Problemas de seguridad de la computación en la nube

Diaz Cely Leonardo.
leondiac@etb.net.co
Universidad Piloto de Colombia

ABSTRACT

The computing in the cloud is emerging as one of the most interesting in the field of information technology topics. Nowadays the big, medium and small organizations are adopting economic resources computing for their business applications, that is to say by introducing a new concept of computing in the cloud in your environment. Basically it is a new concept to provide virtualized resources. The computing in the cloud eliminates the requirements for creating high computing infrastructure cost, is committed to providing flexible IT architecture, accessible over the Internet from various devices, which increases the software capabilities. In a computing environment in the cloud, all information resides in a set of network resources, allowing access to the data through virtual machines, data centers can be located anywhere in the world beyond the reach and control of the users. In the field of security and privacy are multiple the challenges that need to be understood and addressed. There are several issues to be addressed in relation to security and privacy in a cloud environment.

Resumen - La computación en la nube se perfila como uno de los temas más interesantes en el campo de la tecnología de la información. Hoy en día las grandes, medianas y pequeñas organizaciones están adoptando recursos de computación económica para sus aplicaciones de negocio, es decir, mediante la introducción de un nuevo concepto de computación en la nube en su entorno. Básicamente se trata de un nuevo concepto de la provisión de recursos virtualizados. La computación en la nube elimina los requisitos para la creación de infraestructura de computación de alto costo, se compromete a proporcionar una arquitectura de TI flexible, accesible a través de Internet desde diversos dispositivos, lo cual aumentara las capacidades del software. En un entorno de computación en nube, toda la información reside en un conjunto de recursos en red, permitiendo acceder a los datos a través de máquinas virtuales, estos centros de datos pueden estar ubicados en cualquier parte del mundo fuera del alcance y control de los usuarios. En el campo de la seguridad y la privacidad hay múltiples desafíos que necesitan ser comprendidos y abordados. Hay varias cuestiones que deben abordarse en relación con la seguridad y la privacidad en un entorno de nube.

Índice de Términos—Computación en la nube, software como servicio (SaaS), Plataforma como servicio (PaaS), Infraestructura como servicio (IaaS), Denegación de servicio (DoS), Denegación de servicio distribuida (DDoS), Computación en la nube móvil (MCC).

I. INTRODUCCIÓN

La computación en la nube es un término muy amplio utilizado para el reciente desarrollo de la computación basada en Internet. Según el Instituto Nacional de Estándares y Tecnología (NIST), "La computación en la nube se define como un modelo para habilitar el acceso ubicuo de la red bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, dispositivos de almacenamiento y servicios) que pueden ser rápidamente aprovisionados con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios "[1].

La computación en la nube permite ofrecer servicios de computación a través de Internet. 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 mediante Internet sin conocimientos de la gestión de los recursos que se utilizan.

La computación en la nube 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 pagando únicamente por el consumo efectuado.

El cambio que ofrece la computación en la 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, así como también proporciona beneficios para los usuarios que tienen la posibilidad de acceder a ellos aprovechando la transparencia e inmediatez del sistema.

El concepto de seguridad en la nube comenzó en proveedores de servicio de Internet a gran escala, como Google, Amazon y otros que construyeron su propia infraestructura. De entre todos ellos emergió una arquitectura: un sistema de recursos distribuidos horizontalmente, introducidos como servicios virtuales de TI escalados masivamente y manejados como recursos configurables.

II. CLASIFICACIÓN DE LA NUBE

La computación en la nube se puede clasificar con base a los servicios ofrecidos y modelos implementados. De acuerdo con los diferentes tipos de servicios que se ofrecen, la computación en la nube se puede clasificar en tres capas (ver Figura 1). Infraestructura como servicio (IaaS) es la capa más baja que proporciona servicio de soporte de infraestructura básica. Plataforma como servicio (PaaS) es la capa intermedia, que ofrece servicios orientados a la plataforma, además de proporcionar un entorno para alojar aplicaciones de usuario. Software como servicio (SaaS) es la capa superior que cuenta con una completa aplicación que se ofrece como un servicio bajo demanda [2].

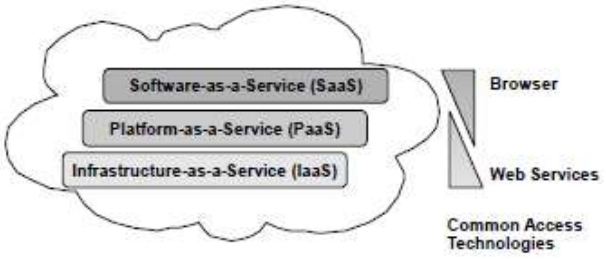

Figura 1. Capas de la nube y tecnologías de acceso
Fuente: On technical Security Issues in Cloud Computing [2]

Software como servicio (SaaS), ofrece el consumo de una gran variedad de aplicaciones proporcionadas por los proveedores del servicio y que se ejecutan en la infraestructura de la nube. Las aplicaciones en la nube son accesibles por varios dispositivos del cliente a través de una interfaz sencilla, como puede ser un navegador web. El consumidor del servicio no gestiona o controla la infraestructura subyacente del servicio, que incluye la red de comunicaciones, los servidores, los sistemas operativos y el almacenamiento.

En la Plataforma como servicio (PaaS), la oferta también incluye un entorno de ejecución de software. Por ejemplo, podría haber un servidor de aplicaciones PaaS que permite al desarrollador implementar aplicaciones basadas en la web sin necesidad de comprar servidores. El Modelo PaaS tiene como objetivo proteger los datos, lo cual es especialmente importante en el caso de almacenamiento como un servicio. En caso de congestión, existe el problema de la interrupción del servicio en un entorno de nube, por lo tanto la necesidad de evitar cortes es importante para asegurar el servicio. La información necesita ser cifrada cuando está alojada en una plataforma por motivos de seguridad. Se han propuesto arquitecturas de computación de la nube que hacen uso de múltiples técnicas criptográficas para la prestación de almacenamiento en la nube [3].

Infraestructura como servicio (IaaS) se refiere a los recursos de hardware para la ejecución de los servicios, por lo general con el uso de la tecnología de virtualización. Con un enfoque de IaaS, varios usuarios utilizan los recursos disponibles. Los recursos pueden ser fácilmente ampliados en función de la demanda de los usuarios y por lo general se utiliza una base de pago por uso. Todas son máquinas virtuales, que deben gestionarse. Por lo tanto se requiere un marco de gobierno para controlar la creación y el uso de máquinas virtuales. Esto también ayuda a evitar el acceso no controlado a la información sensible del usuario.

Independientemente de los modelos de servicios antes mencionados, los servicios en la nube pueden ser clasificados en cuatro formas, dependiendo de los requerimientos del cliente:

- Nube Pública: Hace referencia al modelo estándar en el que el prestador de servicios pone a disposición de cualquier usuario en Internet su infraestructura (esto es, su software o hardware) de forma gratuita o mediante el abono de cierta cantidad relacionada con el volumen o tiempo de uso de los mismos. El uso de nubes públicas permite ampliar fácilmente los recursos necesitados, ya que éstas suelen tener más tamaño que las nubes privadas, normalmente implantadas en una única organización. La información aportada a la nube se almacena con aquella de otros usuarios de los servicios, esto hace que la empresa que contrata el servicio deba ser muy cuidadosa en los requisitos exigidos en el acuerdo con

el proveedor de servicios en lo referente a la protección de datos, estándares de seguridad y garantías sobre posibles pérdidas de información o falta de disponibilidad de la misma [4].

- Nube Privada: La infraestructura de la nube está disponible sólo para un cliente específico y administrado ya sea por la propia organización o un tercero proveedor de servicios. Este utiliza el concepto de virtualización de máquinas, y es una red propia.
- Nube de la Comunidad: Infraestructura utilizada por varias organizaciones por una causa compartida y puede ser manejado por ellos o un tercero proveedor de servicios.
- Nube Híbrida: Combina los modelos anteriormente descritos, de manera que se aprovecha la ventaja de localización física de la información gestionada por las nubes privadas con la facilidad de ampliación de recursos de las nubes públicas. Las principales cuestiones a vigilar en este modelo son la privacidad y la protección de datos, al igual que en la nube pública [4].

Además, con los avances tecnológicos, podemos ver modelos de nube emergentes derivados de las diversas demandas y las necesidades de los usuarios. Con la aparición de las tecnologías de acceso de red de gama alta como 2G, 3G,4G Wi-Fi, Wi-Max etc, y disponibles desde un teléfono, ha surgido un nuevo derivado de la computación en nube. Esto se conoce popularmente como "Mobile Cloud Computing (MCC)". El Mobile Cloud Computing Forum define el concepto de MCC de la siguiente manera: "Mobile Cloud Computing en su forma más simple, se refiere a una infraestructura que tanto el almacenamiento de datos así como el procesamiento de datos tienen lugar fuera del dispositivo móvil [5].

Con un incremento sustancial en el número de implementaciones de computación en la nube, las cuestiones relacionadas con la seguridad y la privacidad se han vuelto más sofisticadas. Con un aumento en el uso de aplicaciones por demanda la posibilidad de ataques cibernéticos también aumenta. Los usuarios tienen que proporcionar con frecuencia la información en línea acerca de su identificación, y esto podría ser utilizado por atacantes para el robo de identidad. A fin de mantener diversos temas de seguridad y privacidad como: confidencialidad, integridad, recuperación de desastres y la gestión de usuarios, los siguientes esquemas se deben implementar para garantizar la seguridad de datos, en cierta medida:

- Un esquema de cifrado que garantice la seguridad de datos, manteniendo los estándares de seguridad contra las amenazas populares al almacenamiento de los datos.
- Los proveedores de servicios deben tener un acceso limitado a los datos, sólo para administrarlo sin poder ver lo que exactamente contiene la información.
- Un control de acceso estricto para evitar el acceso no autorizado e ilegal a los servidores que controlan la red.
- Copia de seguridad de los datos y almacenamiento de datos redundantes para asegurar la recuperación de datos sin problemas en caso de fallo de la infraestructura.
- Gestión de identidad distribuida puede ser usado mediante el uso del Protocolo ligero de acceso a directorios (LDAP), o APIs publicadas (Interfaces de programación de aplicaciones) para conectarse a los sistemas de identidad.

III. OBSTÁCULOS DE LA COMPUTACIÓN EN LA NUBE

Ciertas lagunas en su arquitectura han hecho que la computación en la nube sea vulnerable a diversas amenazas.

Privacidad y seguridad.

El factor fundamental que define el éxito de cualquier nueva tecnología de computación es el nivel de seguridad que proporciona. Si los datos que residen en la nube están seguros con el fin de evitar cualquier tipo de violación de la seguridad o es más seguro almacenar los datos fuera de la nube en nuestros propios ordenadores personales o discos duros?. Al menos que podemos acceder a nuestros discos duros y sistemas siempre que deseamos, pero los servidores de la nube potencialmente podrían residir en cualquier lugar del mundo y cualquier

tipo de falla de Internet nos puede negar el acceso a los datos almacenados en la nube.

Con respecto al entorno de computación en la nube, la privacidad se define como "la capacidad de una entidad para controlar la información que revela sobre sí mismo a la nube, y la capacidad de controlar quién puede acceder a esa información". R. Gellman discute las normas para la recolección, mantenimiento y divulgación de información [6].

Latencia.

La latencia siempre ha sido un problema en la computación en la nube, los factores que se suman a la latencia son: cifrado y descifrado de los datos cuando se mueven en redes no confiables y públicas, congestión y pérdida de paquetes. La congestión se suma a la latencia cuando el flujo de tráfico a través de la red es alta y hay muchas peticiones (que podrían ser de la misma prioridad) que necesitan ser ejecutados al mismo tiempo.

Portabilidad.

Las organizaciones cuando necesitan cambiar el proveedor de la nube, se enfrentan a varios problemas para mover los datos y aplicaciones a otra plataforma en la nube. Tal escenario se denomina como Lock-in y significa quedarse atrapado con un proveedor porque cambiarse es muy costoso, pues la infraestructura de servicio le pertenece al tercero, También hay que pensar en lo que sucedería si este desaparece. Por eso hay que analizarse la historia de la compañía que va a contratarse y su tiempo de permanencia en el mercado [7].

Filtración de datos a través de redes de fibra óptica.

Los riesgos de seguridad para los datos en tránsito se han incrementado en los últimos años. La transición de datos es bastante normal hoy en día y se pueden incluir múltiples centros de datos y otros modelos de nube como la nube pública o privada. La seguridad de los datos que salen de un centro de datos a otro centro de datos es una preocupación importante, ya que se han presentado problemas de seguridad un buen número de veces en los últimos tiempos.

IV. ALMACENAMIENTO DE DATOS Y SEGURIDAD EN LA NUBE

Muchos proveedores de servicios de nube ofrecen almacenamiento como una forma de servicio. Se toman los datos de los usuarios y los almacenan en grandes centros de datos, proporcionando por lo tanto a los usuarios de un medio de almacenamiento. A pesar de las afirmaciones de los proveedores de servicios de nube sobre la seguridad de los datos almacenados en la nube se han dado casos en que los datos almacenados en estas nubes han sido modificados o eliminados debido a algún fallo de seguridad o un error humano.

Varios proveedores de servicios de nube adoptan diferentes tecnologías para proteger los datos almacenados en su nube. La naturaleza virtualizada de almacenamiento en la nube hace que los mecanismos tradicionales no sean adecuados para el manejo de los problemas de seguridad.

Estos proveedores de servicios utilizan diferentes técnicas de cifrado tales como: cifrado de clave pública y clave privada para asegurar los datos almacenados en la nube.

Los proveedores de servicios deben contener todos los puntos que pueden causar pérdida, ya sea debido a algún error humano o generado por el sistema de datos. Por lo tanto, se debe asegurar que las copias redundantes y los datos deben ser almacenados con el fin de manejar cualquier tipo situación adversa que lleve a la pérdida de datos.

La virtualización en general aumenta la seguridad de un entorno de nube. Con la virtualización, una sola máquina se puede dividir en muchas máquinas virtuales, lo que proporciona un mejor aislamiento y seguridad de datos contra ataques de denegación de servicio. La VM (Maquina Virtual) proporciona un banco de pruebas de seguridad para la ejecución de código no probado que no sea de confianza.

V. AMENAZAS A LA SEGURIDAD DE LA COMPUTACIÓN EN LA NUBE

La seguridad requiere un enfoque holístico. El modelo de prestación de servicios es uno de los muchos aspectos que deben tenerse en cuenta para un estudio exhaustivo sobre seguridad en la nube. Seguridad en los diferentes niveles, como el nivel de red, nivel de host y el nivel de aplicación es

necesario para mantener la nube en marcha y funcionando de forma continúa.

Seguridad Básica: La Web 2.0 es la transición que se ha dado de aplicaciones tradicionales hacia aplicaciones que funcionan a través de la web enfocada al usuario final. Se trata de aplicaciones que generen colaboración y de servicios que reemplacen las aplicaciones de escritorio. Web 2.0 es una tecnología clave en favor del uso de software como servicio (SaaS). A medida que la comunidad de usuarios utilizan la Web 2.0 la seguridad se ha vuelto más importante que nunca para tal ambiente.
Los principales ataques que se puede presentar son los siguientes:
A. *Inyección SQL*: Un ataque por inyección SQL consiste en la inserción o "inyección" de una consulta SQL por medio de los datos de entrada desde el cliente hacia la aplicación. Un ataque por inyección SQL exitoso puede leer información sensible desde la base de datos, modificar la información (Insert/ Update/ Delete), ejecutar operaciones de administración sobre la base de datos (tal como parar la base de datos), recuperar el contenido de un determinado archivo presente sobre el sistema de archivos del DBMS y en algunos casos emitir comandos al sistema operativo. Una arquitectura basada en Proxy hacia la prevención de los ataques de inyección SQL detecta de forma dinámica y extrae las entradas de los usuarios sospechosos [8].
B. *Ataque Cross Site Scripting (XSS):* Es un ataque de inyección de código malicioso para su posterior ejecución que puede realizarse a sitios web, aplicaciones locales e incluso al propio navegador. Sucede cuando un usuario mal intencionado envía código malicioso a la aplicación web y se coloca en forma de un hipervínculo para conducir al usuario a otro sitio web, mensajería instantánea o un correo electrónico. Así mismo, puede provocar una negación de servicio (DDos).
C. *Ataque de hombre en el medio:* Es un ataque en el que un usuario malicioso adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas.

Seguridad a nivel de red: Las redes se clasifican en diferentes tipos como: compartidas y no compartidas, públicas o privadas, LAN (*Red* de área local) o WAN (Red de área amplia) y cada una de ellas tienen una serie de amenazas de seguridad para hacer frente. Aunque teniendo en cuenta la seguridad a nivel de red, es importante distinguir entre las nubes públicas y privadas. Hay menos vulnerabilidad en una nube privada en comparación con la nube pública
La seguridad a nivel de red se ve comprometida por los siguientes ataques:
A. *Ataque a los DNS:* El Sistema de Nombres de Dominio (DNS) realiza la traducción de un nombre de dominio a una dirección IP ya que los nombres de dominio son mucho más fáciles de recordar. Pero hay casos cuando al llamar al servidor por su nombre, el usuario es encaminado a otra nube maliciosa en lugar de la que él pidió. Aunque el uso de medidas de seguridad de DNS como Extensiones de seguridad del sistema de nombres de dominio (DNSSEC) reduce los efectos de las amenazas hay todavía casos en que estas medidas de seguridad no resultan adecuadas cuando el camino entre un emisor y un receptor se desvió a través de algún tipo de conexión maliciosa [9].
B. *Ataque de Snifer*: Este tipo de ataques son lanzados por aplicaciones que pueden capturar los paquetes que circulan por una red y si los datos que se transfieren a través de estos paquetes no están cifrados, se puede leer.
C. *Emisión de direcciones reutilizadas*: A cada nodo de una red se le proporciona una dirección IP, el número de direcciones IP que se pueden asignar son limitadas. Un gran número de casos relacionados con la reutilización de la dirección IP se ha observado últimamente. Cuando un usuario en particular se mueve fuera de una red, entonces la dirección IP asociada con él (anterior) se asigna a un nuevo usuario. Por lo tanto aunque la antigua dirección IP está asignada a un nuevo usuario todavía las posibilidades de acceder a los datos por algún otro usuario no es insignificante, debido a que todavía existe la dirección en la caché del DNS y los datos que pertenecen a un usuario en particular pueden llegar a ser accesibles por algún otro usuario que viola la privacidad del usuario anterior.

Seguridad a nivel de aplicación: La seguridad a nivel de aplicación hace referencia a la utilización de los recursos de software y hardware para proporcionar seguridad a las aplicaciones de tal manera que los atacantes no sean capaces de obtener el control sobre estas aplicaciones. Hoy en día, los ataques son lanzados disfrazados como usuarios de confianza y el sistema puede considerarlos como tal, esto permite el pleno acceso por parte del atacante. La razón detrás de esto es que las políticas de seguridad de nivel de red son obsoletas y permiten que sólo los usuarios autorizados tengan acceso a la dirección IP específica. Con el avance tecnológico, estas políticas de seguridad se han vuelto obsoletas ya que ha habido casos en los que la seguridad del sistema se ha violado, después de haber accedido al sistema bajo el disfraz de un usuario de confianza. Con los recientes avances tecnológicos, es muy posible imitar a un usuario de confianza sin ser notado.

Las principales amenazas a nivel de aplicación son:

A. *Problemas de seguridad con el hipervisor*: En un mundo virtualizado el hipervisor permite que múltiples sistemas operativos se ejecuten en un sistema a la vez, proporcionando lo recursos de tal manera que no interfieran unos con otros, por lo tanto la seguridad con respecto al hipervisor es de gran preocupación ya que todos los sistemas huéspedes son controlados por este. Si un hacker es capaz de obtener el control sobre el hipervisor, puede hacer cambios en cualquiera de los sistemas operativos invitados y obtener el control sobre todos los datos que pasan a través del hipervisor.

B. *Ataques de denegación del servicio:* Un ataque DoS es un intento de hacer que los servicios asignados a los usuarios autorizados no estén disponibles. En un ataque de ese tipo, el servidor del servicio está inundado por un gran número de peticiones y por lo tanto el servicio deja de estar disponible a los usuarios autorizados.

C. *Envenenamiento de cookies:* Se trata de cambiar o modificar el contenido de una cookie para tener un acceso no autorizado a una aplicación o una página web. Las cookies contienen básicamente las credenciales de identidad relacionadas con el usuario y una vez que estas cookies son accesibles, el contenido de estas cookies se pueden falsificar para hacerse pasar por un usuario autorizado. Esto se puede evitar ya sea mediante la realización de la limpieza de las cookies regularmente o la implementación de un esquema de cifrado para los datos de la cookie.

D. Manipulación del campo oculto: Al acceder a una página web, hay ciertos campos que están ocultos y que contienen la información relacionada con la página y básicamente son utilizados por los desarrolladores. Sin embargo, estos campos son muy propensos a los ataques de los hackers, ya que pueden ser fácilmente modificados y publicados en la página web.

E. *Ataque de denegación de servicio distribuido*: DDoS no es más que un ataque de negación de servicio pero distribuido, ejecutado a través de una red de computadores zombies. Sin embargo es muy difícil de detener, ya que no se puede diferenciar el origen del ataque para bloquear las solicitudes ya que estas difícilmente se pueden aislar de las de los clientes reales.

F. *Ataque de diccionario:* Un ataque de diccionario es un método que consiste en intentar averiguar una contraseña probando todas las palabras del diccionario. Este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta, ya que muchos usuarios suelen utilizar una palabra existente en su lengua como contraseña para que la clave sea fácil de recordar, lo cual no es una práctica recomendable.

G. *Google Hacking*: Google se ha convertido en la mejor opción para encontrar detalles acerca de cualquier cosa en Internet. Google Hacking se refiere al uso de motores de búsqueda de Google para encontrar información sensible que un hacker puede utilizar para su beneficio. Generalmente, los hackers tratan de averiguar las brechas de seguridad mediante el uso de Google sobre el sistema que desean piratear. Una vez reunida la información necesaria, se lleva a cabo el ataque del sistema objetivo. Un Google hacking se observó cuando datos de acceso de varios usuarios de Gmail fueron robados por un grupo de piratas informáticos.

VI. CUESTIONES DE SEGURIDAD EN LOS MODELOS DE CLASIFICACIÓN DE LA NUBE

Cada una de las formas en que los servicios en la nube pueden ser clasificados tiene sus propias ventajas y limitaciones. Y desde la perspectiva de la

seguridad, hay temas que deben abordarse con una estrategia para evitar fallas en la seguridad.

Nube Pública: En una nube pública, los clientes comparten una misma plataforma y la seguridad de la infraestructura es proporcionada por el proveedor de servicios. Algunos aspectos que se deben tener en cuenta son los siguientes:

A. Se requieren confidencialidad, integridad y disponibilidad para proteger los datos durante todo su ciclo de vida. Los datos deben ser protegidos durante las diversas etapas de la creación, intercambio, archivo, procesamiento, etc. Sin embargo, la situación se vuelva más complicada en el caso de una nube pública en la que no tenemos ningún control sobre las prácticas de seguridad del proveedor de servicios [10].

B. En caso de una nube pública, la misma infraestructura es compartida entre múltiples clientes y las posibilidades de fuga de datos es muy alta. Sin embargo, la mayoría de los proveedores de servicios ejecuta una infraestructura multiusuario. Investigaciones adecuadas en el momento de elegir el proveedor de servicios debe hacerse con el fin de evitar este riesgo.

C. En caso de que un proveedor de servicios de la nube utilice un proveedor de terceros para proporcionar sus servicios en la nube, se debe velar por los acuerdos de nivel de servicio que tienen en el medio, así como cuáles son los planes de contingencia en caso de la ruptura del sistema de terceros.

D. Acuerdos SLAs apropiados definen los requisitos de seguridad, tales como el nivel de cifrado de datos cuando se envía a través de Internet y cuáles son las sanciones en caso de que el proveedor de servicios no lo realice.

Nube privada: Un modelo de nube privada permite al cliente tener el control total de la red y proporciona la flexibilidad para implementar una práctica de perímetro de seguridad de red tradicional. Aunque la arquitectura de seguridad es más fiable en una nube privada, hay riesgos que deben tenerse en cuenta:

A. Técnicas de virtualización son muy populares en las nubes privadas. En tal escenario, los riesgos para el hipervisor se deben analizar con cuidado. Ha habido casos en los que un sistema operativo invitado ha sido capaz de ejecutar procesos en otra máquina virtual invitada o anfitrión. En un entorno virtual las máquinas virtuales son capaces de comunicarse con otras máquinas virtuales, incluyendo las que no se supone que deben hacerlo. Para asegurarse de que solo se comunican con los que se supone se deben comunicar, las técnicas de autenticación y cifrado adecuadas, tales como IPsec [Nivel de seguridad IP], etc deben ser implementadas.

B. El sistema operativo del anfitrión debe estar libre de cualquier tipo de amenaza de malware y supervisado para evitar cualquier riesgo. Además, las máquinas virtuales de los huéspedes no deben ser capaces de comunicarse con el sistema operativo anfitrión directamente.

C. En una nube privada, los usuarios tiene la facilidad de gestionar partes de la nube, y el acceso a la infraestructura a través de una interfaz web o un punto final http. las interfaces deben desarrollarse adecuadamente y técnicas estándar de seguridad de aplicaciones web deben implementarse para proteger la diversidad de las peticiones HTTP que se realizan.

D. Mientras hablamos de la seguridad de Internet estándar, también tenemos que tener una política de seguridad en el lugar para proteger el sistema de los ataques que se originen dentro de la organización.

Así vemos que, aunque las nubes privadas son considerados más seguros en comparación con las nubes públicas, todavía tienen múltiples problemas que si no recibe atención puede conducir a importantes fallos de seguridad.

VII. CONCLUSIONES

La computación en la nube es un nuevo término introducido en el entorno empresarial, donde los usuarios pueden interactuar directamente con los recursos virtualizados. Un cambio importante hacia la nube se está evidenciando actualmente, la nube ofrece beneficios a las empresas que buscan una ventaja competitiva en el entorno actual. Muchos más proveedores se están moviendo en esta área, y la competencia impulsa precios aún más bajos.

Hay muchas nuevas tecnologías emergentes a un ritmo rápido, cada uno con los avances tecnológicos

y con el potencial de hacer la vida de los humanos más fácil. Las empresas que están implementando la computación en la nube están ampliando su infraestructura y deben ser conscientes de los desafíos de seguridad que enfrentan.

La computación en nube tiene la capacidad de convertirse en una potencial solución de TI, segura, virtual y económicamente viable. Sin embargo, debido a la complejidad de la nube, será difícil de lograr la seguridad de extremo a extremo. Nuevas técnicas de seguridad deben ser desarrolladas y las técnicas de seguridad antiguas deben ser ajustadas radicalmente para poder trabajar con la arquitectura de nube.

REFERENCIAS

[1] Peter Mell, Timothy Grance, ―The NIST Definition of Cloud Computing‖ , Jan, 2011. http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf

[2] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi LoIacon, "On technical Security Issues in Cloud Computing", Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[3] Seny Kamara, Kristin Lauter, "Cryptographic cloud storage", Lecture Notes in Computer Science, Financial Cryptography and Data Security, p.1-12

[4] Observatorio de la Sociedad de la Información y Modernización de Galicia: Cloud Computing: La tecnología como servicio, http://www.osimga.org.

[5] Repositorio Institucional de la UNLP: Mobile Cloud Computing y su Relación con Aplicaciones Móviles y Aplicaciones Sensibles al Contexto. http://sedici.unlp.edu.ar/.

[6] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", The World Privacy Forum, 2009. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[7] Universidad de los Andes, Foros Isis: Computación en la Nube, una herramienta que se afianza en la tierra. www. http://forosisis.uniandes.edu.co.

[8] Liu, Y. Yuan, A Stavrou, "SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks", SAC March 8-12, 2009, http://cs.gmu.edu.

[9] Char Sample, Senior Scientist, BBN Technologies,Diana Kelley, Partner, Security Curve, "Cloud computing security: Routing and DNS security threats". http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1359155_mem1, 00.html/

[10] A. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", Proceedings of Advances in Computing and Communications, www. http://link.springer.com/

Leonardo Diaz Cely
Ingeniero en Telemática Universidad Distrital .Estudiante de Especialización en Seguridad Informática Universidad Piloto de Colombia.