ANÁLISIS DE RIESGOS EN SEGURIDAD CLOUD COMPUTING

Roberto Carlos Loaiza Zuluaga
cf0161rcl@gmail.com

Resumen: Hoy en día, una de las tendencias empresariales es apostarle a la computación en la nube, la cual desde el punto de vista de las empresas puede mejorar en gran parte los aspectos tecnológicos, así como facilitar la escalabilidad y por supuesto, beneficios en lo relacionado con aspectos financieros; lo anterior, impulsa a las empresas a demandar recursos teóricamente ilimitados mediante un esquema de pago por consumo o utilización de estos servicios por medio de Internet. Sin embargo, al realizar el cambio a este esquema de computación se requiere el traslado de la información que actualmente está asegurada y en un alto porcentaje controlada en un perímetro local, a un ambiente distribuido y remoto, que como lo están viendo actualmente las entidades puede resultar interesante al presentar nuevos beneficios, tantos como la generación de nuevos riesgos y vulnerabilidades. Teniendo en cuenta esta dificultad de optar o no por la computación en la nube como estrategia corporativa y de negocio, los directivos de las empresas están siendo un poco cautelosos con el fin de evitar nuevos riesgos en sus procesos, esto puede presentarse por la falta de conocimiento o herramientas que les permitan tomar las decisiones más adecuadas. Por tal razón el objetivo principal de este artículo es presentar una propuesta para realizar un análisis de riegos en seguridad, que deberían ejecutar las empresas antes de realizar la implementación en cualquiera de los diferentes tipos de computación en la nube, como son privadas, públicas e hibrida.

Abstract- Today, one of the business trends is bet on cloud computing, which from the point of view of firms can largely improve the technological aspects, as well as provide scalability and of course, benefits in relation financial aspects; above, drives companies to sue theoretically unlimited resources through a system of payment for consumption or use of these services over the Internet. However, to make the change to this scheme computing the transfer of information that is currently insured and in a high percentage controlled in a local scope, a distributed and remote environment, as they are currently viewing is required entities can be interesting to introduce new benefits, as many as the generation of new risks and vulnerabilities. Given this difficulty of use or not to cloud computing as a corporate and business strategy, management companies are being a little cautious in order to avoid new risks in their processes, this may arise from lack of knowledge or tools to make the right decisions. For that reason the main goal of this paper is to present a proposal to conduct a risk analysis in security, they should run companies before deploying to either type of cloud computing, such as: private, public and hybridizes.

Palabras Clave: Análisis de riesgos, computación en la nube Estándar Británico BS7799, riesgo inherente, riesgo residual, tercerización.

1 INTRODUCCIÓN

La computación en la nube hoy en día es conocida como transformación, evolución o revolución [1]. No interesa el nombre que le asignemos, lo verdaderamente importante es que actualmente estos servicios ofrecidos a través de Internet, están cambiando la realidad de hacer los negocios. Actualmente una de las mayores necesidades de las organizaciones, es disponer de la información en cualquier sitio, en un momento determinado y prácticamente desde cualquier tipo de dispositivo. La prestación de estos servicios dependen en gran parte de las necesidades de los consumidores, por tal razón las opciones que deben ofrecer las empresas dedicadas a este negocio, deben ser personalizables y flexibles para que puedan adaptarse a los requerimientos y necesidades de los distintos tipos y clases de empresas.

2 COMPUTACIÓN EN LA NUBE

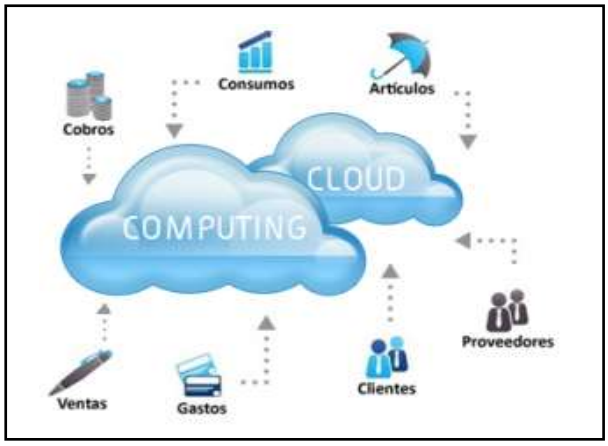

Fig. 1 Cloud Computing. Fuente inBest.me.

El cloud computing o computación en la nube es una manera de contratar nuevos servicios para el procesamiento y tratamiento de la información (hardware, software, comunicaciones, almacenamiento y servicios). Actualmente es utilizada por las empresas y particulares, permitiendo la optimización tanto de costos como recursos que hacen parte de los requerimientos para el tratamiento de los activos de información. Cuando los clientes contratan estos servicios por demanda, lo podemos comparar con los servicios públicos en nuestros hogares, en los que se debe pagar lo que realmente utilizamos o ha sido contratado. Las empresas ya no tienen la necesidad de invertir en infraestructura y tecnología, sino que utiliza la disponible por el prestador de servicio seleccionado, asegurando que no se presenten falta de recursos y en

caso de requerir más por temas de crecimiento, contar con tiempos realmente óptimos con simplemente solicitarlo al proveedor de servicio, por ejemplo, más almacenamiento o crecimiento en cuanto a infraestructura se refiere. Normalmente, los servicios más contratados son soluciones de bases de datos, correo electrónico, aplicaciones de ofimática, de acuerdo a sus necesidades. Una de las principales preocupaciones, es dónde se encuentran los datos teniendo en cuenta que dependiendo del modelo contratado el proveedor de servicios puede a su vez tercerizar partes de sus procesos y prácticamente los datos pueden encontrarse en cualquier lugar del mundo.

3 CARACTERÍSTICAS

Según el National Institute of Standards and Technology-NIST[1], existen cinco características esenciales de la computación en la nube que las empresas deben conocer:

- **Auto-servicio por Demanda**

Este tipo de servicios pueden ser solicitados por el usuario o cliente directamente a través de Internet. En estos casos el cliente paga únicamente por los servicios y su tiempo de uso en función de sus necesidades.

- **Amplio Acceso a la Red**

Una de las principales características de la computación en la nube, es que siempre los servicios se encuentren disponibles, independientemente del tipo de red que se esté utilizando y a la que se pueda tener acceso prácticamente desde cualquier dispositivo (Ej. PCs, smartphones, tablets, etc.).

- **Uso de Recursos Compartidos**

Hace referencia a la cantidad de recursos disponibles que tiene el cliente como hardware, capacidad de procesamiento, almacenamiento y gracias a la virtualización de estos recursos, brindar al cliente sentido de independencia en el sistema contratado.

- **Elasticidad y Rapidez**

Ofrece al cliente despliegue y escalabilidad de manera rápida en sus recursos (teóricamente) ilimitados en el momento que lo requiera.

- **Monitoreo de Servicios**

Se realiza un seguimiento permanente, para la optimización del uso de los recursos de acuerdo a los servicios contratados (Ej. Ancho de banda, procesamiento, almacenamiento, cuentas de usuario).

[1] Instituto Nacional de Normas y Tecnologías, la misión es promover la innovación y la competencia industrial.

4 CLASES

Actualmente, existen tres principales clases de servicios de computación en la nube:

- **(IaaS) Infraestructura como Servicios**

El cliente tiene la posibilidad de contratar capacidad de procesamiento, almacenamiento y comunicación, sobre un servidor o máquina virtual. El cliente no gestiona ni tiene control sobre el centro de datos, pero si controla los datos y los sistemas operativos [2] (por ejemplo, servicio de Dropbox).

- **(PaaS) Plataforma como Servicios**

Da la posibilidad al cliente de desplegar sus propias aplicaciones, servidores de aplicaciones y bases de datos en la infraestructura del proveedor; en este tipo de servicio el cliente tiene control sobre los datos, aplicaciones y parte del entorno donde están alojadas dichas aplicaciones. Ej: Windows Azure[2], Google App.

- **(SaaS) Software como Servicio**

Por medio de una interfaz ligera el cliente puede utilizar aplicaciones web que se ejecutan en la nube, las cuales son ofrecidas por el proveedor, este es uno de los servicios más utilizados en la nube, las utilizan Facebook, web mail y otras redes sociales.

5 TIPOS DE SERVICIOS

Teniendo en cuenta el nivel de apropiación y arquitectura contamos actualmente con cuatro tipos de nube:

- **Nube Privada**

El cliente acondiciona su propia infraestructura para ser utilizada en su propio beneficio, y puede estar ubicada dentro o fuera de la organización con el fin de controlar los accesos solo a quien ellos definan.

- **Nube Comunitaria**

Hace referencia a una única nube la cual es compartida por diferentes empresas o clientes con objetivos y propósitos en común por ejemplo los gobiernos.

[2] Plataforma ofrecida como servicio y alojada en los data centers de Microsoft, paso a ser servicio comercial el 1 de enero de 2010.

- **Nube Pública**

Es propiedad de una organización la cual busca como objetivo prestar sus servicios a múltiples clientes [3], toda la infraestructura pertenece a la organización que vende los servicios.

- **Nube Hibrida**

Generalmente está conformada por dos o más nubes, una privada y una o más públicas que buscan utilizar complementos y compartir recursos, un ejemplo puede ser un banco que utiliza una nube privada para el manejo de la información clasificada como confidencial, y almacena los demás activos de información en una nube pública, con el objetivo de reducir costos y aumentar almacenamiento.

6 ANÁLISIS DE RIESGOS

Con el fin de proteger los sistemas tradicionales, las organizaciones han gastado gran cantidad de dinero en la adquisición de herramientas de seguridad (Firewall, NATs, VPNs, DLP) con el principal objetivo de proteger la información, uno de los principales activos de cualquier organización sin importar su objeto social, ya que sin ella sencillamente no existe ninguna organización. Por el contrario, con los servicios en la nube que mencionamos anteriormente, los cuales son altamente visibles y se encuentran desarrollados para ser accedidos prácticamente desde cualquier ubicación por cualquier persona, las vuelve un blanco muy llamativo para cualquier atacante; por tal motivo se requiere y es primordial realizar una evaluación de las posibles consecuencias a las cuales se estaría enfrentando la organización, en cuanto a seguridad se refiere, antes de iniciar un proceso de migración o implementación de cualquier sistema en la nube. Con el fin de lograr el objetivo vamos a usar la metodología de análisis de riesgos planteada en el estándar británico [4] BS7799[3].

- **Convenciones Matriz de Riesgo Estándar Británico BS7799**

PRINCIPIOS DE SEGURIDAD AFECTADO	P.S.A
INTEGRIDAD	I
DISPONIBILIDAD	D
CONFIDENCIALIDAD	C
PRIVACIDAD	P
Nota: Se utiliza para indicar cual o cuales principios de seguridad de la información están siendo vulnerados.	

Fig. 2 Pilares Seguridad de la Información. Fuente: El autor.

CRITERIOS CUANTITATIVOS		CRITERIOS CUALITATIVOS
Bajo	1	El riesgo se materializará anualmente
Medio	2	El riesgo se materializará semestralmente
Alto	3	El riesgo se materializará trimestralmente
Muy Alto	4	El riesgo se podría materializar mensualmente

Fig. 3 Calificación Probabilidad. Fuente: El autor.

CRITERIOS CUANTITATIVOS		CRITERIOS CUALITATIVOS			
		Legal	Continuidad	Operativo	Económico
Bajo	1	Oportunidades de mejoramiento de acuerdo a los incidentes de riesgo materializados.	No genera interrupción de las operaciones.	Intentos de acceso no autorizado a los sistemas de información focalizados.	Hasta $100 M
Medio	2	Observaciones por incumplimiento de las normas establecidas por los entes reguladores.	Activa al menos uno de los planes de contingencia.	Reproceso de actividades.	Hasta $500 M
Alto	3	Sanciones pecuniarias por incumplimiento repetitivo de las normas establecidas por los entes reguladores.	Obliga a mantener activo los planes de contingencia y continuidad.	Investigaciones por vulnerabilidades presentadas a los sistemas de información por manipulación.	Hasta $1.000 M
Muy Alto	4	Sanciones económicas por incumplimiento repetitivo de las normas establecidas por los entes reguladores.	Afecta la continuidad del negocio.	Fraude y sistemas de información totalmente comprometidos y/o vulnerados.	Superior a $1.000 M

Fig. 4 Calificación Impacto. Fuente: El autor.

[3] Estándar Británico, es un estándar aceptado ampliamente que ha sido utilizado como base para elaborar otros estándares de seguridad de la información incluyendo el ISO 17799.

• Identificación de Vulnerabilidades

Al realizar la identificación de vulnerabilidades podemos encontrar aquellas comunes a todos los sistemas, como las que son propias de los servicios en la nube. **Ver tabla 1**, (vulnerabilidades con sus riesgos, impacto y probabilidad de ocurrencia). En la tabla 1, se relacionan algunas vulnerabilidades, a las cuales estarían expuestas las entidades con la posible migración o implementación de los diferentes tipos de nube, Privada, Pública e Híbrida. Al identificar las vulnerabilidades el experto debe calificar las variables de probabilidad e impacto, con el objetivo de generar como resultado el mapa de riesgos inherente (ver Fig. 6).

ID	CAUSA O VULNERABILIDAD	RIESGOS perdidad de:	IMPACTO	PROBABILIDAD DE OCURRENCIA	TIPO DE NUBE
1	Ataques de ciberdelicuentes a la infraestructura del Cloud Computing.	C,I,D,P	2	2	Privada. Pública. Híbrido
2	Perdida disponibilidad de servicio por distintos aspectos como ataques de código malicioso, informáticos, desastres naturales, etc.	D	1	2	Privada.
3	Multas por incumplimiento de regulaciones nacionales internacionales.	D	2	2	Privada.
4	Sistemas debiles de administración y gestión de usuarios por parte del proveedor del servicio.	C,I,D,P	1	2	Privada. Pública. Híbrido.
5	Pérdida o fuga de información. En la nube, aumenta el riesgo ya que las interacciones entre ellos se multiplica por la arquitectura de la misma.	C,I,P	1	2	Privada. Pública. Híbrido.
6	Aislamiento de datos**.** Los datos en los entornos *cloud* comparten infraestructura con datos de otros clientes por lo que estos se pueden ver comprometidos.	C,I,D,P	1	2	Privada.
7	Inadecuado manejo de incidentes. La investigación de actividades ilegales en la nube puede ser una actividad dispendiosa.	D	1	2	Privada.
8	Perdida de los datos y por ende la confidencialidad de la información se ve expuesta por el desconocimiento de la localización de datos.	C, I,P	1	2	Privada
9	Incumplimiento Normativo.	C,I,D,P	1	2	Privada
10	Exposición accidental de información confidencial en los medios de almacenamiento del Cloud.	C,I,D,P	1	2	Privada

Tabla 1. Identificación de Vulnerabilidades. Fuente: El autor.

• Controles a tener en cuenta para ser implementados

En este punto se relacionan como ejemplo los controles que deberían existir por cada una de la vulnerabilidades identificadas, los cuales al realizar el análisis de riesgos, se debe determinar si se requiere implementar nuevos controles o mejorar los existentes, posterior a este proceso debemos ejecutar la calificación de cada una de las vulnerabilidades aplicando los controles, para poder generar el mapa de riesgos residual. Ver los controles en la **tabla 2**.

ID VULNERABILIDAD	C0NTROLES	TIPO DE NUBE
1	1.) Implementar estándares de seguridad sobre la plataforma tecnológica. 2.) Ejecutar pruebas de vulnerabilidades a la plataforma tecnológica de manera permanente. 3.) Implementar herramientas de seguridad perimetrales como detectores de intrusos y firewall que protejan la plataforma tecnológica contra ataques externos. 4.) Generar los acuerdos de nivel de servicio para controlar la implementación de parches de seguridad y la corrección de vulnerabilidades.	Privada. Pública. Híbrido.
2	1.) El proveedor de Cloud Computing debe tener planes de recuperación de desastres para cada uno de los aspectos específicos. 2.) El proveedor debe contar con un plan de respuesta a incidentes (incluir tiempos de recuperación).	Privada.
3	1.) El proveedor que presta el servicio de Cloud deberá cumplir con regulaciones nacionales e internacionales.	Privada.
4	1.) Especificar cláusulas legales. 2.) Elaborar un procedimiento de administración de usuarios. 3.) Elaborar acuerdos de servicios entre el proveedor de Cloud y las Entidades. 4.) Realizar auditorías frecuentes a la administración de usuarios a cargo del proveedor.	Privada. Pública. Híbrido.
5	1.) Implementar API seguras para el control de acceso. 2.) Proteger el canal de datos con cifrамiento. 3.) Analizar la protección de datos tanto en tiempo de diseño como en tiempo de ejecución. 4.) Definir una norma la destrucción de los datos de manera segura. 5.) Almacenamiento de copias de respaldo con las medidas de seguridad definidas por las Entidades.	Privada. Pública. Híbrido.
6	1.) El proveedor debe garantizar el aislamiento de los datos de los respectivos clientes y de la infraestructura tecnológica de las Entidades a través de VLAN´s o segmentación de la Red. 2.) El proveedor del servicio debe garantizar que los datos en reposo estarán cifrados con los algoritmos internacionalmente aceptados tal como el 3DES, AES 256, entre otros.	Privada.
7	1.) Se debe implementar una herramienta de centralización de log´s la cual debe implementarse en la Entidad para que se administre los datos e información de incidentes desde esta. 2.) Implementar acuerdos de nivel de servicio para la entrega de logs. 3.) Los logs que requieran las entidades de Control, son de alta prioridad.	Privada.
8	1.) Debe quedar identificado y con responsabilidad contractual las necesidades de cumplimiento regulatorio de parte del proveedor. 2.) Para la seguridad física de los centros de datos se debe cumplir con la Norma ANSI/TIA 942, Tier 4 la cuál es la mejor práctica, igualmente, el tratamiento de los datos se subyugue al marco legal del país del suscriptor del servicio y se debe estipular la ubicación geográfica donde quedan almacenados los datos. 3.) La entidad debe monitorear la salud política y económica del país en donde residen los datos y tener un plan para su recuperación en el evento del deterioro de alguna de estas variables (mínimo una calificación de riesgo país BBB). 4.) El personal asignado para administrar los recursos informáticos utilizados para el procesamiento de la información deberá tener disponible de manera inmediata para atender cualquier actividad relacionada con sus funciones o con funciones de contingencia.	Privada.
9	1.) Definir y aplicar procedimientos utilizando herramientas adecuadas para garantizar el ciclo de vida seguro de los datos (creación, utilización, almacenamiento, procesamiento, eliminación o borrado), de todos los medios de almacenamiento de información garantizando que los datos no son recuperables mediante cualquier medio de informática forense, así mismo conservar los registros de destrucción de la información.	Privada.
10	1.) El proveedor debe identificar e implementar los aspectos de seguridad para el cumplimiento de las regulaciones que son impuestas por los entes de control y que rigen a la Entidad.	Privada.

Tabla 2. Controles por tipo de Vulnerabilidades. Fuente: El autor.

A manera de ejemplo se presenta la calificación de algunas de las vulnerabilidades anteriormente mencionadas, en las cuales no se realiza la aplicación de los controles con el fin de presentar el mapa de riesgos inherente. El valor se obtiene multiplicando la probabilidad por el impacto. Ver figura 5.

ID VULNERABILIDAD	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
1	3	2	6
2	3	2	6
3	2	3	6
4	3	3	9

Fig. 5 Calificación Vulnerabilidades. Fuente: El autor.

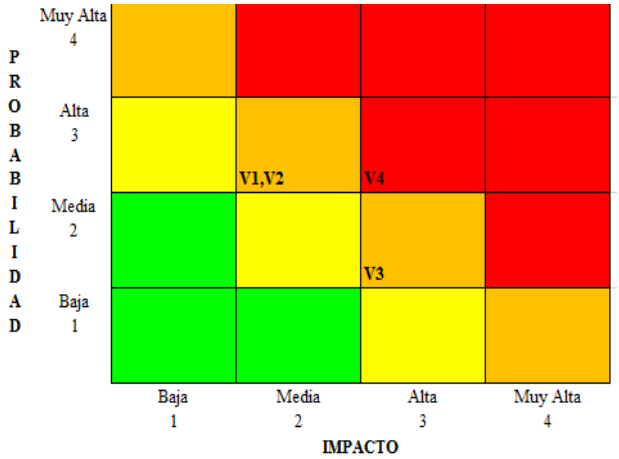

Fig. 6 Mapa de Riesgos Inherente. Fuente: El autor.

En la figura 6, observamos la calificación de las vulnerabilidades graficadas en el mapa de riesgos inherente (Ej. ubicación 3,2), es decir, sin aplicar ninguno de los controles; luego de esto se deben aplicar los controles que puede tener implementados en la organización o los ya presentados en la tabla No. 2, y validar si mitigan la probabilidad y/o impacto y se procede a revisar los resultados obtenidos en la colorimetría definida en el mapa de riesgos resultado que es el residual. El objetivo de esta actividad es presentar el mapa de riesgos residual a la alta dirección en la organización y poder definir la estrategia para el tratamiento adecuado de los riesgos.

7 TIPOS DE INFORMACIÓN

A continuación se detallan los aspectos de seguridad a tener en cuenta de acuerdo al tipo de información que se puede manejar en la nube:

- **Información Confidencial**

Para el tratamiento en Cloud de este tipo de información se debe manejar el mismo nivel de seguridad como si se alojara en la infraestructura interna. Por lo que los proveedores de servicios de Cloud deben tener implementados al menos:

- Un Modelo de seguridad definido y formalizado.
- Un sistema de gestión de la seguridad definido, maduro y formalizado.
- El proveedor de servicios se debe comprometer al cumplimiento de las Normas Nacionales e Internacionales que la Entidad debe cumplir.
- Debe tener implementado un NOC y SOC.
- Definido y probado el proceso de contención de incidentes.
- Para la seguridad física de los centros de datos se debe cumplir con la Norma ANSI/TIA 942 [5], Tier 4[4].
- Para los temas de auditoría y cumplimiento los proveedores de Cloud deben permitir a las Entidades realizar auditorías periódicas y/o entregar Informes SAS 70 tipo II (SSAE 16) de un tercero calificado o de las áreas de control interno.
- Tener una arquitectura de seguridad de propósito exclusivo.
- Compromisos contractuales de entrega y borrado seguro de la información.
- Adelantar procesos de seguridad en los recursos humanos.

- **Información de Uso Interno**

Si la información que se quiere tener en una arquitectura Cloud es información de uso interno y no se tendrá información confidencial, información de los clientes como por ejemplo información sujeta a la reserva bancaria, información personal sensible de clientes o colaboradores, consideramos que el riesgo es menor y se debe tener en cuenta los siguientes aspectos de seguridad (Como información de uso interno se incluye servidores de pruebas, servidores de desarrollo, etc. que no comprometan información confidencial ni información sensible):

Para la transferencia de archivos se debe usar un sistema que garantice la seguridad al gestionar, compartir y proteger la información que se transfiere fuera de la empresa, entre otros se debe:

- Usar protocolos seguros tal como SFTP puerto 22 (Secure Shell o SSH) y sistemas de transmisión de archivos dedicados para cada Entidad.
- Manejar el ciframiento, autenticación, control de acceso y estricta auditoría de los archivos.
- Conservar de forma íntegra, segura, trazable y siempre disponible los archivos digitales en su organización.
- La gestión de intercambios electrónicos seguros y con trazabilidad y siempre disponibles.
- Tener una arquitectura de seguridad.
- Realizar el seguimiento del inventario de imágenes de VM y versiones del sistema operativo que se preparan para Cloud hosting.
- El proveedor de IaaS ofrece algunas de estas imágenes de VM. Cuando se utiliza una imagen virtual del proveedor de IaaS debe someterse al mismo nivel de verificación de la seguridad y el endurecimiento de hosts dentro de la empresa. La mejor alternativa es la de proveer su propia imagen que cumpla con los mismos estándares de seguridad tales como los hosts de confianza interna.
- Establecer evidencias electrónicas para poder realizar análisis forense en un sistema.
- Crear un proceso para efectuar el parcheo de las imágenes en la línea de nube incluyendo sus instancias.
- Revisar periódicamente los registros de actividades sospechosas.
- Gestión de identidades y de acceso: sólo los usuarios autorizados (administradores y equipo de apoyo) tendrían permiso de acceder al sistema. Los usuarios se gestionarían con las credenciales para llevar a cabo acciones de mantenimiento y apoyo. El acceso se efectuaría a través de una conexión segura.

- **Información Pública**

Si la información que se quiere tener en una arquitectura Cloud es información de uso público y no se tendrá información confidencial, información de los clientes sujeta a la reserva bancaria, información personal sensible de clientes o colaboradores, o información que sea de uso interno de las Entidades, consideramos que el riesgo es menor y se debe tener en cuenta los siguientes aspectos de seguridad:

- Crear un proceso para efectuar el parcheo de las imágenes en la línea de nube incluyendo sus instancias.
- Tener una arquitectura de seguridad.
- Tener un proceso de gestión de usuario en donde sólo los usuarios autorizados (administradores y equipo de apoyo) tendrían permiso de acceder al sistema. Los usuarios se gestionarían con las credenciales para llevar a cabo acciones de mantenimiento y apoyo. El acceso se efectuaría a través de una conexión segura.
- Uso de protocolo seguros de conexión HTTPS, FTPS o SFTP, entre otros.
- Revisar periódicamente los registros de actividades sospechosas.

8 CONCLUSIONES

- Al tomar la decisión de migrar o implementar sistemas o servicios en la nube, las empresas deben realizarlo paso a paso cumpliendo las diferentes etapas de levantamiento de requisitos, evaluación y selección del

[4] Data center con un 99.995 de disponibilidad, posibilidad de sostener un caso de improviso sin daños críticos.

proveedor, análisis de riesgos, implementación o mejoramiento de los controles, migración de los sistemas y pruebas de verificación de las mismas, y por supuesto cumpliendo los requerimientos y objetivos estratégicos del negocios y todo el cumplimiento normativo.

- Como lo hemos visto en el desarrollo del articulo la computación en la nube ofrece grandes ventajas que prometen realizar rediseños a los conceptos de servicios computacionales, sin embargo es obligación del cliente efectuar un estudio y análisis previo en cuanto a seguridad se refiere, no solo antes de realizar la migración o implementación, sino durante y después de realizada, utilizando como recomendación un sistema de gestión de seguridad de la información.
- Una adecuada clasificación de activos de información en la organización, ayuda a identificar los riesgos, con el fin de establecer los controles que garanticen la confidencialidad, integridad y disponibilidad de la misma, independientemente del tipo de nube que se seleccione para la prestación de servicios.

9 REFERENCIAS

[1] http://www.sascolombia.com.co/temas/analitica/cinco-caracteristicas-esenciales-de-la-computacion-en-lanube/

[2] https://itunews.itu.int/Es/3703-La-influencia-economica-de-la-nube.note.aspx

[3] http://www.ibm.com/cloud-computing/co/es/what-is-cloud-computing.html

[4] http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/BS.php

[5] http://www.c3comunicaciones.es/data-center-el-estandar-tia-942/

10 BIBLIOGRAFÍA

http://blog.desdelinux.net/la-nube-analisis-a-fondo-de-sus-ventajas-y-peligros/

http://technet.microsoft.com/es-es/magazine/hh750397.aspx

http://inbest.me/entendiendo-la-computacion-en-la-nube