COMPUTACIÓN EN LA NUBE Y SU SEGURIDAD

Díaz Ariza, Wilson Daniel.
daniel8diaz@yahoo.com
Universidad Piloto de Colombia

***Resumen*—**La industria creciente del manejo de la información en la nube, en la que actualmente confluyen una gran cantidad de actores, es una de las tendencias en materia de servicios de computo, en ella convergen una variedad de tecnologías, modelos, proveedores y trae consigo la necesidad urgente de garantizar la protección de la información, desde diferentes perspectivas, como la seguridad y la privacidad. El objetivo del presente artículo es presentar una tendencia en el uso de la información, conocida como Computación en la Nube, mostrando la su funcionalidad y la necesidad subsecuente de implementar, evaluar y fortalecer continuamente todos los elementos de seguridad informática y a su vez, presentar recomendaciones para los usuarios, tendientes a evitar violaciones que pongan en riesgo el manejo de dicha información.

***Abstract*—**The growing industry of information management in the cloud is one of the trends in computer services that involve a vast variety of actors, technologies, models and suppliers. It also implies new challenges from different perspectives such as privacy and security, in order to ensure the information protection. The aim of this paper is to present a trend known as Cloud Computing, showing its functionality and the subsequent need to implement, evaluate and continuously strengthen all elements of informatics security, as well as the importance to work with users in order to avoid breaches of information.

***Índice de Términos*—** Amenazas, computación en la nube, gestión de la información, incidentes, infraestructura, nube, seguridad, seguridad de la información**.**

I. INTRODUCCIÓN

Algunos de los beneficios que puede aportar el manejo de la información en la nube, están representados en la reducción de costos a expensas de aspectos como hardware, software o mantenimiento y del ahorro de espacio físico; mayor eficiencia, potencia y capacidad de almacenamiento e independencia de sistemas operativos. Sin embargo, pueden presentarse inconvenientes, como la carencia de control, dependencia de accesos a conexiones de internet, falta de portabilidad documental entre proveedores de servicios, y la más importante, la necesidad de protección de seguridad y privacidad de datos y programas [1].

II. DEFINICIÓN DE COMPUTACIÓN EN LA NUBE

El término “Nube”, se utiliza como un sinónimo Internet, para dar a entender que lo que está en ella es de alguna forma lejana, grande y de cierta forma accesible, y su símbolo es usado en los diagramas de red.

Existen múltiples definiciones de la Computación en la Nube, las cuales resumo y que son tomadas de diversas fuentes de Internet): (a) Es un modelo informático que se basa en Internet en centros de cómputo remotos, para gestionar los servicios de información y aplicaciones, (b) Es un modelo que permite que usuarios y empresas interactúen con información sin tener que instalar aplicaciones localmente, (c) Es un cambio significativo de la tecnología de información que da un nivel más global a los datos de empresas y usuarios, (d) Es la utilización de Internet para las necesidades de información, (e) Es la evolución de Internet que converge en una variedad de proveedores, (f) Es un estilo de cómputo donde las necesidad es de tecnología de información proporcionan servicios en Internet para organizaciones y clientes, (g) Según definición de la Agencia del Departamento de Comercio de los Estados Unidos (NIST, por sus siglas en inglés) [2] La computación en nube es un modelo para permitir conveniente, acceso a la red bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de gestión o proveedor de servicios interacción. Este modelo de nube promueve disponibilidad y se compone de cinco características esenciales (a petición de autoservicio, acceso a la red amplia, la puesta en común de recursos, elasticidad rápida y servicio medido).

La Computación en la Nube se presenta como un avance en la tecnología de información, que permite acceso a varios participantes de manera rápida, los servicios prestados pueden estar virtualizados permitiendo una mayor oferta y un servicio a menor costo para las organizaciones, lo cual es una de las razones por la que este fenómeno ha tomado fuerza.

La Computación en la Nube proporciona a las organizaciones una infraestructura de gran capacidad para

almacenar datos y ejecutar programas y a su vez los usuarios solo necesitan contar con una buena conexión a la Internet.

El servidor y el software de gestión se encuentran en Internet y son directamente gestionados por el proveedor de servicios, bajo este esquema resulta más sencillo para los usuarios utilizarla.

Pero además hay una expectativa por la seguridad de la información que se encuentra en esos repositorios y como tener un control adecuado de los datos que son puestos en Internet.

III. BENEFICIOS E INCONVENIENTES

A. Ventajas

La Computación en la Nube, tiene las siguientes ventajas frente al modelo de cómputo local:

Reducción de costos operativos y eliminación inversiones. Esto se da porque se elimina la necesidad de tener y mantener una infraestructura TI sumado al licenciamiento de software. Esto reduce o elimina la adquisición de Hardware y Software, puede ser un valor agregado para una organización que está comenzando actividades.

Eliminar gastos adicionales por acondicionamientos o mal dimensionamiento de soluciones de cómputo.

Permite ajustarse a las necesidades. Los sistemas contratados son escalables y permiten ir ajustando a las necesidades de la organización.

Alinea el gasto IT con las necesidades de su empresa.

Conexión centralizada y disponibilidad de conexión desde cualquier lugar y desde cualquier dispositivo, esto permite tener una globalización de la organización.

Mejorar la gestión del personal IT, permitiendo que los recursos se encarguen de actividades relevantes de la organización, tercerizando los servicios a los usuarios finales.

Permite rapidez en poner activo los servicios, porque se reducen tiempos de implementación y configuración de servidores además de puesta en producción de aplicaciones reduciendo los tiempos de inicio de actividades.

Permite la administración de la infraestructura por un ambiente centralizado que da el proveedor del servicio, con el cual se monitorea el servicio, estado de servidores, de aplicaciones y más.

Mejorar la gestión del riesgo permitiendo estar acorde con las normativas, seguridad y reglamentaciones, siempre que el proveedor de servicio garantice.

B. Riesgos

Los riesgos son inherentes a cualquier solución o arquitectura de sistemas de cómputo, para la Computación en la Nube se pueden visualizar los siguientes riesgos:

Se pierde el control de los sistemas de cómputo para la organización a pesar de tener monitoreo y administración de sus servicios.

Desconocimiento de la administración propia del proveedor del servicio, salvo confiar en la reputación y el contrato adquirido.

Se crea una dependencia con el proveedor del servicio y a su vez la organización pierde autonomía. No es lo mismo poseer los servidores localmente a tenerlos en una ubicación remota, que en el ambiente de un proveedor estará en un país lejano y virtualizado.

Se espera tener disponibilidad del servicio, pero esta garantía esta dependiente de factores de riesgo, además que los servidores están compartidos (virtualizados) con más clientes.

Es posible que se presenten, alteraciones en el servicio prestado.

Fallas en la identificación del manejo priorizado de aplicaciones y la transferencia de datos, que puedan en algún momento afectar las operaciones.

En el licenciamiento de software, puede que no todo contemplado para el uso en el ambiente de la Nube.

Protección de la seguridad y privacidad de datos y programas.

Dependencia de acceso a través de Internet, que permita que se quede sin conexión o que el rendimiento se disminuya.

La posibilidad de portabilidad entre aplicaciones construidas para ser utilizadas en diferentes proveedores.

IV. MODELOS DE DESPLIEGUE

La computación en la nube está disponible en los siguientes modelos:

A. Nube privada

La infraestructura de la Nube sólo funciona para una organización. Puede gestionarla la propia organización y puede existir en el local o afuera.

Ventajas: Cumplimiento de políticas internas, Facilidad en trabajo colaborativo, Control de los recursos.

Desventajas: Elevado costo, Dependencia de la infraestructura controlada, Retorno de la inversión lento.

B. Nube comunitaria

La infraestructura de la Nube se comparte con varias organizaciones y se comparten esquemas como seguridad, políticas y consideraciones de cumplimiento.

Ventajas: Cumplimiento de políticas internas, Reducción de costos al compartir, Rápido retorno de la inversión.

Desventajas: Seguridad dependiente del proveedor, Dependencia de la infraestructura controlada.

C. Nube pública

La infraestructura de la Nube se hace disponible al público en general o a un gran grupo industrial y es propiedad de una organización que vende los servicios.

Ventajas: Escalabilidad, Eficiencia de recursos mediante pago por el uso, Ahorro de tiempo y costos.

Desventajas: Comparte infraestructura con más organizaciones, poca transparencia con el cliente, Dependencia de la seguridad.

D. Nube híbrida

La infraestructura de la Nube es una composición de dos o más nubes (privada, comunitaria o pública) única para las entidades pero se limitan juntas por medio de tecnología propietaria o estandarizada que permite la portabilidad de datos y aplicaciones.

Fig. 1. Comparativo modelos de despliegue (Tomado de: Infraestructuras de seguridad en la nube, José Parada Gimeno, responsable de seguridad corporativa de Microsoft España).

V. MODELOS DE SERVICIO

Los modelos del servicio de la Computación en la Nube son:

A. Nube SaaS (Software as a Service)

En este modelo, el software es mostrado como aplicaciones y recursos que son ofrecidos bajo demanda, esto reduce costos y mantenimiento. Son accesibles desde diversos dispositivos utilizando un navegador Web. La seguridad es controlada por el proveedor y la organización tiene acceso administrativo limitado, en la cual no gestiona, ni controla la infraestructura de nube subyacente, red, servidores, sistemas operativos, almacenamiento, capacidades de cada aplicación individual con la posible excepción de establecer de forma limitada la configuración de la aplicación específica del usuario.

B. Nube PaaS (Platform as a Service)

En este modelo el servicio de hardware y software se entrega bajo demanda. Este modelo permite reducir costos, complejidad, mantenimiento, y control. La organización tiene control parcial sobre las aplicaciones y la administración. La seguridad es compartida.

C. Nube IaaS (Infrastructure as a Service)

En este modelo la infraestructura de computo (red, servidores y aplicaciones) es administrada por el proveedor bajo demanda, creando los entornos para ejecución. El proveedor ofrece todos los recursos, aunque la organización se encarga de la selección del ambiente y el entorno de trabajo. La seguridad es responsabilidad de la organización.

VI. SEGURIDAD EN COMPUTACIÓN EN LA NUBE

Según el profesor Javier Areitio, profesor de la Universidad de Deusto [1], “la Computación en la Nube es actualmente la noción más popular en TIC, sus elementos más relevantes son: el almacenamiento, el procesamiento y las redes virtuales”.

Además, el profesor Javier Areitio, menciona que se pueden identificar, desde la perspectiva de la seguridad, cinco principales componentes de la Nube que se resumen a continuación:

1. Servicios de aprovisionamiento en la Nube. Se puede aportar la rápida reconstitución de servicios, permitiendo la disponibilidad (provisión en múltiples centros de datos de múltiples instancias) y las capacidades de honey-net avanzadas. Como principales desafíos identificados, el impacto de comprometer el servicio de aprovisionamiento.

2. Servicios de almacenamiento de datos en la Nube. Las ventajas principales que puede aportar son la fragmentación y dispersión de datos, la replicación automatizada, la provisión de zonas de datos (por ejemplo por país), el cifrado en reposo y en tránsito y la retención automatizada de datos. Como principales desafíos identificados, la gestión del aislamiento y el multi-arrendamiento de datos, el controlador de almacenamiento (presenta un único punto de fallo en caso de verse comprometido) y la exposición de datos a posibles gobiernos extranjeros.

3. Infraestructura de procesamiento en la Nube. Las ventajas principales que puede aportar son la capacidad para proteger masters y sacar imágenes seguras. Como principales desafíos identificados, el multi-arrendamiento de aplicaciones, la dependencia en los hipervisores y el aislamiento de procesos y los mecanismos de sandbox para aplicaciones.

4. Servicios de soporte en la Nube. Las ventajas principales que puede aportar son los controles de seguridad bajo demanda, por ejemplo la autenticación, el logging, los firewalls, etc. Como principales desafíos identificados, el riesgo adicional cuando se integra con aplicaciones del cliente, las necesidades de certificación y acreditación como aplicación separada y las actualizaciones de código.

5. Seguridad perimétrica y de red en la Nube. Las ventajas principales que puede aportar son la protección contra la denegación de servicios distribuida o DDoS, las capacidades VLAN, la seguridad perimétrica como IAM/IDS/IPS, firewall, autenticación, etc. Como principales desafíos identificados, las zonas virtuales con movilidad de aplicaciones".

En los modelos de Computación en la Nube, se identifican los siguientes retos en temas de seguridad:

1) *Necesidad para administrar el aislamiento de los clientes de la Nube en el proveedor. Porque son varios los clientes que deben compartir la misma infraestructura.*

2) *El arrendamiento a varios clientes por parte del proveedor. Son muchos los clientes que comparten los recursos de Hardware y Software, con la adición de estar en diversos sitios geográficos del planeta.*

3) *Por la necesidad de aislar clientes, también se debe aislar los registros de actividades.*

4) *Las garantías de calidad de servicio.*

5) *La dispersión de datos y las leyes de privacidad internacionales.*

6) *La proliferación de atacantes debido al elevado valor de la información corporativa.*

7) *La posibilidad de fallos masivos en ambientes compartidos.*

8) *Necesidades de seguridad como cifrado, para los accesos a los módulos de administración, aplicaciones, y en general los datos.*

Problemas con información sensible y usuarios VIP.

9) *Planificación de contingencias y recuperación ante desastres.*

10) *Auditorias.*

VII. SEGURIDAD EN COMPUTACIÓN EN LA NUBE - AMENAZAS

Un artículo publicado por la Universidad de Cartagena, tuvo como objetivo diseñar un nuevo enfoque para la detección y evaluación de vulnerabilidades en equipos de red mediante la técnica de identificación de servicios, mediante el desarrollo de una herramienta computacional para la Detección de Vulnerabilidades basada en la Identificación de Servicios. En dicho artículo, los autores citan a Li et al. (2010), quienes "proponen un proceso de evaluación de vulnerabilidades de seguridad en entornos de computación en la nube basado en análisis de riesgo y rendimiento". [3]

En un estudio de investigación llevado a cabo en Suecia, los autores identificaron los desafíos comunes y las técnicas de mitigación, así como marcos de prácticas pertinentes para mitigar las vulnerabilidades y los ataques de software en tiempo real en la nube. No pueden hacer una identificación exhaustiva de los retos y las prácticas de mitigación asociada con la computación en nube. Pero reconocen el hecho de que los hallazgos podrían no ser suficientes para generalizar el efecto de los diferentes modelos de servicios que incluyen SaaS, IaaS y PaaS, y también es cierto para los diferentes modelos de implementación tales como privadas, públicas, comunitarias e híbridas. Sin embargo, estudiaron tanto al proveedor de la nube y los clientes de la nube sobre la seguridad, la privacidad, la integridad y temas relacionados y útiles en la identificación de más áreas de investigación que puede ayudar en la mejorar la seguridad, la privacidad, la asignación de recursos y mantener la integridad en el entorno de la nube. [4]

Según, José Parada Gimeno, Responsable de Seguridad Corporativa, Microsoft España, las amenazas de la Computación en la Nube las categoriza en tres grupos:

A. Amenazas derivadas de la Tecnología

Estas amenazas son las que siempre han estado con algunas corporaciones, esas se solucionan con más tecnología.

Las amenazas tradicionales siguen existiendo: Ataques a la capa de aplicación (XSS, ataques de inyección de código) y ataques a la capa de red (ataques DNS, network flooding).

Se potencian otras amenazas como: Ataques a las tecnologías de virtualización.

Nuevos ataques de escalada de privilegios (VM a host o VM a VM).

Romper las barreras de las VM.

Hyperjacking (rootkitting al host o a la VM).

Hay más amenazas pero menos riesgo: La tecnología y procedimientos empleados en proteger los centros de datos de la nube es muy superior a la empleada en nuestras organizaciones.

Gestión de riesgos, de cambios, de regulación, de identidad, de acceso.

Es un problema de confianza y no de seguridad.

B. Amenazas de la parte cliente (PC, dispositivos móviles)

En el nuevo entorno cada PC ha de ser seguro por sí mismo.

La seguridad física: Ya no cuenta con la protección física de nuestras oficinas. Hay que proteger la información a nivel físico (TPM, bitlocker, bitlocker to go, etc).

La seguridad en toda la pila de software: El Software a utilizar ha de estar bien desarrollado (SDL).

El Sistema ha de tener su propio software de seguridad: Firewall, IDS, antivirus.

El Sistema Operativo ha de contar con funcionalidad para conexiones sencillas y seguras.

En el nuevo entorno cada dispositivo ha de ser seguro por sí mismo y cumplir con los requisitos legales.

C. Amenazas filosóficas y de procedimiento

Hay muchas novedades.

Se solucionan con cambios de mentalidad y aprendizaje.

En el nuevo entorno cambian más cosas de las que parecen: Arquitectura de red abierta, ubicuidad de los datos, ubicuidad de los usuarios y sus terminales.

Compartición de Procesos y responsabilidades.

Gestión de la seguridad entre proveedor y cliente: Acceso, identidad, regulación, protección de datos, auditoria y forense.

Además de entender el entorno, es necesario un buen entendimiento entre el proveedor y el cliente.

Según la Cloud Security Alliance (CSA) [7], presentaron en un informe en marzo del 2010, que incluía las siete mayores amenazas de las infraestructuras de Computación en la Nube, en la cual se resumen:

1) ***Abuso y mal uso de la Computación en la Nube.***

Esta amenaza afecta los modelos IaaS y PaaS y está relacionada con acceso poco restrictivo, permitiendo usuarios con código malicioso.

2) ***Interfaces y API poco seguros.***

Como los proveedores de servicios utilizan herramientas como Interfaces y API para controlar los recursos, es necesario que estos estén desarrollados de forma segura, evaluando adecuadamente los problemas de seguridad.

3) ***Amenaza Interna.***

Teniendo en cuenta que el acceso a la información, está dispuesta a los propios usuarios de la organización, en el ambiente de la Nube también se pueden presentar incidentes de seguridad. A esto se le suma el hecho que el proveedor tiene acceso a porciones de información que queda expuesta, como parte de la administración. Por ello el proveedor debe garantizar métodos de control de amenazas internas.

4) ***Problemas derivados de las tecnologías compartidas.***

Esta amenaza afecta a los modelos IaaS, ya que un modelo de Infraestructura formado por Hardware, no se diseñaron para arquitecturas compartidas y esto provoca incidentes de seguridad. Para mitigar este escenario se implementa una defensa en profundidad y se genera una estrategia de seguridad para gestionar los recursos.

5) ***Perdida o fuga de información.***

En la Computación en la Nube los riesgos de pérdida de datos aumentan, debido a la infraestructura.

6) ***Secuestro de sesión o servicio.***

En la Nube si un atacante obtiene las credenciales, puede causar muchos daños. Por ello se debe aumentar la seguridad.

7) ***Riesgos por desconocimiento.***

En una implementación de Computación e la Nube, se debe conocer en gran medida información técnica acerca de la plataforma, el desconocimiento puede desencadenar en brechas de seguridad por desconocimiento.

Según Gartner S. A., [8] una empresa de investigación y consultoría con sede en Estados Unidos, ha realizado un informe llamado: "Assessing the Security Risk of Cloud Computing", del cual se contemplan siete riesgos en la Computación en la Nube, los cuales se resumen:

1) ***Accesos de usuarios con privilegios.***

El tratamiento de los datos sensibles fuera de la organización ya que servicios externos sean vulnerables.

2) ***Cumplimiento normativo.***

Los usuarios son los responsables de los datos así la información este en la Nube.

3) ***Localización de datos.***

Cuando los servicios están en la Nube no se conoce en que ubicación geográfica están los datos.

4) ***Aislamiento de datos.***

En la Nube se comparte la infraestructura con otros clientes, el proveedor debe garantizar el aislamiento de la información.

5) ***Recuperación.***

Los proveedores deben estar en capacidad de recuperar información en caso de desastres.

6) ***Soporte investigativo.***

Las labores de investigación de actividades ilegales en los ambientes de la Nube son imposibles debido a los múltiples clientes y registros de actividad.

7) ***Viabilidad a largo plazo.***

No hay garantías que un proveedor este siempre en el mercado, este puede cerrar, ser absorbido por otra compañía.

VIII. RECOMENDACIONES

Como recomendaciones al iniciar un proceso de computación en la Nube, se tiene:

1) Contar con un equipo interno que tenga conocimientos en temas relacionados con la Computación en la Nube. No es recomendable aventurar y probar en la marcha.

2) Tener conocimiento de conceptos de Seguridad Informática y en especial para Seleccionar estrategias y planes de contingencia. O contar con un especialista que le asista en la solución.

3) Tener un conocimiento de las tecnologías y modelos que están inmersas en la infraestructura de la Nube. Si no conoce lo que desea adquirir no puede esperar buenos resultados y sería mejor optar una infraestructura local o tradicional en la cual tenga más control de sus activos informáticos.

4) Tener conocimiento de las tecnologías de ambientes virtualizados. Es necesario debido a que la virtualización es uno de los pilares de los modelos en la Nube.

5) Tener claro el panorama de los deseos y expectativas con los servicios en la Nube. Puede que no sea necesario llevar a la Nube determinada información o servicio.

6) Tener conocimientos de estándares del mercado. Hay una constante innovación en protocolos, tecnología, seguridades que se deben tener presentes en todo momento.

7) Elegir junto con el proveedor reconocido el Modelo de despliegue más adecuado (Privada, Comunitaria o Pública).Existen proveedores de nombre, como Amazon Web Services Google Apssengine, IBM, entre otros. De todos modos recordamos que estamos poniendo ante ellos nuestra información.

8) Tener conocimientos de la normativa local vigente así como su incidencia en temas relacionados con los servicios y de la Computación en la Nube.

9) Contar con opciones de proveedores certificados y confiables que den total confianza.

10) Tener claridad de que procesos o servicios se van a trabajar localmente y que información se va a trabajar en procesos dentro de la Nube.

11) Tener mecanismos contratados y propios para respaldar adecuadamente la información.

IX. CONCLUSIONES

La proliferación de servicio de Computo en la nube, deben tomarse con calma, analizando si su utilización causa un beneficio para la organización con la prudencia de no caer en una moda tecnológica, sino que esta sea una alternativa a los ciclos de crecimiento empresarial y del área de IT.

Antes de proceder en un proyecto de computación en la Nube debemos estar informados de los aspectos vigentes de este modelo: que incluyen desde el conocimiento hasta la elección de un proveedor adecuado a la necesidad.

La protección de la información y la seguridad, es el aspecto más importante de la elección del modelo, porque ello garantizará que su implementación sea proyectada en el tiempo y así satisfaga las necesidades de las organizaciones.

En la implementación de software se deben contemplar temas como licenciamiento adecuado al ambiente, y las vulnerabilidades posibles a tener en cuenta.

Se debe elegir un proveedor adecuado a las necesidades de la organización y que éste garantice calidad en el servicio, adicionalmente que se encuentre de acuerdo a las leyes y normativas internas y externas.

Se debe analizar bien si el negocio que desarrolla o los objetivos organizacionales serán satisfechos y redundará en beneficios si se toma decisión de utilizar el modelo de Computación en la Nube, porque posiblemente esta no sea la solución a las necesidades de Cómputo.

Finalmente, la información es el activo más valioso que tenemos como persona y como organización, por ello debemos hacer bien una tarea de llevarla hacia Internet y en administración de un tercero. Además, La Seguridad es completamente prioritaria y necesaria para la adopción del modelo computacional en la Nube.

REFERENCIAS

[1] J. Areitio, "Protección del Cloud Computing en seguridad y privacidad," *Revista española de electrónica*, ISSN 0482-6396, N°666, pp. 42–48, 2010.

[2] NIST, http://www.nist.gov/itl/cloud/

[3] Franco, D; Perea, J; Tovar, L. Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Universidad de Cartagena, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática. Información Tecnológica Vol. 24(5), 13-22 (2013).

[4] Aifuobhokhan, M; Tekkali, S. Real-Time Software Vulnerabilities in Cloud Computing Challenges and Mitigation Techniques. Master's Thesis Computer Science. Thesis no: MCS-2011-201. School of Computing Blekinge Institute of Technology. Sweden. 2011. http://www.bth.se/fou/cuppsats.nsf/all/d24bc9368dfe52a2c1257910002a6482/$file/BTH2011Okonoboh.pdf

[5] IBM Red Paper: Cloud Security Guidance
Axel Buecker, Koos Loderwijkx, Harold Moss, Kevin Skapinetz, Michael Waldner 2009
http://issuu.com/dragonjar/docs/cloud_security_guidance/9?e=1640921/5542736

[6] INTECO-CERT, Riesgos y amenazas en Cloud Computing. Marzo 2011,
http://issuu.com/dragonjar/docs/riesgos_y_amenazas_en__cloud_computing/1?e=1640921/3899874

[7] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0", 2010.

[8] Jay Heiser, Mark Nicolett , Gartner, Inc, "Assessing the Security Risks of Cloud Computing", 2008.

[9] Ulrich Lang, "Seguridad en la nube controlada por modelo", IBM, 2012.

[10] La Computación en Nube (Cloud Computing): El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento, Revista Icade. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales. https://revistas.upcomillas.es/index.php/revistaicade/article/view/289

[11] Jon Brodkin, Gartner: Seven cloud - computing security risks, 2008. http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf