ACENDER

Medio: Revista Gerencia
Firma: Acender Consultores
Fecha: edición marzo, 2013
Página: 57
Centimetraje: 26.0 x 20.0 cms.

Cloud computing y estrategia de riesgos

Por José Tuba, Socio Líder Risk Consulting, Acender Consultores.

Resulta clave definir los posibles riesgos que emergen de la implementación del cloud computing en las organizaciones para desarrollar en forma exhaustiva el mapa de riesgos y estrategias para su administración. Clave, ya que este "estilo de computación escalable y elástico en donde las capacidades TI son provistas como servicios a clientes externos utilizando tecnologías basadas en Internet" va en aumento. Se espera que los ingresos globales por servicios de este tipo tengan un crecimiento desde US$40,7 billones a US$241 billones para el año 2020.

Areas de riesgo

Las cifras mencionadas no son menores para un recurso que presenta muchas oportunidades, pero también diversos peligros que van de acuerdo a los servicios que subamos a la nube. Es en este sentido que podemos visualizar seis grandes áreas de riesgo a ser consideradas:

- **Autenticación:** Corresponde a la posibilidad de que usuarios no autorizados puedan acceder como usuarios válidos. Si existe un alto porcentaje de recursos de información de la organización en la nube, este riesgo puede ser importante y significativo.
- **Seguridad y privacidad de datos:** Al externalizar la información en los proveedores de cloud computing, se hace exigible que los mismos cumplan con estándares de protección de datos. El riesgo de pérdida de información puede ser alto en la medida en que no se implementen estrategias de seguridad para la nube.
- **Interfaz con sistemas internos:** La mayoría de las organizaciones no puede externalizar todos los sistemas en el cloud. Es por ello que se hace necesario la construcción de interfaces para estos sistemas y la nube. Estos nuevos elementos incrementan el riesgo de integridad de datos e interoperabilidad de los sistemas.
- **Disponibilidad de sistemas:** Los negocios cada vez dependen más de la disponibilidad de los sistemas, es por ello que los servicios de la nube deben contemplar estrategias y mecanismos que puedan asegurar la misma mediante el respaldo de datos, redundancia y monitoreo de los servicios.
- **Continuidad de negocios:** La continuidad de negocios en el cloud depende del proveedor de servicios y debemos estar preparados para resolver la pregunta: "¿Qué pasa si el proveedor desaparece mañana?". El riesgo se centra en la viabilidad del proveedor de servicios y se deben considerar factores como: riesgo país en donde residen las instalaciones, cibercrimen, fusiones y adquisiciones, entre otros.
- **Propiedad de los contenidos y requerimientos legales:** Al externalizar los sistemas, datos e infraestructura en la nube surgen algunas preguntas como:
- ¿Podemos traer de vuelta los datos si el proveedor desaparece?
- En caso de desacuerdos, ¿cuál es la jurisdicción legal que resolverá las mismas?
- ¿Quién es el dueño de las aplicaciones y qué derechos tiene la organización?

Mapa y estrategias de gestión

La panorámica es clara, resulta relativamente fácil identificar los riesgos que emergen de la implementación del cloud computing; éste es el primer paso y debemos comenzar a desarrollar el mapa de riesgos y las estrategias para la administración de los mismos. Para ello es clave la definición de una serie de Service Level Agreements (SLAs) relacionados con la administración de los riesgos identificados en la nube. Es importante desarrollar los distintos escenarios y conversarlos con el proveedor de servicios para entender cómo puede cubrir cada uno de ellos y, en la medida de lo posible, realizar auditorías externas al proveedor para tener seguridad razonable de que los controles en cloud se encuentran operando.