**COMPUTACION EN LA NUBE**

**(COMPUTER CLOUD)**

**INTRODUCCIÓN**

La computación en la nube (cloud computing) es un paradigma que permite ofrecer servicios de computación a través de Internet a los que podemos acceder desde cualquier lugar teniendo la autorización.

En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio, de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet" sin conocimientos (o, al menos sin ser expertos) en la gestión de los recursos que usan.

"Cloud computing" es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite al usuario acceder a un catálogo de servicios estandarizados y responder a las necesidades de su negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado.

El cambio paradigmático que ofrece computación en nube es que permite aumentar el número de servicios basados en la red. Esto genera beneficios tanto para los proveedores, que pueden ofrecer, de forma más rápida y eficiente, un mayor número de servicios, como para los usuarios que tienen la posibilidad de acceder a ellos, disfrutando de la ‘transparencia’ e inmediatez del sistema y de un modelo de pago por consumo.

Computación en nube consigue aportar estas ventajas, apoyándose sobre una infraestructura ecnológica dinámica que se caracteriza, entre otros factores, por un alto grado de automatización, una rápida movilización de los recursos, una elevada capacidad de adaptación para atender a una demanda variable, así como virtualización avanzada y un precio flexible en función del consumo realizado evitando además el uso fraudulento del software y la piratería.

La computación en nube es un concepto que incorpora el software como servicio, como en la Web 2.0 y otros conceptos recientes, también conocidos como tendencias tecnológicas, que tienen en común el que confían en Internet para satisfacer las necesidades de cómputo de los usuarios.

**ARQUITECTURA DE LA NUBE**

La arquitectura de cloud computing consiste de un conjunto de capas que se encuentran acopladas entre sí para brindar la funcionalidad del sistema, en este caso la arquitectura de *Cloud Computing* es similar a la arquitectura de red, desde un nivel físico hasta un nivel de aplicación. Esto debido a que *Cloud Computing* utiliza protocolos similares a los que se usan en Internet como medio de comunicación, ya seabasado en Web o no basado en Web. La arquitectura genérica de *Cloud Computing* tiene las siguientes capas

mencionadas de abajo hacia arriba:

- Recursos físicos: incluyen elementos como servidores, almacenamiento y red.

- Virtualización: incluye infraestructura virtual como un servicio.

- Infraestructura: incluye software de plataforma como servicio.

- Plataforma: incluye componentes de aplicación como servicio.

- Aplicación: incluye servicios basados en Web y software como servicio

**CARACTERÍSTICAS PRINCIPALES**

**1. Auto-Servicio bajo demanda:** el consumidor podrá aprovisionar recursos computacionales en forma unilateral, según lo requiera, y sin requerimiento de interacción humana con el proveedor del servicio.

**2. Permitir el acceso desde la red (pública, privada, híbrida, comunitaria):** todos los recursos que ofrece la nube están disponibles en la red, y el consumidor no sólo puede acceder a ellos a través de mecanismos estándar, sino que también mediante plataformas heterogéneas como teléfonos móviles, laptops, PDAs, etc.

**3. Asignación de recursos en modo multiusuario.** A diferencia de las aplicaciones de software tradicionales, en el cloud computing el proveedor tiene una única aplicación que abre a todos los usuarios que desean utilizarla, estableciendo unos recursos de acceso y prestaciones distintos para cada usuario. Al ser aplicaciones multiusuario, puede hacer miles de internautas utilizando la misma herramienta a la vez, cada uno con las mismas o distintas prestaciones.

**4. Capacidad de rápido crecimiento:** las unidades de capacidad pueden ser rápidas y fácilmente aprovisionadas (en algunos casos en forma automática), escaladas (crecimiento) o liberadas. Para el consumidor, estos recursos suelen parecer ilimitados, y pueden ser adquiridos en cualquier cantidad y momento.

**5. Servicio medido:** los sistemas de la nube controlan de forma automática y optimizada la utilización de los recursos. Este uso de los recursos puede ser monitoreado y controlado, además, es posible realizar reportes para ambas partes, a fin de establecer la facturación del servicio.

El internauta puede en todo momento decidir qué aplicaciones usar y elegir entre aquellas que son gratuitas y las que no lo son. En el caso de las aplicaciones de pago, el coste irá en función de diversas variables, como el servicio contratado, el tiempo que se ha usado ese servicio, el volumen de tráfico de datos utilizado, etc.

**6. Elasticidad y escalabilidad.** Las aplicaciones en cloud son totalmente elásticas en cuanto a su rapidez de implementación y adaptabilidad. Además, son totalmente escalables, es decir, hoy podemos estar utilizando solo un 10% del total de la aplicación y mañana podemos acceder al 80% de la misma con total normalidad y rapidez, con tan solo comunicarlo a nuestro proveedor y modificar nuestra tarifa de suscripción.

**7. Seguridad.** Cuando se habla de “aplicaciones en Internet”, no se debe entender que nuestros datos están sueltos en la red. Quizás este es el mayor miedo que tienen las empresas y por eso creo que es conveniente explicarlo.

Los datos, cuando están en aplicaciones en cloud, se alojan en DATA CENTERS, empresas específicamente dedicadas a la custodia y salvaguarda de datos de empresas de todo tipo: bancos, entidades financieras, gobierno, multinacionales, pymes, personas como vosotros o como yo…. Son empresas que cuentan con todas las medidas de seguridad necesarias, tanto físicas como de software, de forma que no haya jamás una pérdida de información ni de integridad de los datos.

La única precaución que hay que tener, es encontrar un DATA CENTER o proveedor que nos dé garantías y prestaciones adecuadas al “valor” que damos a nuestros datos. Y eso, es algo que ya hacemos a día de hoy con otros servicios como Internet, teléfono, etc.

**VENTAJAS Y DESVENTAJAS**

**Ventajas**:

· Integración probada de servicios Red. Por su naturaleza, la tecnología de cloud computing se puede integrar con mucha mayor facilidad y rapidez con el resto de sus aplicaciones empresariales (tanto software tradicional como Cloud Computing basado en

infraestructuras), ya sean desarrolladas de manera interna o externa.

· Prestación de servicios a nivel mundial. Las infraestructuras de cloud computing

proporcionan mayor capacidad de adaptación, recuperación de desastres completa y

reducción al mínimo de los tiempos de inactividad.

· Una infraestructura 100% de cloud computing permite al proveedor de contenidos o

servicios en la nube prescindir de instalar cualquier tipo de hardware, ya que éste es provisto por el proveedor de la infraestructura o la plataforma en la nube. La belleza de la tecnología de cloud computing es su simplicidad… y el hecho de que requiera mucha menor inversión para empezar a trabajar.

· Implementación más rápida y con menos riesgos. Podrá empezar a trabajar muy rápidamente gracias a una infraestructura de cloud computing. No tendrá que volver a esperar meses o años e invertir grandes cantidades de dinero antes de que un usuario inicie sesión en su nueva solución. Sus aplicaciones en tecnología de cloud computing estarán disponibles en cuestión de días u horas en lugar de semanas o meses, incluso con un nivel considerable de personalización o integración.

· Actualizaciones automáticas que no afectan negativamente a los recursos de TI. Si

actualizamos a la última versión de la aplicación, nos veremos obligados a dedicar tiempo y recursos (que no tenemos) a volver a crear nuestras personalizaciones e integraciones. La tecnología de cloud computing no le obliga a decidir entre actualizar y conservar su trabajo, porque esas personalizaciones e integraciones se conservan automáticamente durante la actualización.

· Contribuye al uso eficiente de la energía. En este caso, a la energía requerida para el

funcionamiento de la infraestructura. En los datacenters tradicionales, los servidores

consumen mucha más energía de la requerida realmente. En cambio, en las nubes, la energía consumida es sólo la necesaria, reduciendo notablemente el desperdicio.

**Desventajas**:

· La centralización de las aplicaciones y el almacenamiento de los datos origina una

interdependencia de los proveedores de servicios.

· La disponibilidad de las aplicaciones está ligada a la disponibilidad de acceso a Internet.

· Los datos "sensibles" del negocio no residen en las instalaciones de las empresas, lo que podría generar un contexto de alta vulnerabilidad para la sustracción o robo de información.

· La confiabilidad de los servicios depende de la "salud" tecnológica y financiera de los

proveedores de servicios en nube. Empresas emergentes o alianzas entre empresas podrían crear un ambiente propicio para el monopolio y el crecimiento exagerado en los servicios.

· La disponibilidad de servicios altamente especializados podría tardar meses o incluso años para que sean factibles de ser desplegados en la red.

· La madurez funcional de las aplicaciones hace que continuamente estén modificando sus interfaces, por lo cual la curva de aprendizaje en empresas de orientación no tecnológica tenga unas pendientes significativas, así como su consumo automático por aplicaciones.

· Seguridad. La información de la empresa debe recorrer diferentes nodos para llegar a su

destino, cada uno de ellos (y sus canales) son un foco de inseguridad. Si se utilizan

protocolos seguros, HTTPS por ejemplo, la velocidad total disminuye debido a la sobrecarga que estos requieren.

· Escalabilidad a largo plazo. A medida que más usuarios empiecen a compartir la

infraestructura de la nube, la sobrecarga en los servidores de los proveedores aumentará, si la empresa no posee un esquema de crecimiento óptimo puede llevar a degradaciones en el servicio o jitter altos.

· Velocidad de respuesta, sobre todo en sistemas críticos o con grandes volúmenes de

información. Lo normal es de momento, no utilizar la nube para sistemas críticos.

· En caso de fallo de proveedor, existen dificultades para restablecer el servicio, migrarlo a otro proveedor o establecerlo en local.



**TIPOS DE NUBES**

**Nubes públicas**

La ventaja más clara de las nubes públicas es la capacidad de procesamiento y almacenamiento sin instalar máquinas localmente, por lo que no tiene una inversión inicial o gasto de mantenimiento en este sentido, si no que se paga por el uso. La carga operacional y la seguridad de los datos (backup, accesibilidad, etc.) recae íntegramente sobre el proveedor del hardware y software, debido a ello, el riesgo por la adopción

de una nueva tecnología es bastante bajo. El retorno de la inversión se hace rápido y más predecible con este tipo de nubes.

Como inconvenientes se cuenta con el acceso de toda la información a terceras empresas, y la dependencia de los servicios en línea (a través de Internet). También puede resultar difícil integrar estos servicios con otros sistemas propietarios. Es muy importante a la hora de apostar por un servicio en la nube pública, asegurarse de que se puede conseguir todos los datos que se tengan en ella, gratuitamente y en el menor tiempo posible.



**Nubes privadas**

En las nubes privadas, sin embargo, la plataforma se encuentra dentro de las instalaciones del usuario de la misma y no suele ofrecer servicios a terceros. En general, una nube privada es una plataforma para la obtención solamente de hardware, es decir, máquinas, almacenamiento e infraestructura de red (IaaS), pero también se puede tener una nube privada que permita desplegar aplicaciones (PaaS) e incluso aplicaciones (SaaS).

Como ventaja de este tipo de nubes, al contrario que las públicas, es la localización de los datos dentro de la propia empresa, lo que conlleva a una mayor seguridad de estos, corriendo a cargo del sistema de información que se utilice. Incluso será más fácil integrar estos servicios con otros sistemas propietarios.

Sin embargo, como inconveniente se encuentra la inversión inicial en infraestructura física, sistemas de virtualización, ancho de banda y seguridad, lo que llevará a su vez a pérdida de escalabilidad y desescabilidad de las plataformas, sin olvidar el gasto de mantenimiento que requiere. Esta alta inversión supondrá un retorno más lento de la inversión.

**Nubes hibridas**

Las nubes híbridas consisten en combinar las aplicaciones locales con las de la nube pública. Se puede ver también como aplicación privada que se ve aumentada con los servicios de Cloud Computing y la infraestructura. Esto permite a una empresa mantener el control de sus principales aplicaciones, al tiempo de aprovechar el Cloud Computing en los lugares donde tenga sentido.

Por ejemplo, muchas empresas han visto que es más económico usar un IaaS, como por ejemplo Amazon Simple Storage Service (S3), para almacenar imágenes, vídeos y documentos que en infraestructuras propias. El modelo híbrido también se presta a un enfoque incremental.

Incluso la nube híbrida puede ser un buen paso intermedio antes de pasar la mayor parte de las aplicaciones a la nube, ya que es algo menos arriesgado. Por tanto, sería interesante pasar algunas aplicaciones más útiles para la nube a esta y en el momento que se esté más cómodo, mover las que sean necesarias.

Una nube híbrida tiene la ventaja de una inversión inicial más moderada y a la vez contar con SaaS, PaaS o IaaS bajo demanda. En el momento necesario, utilizando las APIs de las distintas plataformas públicas existentes, se tiene la posibilidad de escalar la plataforma todo lo que se quiera sin invertir en infraestructura con la idea de tomar uno de los siguientes caminos:

Si dicha necesidad llegara a ser de carácter estable, sería recomendable incrementar la capacidad de la nube privada e incorporar los servicios adoptados en la pública pasándolos a la nube propia.

Si dicha necesidad es puntual o intermitente se mantendría el servicio en los Clouds públicos, lo que permite no aumentar la infraestructura innecesariamente.

Parece que este tipo de nubes está teniendo buena aceptación en las empresas de cara a un futuro próximo, ya que se están desarrollando softwares de gestión de nubes para poder gestionar la nube privada y a su vez adquirir recursos en los grandes proveedores públicos.

**Nubes combinadas**

Consiste en la combinación de dos o más nubes privadas o publicas, administradas por diferentes usuarios y proveedores. Gracias a esta integración sus usuarios pueden cambiar a servicios proporcionados por nubes públicas con mayor facilidad.

**Nubes comunitarias**

Este tipo de nubes sirven para que varias organizaciones compartan sus recursos de computación y tecnológicos al compartir negocios, servicios y objetivos, y por tanto deciden tomar ventaja de la aplicación del cloud computing conjuntamente. Con menos usuarios que una nube publica y quizás resultando mas costosa su implantación, ofrece mayores niveles de privacidad y seguridad.

**Cloud Software as a Service (SaaS)**

Saas es aquella aplicación ofrecida por un fabricante de software o proveedor de servicios

informáticos a través de Internet, para su uso o utilización por varios clientes. El fabricante es el que en última instancia se ocupa del manteniendo de la privacidad de los datos y la personalización de la aplicación.

En este modelo de servicio, el usuario paga por el uso y por la infraestructura necesaria

(almacenamiento, seguridad, alojamiento, etc.) para el correcto funcionamiento de la aplicación y, a excepción de unos pocos parámetros de configuración, se limita a utilizar la herramienta y sus funcionalidades.

Algunos ejemplos de SaaS son: Google Apps, Documany, TeamBox, Kubbos, Gupigupi, Salesforce, Basecamp, Gmail, Salesforce.com, MediaWiki, Moodle, WordPress, etc.

**Cloud Platform as a Service (PaaS)**

Este modelo de nube amplía las prestaciones del caso anterior, de forma que el consumidor o usuario de esa nube, puede desplegar en ella aplicaciones desarrolladas o adquiridas por él mismo, para ampliar las funcionalidades de dicha nube. Todo esto, por supuesto, se deberá desarrollar en aquellos lenguajes de programación que sean aceptados por el proveedor de la nube.

En este modelo de nube, el usuario no podrá gestionar la infraestructura de la nube, pero tendrá acceso tanto sobre las aplicaciones desplegadas en ella como sobre la configuración de las diversas herramientas que utilice.

Como ejemplos de PaaS: Velneo, Abiquo.com, SimpleDB SQS Google App Engine, entre otros.

**Cloud Infrastructure as a Service (IaaS)**

En el IaaS, se parte de la idea de la externalización de servidores para espacio en disco, base de datos etc., en lugar de tener un control completo de los mismos con el DATA CENTER dentro de la empresa, u optar por un centro de datos y sólo administrarlo. Mediante este modelo de despliegue en Cloud, lo que se tiene es una solución basada en la virtualización, en la que se paga por el nivel de consumo de los recursos:

espacio en disco utilizado, tiempo de CPU, espacio en base de datos, transferencia de datos. La ventaja más inmediata de elegir este tipo de soluciones es la de desplazar una serie de problemas al proveedor relacionados con la gestión de las máquinas y llegar a un ahorro de costes importante, ya que pagaremos solo por lo consumido en función del nivel servicio que nos ofrezca dicho proveedor.

Otro aspecto fundamental a tener en cuenta, es que las Infraestructura como servicio pueden permitir una escalabilidad automática o semiautomática, de forma que podamos contratar más recursos según los vayamos necesitando. Como ejemplos de IaaS: AbiCloud, Amazon, Web Services EC2, GoGrid, entre otros.

Existen diversas soluciones de software para generar IaaS, tanto OpenSource como de ámbito privado: Vmware, Citrix, 3Tera, Abiquo, Enomaly, Eucaplyptus, Proxmox, OpenNebula.org.

**VENTAJAS DE LA COMPUTACIÓN EN NUBE EN TÉRMINOS DE SEGURIDAD**

Apenas resulta necesario reproducir las incontables páginas de material escrito sobre las ventajas económicas, técnicas, arquitectónicas y ecológicas de la computación en nube. Sin embargo, a la luz de la experiencia directa de los integrantes de nuestro grupo de expertos y según las noticias recientes del «mundo real», el examen de los riesgos de la computación en nube en materia de seguridad debe tener su contrapunto en una revisión de las ventajas concretas que ofrece en materia de seguridad. La computación en nube posee un potencial considerable para mejorar la seguridad y la resistencia a los fallos. Lo que sigue a continuación es una descripción de las contribuciones clave que puede realizar.

**LA SEGURIDAD Y LAS VENTAJAS DE LA ESCALA**

En pocas palabras, todos los tipos de medidas de seguridad son más baratos cuando se aplican a gran escala. Por tanto, la misma cantidad de inversión en seguridad puede obtener una mejor protección. Aquí quedan incluidas las distintas medidas defensivas, como el filtrado, la administración de parches, el refuerzo de máquinas virtuales e hipervisores, los recursos humanos y su gestión y control, la redundancia de hardware y software, los sistemas de autenticación seguros, un control eficaz basado en funciones y soluciones federadas de gestión de la identidad por defecto, que también mejora los efectos de red de la colaboración de varios socios implicados en la defensa

**LA SEGURIDAD COMO ELEMENTO DIFERENCIADOR DE MERCADO** La seguridad constituye una prioridad para muchos clientes en nube, los clientes toman las decisiones relativas a la adquisición basándose en el renombre del proveedor en cuanto a confidencialidad, integridad y resistencia a los fallos, así como en los servicios de seguridad ofrecidos por el proveedor, todavía más que en los entornos tradicionales. Éste es un motivo de peso para que los proveedores en nube mejoren sus prácticas de seguridad y generen competencia en este aspecto.

**INTERFACES NORMALIZADAS PARA SERVICIOS DE SEGURIDAD GESTIONADOS** Los grandes proveedores en nube pueden ofrecer una interfaz abierta y estandarizada a los proveedores de servicios de seguridad gestionadas que ofrecen servicios a todos sus clientes. Potencialmente, ello genera un mercado más abierto y disponible de servicios de seguridad, donde los clientes pueden cambiar de proveedor con mayor facilidad e incurriendo en menores gastos de configuración.

**ESCALADA RÁPIDA E INTELIGENTE DE RECURSOS**

La lista de recursos en nube que pueden ser escalados rápidamente bajo demanda ya incluye, entre otros, el almacenamiento, el tiempo de CPU, la memoria, las solicitudes de servicios web y las máquinas virtuales, y el nivel de control granular sobre el consumo de recursos aumenta a medida que las tecnologías mejoran.

**BENEFICIOS DE LA CONCENTRACIÓN DE RECURSOS**

Aunque sin duda la concentración de recursos tiene desventajas para la seguridad (véase Riesgos), posee el beneficio evidente de abaratar la perimetrización y el control de acceso físicos (por recurso unitario) y permite una aplicación más sencilla y económica de una política de seguridad exhaustiva y un control sobre la gestión de datos, la administración de parches, la gestión de incidentes y los procesos de mantenimiento. Obviamente, la medida en que este ahorro se transmite a los clientes varía.

**RIESGOS**

Cabe señalar los siguientes puntos en relación con las siguientes descripciones de riesgos:

 Los riesgos siempre deben entenderse vinculados a las oportunidades de negocio en general y a la actitud hacia el riesgo (en ocasiones el riesgo se ve compensado por la oportunidad).

 Los servicios en nube no sólo tratan de la conveniencia del almacenamiento al que puede accederse desde múltiples dispositivos, sino que incluyen ventajas importantes como una comunicación más conveniente y una colaboración instantánea entre múltiples puntos. Por lo tanto, el análisis comparativo no sólo debe comparar los riesgos de almacenar datos en distintas ubicaciones (en las instalaciones o en la nube), sino también los riesgos que surgen cuando los datos almacenados en las instalaciones (por ejemplo, una hoja de cálculo) se envían por correo electrónico a otras personas para que realicen sus contribuciones, frente a las cuestiones de seguridad de una hoja de cálculo almacenada en la nube y abierta para que dichas personas colaboren. Por lo tanto, los riesgos del uso de la computación en nube deben compararse con los riesgos derivados de mantener las soluciones tradicionales, como los modelos de sobremesa.

 En numerosas ocasiones, el nivel de riesgo variará considerablemente en función del tipo de arquitectura de nube que se esté considerando.

 El cliente en nube puede transferir el riesgo al proveedor en nube, y los riesgos deben considerarse con respecto a la rentabilidad proporcionada por los servicios. Sin embargo, *no todos los riesgos pueden ser transferidos*: Si un riesgo provoca el fracaso de un negocio, perjuicios graves al renombre del mismo o consecuencias legales, es muy difícil, y en ocasiones, imposible, que un tercero compense estos daños.

 El análisis de riesgo incluido en el presente documento se aplica a la tecnología en nube. No se aplica a ninguna compañía u oferta concreta de computación en nube. El objetivo del presente documento no es sustituir a una evaluación de riesgo organizativa de un proyecto concreto.

 El nivel de riesgos se expresa desde la perspectiva del cliente en nube. Cuando se considera el punto de vista del proveedor en nube, se indica explícitamente.

**VULNERABILIDADES**

La lista siguiente de vulnerabilidades no es exhaustiva pero, sin embargo, sí resulta suficientemente detallada para el propósito de nuestro análisis. Contiene información sobre vulnerabilidades de seguridad, tanto específicas de la nube como generales.

 **VULNERABILIDADES AAA**

Un sistema pobre de autenticación, autorización y auditoría podría facilitar el acceso no autorizado a recursos, el aumento de privilegios, la imposibilidad de rastrear el uso indebido de recursos y de incidentes de seguridad en general, etc., a través de:

 almacenamiento inseguro de las credenciales de acceso a la nube por parte del cliente:

 funciones disponibles insuficientes;

 credenciales almacenadas en un equipo transitorio.

Además, la nube hace que los ataques de autenticación basados en contraseñas (práctica fraudulenta que utiliza un troyano para robar contraseñas corporativas) tengan un impacto mucho mayor, ya que las aplicaciones corporativas ahora están expuestas en Internet. Por tanto, la autenticación basada en contraseñas llegará a ser insuficiente y será necesaria una autenticación más robusta o de dos factores para acceder a los recursos en nube.

 **VULNERABILIDADES DEL ALTA DE USUARIOS**

 El cliente no puede controlar el proceso de altas.

 La identidad del cliente no se verifica de manera adecuada en el registro.

 Aparecen retrasos en la sincronización entre los componentes del sistema en nube (temporales y del contenido del perfil).

 Se realizan copias múltiples y no sincronizadas de datos de identidad.

 Las credenciales son vulnerables a la intercepción y a la copia.

 **VULNERABILIDADES DE LA BAJA DE USUARIOS**

Las credenciales dadas de baja todavía son válidas debido a un retraso en la descarga de la revocación.

 **ACCESO REMOTO A LA INTERFAZ DE GESTIÓN**

En teoría, esto permite que las vulnerabilidades en equipos terminales comprometan la infraestructura en nube (cliente individual o proveedor en nube), mediante, por ejemplo, una autenticación débil de las respuestas y las solicitudes.

 **VULNERABILIDADES DEL HIPERVISOR**

Los ataques a la capa del hipervisor son muy atractivos: el hipervisor, de hecho, controla totalmente los recursos físicos y los equipos virtuales que se ejecutan sobre él, así que cualquier vulnerabilidad en esta capa es extremadamente crítica. Explotar una vulnerabilidad del hipervisor equivale potencialmente a explotar todos los equipos virtuales. La primera prueba de concepto de un ataque contra un hipervisor desde una capa inferior la ofrecieron King (y otros) en un artículo (21), en el que los autores introducen el concepto de *rootkit* basado en un equipo virtual. Por entonces, habían sido identificadas algunas vulnerabilidades en los hipervisores más populares (por ejemplo, (22) y (23)), que pueden explotarse sin derechos de acceso de administrador, pero en el momento de redactar este documento no se había aportado ninguna solución para cambiar sus resultados.

Un escenario habitual que permite la explotación de una vulnerabilidad del hipervisor es el llamado *«guest to host escape»*, ejemplo del cual es el «*cloudburst*», una vulnerabilidad del VMware descubierta recientemente y documentada en la referencia (24). Otro escenario es el «*VM hopping*»: en el que el atacante accede ilegalmente a un equipo terminal utilizando algún método estándar y entonces, explotando alguna vulnerabilidad del hipervisor, pasa a controlar otros equipos virtuales que estén ejecutándose en el mismo hipervisor. Para más información, véase: *Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments*, (25).

 **AUSENCIA DE AISLAMIENTO DE LOS RECURSOS**

El uso de recursos por un cliente puede afectar al uso de recursos por otro cliente.

Las infraestructuras de computación en nube IaaS dependen mayoritariamente de diseños de arquitectura en los que los recursos físicos se comparten entre múltiples equipos virtuales, y por tanto, múltiples clientes.

Las vulnerabilidades en el modelo de seguridad del hipervisor pueden conducir a un acceso no autorizado a estos recursos compartidos. Por ejemplo, los equipos virtuales del cliente 1 y el cliente 2 tienen sus discos duros virtual guardados en el mismo LUN (número de unidad lógica) compartido dentro de una red de área de almacenamiento (SAN). El cliente 2 puede ser capaz de mapear el disco duro virtual del cliente 1 en su equipo virtual y ver y utilizar los datos que contiene.

Por último, la falta de herramientas para hacer cumplir un término de servicio (ToS) o un Acuerdo de nivel de servicio (SLA) más específico, como la calidad de servicio (CdS) o los productos de planificación de recursos distribuidos (DRS) podrían permitir a un cliente monopolizar el uso de la nube, con impactos a otros clientes en forma de denegación de servicio o rendimiento pobre.

 **FALTA DE AISLAMIENTO DE LA REPUTACIÓN**

Las actividades de un cliente pueden afectar a la reputación de otro cliente.

 **VULNERABILIDADES EN LA CODIFICACIÓN DE LA COMUNICACIÓN**

Estas vulnerabilidades se refieren a la posibilidad de leer datos en tránsito, por ejemplo, ataques con intermediarios (MITM), autenticación pobre, aceptación de certificados autofirmados, etc.

 **FALTA O DEBILIDAD EN LA CODIFICACIÓN DE ARCHIVOS Y DATOS EN TRÁNSITO**

El no codificar los datos en tránsito, los datos mantenidos en archivos y bases de datos, las imágenes de equipos virtuales sin montar, las imágenes y datos forenses, los registros importantes y otros datos.

**CONCLUSIONES**

La computación en la nube es un sistema novedoso, al que cada vez se unen mas usuarios y empresas. Tiene muchas ventajas y como suele pasar en los sistemas nuevos también tiene muchos inconvenientes, sobre todo en la seguridad, dependencia del acceso a Internet y de los proveedores de cloud, además la poca madurez de las aplicaciones. Es un sistema que está en sus primeras fases de desarrollo pero

cuenta con la ayuda de google y Microsoft y se espera que madure pronto.

Las ventajas de cloud computing podemos aprovechar sobre todo para empezar un negocio rápidamente sin grandes inversiones ni instalaciones físicas. Para los sistemas con datos “sensibles” es más recomendable tener la nube privada o hibrida.

En el futuro lo que se espera de los proveedores de cloud computing es que mejoren la seguridad y ofrezcan aplicaciones con menos fallos y modificaciones menos frecuentes.

Muchas empresas ya tienen sus partes menos sensibles en la nube y en el futuro cercano se espera que la mayoría se migre completamente a la nube.

**BIBLIOGRAFIA**

1. Wikipedia - http://es.wikipedia.org/wiki/Computación\_en\_la\_nube

2. Societic - http://www.societic.com/2010/06/cloud-computing-tipos-de-nubes-de-aplicaciones/

3. Societic - http://www.societic.com/2010/04/cloud-computing-modelos-de-servicio-y-tipos-de-nube/

4. Master ACSI, UAL - http://masteracsi.ual.es/wiki/avs/index.php/Unidad\_4.\_Cloud\_computing

5. ownCloud - http://owncloud.org