.Seguridad
Cultura de prevención para TI
Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

PERSPECTIVAS: TODO DEPENDE DEL CRISTAL CON QUE SE MIRE LA NUBE

Jesús Mauricio Andrade Guzmán
Célica Martínez Aponte

información

numero-08

El mundo de la TI como lo conocíamos hace un par de años ha evolucionado notoriamente debido a la aparición del *Cómputo en la Nube o Cloud Computing*. Grandes empresas como *Google, Amazon, Microsoft* e *IBM* han visto en esta tecnología una gran oportunidad de negocio, al explotar cada una de sus capas: *Paas, Saas* e *Iaas* (Plataforma, *software* e infraestructura como servicios), e innovar para brindar diferentes beneficios a sus usuarios.

Esta nueva tendencia implica ventajas y desventajas desde la perspectiva con la que se analice, es decir, depende del cristal con que se mire la nube. Posiblemente, la mayor desventaja en cualquiera de sus perspectivas es que para acceder a cualquier servicio en la nube es necesario contar con una conexión a Internet.

Si nos adentramos en la nube podemos visualizar las siguientes perspectivas:

Empresas en la nube

Gradualmente, se han ido implementando tecnologías de cómputo en la nube en el mundo de los negocios; tanto pequeñas, medias y grandes empresas han comenzado a adoptar estas soluciones.

Toda empresa busca reducir sus costos, y esta tecnología permite reducir los referentes a equipo, pues

sólo se paga por lo que se usa (pago por uso), los servicios son en demanda y su disponibilidad es inmediata. Asimismo, integra actualizaciones, soporte técnico, espacio físico, no se deben pagar costos por equipos obsoletos o en desuso, ahorro de energía, reducción de personal especializado; lo cual permite que las empresas se enfoquen en lo realmente importante, como es mejorar la tarea productiva e impulsar su crecimiento en el mercado al interactuar con los clientes y realizar la labor de venta por medios electrónicos.

Las empresas verán en el cómputo en la nube la oportunidad de lograr su eficiencia.

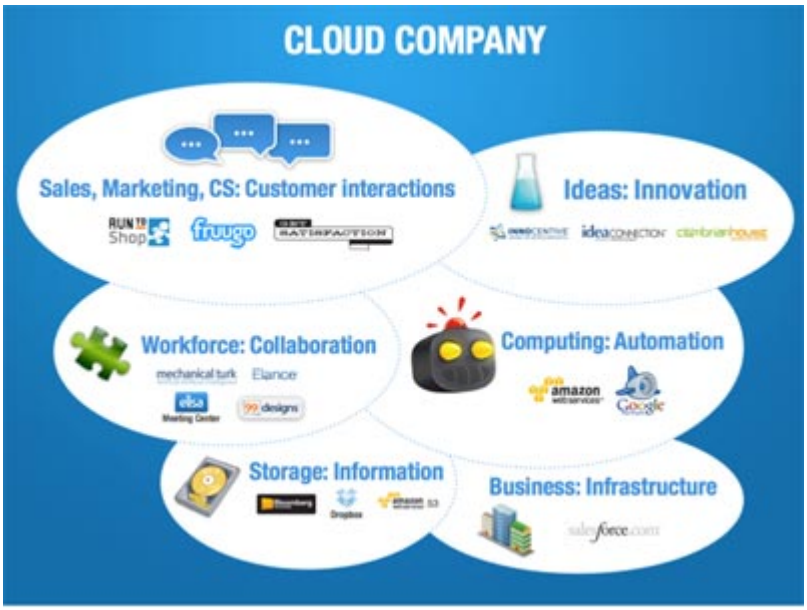

Fig. 1 Cortesía Humanismo y colectividad

Jay Hallberg, cofundador y vicepresidente de *Spiceworks*, afirma que las pequeñas empresas al contar con *outsoursing* de TI, están migrando más rápido sus servicios a la nube, mientras que las más grandes al haber realizado una inversión en infraestructura, son más cautelosas en ello.

Para el 2013, como indicó Gartner se estima que más del 70% de las aplicaciones (APaas) serán desarrolladas por proveedores externos a la misma empresa, es decir que no será necesario contar con áreas dedicadas a esta labor.

Entretenimiento sobre nubes

Nintendo ha declarado su interés en el cómputo en la nube, diciendo que muchos tipos de juegos (aunque no todos) pueden aprovechar esta tecnología en el futuro. Existen proveedores de juegos en la nube como*ONLIVE*[1] o *Steam*[2], los cuales ofrecen una gran diversidad de juegos y una red para los jugadores en la que pueden iniciar juegos multi-jugador, descargar versiones de prueba que permitan tener un contacto más directo entre los distribuidores y los usuarios, sin tener que comprar el videojuego; actualizaciones automáticas de los juegos ofertados, entre otras características.

La tendencia de los videojuegos en la nube apunta a que seguirán siendo un éxito; esto lo podemos ver actualmente en redes sociales como*Facebook,* con juegos como *FarmVille* (desarrollado por el estudio *Zinga*

e integrado inicialmente a esta red social), el cual ahora es posible jugarlo incluso en dispositivos móviles y actualmente cuenta con millones de usuarios en línea.

Antes de las redes sociales como las conocemos hoy en día, ya podíamos ver las tendencias de esto en programas de mensajería instantánea como el Live Messenger de Microsoft, que desde hace ya unos años ofrece juegos a los usuarios, aunque no con el mismo impacto.

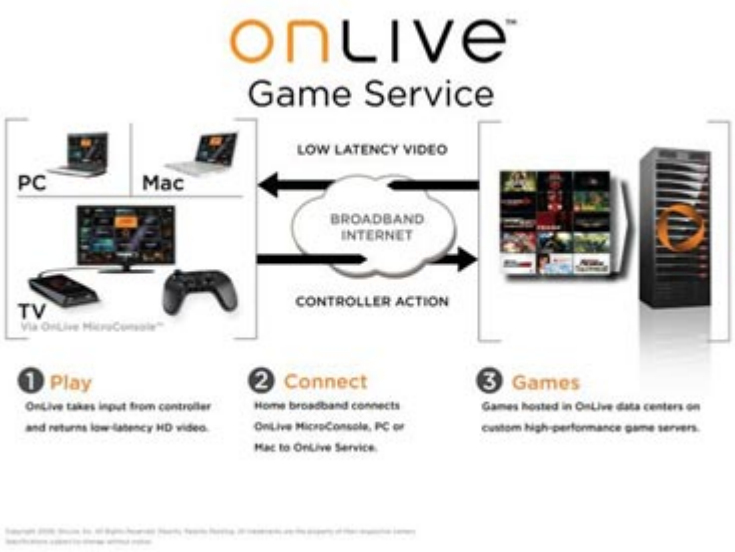

Fig. 2 Cortesía Cnet News

La nube desde el enfoque de seguridad de la información

Conforme el cómputo en la nube alcanza mayor popularidad, las amenazas a las que se expone van en aumento, debido a que resulta más atractivo para los atacantes. A lo largo del tiempo ya se han observado casos conocidos sobre vulnerabilidades aprovechadas en estos servicios, tales como: en la infraestructura en la nube de *Amazon*, el servicio de *MobileMe* de*Apple* y ataques en la plataforma de *Salesforce*.com. Por lo que se espera que estas vulnerabilidades se agudicen y día con día, se perfeccionen los métodos para explotarlas.

Ya en el año 2009 se demostró a través de las conferencias de *BlackHat*USA las vulnerabilidades que existen en los métodos de autenticación utilizados por las firmas de *Microsoft* y *Amazon* en sus servicios de cómputo en la nube.

A continuación, se listan algunos de los riesgos que implica el utilizarlos:

Todos los datos pueden estar en riesgo

El hecho de migrar todos los datos a los servicios de cómputo en la nube sería como “poner todos los huevos en la canasta”, debido a que los riesgos en los niveles de seguridad, la falta de políticas, leyes y estándares claros en torno a los servicios del cómputo en la nube hacen que se pongan en riesgo todos los datos de una organización.

Alojar información sensible de la organización en servidores *CRM* o *ERP* que se encuentran en la nube conlleva el riesgo de perderse en caso de un error en el servidor o un ataque informático. Además no se debe olvidar que el acceso a la información queda sujeto a la disponibilidad y velocidad del servicio de Internet, por lo que ataques como la Negación de Servicios (*DoS*), Negación de Servicios Distribuidos (*DDoS*) y propagación de código malicioso, los cuales se agudizarán conforme las empresas almacenen información sensible en servidores remotos.

Confiabilidad

Muchos de los servicios de cómputo en la nube están basados en la instalación de un equipo preconfigurado a través de una imagen, por ejemplo el servicio de *Amazon´s Elastic Compute Cloud* (*EC2*), en el que el primer paso del proceso es generar una imagen que contenga los datos, aplicaciones, librerías y configuraciones para los clientes de *Amazon Web Services*. La pregunta sería: ¿realmente la gente puede confiar en la ejecución de equipos que han sido creados por otras personas? Si se descubre un hueco de seguridad en la imagen o sistema predefinido implicará la explotación de manera masiva tal como ocurre hoy en día en los Sistemas Operativos y Aplicaciones.

Confianza en las contraseñas

Otro de los riesgos de los servicios en la nube, es la escasa autenticación con que cuentan estos servicios. La seguridad de cualquier cuenta en la nube radica sólo en la contraseña con la que el usuario ingresa al servicio. Un ejemplo reciente ha sido los constantes ataques a los servicios de *Twitter* y *Facebook*, que por el empleo de contraseñas débiles los atacantes han podido robar y hacer públicos datos sensibles de organizaciones y perfiles de usuario.

Sin embargo, el robo de contraseñas no es la única manera de poner en riesgo la autenticación, sino también los débiles sistemas de recuperación de contraseñas con que cuentan estos servicios. En muchos de ellos, el servicio en la nube renueva la contraseña del usuario a través de un link que puede ser fácilmente vulnerado a través de ataques como *phishing* e ingeniería social. Aunado a esto, existe el riesgo de que el usuario siga ingresando contraseñas débiles sin forzarlo a cambiarla constantemente debido a que no se tiene control en la implementación de políticas de seguridad.

Cifrado en los servicios en la nube

Algunos de los proveedores de servicios en la nube no ofrecen cifrado en sus servicios, o bien algunos métodos de cifrado no son lo suficientemente robustos y pueden derivar en alto riesgo de seguridad en la integridad de la información.

No todo lo que se mira desde la perspectiva de seguridad implica un riesgo en la nube, también se han

desarrollado soluciones de seguridad para mitigar amenazas a las TI. Un ejemplo de ello son las tecnologías en la nube para combatir códigos maliciosos, lo cual ha revolucionado la forma en que se concebía el software antivirus, dado que en los tradicionales se almacenan sus firmas en una base de datos local y requieren de una constante actualización. En cambio los antivirus en la nube alojan esta base de datos en el servidor remoto del proveedor y permite extraer muestras de códigos sospechosos para generar una nueva firma de manera más rápida y compartirla con todos los clientes en la nube, por lo que se puede decir que esta nueva tendencia en la detección de código maliciosos es más eficiente e inteligente. Algunos productos que ofrecen esta solución son: *Panda Cloud, Trend Micro HouseCall, Immunet Protect, Kaspersky Cloud AV*, entre otros.

Fig. 3 Cortesía Dragon Jar

Otros servicios disponibles en la nube que fortalecen la seguridad en las TI son *firewalls*, soluciones *antispam*, mecanismos de autenticación y distribución de actualizaciones.

Regulaciones

El cómputo en la nube es un desarrollo nuevo que en la perspectiva legal se deberá enfrentar al reto de cómo adaptarse a este modelo de negocio, en el que buena parte de la información y aplicaciones que manejan los proveedores de servicios se encuentran en la nube, es decir en cualquier parte del mundo, fuera de la frontera física y legal del país de origen. Harán falta marcos jurídicos centrados en cómo funcionan los sistemas que operan en los servicios de computación en la nube, en la responsabilidad jurídica que hay en cada país. Pero también habrá que garantizar que los proveedores de servicios en esta nueva plataforma obtengan la certificación adecuada de instituciones para que no sea posible acceder a centros de datos y mirar. Además, herramientas de gestión, control y medición para hacer un seguimiento del recorrido que hacen los datos en la nube.

El marco legal debe regular el cómo, cuándo y dónde se accede a la información, la trazabilidad de los datos, quién tendrá derecho a auditar los incidentes en la nube y con qué herramientas, o temas legales como la imposibilidad de tener datos confidenciales fuera de las fronteras físicas (es decir, en la nube).

Conclusiones

De acuerdo a las perspectivas del cómputo en la nube se puede concluir:

> *• Sin Internet no hay nube.*
> *• El cómputo en la nube impacta fuertemente a las pequeñas empresas, dado que son las que han ido adoptando esta tecnología para poder acceder a diferentes servicios sin tener que representar un costo muy elevado para ellas.*
> *• Al reducir los costos en la infraestructura de TI se favorece al cómputo verde o ecológico.*
> *• Así como se incrementan las vulnerabilidades de los servicios en la nube, existen también mecanismos de mitigación basados en esta misma tendencia.*

El mecanismo de intercambio de información en la nube hace de esta tecnología una muy completa y de grandes alcances, al masificar la producción de computadoras, por ejemplo: la aparición de las *netbooks*, dispositivos compactos y de costo menor a través de las cuales los usuarios finales, y no necesariamente las organizaciones, pueden aprovechar también muchos de estos recursos.

La tendencia de ataques que desean vulnerar esta tecnología será una constante en el futuro, por lo que las autoridades de aquellos países que alojan los servidores y los periféricos usuarios deberán coordinar medidas reactivas ante ello.

Referencias:

- http://news.cnet.com/onlive-could-threaten-xbox-ps3-and-wii/
- http://www.net-security.org/
- http://www.readwriteweb.com/

- http://www.forbes.com/2009/07/30/
- http://www.bsecure.com.mx/la-ley-y-el-desorden/
- http://es-la.facebook.com/note.php?note_id=120736601292966
- http://www.csospain.es/Piden-un-marco-legal-internacional-para-la-cloud
- http://www.eschoolnews.com/2010/01/21/
- http://www.cioal.com/index.php?
- http://www.dragonjar.org/listado-de-anti-virus-en-la-nube.xhtml

---