

## Día Internacional de la Seguridad de la Información

### **acens da cinco claves para vencer los miedos y los mitos de la seguridad en la nube**

- *Según Gartner el 2012 se cerrará con un incremento del 20% en el uso del cloud computing por parte de las empresas pero el 50% de los CIOs reconoce no saber aún qué nube se adapta mejor a las necesidades de su empresa.*
- *acens recuerda que, además del desconocimiento, el principal inhibidor para adoptar soluciones de cloud computing es la desconfianza en los apartados de seguridad y disponibilidad.*

**Madrid, 29 de noviembre de 2012.-** Con motivo del Día Internacional de la Seguridad de la Información que se celebra mañana, **acens** ([www.acens.com](http://www.acens.com)), proveedor líder de servicios de **Cloud Hosting**, Hosting, Housing y Soluciones de Telecomunicaciones para el mercado empresarial, ha dado a conocer cinco claves para ayudar a los usuarios y a las empresas a vencer los miedos y los mitos que rodean a la nube en cuestiones de seguridad.

Los beneficios que ofrece la nube harán que el 2012 se cierre con un incremento del 20% en el uso del cloud computing por parte de las empresas, según Gartner. Aún así, el desconocimiento sigue siendo uno de los principales frenos para la adopción de este tipo de soluciones. De hecho, el 50% de los CIOs reconoce no saber todavía qué tipo de nube se adapta mejor a las necesidades de su negocio y 8 de cada 10 afirma estar muy preocupado por los riesgos que se crean en este nuevo entorno tecnológico.

En este contexto, acens ofrece cinco recomendaciones básicas para ayudar a las empresas interesadas en acometer un proyecto en la nube, a conocer mejor las necesidades y criterios de seguridad que deben de tener en cuenta.

- 1) **“La nube no es real”** Falso, ya que existe físicamente. Además, hay que desmitificar las dificultades del cloud, porque contratar servicios en la nube no es tan complicado y se puede hacer con total garantía en España. Lo que ocurre es que han proliferado infinidad de acrónimos para referirse a cosas que no siempre son lo mismo y eso genera cierta confusión. Por eso no sólo hay que conocer y analizar bien todos los detalles de la nube sino saber también dónde está ubicada, ya que poder acceder a ella o conocer a la gente que está detrás de la gestión supone una dosis extra de tranquilidad y facilita muchas de las operaciones del día a día.
- 2) **“Con proteger la nube basta”** Falso, no tiene sentido exigir al proveedor de la nube las mayores medidas de seguridad para garantizar entornos seguros de acceso y trabajo y luego descuidar las políticas internas de seguridad dentro de la empresa. Hay que analizar bien las medidas que hay que implementar y analizar los riesgos. En cualquier caso, un buen servicio en la nube debe garantizar el control, la gestión y el acceso a los datos y aplicaciones bajo estrictas normas de seguridad y acorde a los permisos establecidos por el cliente para interferir en su entorno cloud.
- 3) **“Con la seguridad de la tecnología cloud es suficiente”** Falso. La seguridad y la disponibilidad son parámetros que no dependen de la tecnología en sí, sino de la plataforma del proveedor de servicios cloud. Lo mejor es hacer un análisis

riguroso de la infraestructura y contar con medidas para prevenir incidencias. Desde opciones más avanzadas como contar con un equipo de monitorización o una infraestructura redundante de red y almacenamiento, hasta cuestiones más básicas como hacer una copia de toda la información más relevante de las máquinas, para que en caso de pérdida, manipulación o borrado se pueda recuperar desde un archivo aislado hasta un servidor.

- 4) **“La seguridad en la nube también debe ser multiplataforma”** Verdadero. Con una penetración de smartphones en España del 55,2% -según comScore- cualquier proyecto en la nube debe contemplar el acceso ubicuo y multiplataforma. Los usuarios y empleados querrán acceder desde redes públicas y privadas desde diferentes dispositivos –PC, portátil, smartphone, tablet...– por lo que una buena política de seguridad debería proteger estas vías. Hay soluciones para crear dos redes separadas, aquella que tiene conexión con el exterior, dotada de direccionamiento IP público, y una red privada con direccionamiento privado que es de uso exclusivamente interno. Otra recomendación es trabajar con tecnologías y productos estándares del mercado ya que la migración e integración de equipos, o incluso la replicación de entornos y sistemas será más rápida y sencilla.
  
- 5) **“No saber dónde está la nube reduce las preocupaciones”** Falso, pues recordemos que el desconocimiento de la ubicación de la nube no exime de las responsabilidades en materia de protección de datos. Un buen proveedor de cloud debe cumplir con las normativas legales en materia de protección de datos, como puede ser en España la LOPD para salvaguardar la confidencialidad y la seguridad de la información y que datos críticos de la compañía no circulen de un país a otro. A veces las empresas insisten en tener los datos en servidores diferentes a otra empresa y se olvidan de que al guardar sus datos en la nube, ésta puede estar alojada en un país donde se autoriza, en circunstancias particulares, al acceso a esa información por parte de determinadas autoridades.

## Los aspectos legales del cloud

### Seguridad y disponibilidad en la nube

### White Paper: tipos de Cloud Hosting: público privado e híbrido

#### Acerca de acens

**acens**, adquirido por Telefónica en junio de 2011, es una empresa pionera en el desarrollo de las soluciones de Cloud Hosting más completas y competitivas del mercado, proveedora de servicios de “Hosting”, “Housing” y Soluciones de Telecomunicaciones para el mercado empresarial. Desarrolla su actividad desde 1997, cuenta en la actualidad con presencia en Madrid, Barcelona, Valencia y Bilbao, y posee dos Data Centers con más de 6.000 metros cuadrados, siendo una empresa líder en su sector de actividad. En la actualidad, la cartera de clientes supera las 100.000 empresas, con un amplio abanico de servicios contratados que comprenden desde el alojamiento de páginas Web hasta soluciones de VPN (Red Privada Virtual) con “outsourcing” de servidores y aplicaciones y tránsitos de salida a Internet y soluciones de nube híbrida, públicas y privadas para cubrir todas las necesidades tecnológicas y de negocio de las empresas.

**acens** gestiona casi 400.000 dominios en Internet, aloja miles de servidores y administra un caudal de salida a Internet superior a los cuatro Gigabits a través de una red troncal multioperador con presencia en los puntos neutros (Espanix, Catnix...).



acens Cloud Hosting ofrece a pequeñas y grandes empresas modelos de trabajo más flexibles, seguros y eficaces, tanto en entornos de clouds privados como en públicos y mixtos.

**Para más información:**

Noizze Media para **acens**  
*Carmen Tapia / Ricardo Schell*  
[ctapia@noizzemedia.com](mailto:ctapia@noizzemedia.com) / [ricardo.schell@noizzemedia.com](mailto:ricardo.schell@noizzemedia.com)  
646 892 883 / 699 983 936

**acens**  
*Inma Castellanos*  
[Inma@acens.com](mailto:Inma@acens.com)  
[@inmacastellanos](https://twitter.com/inmacastellanos)