Seguridad en la nube

Los servicios en la nube son una realidad que supone nuevos retos para los usuarios de servicios informáticos. ¿Qué beneficios conlleva? ¿Y qué riesgos supone? ¿Qué precauciones se deben tomar antes de contratarlos? Analizamos las pautas de ISACA para asegurar la aportación de valor y el control de riesgos de los servicios en la nube.

ANTONIO RAMOS
Vicepresidente de ISACA Madrid

Si hay una tendencia clara en la contratación informática es el crecimiento de los servicios de computación en la nube. Estos servicios son una evolución de los tradicionales outsourcings basados en la automatización del aprovisionamiento, gracias a las capacidades que han supuesto las tecnologías de virtualización.

Según han resaltado organizaciones como ISACA **(1)** los principales beneficios de este tipo de servicios en la nube son: La contención del coste, dado que la nube ofrece la opción de escalabilidad sin los compromisos financieros necesarios para adquirir y mantener la infraestructura necesaria. La inmediatez, ya que en munchos casos se pueden usar los servicios en el mismo momento en el que se adquieren, haciendo los negocios mucho más ágiles y reduciendo los costes derivados de demoras. La disponibilidad, puesto que los proveedores tienen infraestructura y ancho de banda para satisfacer los requisitos de negocio de acceso, almacenamiento y procesamiento. La escalabilidad, ya que con una capacidad no limitada, los servicios en la nube ofrecen una mayor flexibilidad para las necesidades TI de los usuarios. La eficiencia, puesto que al reasignar actividades al proveedor, el negocio puede enfocar sus esfuerzos en investigar, innovar y en el desarrollo. Y por último, la resiliencia, gracias a las soluciones de los proveedores que pueden ser útiles en escenarios de desastre, así como para balanceo de tráfico.

Riesgos de los servicios en la nube

Como cualquier tipo de servicio, la computación en la nube, además de beneficios, conlleva una serie de riesgos que es necesario con-

	Factores de riesgo	
	Aumentan	Se reducen
Comparativa en función del **modelo de servicio**		
IaaS	• Requisitos legales transfronterizos • Multitenencia y fallos de aislamiento • Falta de visibilidad sobre las medidas de seguridad • Ausencia de PCN y respaldos • Seguridad física • Eliminación de datos • *Offshoring* de infraestructura • Manteninimiento de seguridad de máquinas virtuales • Autenticidad del proveedor cloud	• Escalabilidad y elasticidad • Continuidad de negocio y respaldo • Gestión de parches
PaaS	• Mapeo de aplicaciones • Vulnerabilidades relacionadas con SOA • Eliminación de aplicaciones	• Menor tiempo de desarrollo
SaaS	• Propiedad de los datos • Eliminación de datos • Falta de visibilidad sobre el ciclo de vida de desarrollo • Gestión de identidades y accesos • Estrategia de salida • Mayor exposición de aplicaciones • Facilidad de contratación • Falta de control sobre el proceso de gestión de versiones • Vulnerabilidades del navegador	• Mejoras de seguridad • Gestión de parches de aplicaciones
Comparativa en función del **tipo de despliegue**		
Pública	• Compartición total de la nube • Daños colaterales	• Reputación pública
Comunitaria	• Compartición de la nube	• Mismo grupo de entidades • Acceso dedicado para la comunidad
Privada	• Compatibilidad de aplicaciones • Inversión requerida • Habilidades *cloud* requeridas para TI	• Puede ser construida insitu • Rendimiento
Híbrida	• Interdependencia *cloud*	

TABLA 1. Comparativa de los factores de riesgo

siderar a la hora de seleccionar el servicio más adecuado a las necesidades del usuario. Además de los riesgos típicos de cualquier contratación informática, la utilización de servicios en la nube supone la aparición de nuevos riesgos y el incremento o disminución de los relativos de operar el sistema internamente en función del modelo de servicio y el tipo de despliegue, como se puede apreciar en la TABLA 1 **(2)** .

Debida diligencia en la contratación

Por lo tanto, para asegurar que se ob-

tienen los beneficios esperados de la contratación de servicios en la nube, controlando los riesgos existentes, es necesario llevar a cabo un proceso de selección adecuado que analice estos aspectos de los potenciales servicios en la nube. Cualquier proceso de contratación de servicios en la nube debería ir precedido por un proceso de *due diligence* que evalúe, al menos, los siguientes aspectos **(3)** :

• Conocimiento del proveedor, para asegurar que no se trata de un intermediario de un tercero que pretende utilizar la información para fines distintos a los autorizados.

• Derecho a auditar, para que se pueda verificar la existencia y efectividad de los controles de seguridad especificados en el Acuerdo de Nivel de Servicio (ANS).

• Continuidad asegurada, es decir, el proveedor debe contar con la estabilidad financiera para proporcionar un servicio continuado o devolvernos el servicio en caso de cese de operaciones.

• Transparencia de procesos y políticas de seguridad, para poder evaluar si las medidas de seguridad implementadas por el proveedor responden a las necesidades del usuario en función de la criticidad del proceso de negocio que va a soportar el servicio en la nube, por ejemplo, mediante la creación de sistemas de etiquetado de seguridad como ha propuesto la Estrategia de Ciberseguridad de la UE **(4)** .

NOTAS

(1) "Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives", ISACA, 2009.

(2) Elaborada sobre la base de la información en "Security Considerations for Cloud Computing", ISACA, 2011

(3) "IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud", ISACA, 2011

(4) El primer sistema de etiquetado de seguridad de los servicios TIC ha sido propuesto por la agencia de calificación LEET Security, *www.leetsecurity.com*

SOBRE ISACA

Una de las principales actividades de ISACA es la generación de conocimiento. Además de esta actividad de investigación, cuyo ejemplo más paradigmático es el marco de gobierno de las TIC, COBIT5, ISACA como asociación de profesionales realiza otro tipo de actividades orientadas al networking para lo que se organiza en base a capítulos (existen más de 200 capítulos en el mundo, tres de los cuales, en España: Barcelona, Madrid y Valencia que aglutinan más de 1 600 profesionales -1 100 de los cuales pertenecen al capítulo de Madrid).

Estos capítulos realizan sus propias actividades en sus zonas geográficas de influencia, orientadas al *networking* (como los #juevesISACA que se celebra el primero de cada mes o las Jornadas Técnicas anuales), a la formación de profesionales y, finalmente, a concienciar a la sociedad de la importancia de los profesionales que conformamos la asociación (auditores de sistemas, responsables de seguridad, especialistas en gobierno de las TIC y gestores de riesgo) y a defender sus derechos e influir para que sea reconocida su labor.

Finalmente, la actividad estelar de ISACA es la gestión de cuatro certificaciones profesionales (CISA© – *Certified Information Systems Auditor,* CISM© – *Certified Information Security Manager*, CGEIT© – *Certified in the Governance of Enterprise IT* (CGEIT) y CRISCTM – *Certified in Risk and Information Systems Control*) y cuatro certificados (*COBIT5 Foundation, Implementation* y *Assessor* y, finalmente, *CSX Foundation* dedicada a ciberseguridad).