aporta la escalabilidad necesaria para optimizar el uso de los recursos ante periodos valle y pico, lo que añade una gran agilidad al negocio. Todo ello supone además poder abordar el desarrollo de nuevos productos con más rapidez y acelerar los tiempos de llegada al mercado. La disponibilidad de las aplicaciones desde cualquier punto con acceso a Internet y la capacidad de continuidad de los servicios ante imprevistos son también importantes beneficios.

Pero en el nuevo modelo no todo son ventajas; también introduce inconvenientes. La práctica generalidad de los expertos coincide en que Cloud Computing, como servicio externo, implica un alto consumo de ancho de banda, sobre todo con aplicaciones intensivas en recursos informáticos, ya sea en capacidad de servidor o de almacenamiento. Esto obliga a buscar una manera de minimizar el problema con la ayuda

del proveedor. Firmas de ocio y entretenimiento, de ingeniería o sanidad pueden llegar a generar y a acceder a un volumen de Terabytes de dos dígitos.

Relacionado con lo anterior se encuentran los problemas de rendimiento que podrían aparecer al trabajar con un servicio cloud de un proveedor externo teniendo en cuenta la latencia de la red, algo totalmente negativo para determinados perfiles de negocio. La elección del proveedor correcto ayudará a minimizar o incluso eliminar estos inconvenientes. Cuando además la aplicación que se va a pasar a la ‘nube’ del proveedor es crítica para el negocio, con criterios estrictos de accesibilidad y exposición, la opción cloud pública puede no ser la mejor idea.

### **“Buena parte de los CIO optan por el despliegue de clouds privadas”**

Finalmente, además de añadir inconvenientes en la gestión de los datos, las clouds públicas implican considerables problemas de seguridad en cuanto a protección, accesibilidad y privacidad de la información.

Hasta el punto de que aún hoy la seguridad del modelo público de cloud sigue siendo uno de sus factores inhibidores fundamentales. Tal vez sea esta la razón por la que una buena parte de los CIO opten por el despliegue de clouds privadas.

### HACIA ENTORNOS HÍBRIDOS.

Esta combinación de ventajas e inconvenientes de Cloud Computing, junto con la falta de madurez de la que adolecen todavía algunas ofertas, lleva a muchas organizaciones a preguntarse si este tipo de servicios externos se adapta a las necesidades de su negocio. Antes de comprometerse con un proveedor de servicios cloud, los responsables TI deberían analizar sus necesidades y requisitos específicos, y el impacto en los procesos de negocio que supondrá depender de una infraestructura y unos recursos compartidos y públicos. En muchos casos, la solución idónea será adoptar entornos mixtos de cloud público y privado, en función de la criticidad y de la naturaleza de cada aplicación. Tales combinaciones específicas tienen el potencial de crear soluciones adaptadas estrechamente a las necesidades propias del negocio y a las distintas actividades –y sus aplicaciones asociadas- de la compañía.

**“El 55% de los entrevistados por la firma consultora reconoció sentirse más atraído por el concepto de clouds privadas que por el de clouds públicas, mientras que un 22% aseguró encontrar atractivas ambas alternativas” – fuente IDC -**

Con mucha probabilidad, las clouds privadas y los escenarios mixtos serán la opción mayoritaria de las organizaciones. Aunque –según una reciente investigación de Brocade- el 60% de los CIO europeos prevé migrar a Cloud Computing, de acuerdo con un estudio casi simultáneo realizado por IDC más de la mitad de las empresas prefieren las clouds privadas. El 55% de los entrevistados por la firma consultora reconoció sentirse más atraído por el concepto de clouds privadas que por el de clouds públicas, mientras que un 22% aseguró encontrar atractivas ambas alternativas.

Un buen ejemplo de adopción con éxito del modelo privado de Cloud Computing es el grupo de investigación y desarrollo de Intel, que gracias al despliegue de una infraestructura y plataforma como servicio, consiguió mejorar su tasa de utilización de recursos de servidor de un 59% en la primera mitad de 2006 a un 80% en la actualidad. Con la reducción del gasto en infraestructura obtenida la compañía espera ahorrar casi 200 millones de dólares. Cifra que explica por sí sola que Intel decidiera a principios de 2009 construir una cloud privada para el resto de sus departamentos y oficinas.

Las alternativas no se acaban aquí. Una solución idónea para muchas organizaciones consiste en la creación de entornos híbridos donde se combinen los modelos clouds virtualizados, gestionados interna o externamente, con modelos convencionales basados en la utilización de servidores físicos dedicados. Como señala Forrester Research, existen múltiples formas de combinar opciones cloud y opciones de informática tradicional. Para la consultora, el éxito vendrá determinado por el diseño de la estrategia, enfoque y despliegue más adecuados para las circunstancias y requisitos específicos del negocio, estableciendo las bases que permitan, si es necesario, ir migrando incrementalmente a servicios de infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS), según las necesidades de la organización.

### SELECCIÓN DE OFERTAS.

En cualquier caso, las cloud públicas son ya una alternativa real al alcance de aquellas organizaciones para las que –por razones de costes, de flexibilidad o de agilidad- decidan sacar partido de sus ventajas, al menos para determinadas aplicaciones y procesos de negocio. IDC ha estudiado la naturaleza de las aplicaciones residentes en la ‘nube’, llegando a la conclusión de que las más habituales son las de gestión, colaboración, recursos humanos y de negocio, así como las de capacidad de servidor y de almacenamiento.

Como con cualquier servicio de externalización, a la hora de contratar este tipo de ofertas es fundamental garantizarse un acuerdo de nivel de servicio (SLA) que satisfaga los requisitos y exigencias del negocio.

Por lo general, en lo que se refiere a tiempo de actividad, los proveedores de cloud garantizan al menos un 99%, aunque hay que tener muy en cuenta el periodo imputable a dicha tasa. No es lo mismo garantizar un 99% de actividad anual, mensual o semanalmente. Hay proveedores que incluso prometen tasas del 100%, pero sólo en lo que se refiere a determinados fallos.

Es habitual que, respecto a las tasa de actividad, se achaque a los SLA de Cloud Computing estar lejos de los clásicos “cinco nueves” (99,999%) garantizados en otro tipo de entornos y servicios. Esta corriente de opinión parte de la idea preconcebida de que los centros de datos de empresa proporcionan tasas de actividad mucho mayores que los ofrecidos por los proveedores de cloud. Algo que para otros expertos no siempre es así. La firma de investigación HyperStratus, especializada en virtualización, Cloud Computing y otras tendencias innovadoras, recuerda además que los proveedores de cloud no sólo suministran infraestructura –campo en el que se centran exclusivamente las métricas comúnmente aplicadas a los centros de datos internos-, sino también capacidad de software. Para HyperStratus, a medida que nos adentramos en la próxima generación de aplicaciones, las métricas tradicionales de disponibilidad se vuelven más inapropiadas para el nuevo modelo. En un mundo de aplicaciones que abarcan cientos o miles de máquinas (o múltiples centros de datos), es inadecuado aplicar métricas diseñadas para entornos con pequeñas aplicaciones corriendo sobre hardware caro. Quizá es el momento de que surja un nuevo concepto de SLA.

Un factor a tener también en cuenta es que, por su naturaleza, la cloud pública introduce alguna latencia de red, aunque los expertos recuerdan que no se trata de un fenómeno ajeno a los entornos privados. En las empresas distribuidas geográficamente y dependientes de varios centros de datos por todo el mundo, el usuario final también sufre determinada latencia en función de su ubicación. CIMI aconseja al respecto realizar un diagrama del flujo de las transacciones y los datos, teniendo en cuenta las peticiones de datos, sus fuentes y sus movimientos, e identificando todos los procesos.

Así se conocerán todos los puntos entre los que fluyen los datos y se podrá evaluar y gestionar las posibles vulnerabilidades del comportamiento de la red en la cloud pública en cuanto a latencia, tiempos de respuesta y capacidad de proceso.

**“Hay que exigir al proveedor formas claras y contrastables de comprobar que se está recibiendo el nivel de servicio prometido. La disponibilidad de informes sobre tendencias, estadísticas de rendimiento y monitorización en tiempo real es fundamental”**

En general, a la hora de contratar un servicio de cloud, además de las cuestiones ya planteadas, habrá que considerar el soporte de aplicaciones que ofrece el proveedor; así como conocer a fondo el nivel de soporte y asistencia en aspectos como, por ejemplo, la optimización o reescritura de las aplicaciones para que puedan sacar el máximo partido a la plataforma cloud del proveedor. Igualmente, conviene realizar pruebas de escalabilidad de la plataforma del proveedor.

Por encima de todo, al igual que con los contratos de externalización de otro tipo, hay que exigir al proveedor formas claras y contrastables de comprobar que se está recibiendo el nivel de servicio prometido. La disponibilidad de informes sobre tendencias, estadísticas de rendimiento y monitorización en tiempo real es fundamental, así como la clase de penalizaciones contempladas.



Fuente: Gartner (junio 2009)

En el proceso de selección de proveedor, conviene seguir los análisis de mercado realizados por las firmas de investigación, como el Cuadrante Mágico

de Servicios Bajo Demanda de Web Hosting y Hosted Cloud System Infrastructure de 2009 realizado por Gartner. La consultora posiciona en el cuadrante de “Líderes” a firmas como Terremark, a la que considera especialmente bien situada, con precios que se mueven en una franja media, por sus servicios de infraestructura virtualizada basada en tecnología de VMware y sus ofertas de hosting utility Infrastructure y Enterprise Cloud VDC, así como colocation independiente de operador. “Terremark es un innovador en tecnología con un muy buen servicio al cliente, un buen portal para usuarios y una automatización expansiva. Cuenta con una hoja de ruta de infraestructura cloud agresiva y bien diseñada, especialmente focalizada en los requisitos de las empresas”. La consultora destaca además el soporte de ingeniería de Terremark, sus capacidades de autogestión y su excelente posición en el sector gubernamental.

#### DERECHOS Y RESPONSABILIDADES.

Como guía de consulta, también es aconsejable conocer las conclusiones de Gartner Global IT Council for Cloud Services, que resume en siete puntos los derechos y responsabilidades de los clientes de servicios en la ‘nube’ cuyo seguimiento “permitirá a proveedores y usuarios trabajar juntos de la forma más productiva”. De manera esquemática, estos puntos son:

- \* Derecho a conservar la propiedad, uso y control de los datos propios.
- \* Derecho a conseguir SLA que definan claramente la responsabilidad y los procesos de reparación de los fallos potenciales.
- \* Derecho a la notificación y elección ante los cambios que afecten a los procesos de negocio del cliente.
- \* Derecho a conocer las limitaciones técnicas o requisitos iniciales del servicio.
- \* Derecho a conocer los requisitos legales de jurisdicción a los que está sujeto el proveedor.
- \* Responsabilidad de conocer y adherirse a los requisitos de licencias de software.
- \* Conocer los procesos de seguridad seguidos por el proveedor.

**“Hay cuatro preguntas clave sobre seguridad a las que el proveedor habrá de dar respuesta con credibilidad: ¿dónde residen los datos?, ¿cómo se protegen?, ¿quién tendrá acceso físico a las máquinas donde residen?, ¿qué procesos de recuperación de desastres se aplicarán?”**

Es precisamente este último punto una de las grandes cuestiones hoy en debate en torno a cloud computing. Según ISF (International Security Forum), entre las principales áreas de preocupación se encuentran las relacionadas con la gestión de identidades y credenciales de usuarios, la protección frente a nuevas formas de malware y las cuestiones regulatorias y legales. Mientras un sector de la opinión sigue viendo estos problemas de seguridad como la gran barrera para su adopción como servicio externo, no faltan los que confían en la capacidad del mercado para desarrollar mecanismos de protección que minimicen los riesgos. Como la iniciativa Trusted Cloud puesta en marcha por Novell y Cloud Security Alliance (CSA) para diseñar un modelo de referencia que permita disponer de una certificación que securice la adopción de cloud. Este modelo ayudará a los proveedores de Cloud Computing a desarrollar prácticas y configuraciones seguras e interoperables para la gestión de identidades, acceso y cumplimiento normativo.

En cualquier caso, a la hora de contratar un servicio cloud hay tres preguntas clave sobre seguridad a las que el proveedor habrá de dar respuesta con credibilidad: ¿dónde residen los datos?, ¿cómo se protegen?, ¿quién tendrá acceso físico a las máquinas donde residen?, ¿qué procesos de recuperación de desastres se aplicarán? El proveedor seleccionado deberá demostrar que sigue las mejores prácticas del sector y disponer de las herramientas adecuadas para realizar su operativa, como es el caso de Terremark. La compañía sigue las normas y prácticas ITIL (IT Infrastructure Library) y cuenta, entre otras, con las certificaciones SAS 70 Tipo II, VISA CISP y Safe Harbor, que ayudan a sus clientes a cumplir normativas como las leyes Sarbanes-Oxley, PCI, GLBA e HIPAA.