Explorando Cloud Computing y su seguridad

Fausto Castañeda Muñoz, Ricardo Alberto Tovar
Fausto.castaneda@hotmail.com, ricardoatv1@gmail.com
Universidad Piloto de Colombia

Resumen— La computación en la nube es un modelo que permite el acceso por demanda en la red, a un conjunto de recursos informáticos configurables. En la actualidad existen diferentes empresas que prestan servicios de este modelo como: Icloud, Google, Microsoft entre otras. Cloud Computing cuenta básicamente con tres modelos de servicio: SaaS, PaaS y LaaS y en cuanto a arquitectura dispone de dos modelos: Grid computing y computación transaccional. El futuro de este modelo apunta a prestar servicios que remplacen todas las aplicaciones de escritorio frente a un explorador, de igual forma es necesario conocer retrospectivamente como se ha planteado la seguridad para este tipo de infraestructuras y que aspectos importantes se tienen que considerar en el momento de abordar este tema.

Índice de Términos—*Cloud Computing, Computación, nube, SaaS, PaaS, LaaS, Infraestructura, Plataforma, Servicio, DMZ, IDS.*

Abstract— Cloud computing is a model that allows access demand on the network, a set of configurable computing resources. In the news there are several companies that provide this model as iCloud, Google, Microsoft and others. Cloud computing has three basic service models: SaaS, PaaS and LaaS and in architecture has two models: Grid Computing and transactional computing. The future of this model aims to provide services that replace all desktop applications compared to a browser. is equally necessary to know in retrospect as security has been raised for this type of infrastructure and important aspects have to be considered at the time to address this issue.

Keywords—*Cloud Computing, Compute, Cloud, SaaS, PaaS, LaaS, Infrastructure, Platform, Service, DMZ, IDS.*

I. INTRODUCCIÓN

El modelo de computación en la nube apuesta a una nueva era de la computación, rompiendo con las actuales estructuras de mercado y arquitectura de productos de Software. Cloud Computing surgió con el propósito de solucionar las continuas dificultades presentadas en los proyectos y productos que actualmente existen en la industria del software al igual que los altos costos de adquisición de TI, el mantenimiento y la estabilidad de las plataformas tecnológicas entre otras.

El objetivo de este documento es abrir un panorama al modelo de computación en la nube, sus características esenciales, arquitecturas, tendencias futuras y conocer cual han sido los aspectos relevantes tenidos en cuenta en materia de seguridad.

II. DEFINICION

El término computación en la nube ha sido tomado posiblemente a la continua simbología que se utiliza para referirse al término Internet con lo que realmente estaríamos hablando de “Computación en Internet”

Computación en la nube es un modelo para permitir acceso por demanda a la red, a un pool compartido de recursos informáticos configurables como son las redes, servidores, almacenamiento, aplicaciones y servicios, que puede ser rápidamente aprovisionado y liberado con muy pocos esfuerzos de gestión.

El modelo de gestión en la nube promueve disponibilidad y está compuesto por 5 características esenciales (autoservicio en demanda, extenso acceso a la red, puesta común de recursos, rápida elasticidad, servicio medido), tres modelos de servicio SaaS, RaaS, LaaS y 4 modelos de despliegue, privado, comunitario, público e híbrido.

La computación en la nube se ha posicionado en el mercado como una tecnología o para algunos como una opción más que considerar en la búsqueda de soluciones personales y empresariales que ofrecen servicios a través de Internet.

III. CARACTERÍSTICAS

Entre algunas características destacadas en el modelo de computación en la nube encontramos:

Servicio bajo demanda: Mediante este modelo los clientes pueden acceder tanto a servicios como almacenamiento y servidores de red, el tiempo de uso y el volumen de tráfico entre otros. Esta característica permite un modelo de autoservicio que se acomoda a las necesidades específicas del cliente, cabe anotar que estas pueden ser variables en el tiempo.

Elasticidad y escalabilidad: La computación en la nube permite una entrega de servicios de manera rápida y elástica, incluso en algunos casos puede ser de manera automática. El modelo de la nube proporciona alta escalabilidad, permitiendo a los clientes la utilización de una pequeña parte de la aplicación en un momento dado y luego acceder a la totalidad de esta.

Supervisión del Servicio: En el modelo de computación en la nube el uso de recursos puede ser monitoreado, controlado y notificado, garantizando la transparencia tanto para el proveedor como para el cliente, esta característica hace que sea seguro.

IV. MODELOS DE IMPLEMENTACIÓN

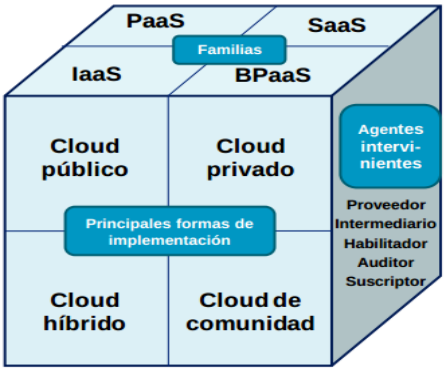
Existen básicamente tres modelos de implementación de computación en la nube, estos modelos están orientados a servicio.

Nube privada: En este modelo la infraestructura de la nube es operada solamente por una organización. Puede ser operada por una organización o por un tercero.

Nube pública: La infraestructura de la nube en este modelo está disponible para el público en general o para un grupo de industrias y su propietario es una organización que provee los servicios de computación en la nube.

Nube comunitaria: En este caso, la infraestructura de la nube es compartida por varias organizaciones y soporta una comunidad específica que puede tener objetivos en común.

Nube híbrida: La infraestructura de la nube puede tener una composición de una o varias nubes, que siendo entidades únicas, permanecen unidas por estándares o tecnologías.



Cubo de calificación de soluciones de Cloud Computing
Fuente
http://www.orsi.jcyl.es/web/jcyl/ORSI/es/Plantilla100Detalle/1262860952313/1262860952313/12 84152333822/Redacción)

V. ESQUEMA DE FUNCIONAMIENTO

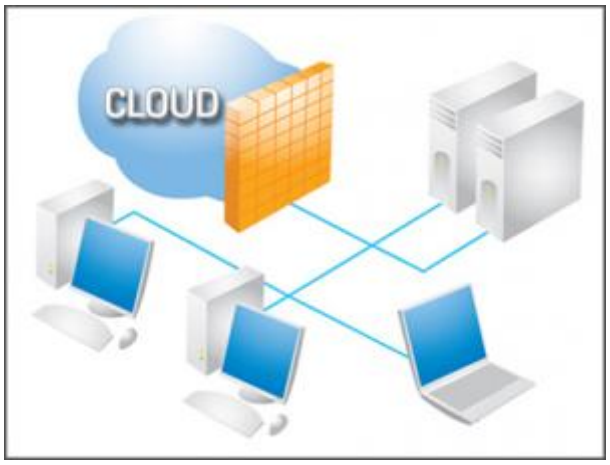
La computación en la nube se basa en una arquitectura multiusuario, que consiste en una única aplicación la cual es compartida por todos los clientes, lo contrario a las aplicaciones de software tradicional que consiste en copias distintas del producto para cada usuario.

VI. FUTURO DE LA COMPUTACIÓN EN LA NUBE

No es difícil imaginar un futuro con una gran proliferación de operadores y usuarios del Cloud Computing, y teniendo en mente la naturaleza colaborativa de esta modalidad de trabajo, todo indicaría que el futuro de la nube será lo que algunos mencionan como ínter nube, varias nubes interconectadas, aprovechando recursos e información, comunicándose entre sí. Esto abre puertas a mayores chances de interacción e ilusiona pensar la manera en que se multiplicarán los beneficios para el usuario. Por ejemplo, la posibilidad de cambiar de proveedor libremente a través de migraciones seguras y transparentes, garantizando la continuidad de los procesos. La

oferta de servicios crecería todavía más y los costos serían menores. Para llegar a esos niveles de interoperabilidad hace falta avanzar en varios aspectos, no solamente inversión y coordinación entre los distintos agentes que proveen los servicios, deberán desarrollarse aún interfaces, reglamentaciones, estándares de seguridad y hardware.

VII. RETROSPECTIVA DE LA SEGURIDAD CLOUD COMPUTING



Cloud Computing Diagram
Fuente – www.altrantelecom.wordpress.com

Si se efectuara una mirada retrospectiva al tema de la seguridad se podría mencionar que en el pasado han sido diferentes y amplias las preocupaciones que se han tenido a través del tiempo, el tema ha sido muy dinámico y mientras hacia los años 80 la principal preocupación era la seguridad de los recursos físicos, el aseguramiento de los llamados "fierros" o máquinas, los controles de acceso, ya en los 90 se introdujeron nuevos conceptos como la utilización de seguridad perimetral, conceptos como DMZ (Zonas desmilitarizadas), IDS (Sistemas de detección de intrusos) y en ese sentido la seguridad migró a una nueva visión con dispositivos ya electrónicos.

Ya en los años 2000, se evidencia algo que si bien es cierto no era nuevo como componente fundamental dentro de los contados para IT con el ingreso de los últimos avances electrónicos toma bastante fuerza, el eslabón más débil en la cadena "el factor humano" y es allí donde surgen diferentes conceptos y tecnologías que aumentan la seguridad.

Conceptos como gobernabilidad y framework de seguridad, controles gerenciales de acceso, controles y perfilamiento de usuarios y segregación de cuentas privilegiadas son algunos de los nuevos ingredientes en el tema de seguridad que pretenden cerrar la brecha vulnerable en el componente humano.

Ahora el nuevo reto en el tema de seguridad informática es el Cloud Computing el cual al ofrecer nuevas alternativas de procesamiento de información plantea un gran interrogante y preocupación a la hora de resguardar y brindar seguridad a la información bajo estas plataformas.

Algunos avances se han dado con la creación de organizaciones como "Cloud Security Alliance" desde donde se fomentan el uso de buenas prácticas y donde se han impulso programas como certificaciones en seguridad para proveedores de Cloud Computing.

VIII. ASPECTOS DE LA SEGURIDAD

Dado que el tema de seguridad en Cloud Computing es un tema muy importante y es muy probable que paulatinamente se vayan superando los inconvenientes que hoy se plantean, sería importante evaluar algunos aspectos que se permitirán brindar seguridad y tranquilidad a los usuarios que pretendan acceder a este tipo de servicios:

- ✓ Qué tipo de legislaciones aplicaría sobre la información que repose en este medio. ¿Necesitaríamos nuevas normas o leyes?
- ✓ Como serían los procesos de carga y descarga de información de una persona o empresa que desee acceder a estos servicios, y con qué seguridades se efectuaría.
- ✓ Cómo serían manejados los cambios con respecto a bases, aplicaciones, usuarios, sistemas distribuidos, etc. que tenga que hacer en un entorno de Cloud Computing.

La C.S.A. (Cloud Security Alliance) recomienda que los clientes tengan una visión clara de cómo se manejan todos sus datos, pasa con mucha frecuencia que la empresa puede estar trabajando con terceros, lo que puede representar un riesgo de seguridad. Por

ejemplo, los servicios de backup o redundancia que se ofrecen en la nube, pueden estar utilizando la plataforma de almacenamiento de una tercera empresa. Los clientes deberían saber en qué consiste toda la cadena de suministro de sus datos para asegurarse de que está convenientemente protegida en todo el proceso.

Actualmente se toman algunas medidas de seguridad para brindar protección y confianza a los usuarios de Cloud Computing como modelos de gestión de identidades; sin embargo diferentes estudios demuestran que el 40 % de las empresas que regularmente utilizan servicios de almacenamiento o procesamiento de datos en la nube sufrieron al menos una pérdida de datos.

IX. PRIMERAS PRUEBAS

Existen algunas empresas que se han arriesgado a efectuar pruebas iniciales y buscar mejoras para ofrecer soluciones, empresas como Security Advisor, han apostado por la estrategia de vivir la experiencia de operar en la nube, con todas las dificultades que puede tenerse en un inicio. Así, es posible ensayar las mejores prácticas, entrenar estrategias y luego entregar a los clientes un servicio probado y mucho más robusto.
En este proceso las empresas que han decidido probar como pioneras deberán enfrentarse a aspectos importantes como:

- ✓ Disponibilidad de la información.
- ✓ Recuperación ante desastres y continuidad del negocio.
- ✓ Incidentes de seguridad ocurridos bajo el modelo.
- ✓ Transparencia en la utilización de los datos.
- ✓ Pérdidas de control físico y esto infiere la privacidad y el control que se pueda tener de los datos, sin tener en cuenta que se pueden estar enfrentado a nuevas vulnerabilidades y diferentes alternativas de amenazas.

X. ¿QUÉ TENER EN CUENTA AL MOMENTO DE UTILIZAR SERVICIOS DE CLOUD COMPUTING?

Desde el año 2011 se ha venido hablando de algunos ítems a tener en cuenta para mejorar la seguridad de la información en la nube, es importante mencionar algunos de ellos como aspectos a tener en cuenta en la utilización de este tipo de servicios:

- ✓ Si se está hablando de un entorno o servicio de Cloud Computing es importante tener la precaución de cifrar los datos.
- ✓ Como uno de los temores es que la información sea interceptada en el camino se debe garantizar que los datos deben llegar a su destino, razón por la cual se recomienda usar por ejemplo webfiltering, lo que podría evitar un phishing.
- ✓ Para asegurarse de la integridad de la información que vuelve, se debe contar con un buen antivirus que se mantenga actualizado permanentemente.

Igualmente es fundamental tener en cuenta los riesgos que aquejan y a los cuales se ven expuestos los usuarios de Cloud Computing, riesgos que en su momento fueron expuestos por la CSA (Cloud Security Alliance):

- ✓ Ingresos abusivos al sistema de Cloud Computing, ya que cualquier persona que pudiera pagar o con una tarjeta de crédito en la mano puede acceder al servicio con la consecuente proliferación de spammer, creadores de código malicioso y otros criminales que utilizan la nube como centro de operaciones.
- ✓ Ya que los proveedores de servicios ofrecen interfaces para interactuar con los usuarios o recursos todo proceso de acceso, cifrado y autenticación se efectúa por medio de esas interfaces lo que las hace más franqueables.
- ✓ Las amenazas internas como en cualquier sistema son un problema a tratar ya que pueden darse ataques de empleados descontentos, accidentes por error o desconocimiento, etc.
- ✓ Problemas derivados de las tecnologías compartidas ya que los componentes físicos aún no están completamente diseñados para ambientes compartidos, lo cual puede generar en algún momento una falla abriendo una brecha de seguridad.
- ✓ Pérdida o fuga de la información la cual ha sido ampliamente tratada en el desarrollo de este artículo.

- ✓ Secuestros de sesión o de servicios.
- ✓ La localización de los datos no es muy clara y a ciencia cierta no se determina en donde se encuentran realmente alojados.
- ✓ Aislamiento de los datos lo cual debe ser garantizado por el proveedor, ya que en un ambiente Cloud se pueden tener datos alojados al lado de otros clientes.
- ✓ Recuperación de datos tratado de igual forma en este artículo y aspecto fundamental al momento de garantizar la seguridad y continuidad de la operación.

XI. CONCLUSIONES

La computación en la nube es una tendencia que se ha posicionado a nivel empresarial como una alternativa para el desarrollo y hosting de aplicaciones web. Existe una gran variedad de proveedores de servicios en la nube, lo que permite a las empresas tener una amplia variedad de ofertas en cuanto a plataformas, capacidades, planes y tarifas. Las tendencias y paradigmas que incorpora la computación en la nube generan un cambio y nuevas dinámicas en la cultura empresarial, lo cual debe tener como consecuencia la rápida adaptación de los departamentos de TI a los nuevos entornos.

Mientras una empresa en la actualidad tiene control total de su información, Cloud Computing pretende cambiar este paradigma, enfrentando a las organizaciones a la incertidumbre, inseguridad y desconfianza que genera el entregar a terceros los activos de la compañía. El modelo Cloud Computing toma como supuesto la globalización de las conexiones a Internet, requiriendo altos niveles en recursos como el ancho de banda y una conexión full time a Internet. Para las empresas la inversión en los departamentos de TI disminuiría, permitiéndoles centrarse en el objetivo propio de la organización y no consumir esfuerzo y recursos en actividades externas a la misión organizacional.

XII. REFERENCIAS

[1]. Mell, P. and Grance, T. The NIST Definition of Cloud Computing. Gaithersburg: National Institute of Standards and Technology, 2011.2. Salesforce. http://www.salesforce.com/es/cloudcomputing/.

[2]. Google App Engine- Wikipedia, http://en.wikipedia.org/wiki/Google_App_Engine.

[3]. Azure Services Platform – Wikipedia, http://en.wikipedia.org/wiki/Azure_Services_Platform.

[4]. Windows Azure Offers, http://www.microsoft.com/windowsazure/offers/.

[5]. Amazon Web Services – Wikipedia, http://en.wikipedia.org/wiki/Amazon_Web_Service

[6]. Engine Yard - Wikipedia, http://en.wikipedia.org/wiki/Engine_Yard.

[7]. Engine Yard, http://www.engineyard.com.

[8]. Software as a Service (SaaS): ¿Qué es? http://geeks.ms/blogs/ciin/archive/2007/10/05/software-as-a-service-sas-191-qu-233-es.aspx.11.

[9]. References Cloud Security Alliance – http://www.cloudsecurityalliance.org/guidance.html TREND Micro – Www.trendmicro.com/go/enterprise …

[10]. 1024.com. "El futuro de la Seguridad Informática.

[11] ¿Dónde está el Perímetro? Ricardo De Lellis KPMG Suiza 2011.

[12]. REVISTA GERENCIA SEGURIDAD "Seguridad en la nube. El próximo desafío del cloud computing" Marzo 2014.

[13]. LOGICALLIS "Seguridad Informática en tiempos de Cloud Computing" Marzo. 2011

Autores

Fausto Castañeda Muñoz
Ing. de Sistemas
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia.

Ricardo Alberto Tovar
Ing. de Sistemas
Est. Especialización en Seguridad Informática
Universidad Piloto de Colombia.