PUNTO SEGURIDAD, SEGURIDAD EN TIC | NÚMERO 8 | OCTUBRE 2010 | ISSN EN TRÁMITE | REVISTA BIMESTRAL

Editorial

"*Andar en las nubes*", ese dicho nos refiriere a que, a pesar de estar presentes físicamente en determinado momento, nuestra mente está viajando a otros lugares a través del pensamiento, dicha ausencia permite que aquellos momentos vuelvan por un instante, para que al despertar se guarden en nuestra memoria.

Desde esta perspectiva, la realidad y la nube parecen antagónicas, pero en sí son hechos reales como las vivencias, el trabajo y las relaciones personales quienes nos hacen "*andar por las nubes*", el balance de esto aparece cuando nos plantamos en una o en otra como es debido para así poder vivir la experiencia adecuadamente.

Esta relación ha trascendido los textos literarios o la tradición oral, ahora la metáfora se aplica a una tecnología informática utilizada desde hace algún tiempo, pero que en nuestros días ha cobrado gran importancia y crecimiento, ésta es el *Cómputo en la nube*, en ella, tal como ocurre con el dicho, la información no está presente, sino resguardada a la distancia y puede ser invocada a través de diversos servicios disponibles en Internet.

En este número 8 de la **Revista .Seguridad,** se explica a qué se refiere esta alegoría de la computación, cuáles son sus usos, sus criterios de privacidad para resguardar la información, las tendencias y los *tips* para poder utilizar los servicios que ofrece de manera segura.

El aumento de personas y empresas usuarias de esta tecnología hace apremiante analizarla, muchos desconocen a ciencia cierta las amenazas que pueden encontrar en ésta, por ello es necesario informarlos e incluirlos dentro de la cultura de seguridad en cómputo como mejor alternativa de prevención.

¡Bienvenido! Esperamos esta edición sea de tu agrado.

Galvy Ilvey Cruz Valencia
Subdirección de Seguridad de la Información

Beatriz Verónica Gutiérrez Galán y Francisco Carlos Martínez Godínez

En el modelo tradicional de implementación de Tecnologías de Información (TI), las organizaciones destinan recursos materiales, humanos y tecnológicos, los cuales se agrupan en un área encargada de solucionar los problemas relacionados con la infraestructura informática y el desarrollo de aplicaciones para la organización.

La mayoría de dichas áreas, se ven obligadas a dedicar una buena parte de su tiempo en las tareas de implementar, configurar, dar mantenimiento y actualizar proyectos relacionados con la infraestructura de su organización, lo cual, normalmente no supone un valor añadido en el balance final de la producción de la misma.

Por otro lado, se observa que la distribución de servicios tales como: la energía eléctrica, el agua potable o la telefonía; dejan al proveedor la total responsabilidad de generar, organizar y administrar todo lo necesario para que el usuario final reciba lo acordado, pagando éste únicamente por el uso que hace de los mismos, mientras que el proveedor se encarga de precisar los mecanismos por medio de los cuales determina el consumo por el que se genera el cobro.

De esta manera surge una pregunta interesante: ¿por qué no implementar servicios o recursos de internet bajo un esquema similar al descrito, donde el proveedor proporcione lo requerido y el usuario pague únicamente por el uso que hace?

Si esto ocurriera, el usuario no tendría por qué preocuparse por adquirir equipos de cómputo y su respectivo mantenimiento, actualizar las aplicaciones o sistema operativo, pues sería responsabilidad del proveedor.

Es por este motivo, que las organizaciones están dirigiendo sus miradas hacia esta tecnología conocida como cómputo en la nube (*cloud computig*), la cual es capaz de minimizar el tiempo empleado en actividades de menor valor y permitir al personal que labora en áreas de tecnologías de información, centrar su atención en actividades estratégicas que tienen un impacto real en los procesos de negocio de la organización.

El uso de este concepto se está extendiendo con una velocidad considerable, dando como resultado un incremento en el número de empresas que proporcionan servicios a través de esta tecnología, así como de organizaciones que están pensando seriamente en la adopción del cómputo en la nube como una alternativa totalmente viable.

“El cómputo en la nube es un paradigma que permite ofrecer servicios de cómputo a través de internet, en este contexto la nube es una metáfora de internet” [1]. Los tipos de servicios que

pueden ser proporcionados a través de la nube son extensos. De acuerdo con este modelo, el cliente paga a un proveedor por un servicio o por el uso de un recurso determinado (memoria, almacenamiento, procesamiento, software, bases de datos, etc.) y éste le proporciona dicho servicio a través de internet.

La comercialización y estandarización de tecnologías; la virtualización y el crecimiento de arquitecturas de software orientadas al servicio y el aumento en la confiabilidad de las soluciones empresariales de internet; son las bases sobre las que el cómputo en la nube ha logrado crecer.

Estas tres tendencias, de acuerdo con Christy Pettey, analista de Gartner Daryl Plummer, en su artículo ***Gartner Says Cloud Computing Will Be As Influential As E-business*** [2], constituyen una discontinuidad que creará una nueva forma de relación entre aquellos que utilizan servicios de TI y quienes los ofrecen. Esencialmente esto significará que los usuarios serán capaces de centrar su atención en lo que el servicio proporciona en lugar de preocuparse en cómo se implementa o donde se aloja.

Ventajas

Costos. Podría ser la ventaja más atractiva que presenta el cómputo en la nube, y si no lo es, al menos es la más evidente de todas las que ofrece esta tecnología. Al dejar la responsabilidad de la implementación de la infraestructura al proveedor, el cliente no tiene que preocuparse por comprar equipos de cómputo, capacitar personal para la configuración y mantenimiento de éstos, y en algunos casos, por el desarrollo del software. Además el usuario de estos servicios únicamente paga por los recursos que utiliza, permitiéndole diseñar un plan de pago normalmente a partir del tiempo en que éste se utiliza (memoria, procesamiento, almacenamiento).

Competitividad. Al no tener que adquirir equipos costosos, las pequeñas empresas pueden tener acceso a las más nuevas tecnologías a precios a su alcance pagando únicamente por consumo. De este modo las organizaciones de cualquier tipo podrían competir en igualdad de condiciones en áreas de TI con empresas de cualquier tamaño. La ventaja competitiva no está en aquel que tiene los recursos de cómputo sino en quien los emplea mejor.

Disponibilidad. El proveedor está obligado a garantizar que el servicio siempre esté disponible para el cliente. En este sentido, la virtualización juega un papel fundamental, ya que el proveedor

puede hacer uso de esta tecnología para diseñar una infraestructura redundante que le permita ofrecer un servicio constante de acuerdo a las especificaciones del cliente.

Abstracción de la parte técnica. Como se mencionó al hablar de costos, el cómputo en la nube permite al cliente la posibilidad de olvidarse de la implementación, configuración y mantenimiento de equipos; transfiriendo esta responsabilidad al proveedor del servicio.

Acceso desde cualquier punto geográfico. El uso de las aplicaciones diseñadas sobre el paradigma del cómputo en la nube puede ser accesible desde cualquier equipo de cómputo en el mundo que esté conectado a Internet. El acceso normalmente se hace desde un navegador web, lo que permite a la aplicación ser utilizada no únicamente desde una computadora de escritorio o una computadora portátil, sino que va más allá, permitiendo al usuario hacer uso de la aplicación incluso desde dispositivos móviles como *smartphones*.

Escalabilidad. El cliente no tiene que preocuparse por actualizar el equipo de cómputo sobre el que se está corriendo la aplicación que utiliza, ni tampoco por la actualización de sistemas operativos o instalación de parches de seguridad, ya que es obligación del proveedor del servicio realizar este tipo de actualizaciones. Además, éstas son transparentes para el cliente, por lo que la aplicación debe de continuar disponible para el usuario en todo momento aún cuando se esté realizando el proceso de actualización del lado del proveedor. Las actualizaciones y nuevas funcionalidades son instaladas prácticamente de manera inmediata.

Concentración de esfuerzos en los procesos de negocio. Como resultado de las ventajas antes mencionadas, el cliente pude concentrar más recursos y esfuerzos hacia un aspecto más estratégico y trascendente, que tenga un impacto directo sobre los procesos de negocio de la organización, transfiriendo al proveedor la responsabilidad de la implementación, configuración y mantenimiento de la infraestructura necesaria para que se ejecute la aplicación.

Desventajas

Privacidad. Es comprensible la percepción de inseguridad que genera una tecnología que pone la información (sensible en muchos casos), en servidores fuera de la organización, dejando como responsable de los datos al proveedor de servicio. El tema a tratar aquí, es el de la privacidad, ya que para muchos es extremadamente difícil el confiar su información sensible a terceros y

consideran que lo que propone el cómputo en la nube pone en riesgo la información vital para los procesos de negocio.

Disponibilidad. Si bien es cierto que se incluyó a la disponibilidad previamente como una ventaja, ésta queda como una responsabilidad que compete únicamente al proveedor del servicio, por lo que si su sistema de redundancia falla y no logra mantener al servicio disponible para el usuario, éste no puede realizar ninguna acción correctiva para restablecer el servicio. En tal caso, el cliente debería de esperar a que el problema sea resuelto del lado del proveedor.

Falta de control sobre recursos. Al tener toda la infraestructura e incluso la aplicación corriendo sobre servidores que se encuentran en la nube, es decir, del lado del proveedor, el cliente carece por completo de control sobre los recursos e incluso sobre su información, una vez que ésta es subida a la nube.

Dependencia. En una solución basada en cómputo en la nube, el cliente se vuelve dependiente no sólo del proveedor del servicio, sino también de su conexión a internet, debido a que el usuario debe estar permanentemente conectado para poder alcanzar al sistema que se encuentra en la nube.

Integración. No en todos los entornos resulta fácil o práctica la integración de recursos disponibles a través de infraestructuras de cómputo en la nube con sistemas desarrollados de una manera tradicional, por lo que este aspecto debe ser tomado en cuenta por el cliente para ver qué tan viable resulta implementar una solución basada en la nube dentro de su organización.

El cómputo en la nube se puede dividir en tres niveles en función de los servicios que ofrecen los proveedores. Desde el nivel más interno hasta el más externo se encuentran: Infraestructura como Servicio, Plataforma como Servicio y Software como Servicio. A continuación se describen brevemente cada uno de estos niveles:

Infraestructura como Servicio (IaaS - Infraestructure as a Service)

“La Infraestructura como un servicio es un modelo de aprovisionamiento, en el cual una organización coloca ‘fuera de ella’ el equipo usado para soportar operaciones, esto incluye el

almacenamiento de la información, el hardware, servidores y componentes de redes. El proveedor del servicio. En ocasiones la IaaS es referida también como Hardware as a Service o HaaS" [3].

La ventaja más evidente de utilizar una IaaS, es la de transferir hacia el proveedor problemas relacionados con la administración de equipos de cómputo. Otra ventaja atractiva es la reducción de costos, como ocurre en general en las tecnologías asociadas al cómputo en la nube, al pagar únicamente por lo consumido. Además las Infraestructuras como Servicio permiten escalabilidad prácticamente automática y transparente para el consumidor, dejando la responsabilidad a los proveedores de los servicios.

Otras de sus características son: la conectividad a Internet que provee, los servicios basados en políticas y la disposición de un escritorio virtual.

Plataforma como Servicio (PaaS - Platform as a Service)

La computación en la nube y su rápido crecimiento ha requerido "incluir plataformas para crear y ejecutar aplicaciones personalizadas, a este concepto se le conoce como PaaS (o en español Plataforma como un Servicio). Las aplicaciones PaaS también son conocidas como de sobre-demanda basadas en Web o soluciones SaaS" [4].

El proveedor, además de resolver problemas en la infraestructura de hardware, también se encarga del software. El cliente que hace uso de este tipo de soluciones no necesita instalar, configurar ni dar mantenimiento a sistemas operativos, bases de datos y servidores de aplicaciones ya que todo esto es proporcionado bajo esta plataforma.

Una plataforma como servicio (PaaS) resuelve más problemas si se compara con una solución que sólo ofrece una infraestructura como servicio (IaaS), ya que presenta muchas limitaciones relacionadas con el entorno de ejecución. Entre éstas se encuentran el tipo de sistema, el lenguaje de programación (en algunos casos las bibliotecas que éstos podrán utilizar), el manejador de bases de datos.

Empresas como Amazon.com, eBay, Google, iTunes y YouTube son algunas de las que emplean este modelo y hacen posible accesar a nuevas capacidades y nuevos mercados a través del

navegador Web, las PaaS ofrecen un modelo más rápido y ventaja costo-beneficio para el desarrollo de aplicaciones y entrega". [5]

Software como Servicio (SaaS – Software as a Service)

"Es el más conocido de los niveles de cómputo en la nube. El SaaS es un modelo de distribución de software que proporciona a los clientes el acceso a éste a través de la red (generalmente Internet). De esta forma, ellos no tienen que preocuparse de la configuración, implementación o mantenimiento de las aplicaciones, ya que todas estas labores se vuelven responsabilidad del proveedor. Las aplicaciones distribuidas a través de un modelo de Software como Servicio pueden llegar a cualquier empresa sin importar su tamaño o ubicación geográfica." [6]

Este modelo tiene como objetivo al cliente final que utiliza el software para cubrir procesos de su organización. El Software como Servicio (SaaS) se puede describir como aquella aplicación consumida a través de Internet, normalmente a través del navegador, cuyo pago está condicionado al uso de la misma y donde la lógica de la aplicación así como los datos residen en la plataforma del proveedor. Ejemplos de *SaaS son Salesforce, Zoho, y Google App.*

Experiencia con el cómputo en la nube

Una usuaria integrante de la Subdirección de Seguridad de la Información, comenta un poco sobre sus impresiones después de haber utilizado el cómputo en la nube para resolver un problema de trabajo en conjunto:

"*Mi primera experiencia con el cómputo en la nube fue en una ocasión en que trabajé un proyecto en equipo.*

Cada uno de los integrantes nos encontrábamos físicamente en zonas geográficas lejanas, y para la toma de decisiones, era importante que tuviéramos en un sólo equipo el desarrollo del proyecto y que todos pudiéramos manipularlo, dicho de otra manera, compartir el área de trabajo.
Utilizar el cómputo en la nube nos permitió resolver este problema.

Primeramente se montó en la computadora personal de uno de los integrantes, y utilizando una herramienta disponible dentro del cómputo en la nube, el resto del equipo podía visualizar las acciones que se llevaban a cabo por parte de la persona que controlaba el proyecto, y en cualquier momento, gracias a esta misma herramienta, cualquiera de los otros miembros podía tomar el control del trabajo.

Por otro lado, en la realización del reporte final, se elaboró una presentación en una plataforma donde también se aplica este mismo concepto. Mediante ella, todos los colaboradores manipulamos el mismo archivo, lo que nos permitió ahorrarnos tiempo en vez de estar enviado y reenviado el archivo por correo."

Ella comenta que la utilización de esta tecnología fue fundamental para la oportuna y adecuada integración del equipo de trabajo, así como de las respectivas partes del proyecto, además resalta que una de las ventajas que ofrece este paradigma es el ahorro de tiempo.

Conclusiones

Esta tecnología, como sucede normalmente, presenta un crecimiento gradual. Si bien es cierto que el cómputo en la nube es una tecnología que ya se utiliza desde hace algunos años, aún falta que sea completamente absorbida como una tendencia central en las organizaciones.

El nivel de aceptación entre las organizaciones variará dependiendo del tamaño de éstas. Las medianas y pequeñas empresas ya empiezan a adoptar soluciones basadas en cómputo en la nube, mientras que las grandes organizaciones lo hacen de acuerdo a necesidades particulares.

En la otra cara de la moneda, se encuentran los usuarios finales, a quienes el cómputo en la nube les ha cambiado la forma de realizar sus actividades, mejorando en la mayoría de los casos y permitiéndoles colaborar de una manera distinta con otros usuarios en diferentes lugares, tener acceso a las aplicaciones que requieren desde su navegador web y prácticamente desde cualquier equipo, incluso desde sus dispositivos móviles.

Referencias:

[1] http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_nube
[2] http://www.gartner.com/it/page.jsp?id=707508
[3] http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1358983,00.html
[4] http://www.salesforce.com/paas/
[5] http://msdn.microsoft.com/en-us/magazine/ee309870.aspx

Julio César García Vizcaíno y Galvy Ilvey Cruz Valencia

Hablar de criterios e implicaciones de privacidad de la computación en nube, es tratar un tema un tanto acotado y poco difundido, aunque muy usado, entre los usuarios de esta tecnología.

El vertiginoso intercambio de datos entre individuos y organizaciones en la actualidad es de gran volumen en Internet. En los últimos años, se ha generalizado el uso de proveedores de tecnología que ofrecen sus servicios desde la red.

El acceso a este tipo de servicios está muy arraigado entre los usuarios, basta mencionar servicios como *flickr*[1], *Amazon S3*[2] o *Salesforce*[3]. Los procesos basados en la nube son la mayor parte del mercado de los servicios de este tipo, e incluye publicidad, comercio electrónico, recursos humanos y procesos de pago.

Una de las principales formas de generar confianza, entre proveedores y usuarios (clientes), es ponerse de acuerdo sobre quién obtiene qué derechos, y quién asume responsabilidades de lo que pase con la información en la nube.

La novedad es la misma de siempre: la preocupación; ya que muchos de los asuntos de privacidad en la nube son objeto de constantes inquietudes acerca de:

- La información dispuesta a través de servidores y aplicaciones externos.
- La manera en cómo las personas y las organizaciones conforman su postura ante las políticas aplicables, regulaciones estándar, contratos y políticas de intercambio.
- La metodología con la que la información es puesta en la nube y cómo permanece en ella, así como también la certidumbre de que al borrarla, realmente sea así.
- Las palabras clave generadas para mostrar y acceder a la información para modificarla, copiarla u otros usos.

Estas consideraciones deberían llevar a la difusión de mecanismos reguladores que orienten a los usuarios a un empleo más definido de estos servicios, así como de las ventajas y desventajas que pueden encontrar en las políticas de privacidad que los proveedores otorgan.

La introducción de criterios de privacidad es esencial para resolver las preocupaciones de los usuarios. Algunas políticas de privacidad de estos sitios de almacenamiento son a la vez que explicitas, requirentes para los usuarios. Un ejemplo se encuentra en la *Declaración de derechos y responsabilidades de Facebook*, en la cual la empresa específica que la propiedad intelectual del

1 http://www.flickr.com Sitio web dedicado al almacenamiento de imágenes, fotos, etc.
2 http://aws.amazon.com/s3/ Página que proporciona servicios de almacenamiento en la nube
3 http://www.salesforce.com Página que ofrece servicios de recursos humanos y marketing en la nube.

contenido es del usuario, pero al aceptar las condiciones, se le otorga a la empresa un permiso extensible de uso del contenido, mismo que se cancela sólo con la desactivación o eliminación de la cuenta.

El correcto establecimiento de políticas de privacidad de la información en este tipo de servicios (sea *SaaS*[4], *PaaS*[5], *IaaS*[6]) evita que datos como: nombre, tarjeta de crédito, registros biométricos, etc., puedan ser usados para distinguir o rastrear la identidad de un individuo; y éstos se utilicen para cometer fraudes, robos de identidad, envío de correo no deseado, entre otros.

No obstante, falta preocupación de los proveedores respecto a las consecuencias de no tener control adecuado sobre la privacidad de la información de sus clientes; un hecho concreto ocurre en la declaración de políticas de Amazon[7] o Facebook[8], en las que se aclara a los clientes que no se respalda la seguridad del servicio, pues éste se ofrece tal cual y sin ningún tipo de garantía.

Los miedos de los usuarios están justificados, pues no existe una figura legal que establezca discernimientos sobre cuándo una información puede hacerse pública, cuándo debe estar asegurada, o bien, cuándo es robada.

Empresas como *Microsoft* han clamado por la instauración de una legislación específica para la seguridad de la nube, aunque reconoce que "necesita hacer políticas de seguridad más transparentes, pero además el gobierno de Estados Unidos debería introducir políticas específicas de protección de datos para el cómputo en nube y reprimir con más eficacia a usuarios maliciosos que afecten a centros de datos."[9]

Del lado mexicano, el avance en cuanto a privacidad y protección de la información ha crecido lentamente, no obstante el 5 de julio de este año se publicó en el *Diario Oficial de la Federación* la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, en la cual se preservan en esencia la privacidad, confinación y autodeterminación de la información de las personas.

---

4 Software as a Service: el usuario utiliza las aplicaciones del proveedor en su infraestructura de nube.
5 Platform as a Service: el usuario utiliza la infraestructura del proveedor mediante aplicaciones creadas o adquiridas por el usuario.
6 Infrastructure as a Service: el usuario utiliza el procesamiento, almacenamiento, redes y otros recursos computacionales para desplegar y ejecutar software arbitrario.
7 De la declaración de Condiciones de Uso de Amazon Inc., sobre Exclusión de garantías y limitación de responsabilidad (en) http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=508088
8 De la Declaración de derechos y responsabilidades de Facebook, Punto 15, inciso 3 (en) http://www.facebook.com/terms.php
9 Rosalie Marchal, Microsoft calls for cloud security legislation (en) http://www.v3.co.uk/v3/news/2256559/microsoft-calls-increased-cloud
10 DOF, 5 de julio de 2010 (en) http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

En esta ley se hace observación sobre el consentimiento, el cual se entiende como la "manifestación de la voluntad del titular de los datos personales mediante la cual se efectúa el tratamiento de los mismos"[10].
El criterio de consentimiento aplicado a las políticas de uso de los servicios de cómputo en la nube podría servir para dar contexto y referencia sobre lo que usuarios podrían exigir en caso de presentarse una infiltración o violación a las sesiones privadas en este tipo de servicios, aunque debemos ser conscientes que la amenaza siempre estará presente.

Entre los riesgos que más persisten bajo este panorama se pueden mencionar:

- El uso permitido de información por parte del proveedor podría no estar claramente definida en los términos del servicio o contrato, permitiendo al proveedor, por ejemplo, usarla para sus propósitos o venderla a terceros. Por ejemplo la red social *Hi5*[11] específica que parte de la información personal del miembro es revelada durante todo el año a terceros para propósitos publicitarios, y que si el usuario desea saber a quién se proporcionó estos datos requiere solicitarla al administrador de la red.
- El proveedor podría ser requerido para permitir a autoridades judiciales locales o extranjeras buscar en la información resguarda por éste. Un caso[12] reciente al respecto sucedió en el Reino Unido, en el cual un joven de 16 años fue arrestado por no proporcionar a las autoridades la contraseña de su equipo, pues se sospechaba que él ejecutaba actividades ilícitas a través de la red.
- La información almacenada por el proveedor podría verse comprometida, sin informar a las autoridades competentes o a los usuarios afectados por el incidente.
- El proveedor podría no tomar las medidas necesarias para evitar perder accidentalmente la información
- Que los proveedores no garanticen al usuario que su información no sea expuesta durante el intercambio de datos con otros usuarios a través de estos servicios.
- La viabilidad del proveedor. ¿Qué sucede con la información si el proveedor queda en banca rota? Empresas como *Facebook*, indican en su declaración de políticas que si esto ocurriera la información sería respaldada, se transferiría con el proveedor que adquiriera la marca y se respetarían las políticas de privacidad convenidas cuando se creó la cuenta.
- La eliminación completa de la información del usuario en la infraestructura de nube existe dentro del decálogo de políticas, por ejemplo en la de Google Inc. se establece que "debido a la forma en que *Google* mantiene ciertos servicios, una vez que se haya eliminado la información, es posible que las copias residuales tarden algún tiempo en eliminarse de los servidores activos y que permanezcan en los sistemas de copia de seguridad".[13]

10 DOF, 5 de julio de 2010 (en) http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010
11 Políticas de privacidad de Hi5 (en) http://hi5.com/friend/displayPrivacy.do
12 http://www.seguridad.unam.mx/noticias/?noti=4074 - Encarcelan a hombre por negar contraseña de computadora
13 Políticas de privacidad de Google Inc. (en) http://www.google.com/intl/es/privacypolicy.html

El proveedor y el usuario deberían cumplir con los siguientes lineamientos para procurar la privacidad de la información:

Proveedor:

- Garantizar al usuario proporcionar toda divulgación en relación con las prácticas y procedimientos de seguridad que se incluyen en los Niveles de Servicio.
- Divulgar al usuario la localización geográfica de la información.
- Informar al usuario cuando el proveedor esté obligado a entregar su información a una autoridad legal.
- Contar en los términos del servicio con una cláusula que garantice que se niega el acceso a los datos como política general.
- Aplicar los requisitos de acceso a la información impuestas por el usuario.
- No podrá reclamar la propiedad de cualquier información agregada, creada, generada, modificada, almacenada, o en cualquier otra forma asociada con la propiedad intelectual del usuario, esfuerzo de ingeniería o creatividad de medios de comunicación.
- Especificar qué puede y no hacer el proveedor con la información del usuario.
- Proporcionar al menos un mecanismo de acceso, por ejemplo una *API*[14], para la manipulación de la información del usuario.
- Garantizar que se realicen copias de seguridad de la información del usuario y no mezclarla con la de otros usuarios.
- Avalar que se utiliza un cifrado robusto de almacenamiento de la información, el cual imposibilite el acceso a la misma cuando ésta sea reciclada, enajenada o accedida por cualquier medio distinto a las solicitudes, procesos o entidades autorizadas.
- Destruir la información, cuando el usuario lo solicite, en todas las localizaciones físicas y lógicas.
- Entregar reportes de auditorías, las cuales especifiquen que sus planes de continuidad del negocio funcionan.
- Explicar cómo monitorea y controla el acceso a la información realizado por sus empleados.

Usuario:

- Comprender cómo se mantiene la privacidad y hacer evidente el compromiso de ésta en pro del cliente.
- Considerar leyes y directivas del país donde la información se ubica físicamente.
- Realizar una evaluación de la información y sistemas propuestos a trasladar hacía la nube.

14 Application programming interface: representa una interfaz de comunicación entre componentes de software.

- Conducir, si se cuenta con los conocimientos necesarios, una evaluación del impacto de la privacidad para identificar y mitigar los riesgos derivados de la privacidad de la información.
- Determinar quién debería tener acceso a la información, cuáles son sus derechos y privilegios y bajo qué condiciones se otorga el acceso.
- Generar una política de denegación por defecto.
- Definir e identificar la clasificación de la información.
- Revelar información cuando sea requerida por una autoridad legal.
- Cifrar la información almacenada en la infraestructura en nube y la que está en tránsito.
- Comprender los mecanismos de compartición para aislar a los distintos usuarios y su correspondiente información.
- Comprender los procesos de retiro de almacenamiento por del proveedor.
- Desarrollar planes de retención y destrucción de la información.

La computación en nube puede representar una mejora en la privacidad de información de aplicaciones no críticas. Sin embargo la transparencia es crucial, los usuarios deben poder evaluar y comparar las prácticas de seguridad de cada proveedor. Actualmente, la migración de información crítica continúa siendo muy riesgosa (incluso en nubes privadas).

Desde esta perspectiva, las preocupaciones por la privacidad continuarán a la alza, ya que la información, en distintos formatos, procesada y almacenada en la nube, usualmente contiene datos personales o información sensible de las organizaciones, los cuales siempre resultan atractivos para los delincuentes cibernéticos.

Referencias:

http://www.slideshare.net/chemai64/seguridad-en-dispositivos-mviles
Cloud Computing, *William F. Pelgrin, Cyber Security Tips Newsletter. Abril 2010, Volume 5, Issue 4*
http://www.msisac.org/awareness/news/2010-04.cfm

Privacy Compliance, Homeland Security. 28 de julio 2010
http://www.dhs.gov/files/publications/gc_1209396374339.shtm

Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies, CIO Council. Agosto 2010.

Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance. Diciembre 2009.

Gartner Global IT Councils for Cloud Services, Gartner. 2010.

The 'Cloud Computing Bill of Rights': 2010 edition, James Urquhart. 7 de junio de 2010 http://news.cnet.com/8301-19413_3-20006756-240.html

Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, Robert Gellman. 23 de febrero de 2009.

Taking Account of Privacy when Designing Cloud Computing Services, Siani Pearson, 2009, http://www.hpl.hp.com/techreports/2009/HPL-2009-54.pdf

Privacy and Cloud Computing Challenges, Rebecca Herold, 16 de abril de 2010, https://www.infosecisland.com/blogview/3539-Privacy-and-Cloud-Computing-Challenges.html

Diario Oficial de la Federación, 5 de julio de 2010, http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

Políticas de privacidad de Google Inc., actualizadas al 3 de octubre de 2010, http://www.google.com/intl/es/privacypolicy.html

Políticas de privacidad de Hi5, actualizada al 4 de octubre de 2010, http://hi5.com/friend/displayPrivacy.do

Políticas de privacidad de Facebook, actualizada al 5 de octubre de 2010, http://www.facebook.com/policy.php

Declaración de derechos y responsabilidades de Facebook, actualizada al 5 de octubre de 2010, http://www.facebook.com/terms.php

Condiciones de uso Amazon Inc. (sin fecha de actualización) http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=508088

Célica Martínez Aponte y Jesús Mauricio Andrade Guzmán

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.

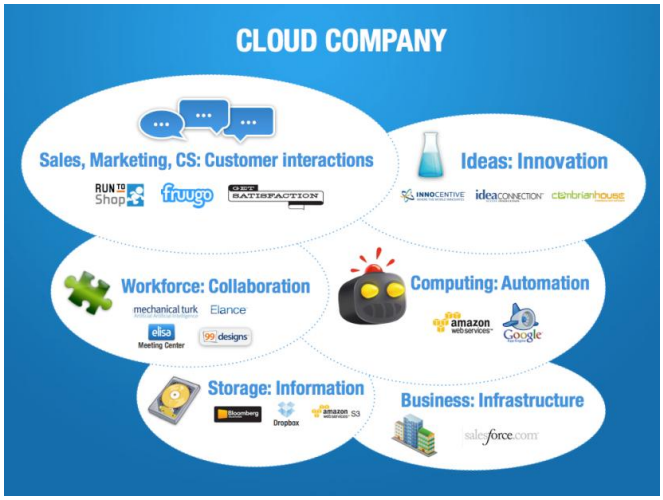
Si nos adentramos en la nube podemos visualizar las siguientes perspectivas:

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.



http://humanismoyconectividad.wordpress.com/2010/06/26/en-la-nube/

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*[7] o *Steam*[8], 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.

[7] Es una solución de juegos en la nube que ofrece videojuegos bajo demanda bajo una cuota mensual que permite comprar juegos o sólo rentar tiempo de juego (pagando por días de acceso al juego)

[8] Plataforma de videojuegos en línea que se ofrece como un programa cliente para Windows o Mac que permite conectarse a una red de jugadores y distribuidores de juegos, todo a través de la nube. Su oferta es en forma de tienda en línea para que los usuarios tengan una plataforma para comprar y mantener actualizados sus juegos.

Perspectivas: Todo Depende con el Cristal con que se Mire la Nube

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.

http://news.cnet.com/onlive-could-threaten-xbox-ps3-and-wii/

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.

http://www.dragonjar.org/listado-de-anti-virus-en-la-nube.xhtml

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/article.php?id=1469&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader
http://www.readwriteweb.com/archives/the_cloud_isnt_safe_or_did_blackhat_just_scare_us.php
http://www.forbes.com/2009/07/30/cloud-computing-security-technology-cio-network-cloud-computing.html
http://www.bsecure.com.mx/la-ley-y-el-desorden/cloud-computing%e2%80%a6-%c2%bfuna-tormenta-legal-se-avecina/
http://es-la.facebook.com/note.php?note_id=120736601292966
http://www.csospain.es/Piden-un-marco-legal-internacional-para-la-cloud/seccion-politicas/noticia-91834
http://www.eschoolnews.com/2010/01/21/microsoft-calls-for-cloud-computing-regulations/
http://www.pcwla.com/pcwla2.nsf/articulos/CB7E1AA43477D23C8525776400135454
http://www.datacenterdynamics.com/ME2/Audiences/dirmod.asp?sid=&nm=&type=news&mod=News&mid=9A02E3B96F2A415ABC72CB5F516B4C10&AudID=8DE637502217499CB2D53BD20E2E2404&tier=3&nid=915952142BF34C6FA9546FA85F9D4B49
http://www.cioal.com/index.php?option=com_content&view=category&layout=blog&id=1&Itemid=221&limitstart=10
http://www.dragonjar.org/listado-de-anti-virus-en-la-nube.xhtml

Anaid Guevara Soriano y José Reinel Ramírez Solares

Hoy en día se escucha hablar mucho del término *cloud computing*, que en español se interpretaría como "cómputo en la nube", éste parece ser novedoso, sin embargo, muchas de sus aplicaciones se utilizan diariamente sin darse cuenta, por ejemplo en: las redes P2P, muchos servicios gratuitos de *Google*, el proyecto *SETI@Home*, ciertos servicios web curiosos, e incluso algunos sistemas operativos como *Jolicloud*. Estos sistemas se gestionan en la nube y el usuario final tan sólo se conecta utilizando la potencia de los servidores sin necesidad de tener éstos consigo. A veces es necesario un pequeño programa cliente, hecho a medida. Pero en la mayoría de las ocasiones basta tan sólo un navegador web.

Un grupo de expertos del *NIST* (*National Institute of Standards and Technology*) realizó un estudio sobre los principales problemas de seguridad que aún hay que superar para poder aplicar esta tecnología a un nivel mucho más amplio. Pero existen diversas opiniones de primer nivel que ven problemas mucho más serios, asociados a la privacidad y a la libertad del usuario.

La estructura del sistema permite el acceso a un grande y poderosos equipo de cómputo sin necesidad de mantenimiento por parte del usuario. Esto hace que sea una plataforma ideal para el desarrollo de proyectos científicos que necesitan computadoras de gran potencia y que de otra manera no podrían tener acceso a ellas. Sobre este modelo de funcionamiento también se soportan sistemas de gestión internos de empresas, como *Opentaps*, así como un modelo de negocio dirigido a ellas. Proveedores de servicios en la nube son *Sun*, *IBM*, *Amazon* y *Google* entre otros. Y entre sus clientes hay grandes empresas, como *General Electric.*

El modelo de servicios del entorno de computación en nube está comprendido por tres opciones centrales (Fig. 1):

- **El software como Servicio (SaaS).** Comprende aplicaciones para usuarios finales entregadas como servicios, en lugar de software en-premisa.
- **La plataforma como Servicio (PaaS).** Provee una plataforma para aplicaciones o *middleware* como un servicio en el que los desarrolladores pueden crear y desplegar aplicaciones personalizadas.
- **La infraestructura como Servicio (IaaS).** Concierne el hardware, la tecnología para el almacenamiento, funcionamiento de sistemas operativos e informáticos; otras infraestructuras entregadas como fuera-de-premisas, servicios bajo demanda en vez de dedicados y recursos en el sitio, tales como el *Amazon Elastic Compute Cloud* (Amazon EC2) o el *Amazon Simple Storage Service* (Amazon S3).

Tips de Seguridad para el Cómputo en Nube

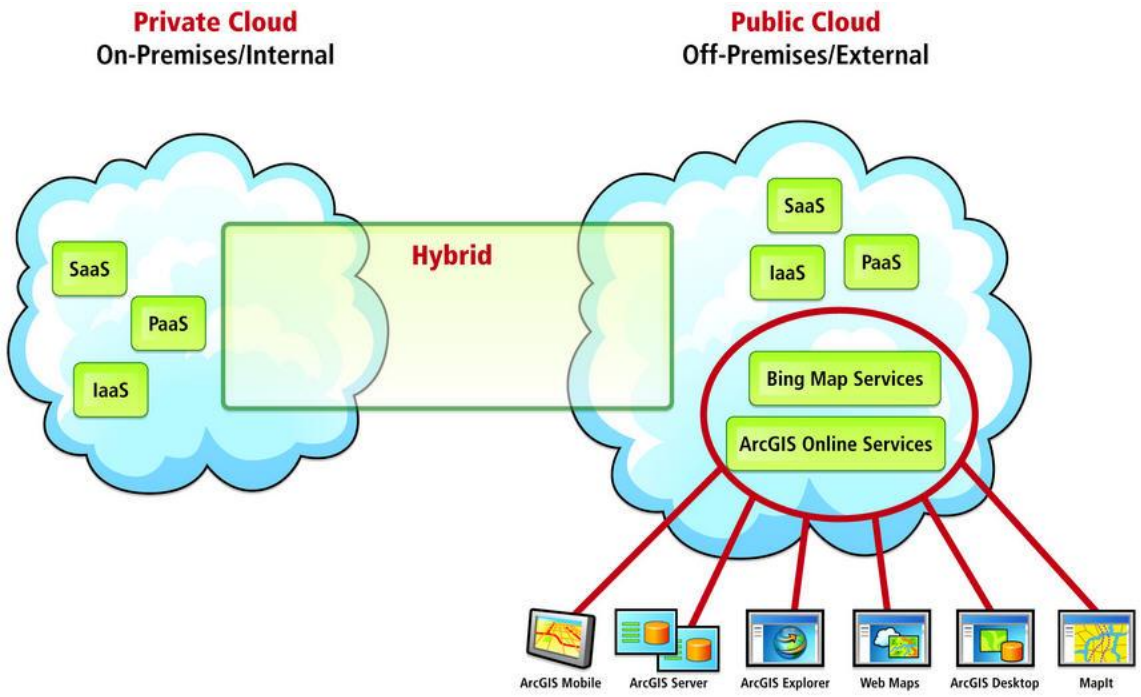


Fig. 1.

A pesar de ello, cabe destacar que si bien es cierto que el *cloud computing* trae consigo grandes ventajas, también es cierto que cuanta más crítica es la aplicación más importante es la fiabilidad del sistema, así como la seguridad de los datos. Por consiguiente, se tiene una mayor susceptibilidad a ser víctima de un ataque con fines maliciosos.

A continuación se enuncian algunos de los *tips* respecto a las medidas esenciales de seguridad que se deben considerar para poder hacer uso de la nube de manera segura, evitando así la mayoría de los riesgos que esto implica:

1.	Considerar la guía de la *Alianza de Seguridad en Cómputo* referente a la nube

Los puntos más destacados de esta guía son:

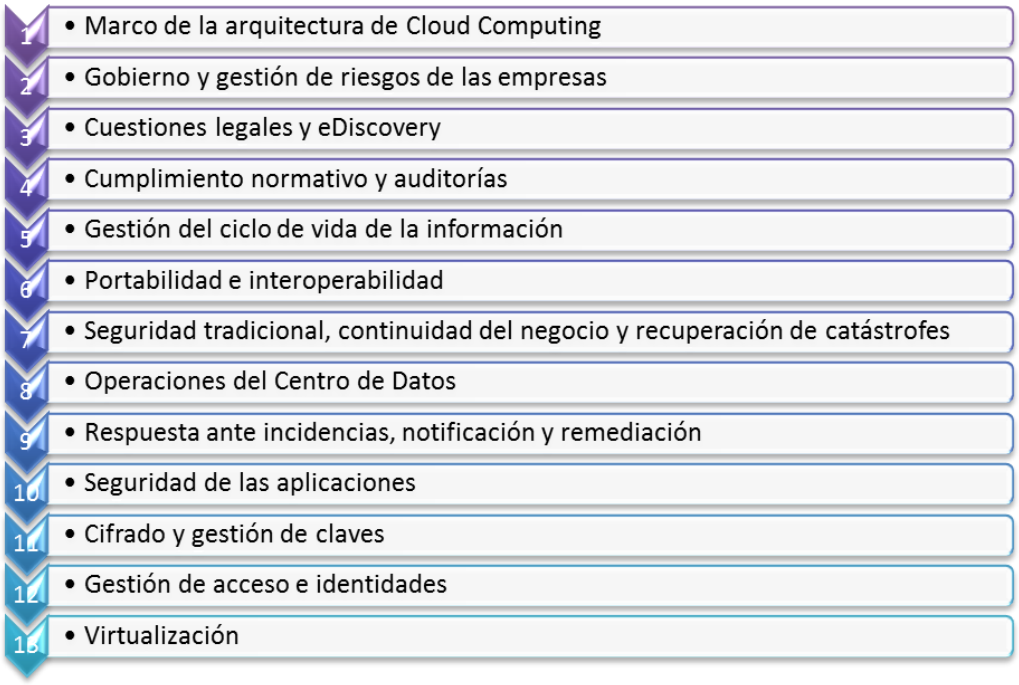


Fig. 2

Para una lectura a detalle de cada uno, sugerimos dirigirse a:
http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

2.	Elegir adecuadamente la contraseña

Otro asunto preocupante de los servicios del cómputo en la nube es que, a pesar de las medidas de protección que implementan todas las empresas, la seguridad de las cuentas de los usuarios depende de la contraseña asignada a cada una de éstas. Un ejemplo de las consecuencias dadas por utilizar contraseñas inseguras fue evidente hace poco en el caso *Twittergate*, en el que un cracker obtuvo numerosos documentos corporativos pertenecientes al popular servicio de microblogging, *Twitter*, y los publicó en el sitio de noticias y tecnología *TechCrunch*. Estos documentos estaban alojados en *Google Docs* y a pesar de que *Google* no puede aceptar la responsabilidad por la fuga de información, los archivos no hubieran sido robados en primer lugar si hubieran estado albergados detrás de un firewall. En lugar de eso, la información clave de la compañía estuvo a punto de ser descubierta, “a un password descifrado de distancia”.

La diferencia entre una red corporativa y una cuenta en línea es que en un ecosistema de negocios, los administradores pueden crear políticas para la creación de contraseñas que los obliguen a mantener ciertos niveles de complejidad y a crear nuevas contraseñas periódicamente. No obstante, en la nube, tenemos la libertad de establecer lo que sea como contraseña y no volver a cambiarla nunca más. Ésta es un área que aún necesita mucho trabajo. Por tal situación se recomienda:

1. Selección de contraseñas “fuertes”, difíciles de descifrar.
2. Mantenerlas en secreto.
3. No transferirlas.
4. No escribirlas en papeles de fácil acceso o en archivos sin cifrar.
5. No habilitar la opción “recordar clave en este equipo”, que ofrecen los programas.
6. No enviarlas por correo electrónico.
7. Cambiarlas frecuentemente.

3.	Cifrar datos en la nube

Otra de las debilidades (poco conocidas) de cómputo en la nube es que pocas máquinas tienen acceso a los números generados al azar que se necesitan para cifrar información.

Los detalles de este lío son excesivamente técnicos pero el resultado es que la inherente naturaleza de la computación virtual hace mucho más simple la tarea a los hackers y crackers porque les permite adivinar con facilidad los números utilizados para generar las llaves de cifrado.

Si bien éste no es un problema inmediato que atenta contra la integridad de la nube, sí requerirá investigación a largo plazo.

Para el cifrado de datos en la nube se recomienda:

1. Administración remota segura. Cifrado del tráfico.
2. Clasificar y cifrar información sensible con aplicaciones de cifrado confiables.
3. Utilizar tecnologías de cifrado de punto a punto (**VPN**).
4.

4.	Usar adecuadamente los servicios de la nube

Si consideramos los problemas ya descritos, probablemente pensaremos dos veces antes de confiar en los servicios que funcionan a través de la nube.

Pero, ¿En verdad es tan malo? ¿Es la nube una plataforma peor de lo que ya tenemos?

En realidad, a pesar de que la nube traerá bajo el brazo un paquete de retos y amenazas con las que estaremos lidiando en el futuro inmediato, esto será precisamente durante las primeras fases de la transición. Tampoco presenta amenazas necesariamente peores que las del sistema tradicional.

Al final de cuentas, el mercado como ente regulador y espontáneo hará que los desarrolladores y propietarios de servicios para la nube hagan propuestas cada vez más sólidas y seguras. Serán justamente esas personas las mejor recompensadas por sus esfuerzos y, sus plataformas, las que adoptarán los usuarios.

Los servicios que funcionan a través de la nube no son como deberían ser actualmente, pero en poco tiempo podrán competir fácilmente con cualquier otra plataforma. En efecto, podría llegar el día donde sean consideradas incluso más seguras. Hasta entonces, los usuarios deben proceder con precaución cuando se muden a la nube. Al menos, deben hacerlo conscientes de las capacidades y los riesgos que ello implica.

5.	Precisar información a compartir y por compartir

1. Clasificar la información sensible y separarla de la información pública.
2. Crear cuentas de acceso a la información pública con mínimos privilegios.

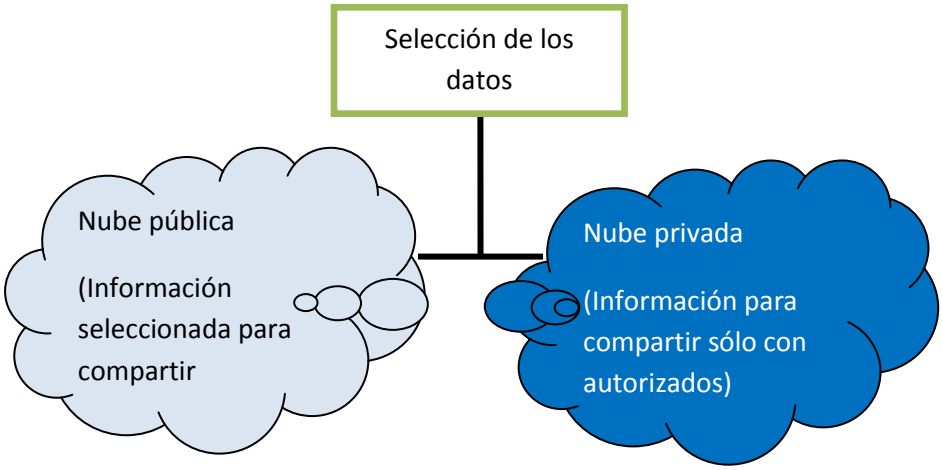


Fig. 3

6.	Aplicar “mejores prácticas” de seguridad al momento de configurar las aplicaciones

Es necesario que los usuarios incorporen buenas prácticas para proteger el entorno de información y prevenir aún más la posibilidad de formar parte del conjunto que engloba a potenciales y eventuales víctimas de cualquiera de las amenazas, quienes constantemente buscan sacar provecho de las debilidades humanas. Para ello se obligatorio conocer los peligros latentes y la forma de detenerlos a través de mecanismos de prevención.

1. Cambiar usuarios y contraseñas por default.
2. Cambiar periódicamente la contraseña de administración.
3. Quitar servicios y cuentas no utilizados.
4. Actualizar frecuentemente sus aplicaciones con los “parches de seguridad”.
5. Copias de Seguridad de los archivos de configuración de las aplicaciones.
6. Descargar las aplicaciones y actualizaciones de sitios confiables.

7.	Registrar de manera exhaustiva el entorno para detectar actividades o cambios no solicitados ya sea en procesos, tareas o documentos

1. Monitoreo de servicios críticos.
2. Utilización de herramientas que buscan y detectan problemas de seguridad; localizan intrusos y controlan cambios.
3. Análisis periódico de logs (bitácoras).
4. Crear respaldos de configuraciones.
5. Utilizar antivirus y *anti-spyware*.

8.	Aplicar conforme a lo dispuesto por el proveedor de servicios, parches y corrección de vulnerabilidades.

1. Descargar las aplicaciones y actualizaciones de sitios confiables del proveedor.
2. Aplicar parches en ambiente de prueba antes de aplicarlos a los servidores de producción.
3. Elaborar y mantener respaldos de su información personal o de datos críticos, de lo contrario, si algo le pasa al sistema no podrá recuperar su trabajo.

9.	Establecer de forma regular un análisis de vulnerabilidades y auditorías de la configuración

Realizar auditorías y análisis de vulnerabilidades permitirá identificar debilidades en aquellos puntos susceptibles a algún ataque malicioso, los cuales pueden propiciar diversos daños, por ejemplo atentar contra la confidencialidad, integridad y disponibilidad de los datos concentrados en dicha nube.

Referencias:

CLOUD SECURITY ALLIANCE (CSA). “Top Threats to Cloud Computing V1.0”, marzo 2010, auspiciada por HP, 14 PP. (en) http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
http://www.rsa.com/innovation/docs/CLWD_BRF_1009.pdf
http://www.maestrosdelweb.com/editorial/amenazas-seguridad-en-la-nube-cloud-computing/
http://www.tendencias21.net/Problemas-de-seguridad-en-la-nube_a3381.html
http://www.bsecure.com.mx/en-linea/the-cloud-reloaded-seguridad-en-la-nube/

DIRECTORIO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dr. José Narro Robles
Rector

Dr. Sergio Alcocer Martínez de Castro
Secretario General

DIRECCIÓN GENERAL DE SERVICIOS DE
CÓMPUTO ACADÉMICO

Dr. Ignacio de Jesús Ania Briseño
Director

M. en C. Ma. de Lourdes Velázquez Pastrana
Directora de Telecomunicaciones

Ing. Rubén Aquino Luna
Subdirección de Seguridad de la Información
UNAM-CERT

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico

CRÉDITOS

PUNTO SEGURIDAD, DEFENSA DIGITAL

Galvy Ilvey Cruz Valencia
Edición

Beatriz Verónica Gutiérrez Galán
Francisco Carlos Martínez Godínez
Julio César García Vizcaíno
Galvy Ilvey Cruz Valencia
Célica Martínez Aponte
Jesús Mauricio Andrade Guzmán
Anaid Guevara Soriano
José Reinel Ramírez Solares
Colaboraciones

Ing. Rubén Aquino Luna
Subdirección de Seguridad de la Información
UNAM-CERT

Galvy Ilvey Cruz Valencia
Rubén Aquino Luna
Revisión de Contenidos

Act. Guillermo Chávez Sánchez
Coordinación de Edición Digital

Diana Chávez González
Coordinación de la Producción Digital

Lic. Lizbeth Luna González
Dolores Montiel García
L.D.C.V. Carolina Silva Bretón
Diseño Gráfico

Liliana Minerva Mendoza Castillo
Formación

2010 D.R. Universidad Nacional Autónoma de México
Revista elaborada por la
Dirección General de Servicios de Cómputo Académico