Cloud computing: ¿amigo o enemigo?

Tipos, modelos, ventajas y consideraciones

Cloud computing es un nuevo modelo de prestación de servicios de negocios y tecnología, que permite al usuario acceder a un catálogo de prestaciones estandarizadas pagando únicamente por el consumo efectuado. De su implementación, beneficios y riesgos, se trata en este artículo.

Ing. Francisco Michelich, Director Comercial de The ISNS Group
fmichelich@isnsgroup.com

Desde tiempos antiguos, los avances tecnológicos han sido una de las piezas fundamentales en la evolución del hombre. Técnicas para manipular materiales y conferirles nuevas formas, elementos de medición, creación de aleaciones y el surgimiento de máquinas de cómputos digitales son sólo algunos de los avances que primero vienen a nuestra memoria. Pero, ¿qué avances podemos esperar en el futuro? Muchos especialistas coinciden en que estarán íntimamente relacionados con cloud computing. Cloud Computing o "computación en la nube" es un término que refiere a la utilización de múltiples servidores de computación conectados vía una red digital, como si fueran una sola computadora. La "nube" (o "cloud"), en sí misma, no es más que una virtualización de los recursos-redes, servidores, aplicaciones, almacenamiento de datos y otros servicios a los que el usuario final tiene acceso en función de su demanda particular. Si bien es una tendencia creciente mudar la infraestructura de las empresas a la nube, existen algunas particularidades que no deberían ser tomadas a la ligera. Algunos han afirmado que se trata de "los cimientos de la computación de las próximas generaciones", pero, ¿es realmente conveniente utilizar este novedoso servicio?

TIPOS DE NUBES

Comencemos por identificar los distintos tipos de posibilidades que ofrece la nube. En función de su modelo de implementación, éstas se pueden clasificar como:

- PRIVADAS: si su infraestructura está destinada a una sola organización, ya sea que esté administrada por la empresa internamente o por otra compañía, y que esté hosteada internamente o externamente.
- PÚBLICAS: las aplicaciones, capacidad de almacenamiento y otros recursos se ofrecen al público por parte de un proveedor de servicios. Algunos de ellos, como Amazon AWS, Microsoft o Google, son dueños de la infraestructura y ofrecen acceso únicamente a través de Internet, sin la posibilidad de una conexión directa.
- COMUNITARIAS (Community): se comparte la infraestructura entre varias organizaciones con intereses comunes (seguridad, Compliance, etc.), sea administrada por la empresa internamente o por otra compañía, y que esté hosteada internamente o externamente. En éstas, existe una cantidad de clientes mucho menor a las Clouds Públicas pero mayor a las Privadas.
- HÍBRIDAS: surge de la combinación de dos o más tipos de nubes (privadas, públicas o comunitarias), que si bien permanecen como entidades únicas, están íntimamente relacionadas, ofreciendo los beneficios de múltiples modelos de implementación.

Además del tipo específico, según su modelo de servicio, una nube puede ser:

- IAAS (Infraestrucure as a Service): el proveedor de servicios ofrece computadoras físicas o virtuales, almacenamiento de archivos, firewalls, direcciones IP y otros recursos. En este modelo, es el usuario el responsable de instalar las imágenes de los sistemas operativos, así como también las aplicaciones. El mantenimiento y patching también deberá ser realizado por el usuario. IaaS entonces hace referencia a las facilidades dadas a organizaciones, que ofrecen a sus usuarios capacidad de almacenamiento extra en servidores y data centers.
- PAAS (Platform as a Service): en este modelo, el proveedor entrega una plataforma de computación, que típicamente incluye un servidor web, bases de datos, un sistema operativo y un entorno de ejecución de lenguajes de programación. De esta forma, los desarrolladores de aplicaciones pueden diseñar y correr sus soluciones en una plataforma cloud sin incurrir en altos costos de adquisición de hardware.
- SAAS (Software as a Service): para este modelo, son los proveedores quienes instalan y operan las aplicaciones a las cuales los usuarios tienen acceso. Por lo tanto, los usuarios no manejan la infraestructura o plataforma sobre la cual corren las aplicaciones, lo que simplifica el mantenimiento y soporte. Estos servicios se contratan mediante una tarifa mensual o anual en función de la cantidad de usuarios por lo que el precio es escalable y se ajusta a cada situación según la demanda. Algunos ejemplos son Google Apps, Salesforce.com o Microsoft Office 365.

BENEFICIOS

Una vez explicadas las posibles configuraciones de los diferentes

tipos de nubes y servicios, repasemos algunos de los beneficios principales del cloud computing:

- Acceso a un gran número de aplicaciones sin necesidad de descargar o instalar.
- Acceso a las aplicaciones desde cualquier computadora, en cualquier parte del mundo.
- Los usuarios pueden evitar gastos en hardware y software y utilizar sólo lo que necesitan.
- Ahorros en mantenimiento y soporte de aplicaciones y/o infraestructura.
- Mayor elasticidad para clonar tareas entre distintas máquinas virtuales y distribuir la carga de trabajo.
- Las compañías pueden compartir recursos en un mismo lugar.
- Escalabilidad en función de la demanda de recursos.
- El consumo se factura como un servicio tradicional (gas, luz, etc.), con mínimos costos de contratación y una tarifa mensual según la utilización.

Todo parecería indicar que, por su capacidad para evitar inversiones en hardware y software y la flexibilidad que ofrecen los distintos modelos, el cloud computing debería ser implementado en todas las organizaciones, pero, ¿existen costos ocultos? ¿Cómo se garantiza la seguridad de la información en estos sistemas?

La respuesta es sí, existen varios riesgos, algunos de importante peso específico, que pueden generar no sólo grandes costos ocultos sino que también pueden dejar a la compañía fuera del negocio.

¿CUÁLES SON LOS RIESGOS?

- Los usuarios no poseen físicamente el almacenamiento de sus propios datos, lo que provoca que la responsabilidad y el control de los mismos esté a cargo del proveedor del servicio.
- Los usuarios pueden volverse dependientes del proveedor del servicio, quitando flexibilidad o capacidad de respuesta a resoluciones estratégicas.
- La continuidad del negocio, así como la recuperación ante un desastre (disaster recovery), estará en manos del proveedor.
- ¿Cómo se realizaría una migración de contenidos de un proveedor de cloud services a otro? ¿Quién podría garantizar que ningún dato se extraviara o fuera extraído en el proceso?
- ¿Qué sucede si el proveedor tiene un problema que le impide operar correctamente? ¿Qué sucede si el proveedor quiebra y queda fuera del negocio?

Cómo se observa, se están "tercerizando" muchos riesgos al proveedor. Esto puede ser bueno, siempre que el proveedor demuestre estar más apto para manejarlos que la propia empresa, pero ¿hasta dónde es aconsejable? Siempre que exista riesgo, éste es mayor al 0%, es decir, existe por menor que sea. Por lo tanto, imagine una situación en la que no sólo tiene un problema de operaciones por inconvenientes ocasionados por su proveedor, sino que además puede afrontar una disputa legal al respecto. Considere los costos y la asignación extra de recursos que le generaría tal situación. Lo que es peor, podría ser víctima de una fuga de información vital acerca de su negocio, de un cliente o de un producto, que podría impactar tan fuerte una vez hecho pública que podría dejarlo sin la posibilidad de continuar con su actividad, traducida en pérdidas en valor por acción, pérdida de valor de marca y falta de credibilidad para garantizar la seguridad de la información. Por lo tanto, si bien se tercerizan riesgos, no se terceriza la responsabilidad frente a los clientes de la empresa.

Como se recordará, en abril de 2011 Amazon experimentó un colapso de su nube EC2 (Elastic Compute Cloud), generando una caída de los sitios de varias compañías de primer nivel mundial y ocasionando en algunos casos pérdida de información.

Especialistas como Gartner recomiendan algunos puntos a tener en cuenta durante la selección de un proveedor:

1. Acceso de usuarios privilegiados: es de vital importancia poder contar con información específica acerca de la contratación de usuarios con privilegios por parte del proveedor, así como también un control de los accesos de estos a los datos de la empresa.
2. Cumplimiento de regulaciones: dado que las empresas son responsables por la integridad de los datos de sus clientes (aún si están administrados externamente por un proveedor de servicios), debería hacerse hincapié en las auditorías externas y certificaciones de seguridad con las que cuenta cada proveedor, para contar con una garantía de que cumplen lo que predican.
3. Ubicación de los datos: al utilizar la nube no siempre se tiene un conocimiento exacto de la ubicación de los datos y, muchas veces, hasta se desconoce el país en el que están alojados. Es por ello que se recomienda consultar si los proveedores estarían dispuestos a comprometerse por contrato a realizar el almacenamiento y procesamiento de los datos en una jurisdicción específica.
4. Segregación de los datos: la información está, generalmente, almacenada en un entorno con información de otros clientes que contrataron servicios en la nube. Si bien la encriptación es la alternativa recomendada, es necesario averiguar cómo se segrega la información en detalle. Muchas veces, accidentes durante la encriptación de datos pueden volver la información totalmente corrupta o dificultar el acceso. Estos algoritmos y esquemas de procesamiento, deberían ser testeados por especialistas con vasta experiencia.
5. Recuperación ante desastres: Todo proveedor digno de consideración debería contar con un Plan de Recuperación ante Desastres, que especifique la capacidad de realizar una restauración completa, y detallar la cantidad de tiempo que tomará.
6. Capacidad de investigación: la naturaleza de estos modelos, donde la información está en una ubicación compartida con datos de

otros clientes y que, además, poseen una dinámica en la que los hosts y data centers cambian en función de la variación de la demanda, hacen muy difícil investigar actividades ilegales o inapropiadas. Es recomendable poder contar con una obligación contractual por parte del proveedor, que especifique que puede encargarse de ciertos tipos de investigación. Si esto no es posible, habrá que asumir que estos controles no pueden practicarse.

7. Continuidad a largo plazo: El proveedor debe poder garantizar que, ante una migración de datos (por cambio de proveedor, o absorción del proveedor por parte de una empresa de mayor tamaño), éstos estarán disponibles en el formato que corresponda, para poder luego importarse a una aplicación de reemplazo.

RECOMENDACIONES DE ISNS GROUP

Además de las pautas y recomendaciones enumeradas anteriormente, los especialistas de ISNS Group recomiendan:

- Categorizar la información según distintos niveles de criticidad, por lo cual en función de ello se decidirá qué subir a la nube y qué no.
- La información en la nube, pública o privada, debería estar siempre encriptada, reduciendo las posibilidades de exposición de la información en caso de que sucediera un siniestro.
- Ya sea contratando un servicio cloud o persiguiendo el cumplimiento de la propia política interna de recuperación ante desastres, debe garantizarse que los backups de la información estén alojados en una ubicación física distinta a la de los servidores operativos, por lo que en caso de inundación, terremoto, falla en la red eléctrica u otra anomalía, éstos no se vean afectados (muchos proveedores de servicios cloud alegan tener backups seguros, pero si están localizados en la misma "caja" -"box"-, o en una "caja" distinta en el mismo data room, ese backup podría estar comprometido).

Algunas proyecciones estiman un crecimiento anual del 25% de los servicios cloud corporativos. El fuerte crecimiento esperado, podría indicar que todavía nos encontramos en la fase de introducción o fase de crecimiento de la tecnología cloud en el mercado. Por lo tanto, podría ser recomendable esperar la fase de madurez y asentamiento de la curva de ciclo de vida, que seguramente traerá aparejado avances tecnológicos y nuevas herramientas que ayuden a mitigar algunos de los riesgos actuales.

Por supuesto que la decisión de optar por este tipo de tecnologías es de cada compañía, pero también es de ellas la responsabilidad de asegurar continuidad a su negocio y el de sus clientes. Esperamos un futuro emocionante, de nuevas oportunidades y herramientas para el mundo de los negocios. De todas maneras, recomendamos que especialistas realicen un puntilloso análisis de la situación y actúen con extrema cautela antes de adoptar servicios en la nube. ■