MANEJO DEL RIESGO Y SEGURIDAD EN EL CONSUMO DE SERVICIOS DE TI EN CLOUD COMPUTING

SECURITY AND RISK MANAGEMENT WHEN USING CLOUD-COMPUTING IT SERVICES

Abstract
This thematic exploration is framed within the research area of Information Security, and represents a contribution in terms of precise inputs aimed at illustrating good Risk and Security Management practices to organizations that use cloud computing services. This exploration attempts to provide readers with the definition of some key points to be considered when minimizing the impact and likelihood of occurrence of events that threaten the information security of organizations while using services associated to Cloud-type "Information Technologies".

Keywords: Cloud computing, IaaS, PasS, service provider, SasS, information Security.

Resumen
Este articulo presenta una exploración temática que se encuentra enmarcada dentro de la línea de investigación de Seguridad de la Información, y busca contribuir con aportes precisos encaminados a dar un buen manejo al Riesgo y a la Seguridad de las organizaciones que consumen servicios en Cloud Computing. Se pretende aportar a los lectores la definición de puntos claves a tener en cuenta buscando minimizar el impacto y posibilidad de ocurrencia de eventos que atenten contra la seguridad de la información de las organizaciones cuando estas deciden ingresar en las tecnologías de información de tipo Cloud.

Palabras clave: Cloud computing, IaaS, PasS, proveedor de servicios, SasS, seguridad de la información.

Erick Sepúlveda O.
Ingeniero de Sistemas, estudiante de la Especialización en Teleinformática en la Universidad Distrital Francisco José de Caldas.
esepulvedao@correo.udistrital.edu.co

Octavio J. Salcedo
Ingeniero de Sistemas, MSc. en Teleinformática de la Universidad Distrital, MSc. en Economía, docente Universidad Distrital "Francisco José de Caldas".
ojsalcedop@udistrital.edu.co

Ernesto Gómez Vargas
Ingeniero Electrónico, MSc. en Teleinformática, Candidato a Doctor en Ingenieria, Docente de planta de la Universidad Distrital "Francisco José de Calda"
egomez@udistrital.edu.co

Tipo: Artículo de revisión

Fecha de Recepción: Sept. 27 de 2010
Fecha de Aceptación: Nov. 5 de 2010

1. INTRODUCCIÓN

Es evidente que en la actualidad las organizaciones a nivel mundial requieren satisfacer mayores necesidades de servicios de TI, y si a esto se suma la expansión e innovación proporcionada por el auge de Internet, se vislumbra que basados en la plataforma mundial que provee la red de redes, la computación Cloud es una de las opciones más favorables para lograr avances en innovación, en productividad al mismo tiempo

que se logra reducir costos [1].

Esta arquitectura de consumo, ofrece la posibilidad de obtener múltiples servicios de terceros, lo que permite que la organización no tenga que realizar grandes inversiones en la infraestructura tecnológica (Almacenamiento, procesamiento, desarrollo de software entre otros muchos servicios disponibles), logrando concentrar los recursos en el núcleo del negocio [2].

La descentralización que conlleva este modelo, es una tendencia cada vez mayor de almacenar datos en lugares de otros, que señala el final del hardware e incluso de los sistemas operativos; en breve solo se necesitará un navegador [3].

En la actualidad, esta estructura como tecnología innovadora tiene grandes beneficios:

- **Eficiencia.** Mejor utilización de activos informáticos, facilidad de consolidación contra sistemas desacoplados o independientes, ascenso de la productividad en desarrollo de software y en la gestión de aplicaciones y redes.
- **Agilidad:** Posibilidad de contratar servicios con los proveedores de confianza, aumento o reducción de la capacidad casi instantánea, sensibilidad a las necesidades urgentes de la compañía.
- **Innovación:** Cambio de enfoque en la propiedad y gestión de activos informáticos de la compañía, oportunidades de negocios del sector privado, fomento de la cultura empresarial, vinculación de nuevas y mejores tecnologías [4].

Sin embargo, el origen y destino de las transacciones dejan de tener un valor absoluto y pasan a tener valores relativos: la información no siempre se halla donde realmente parece y no siempre es tratada donde parece que se está procesando [5], estas situaciones de no tener control físico de los datos que se almacenan, procesan o trasmiten en la nube implica que los riesgos y vulnerabilidades aumenten.

De otro lado las aplicaciones no tienen soporte físico y se acceden a través de la red para su uso on-line, es decir, se ejecutan en servidores del SP en forma de hosting [6]. Si estas falencias no son cuidadosamente estimadas y controladas, la seguridad de los datos puede ser vulnerada, perdiendo la confidencialidad, la autenticidad o la integridad, como agravante de este evento, se suma que la información es el activo más preciado del núcleo del negocio de las organizaciones.

En el desarrollo de esta exploración documental se recopilan tendencias innovadoras, manejo del riesgo y de la seguridad de la información, dentro del consumo de servicios de TI accedidos dentro de computación Cloud.

2. CLOUD COMPUTING

La Cloud (Fig. 1), ha cambiado paradigmas y el modo de concebir los servicios informáticos a nivel mundial, haciendo referencia a una filosofía integradora de aplicaciones, implementada sobre redes optimizando la usabilidad y la velocidad [7], permitiendo a las empresas el uso de estos de una manera práctica, de fácil implementación y sin realizar grandes inversiones en hardware y recursos humanos.

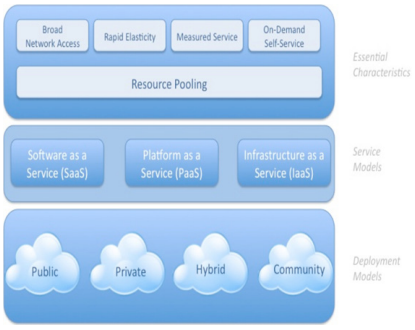

Fig. 1. Representación visual cloud computing [8].

La optimización de los recursos lograda bajo la figura de la nube, es plasmada por

MIT Sloan (Fig. 2), en donde Cloud y los servicios compartidos se encuentran en la cumbre.

2.1 Que es la computación en la Web

Es un modelo para habilitar un cómodo acceso en red por demanda a un pool compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se puede conformar y proveer rápidamente con un minúsculo esfuerzo administrativo o una interacción mínima con el proveedor de servicios [10].

Conceptualizando esta definición se podría definir como un modelo de computación, que permite el acceso y consumo por demanda de diferentes recursos de TI a través de Internet.

2.2 Características principales

- On-demand self-service (Autoservicio). Los consumidores pueden abastecerse de manera unilateral según sus necesidades, sin requerir la interacción humana con el o los abastecedores de servicios.
- Broad network access (Amplio acceso a la red). Los recursos de TI están disponibles y son accesibles a través de mecanismos estandarizados por lo que los clientes pueden consumirlos desde plataformas heterogéneas.
- Resource pooling (Reservas). El proveedor pone sus recursos en repositorios comunes para que puedan ser utilizados por múltiples consumidores, cuando existe disponibilidad de estos son asignados dinámicamente en función de la demanda de los usuarios.
- Rapid elasticity (Rapidez y elasticidad). Los servicios pueden ser suministrados rápida y flexiblemente, inclusive en algunos escenarios de manera automática, lo que permite a la organización consumidora redimensionar su infraestructura en cualquier momento.
- Measured Service (Servicio supervisado). Los sistemas Cloud controlan y optimizan el uso de los recursos de manera automática, utilizando una capacidad de evaluación adecuada para cada tipo de prestación [8].

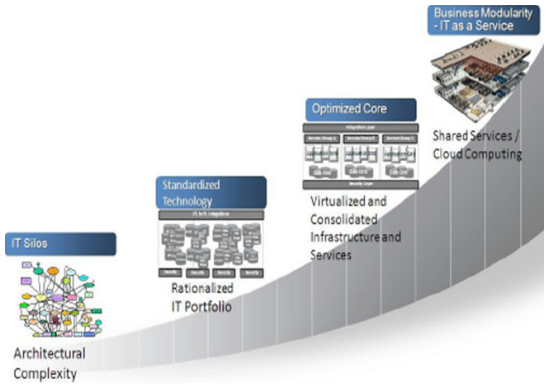

Fig. 2. Modelo de madurez en la arquitectura de optimización de los recursos de TI [9].

2.3 Modelos de implementación

Acorde con la infraestructura y la forma de acceso a la nube, existen cuatro modelos de implementación.

Nube Privada. Los servicios y recursos compartidos solo se encuentran disponibles a los usuarios de la propia empresa, de esta manera pueden lograr unos niveles de seguridad o confidencialidad que no se ofrecen de manera genérica en las nubes de Internet [11].

Nube Pública. La infraestructura esta a disposición de cualquier usuario, pero es propiedad del proveedor, llevando a que los trabajos de todos los clientes se mezclen en los servidores, sistemas de almacenamiento, y otras infraestructuras de Cloud [12].

Nube Comunitaria. En este modelo los componentes disponibles, son compartidos por varias organizaciones con objetivos y/o necesidades similares, los recursos pueden ser gestionados por estas o por un tercero.

Nube Hibrida. Se compone por dos o más nubes (privadas, comunitarias o públicas), las cuales se mantienen como objetos separados, pero a través estándares establecidos pueden compartir diferentes recursos.

Lo anterior implica que el modelo Cloud no tiene porque estar siempre externalizado sino que es perfectamente viable la construcción de estructuras corporativas, de manera que los actuales centros de proceso de datos operen en este modelo [6].

2.4 Modelos de servicios

Conforme con el tipo de prestación que se provee a los usuarios (Software, Plataforma o Infraestructura) existen tres modelos de servicios (Fig. 3).

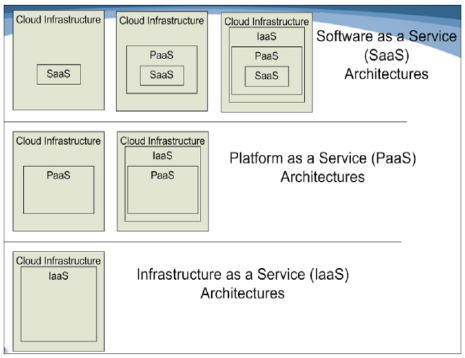

Fig. 3. Arquitectura de modelos de servicio [13].

Cloud Infrastructure as a Service (IaaS). El servicio del que se abastece el usuario, corresponde a los recursos computacionales necesarios para que dentro de la infraestructura provista en la nube, el cliente pueda implementar o ejecutar el software que desee, en apoyo de sus funciones o necesidades especificas.

Cloud Platform as a Service (PaaS). Se refiere a la capacidad para que el cliente cree en la infraestructura brindada por el proveedor aplicaciones desarrolladas (in house) o adquiridas a la medida, que hayan sido implementadas utilizando lenguajes y/o herramientas de programación respaldadas por el SP.

Cloud Software as a Service (SaaS). En este modelo el contratante se sirve de aplicaciones de propiedad del contratista, que se ejecutan en la infraestructura (Cloud) provista por el vendedor de servicios de software (Fig. 4).

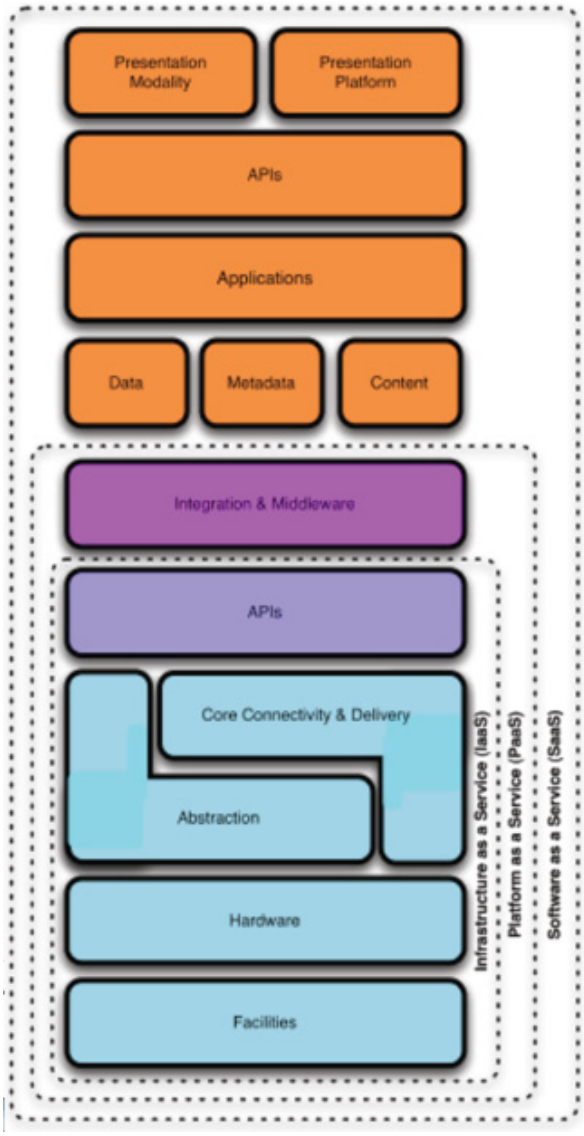

Fig. 4. Modelo de referencia en cloud computing [8].

IaaS. incluye todos los recursos de infraestructura como son: las instalaciones físicas, equipos de cómputo y de comunicaciones, adicionalmente proporciona un conjunto de APIs que permiten al usuario la gestión

e interacción con la infraestructura.
PaaS. Se ubica por encima de los servicios IaaS, este agrega un nivel adicional de integración y capacidad de middleware, que permite a los desarrolladores de software, agregar aplicaciones sobre la plataforma.

SaaS. Se crea a partir de las dos capas inferiores y proporciona un entorno operativo completo

Incluyendo aplicación, presentación, y capacidades de gestión [8].

Gráficamente en las Fig. 3 y 4, se puede observar como los servicios IaaS son la base estructural, de todos los otros servicios Cloud, y de manera ascendente los de tipo SaaS se basan en servicios IaaS, y PaaS, lo que genera una relación directa entre las funcionalidades, privilegios, riesgos y posibles problemas de seguridad entre los tres modelos.

3. SEGURIDAD DE LA INFORMACIÓN

Se define como la protección de la información de un amplio rango de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales [14], esto dentro del concepto clásico de la confidencialidad, integridad y disponibilidad.

La arquitectura Cloud maneja un nivel de abstracción entre la infraestructura física y la información de la organización, difiriendo de la computación tradicional en donde el propietario de los datos tiene el control directo de la componente informática que los puede afectar, este cambio indica que al estar dividida la responsabilidad entre la compañía consumidora, y los vendedores de servicios [15], es indispensable implementar medidas efectivas que lleven a su aseguramiento.

ENISA (Agencia Europea de Seguridad de redes e información) propone la siguiente división de responsabilidades Cliente/Proveedor de acuerdo con el modelo de servicios mostrados en la tabla 1.

En Cloud es pertinente seguir la ruta sugerida por el estándar internacional ISO/IEC 27001-2005, el cual dentro de su ámbito de aplicación define los requisitos para establecer, implementar, operar, monitorear, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) [17], adoptando el modelo del proceso Planear-Hacer-Chequear-Actuar, el cual inicia tomando los requerimientos de seguridad de la organización, a través de las acciones y procesos (PDCA) en un ciclo de mejoramiento permanente, genera resultados de seguridad de la información manejada (Fig. 5).

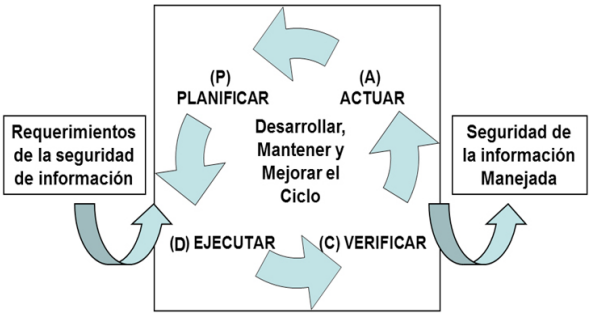

Fig. 5. Modelo PDCA sistema de gestión de seguridad de la información [18].

- **Planear:** Corresponde al estudio de la situación de seguridad de la Organización con el fin de estimar las medidas a implantar [19], en función los requerimientos establecidos, intereses y necesidades organizacionales basadas en la visión de negocio [20].
- **Ejecutar:** Concierne a implementar y operar la política, controles, procesos y procedimientos establecidos en la fase de planeación.
- **Verificar:** Evaluar el cumplimiento de la política y efectividad de los controles establecidos.
- **Actuar:** Atañe a la toma de acciones correctivas y preventivas una vez verificado el sistema [19].

Tabla 1. División de responsabilidades Cliente / Proveedor [16].

Software as a Service - SaaS	
Consumidor	**Proveedor**
• El cumplimiento de la ley de protección de datos en relación con sus datos. • Gestión y mantenimiento del sistema de administración de identidades. • Gestión de la plataforma de autenticación (incluyendo la aplicación de la directiva de contraseñas).	• Soporte de la Infraestructura físico (instalaciones, espacio de rack, energía, refrigeración, cableado, etc). • Seguridad y disponibilidad de la infraestructura física (servidores, almacenamiento, ancho de banda, etc). • Gestión de parches sistema operativo y los procedimientos de hardening. • Configuración de la plataforma seguridad (Firewalls, IDS / IPS etc). • Sistemas de monitoreo. • Mantenimiento de la plataforma (servidores, antivirus, IDS / IPS, filtrado de paquetes). • Monitoreo de Registros (Logs).
Plataform as a Service - PaaS	
• Gestión y mantenimiento del sistema de administración de identidades. • Gestión de la plataforma de autenticación (incluyendo la aplicación de la directiva de contraseñas).	• Soporte de la Infraestructura físico (instalaciones, espacio de rack, energía, refrigeración, cableado, etc). • Seguridad y disponibilidad de la infraestructura física (servidores, almacenamiento, ancho de banda, etc). • Gestión de parches sistema operativo y los procedimientos de hardening. • Configuración de la plataforma seguridad (Firewalls, IDS / IPS etc). • Sistemas de monitoreo. • Mantenimiento de la plataforma (servidores, antivirus, IDS / IPS, filtrado de paquetes). • Monitoreo de Registros (Logs).
Infraestructure as a Service - IaaS	
• Gestión y mantenimiento del sistema de administración de identidades. • Gestión de la plataforma de autenticación (incluyendo la aplicación de la directiva de contraseñas). • Gestión de parches sistema operativo y los procedimientos de hardening sobre la infraestructura alquilada. • Configuración de la plataforma seguridad alquilada (Firewalls, IDS / IPS etc). • Monitoreo de los sistemas alquilados. • Mantenimiento de la plataforma (servidores, antivirus, IDS / IPS, filtrado de paquetes). • Monitoreo de Registros (Logs).	• Soporte de la Infraestructura físico (instalaciones, espacio de rack, energía, refrigeración, cableado, etc). • Seguridad y disponibilidad de la infraestructura física (servidores, almacenamiento, ancho de banda, etc). • Sistemas de Host (Hyper Visor, firewall virtual etc).

3.1 Evaluación y manejo del riesgo

Cloud presenta los mismos riesgos de los sistemas convencionales más otros nuevos específicos [21], por lo que los avances que las organizaciones tienen para su manejo son útiles, pero adicionalmente es necesario realizar los ajustes precisos para controlarlos dentro de este nuevo tipo de computación.

Cualquier organización que pretenda implementar un sistema de seguridad de la información debe realizar una evaluación, proceso donde se deben identificar, cuantificar y priorizar los riesgos en concordancia con sus objetivos y necesidades.

Los cuatro principales puntos a estimar y controlar de acuerdo con SUN Microsystem son: Riesgo del Negocio, Riesgos Técnicos o de la Arquitectura, Cumplimiento y Cuestiones Reglamentarias, Falta de visibilidad (Referente a procesos y procedimientos del proveedor de servicios) [22].

Los resultados de la evaluación son el punto de partida para decidir las acciones a seguir y también para implementar los controles específicos que lleven a la protección de la compañía.

Para los riesgos definidos en la etapa de evaluación, es necesario decidir el manejo que se dará a estos, las posibles opciones para el tratamiento deben incluir:

- Aplicar los controles apropiados con el fin de reducirlos superlativamente.
- Aceptación objetiva, siempre y cuando cumplan con la política y el criterio de tolerancia de la organización.
- Disminuir al máximo las acciones que podrían causar su ocurrencia.
- Transferir los riesgos asociados a otros grupos como aseguradores o proveedores.

4. RECOMENDACIONES PARA LA SEGURIDAD EN CLOUD COMPUTING

En concordancia con lo definido anteriormente, respecto de la existencia de tres modelos de servicio y los cuatro modelos de implementación, es claro que las problemáticas difieren de acuerdo con la figura que adopte cada empresa.

Según ISACA (Asociación de Auditores de Sistemas de Información y Control) en materia de seguridad y riesgo, los puntos más relevantes a tener en cuenta de acuerdo con el modelo de despliegue son:

Tabla 2. Consideraciones de riesgo y seguridad por modelo de implementación [23].

Modelo	Consideraciones
Nube Privada	• Servicios en la nube con riesgo mínimo. • Es posible que no proporcione la escalabilidad y agilidad de los servicios de la nube pública.
Nube Comunitaria	• Igual que la nube privada, pero adicionalmente: • Los datos pueden estar almacenados con los de los competidores.
Nube Publica	• Igual que la nube comunitaria, pero adicionalmente: • Los datos pueden estar almacenados en ubicaciones desconocidas y pudieran no ser fáciles de recuperar.
Nube Híbrida	• El riesgo agregado de combinar dos modelos de implementación diferentes. • La clasificación y el etiquetado de datos ayudará al gerente de seguridad a garantizar que los datos se asignen al tipo de nube correcto.

En lo referente a los tipos de servicios de Infraestructura IaaS, Plataforma PaaS y Software SaaS, las consideraciones se detallan en la tabla 3.

Tabla 3. Consideraciones de riesgo y seguridad por modelo de servicio [23].

Modelo	Consideraciones
Infraestructura como un servicio (IaaS)	Opciones de minimizar el impacto si el proveedor de la nube experimenta una interrupción del servicio
Plataforma como un servicio (PaaS)	• Disponibilidad • Confidencialidad • La privacidad y la responsabilidad legal en caso de una violación de la seguridad • Propiedad de los datos • Preocupaciones acerca del e-discovery
Software como un servicio (SaaS)	• ¿Quién es el dueño de las aplicaciones? • ¿Dónde residen las aplicaciones?

4.1 Control de acceso e identidad

La seguridad de la identidad preserva la integridad y la confidencialidad de los datos y las aplicaciones, a la vez que ofrece acceso de disponibilidad inmediata a los usuarios adecuados [24].

En Cloud las funciones esenciales para la efectiva gestión de acceso e identidades no varían drásticamente respecto de la computación tradicional.

- **Mantenimiento de identidades:** De acuerdo con la responsabilidad concertada entre consumidor/proveedor, debe realizarse una gestión segura y puntual de las altas y las bajas de los usuarios que acceden a los servicios.
- **Autenticación:** Debe garantizarse que al utilizar los servicios, se verifique la legitimidad de los usuarios de manera fiable, aplicando gestión de credenciales, técnicas de comprobación de usuarios fuerte y/o delegada.
  Integrar la autenticación Cloud, con los sistemas de autorización de ingreso propios de la compañía como Single Sing-on, acceso biométrico, sistemas basados en LDAP, Certificados Digitales y Kerberos.
- **Federación:** Verificar que los proveedores de servicios y de identidades (IdP), cumplen con alguno de los principales estándares vigentes como SAML y/o WS-Federation.
  De manera coherente con las necesidades, se puede disponer de firmas digitales para transacciones críticas.
- **Gestión de perfiles de usuario:** Se deben definir perfiles de usuario acordes con las políticas, funciones y jerarquía organizacional, utilizándolos para controlar el acceso y facilitando la realización de las auditorías pertinentes.

4.2 Cifrado y manejo de claves

Es indispensable que clientes y proveedores tomen medidas para evitar la intercep-

tación y/o acceso no autorizado a los datos. Se puede minimizar en un gran porcentaje la posibilidad de ocurrencia de estos eventos no deseados realizando una correcta gestión de claves.

- **Cifrado:** El SP debe brindar un portal o herramienta encriptada, que permita al usuario la gestión de recursos de la nube de manera segura [25].
  Los datos estáticos que por políticas son relevantes deben permanecer cifrados, de ser el caso el cliente puede encriptarlos antes de ser entregados al proveedor.
  La información que transita en las redes debe viajar cifrada de origen a destino.
  Las copias de seguridad deben almacenarse encriptadas, previniendo que estén disponibles a clientes no autorizados que pretendan restaurarlas.
- **Manejo de Claves:** Los almacenes de claves tienen que estar protegidos, durante su almacenamiento, en tránsito y en backup.
  El acceso a los repositorios de claves solo debe permitirse a las entidades específicas que las requieran.
  Exigir al proveedor la documentación del ciclo de vida de la gestión de claves: generación, uso, almacenamiento, respaldo, recuperación y borrado.

4.3 Datacenter masivos

Al interior de esta arquitectura, la información y las aplicaciones de los clientes, se encuentran compartiendo recursos informáticos en centros de cómputo, por lo que se deben establecer procedimientos que garanticen su protección.

En esta exploración se resaltan los siguientes puntos a tener en cuenta a la hora de interactuar con el abastecedor.

Exigir las certificaciones y/o acreditaciones técnicas respectivas que rigen respecto a centros de cómputo.

- Requerir que la operación del centro de datos sea llevada por personal idóneo para tal fin.
- Solicitar planes de auditoria interna.
- Instar la aplicación de políticas efectivas de control de cambios para los componentes de la infraestructura (hardware, software, equipos activos de comunicaciones).
- Firmar acuerdos de entendimiento de los contratos, que permitan tener claridad entre las partes que intervienen en la prestación y utilización del servicio.
- Solicitar entrega periódica de informes de incidentes y rendimiento de la infraestructura.

4.4 Disposiciones legales y contractuales.

Para las organizaciones que hacen uso de prestaciones en Cloud, el manejo de su información varía drásticamente a la forma tradicional, dado que ahora se involucra un tercero.

El entregar el manejo de este activo a otro, crea nuevos retos legales y contractuales que deben ser tenidos en cuenta, principalmente por la una posible falta de control y la transparencia a causa naturaleza distribuida de los componentes de la nube [26].

La extensión del Cloud Computing tiene un impacto en ámbitos como la protección de datos personales, la propiedad intelectual y la responsabilidad de los proveedores de servicios intermediarios [27].
Algunas estrategias a seguir para minimizar el riesgo legal son:

- Creación de grupos multidisciplinarios, entre los equipos legales, contractuales y de tecnología, para dar fortaleza a la formulación de los pliegos de condiciones, contratos y acuerdos de niveles de servicios (ANS).
- Exigir herramientas que garanticen la autenticidad de la información (del negocio, logs, etc.) para que sea valida en

cualquier escenario de reclamación o litigio.
- Los términos contractuales y post-contractuales deben ser totalmente rigurosos con los ítems de custodia de los datos, devolución de activos de información, cumplimiento de la normatividad o legislación nacional e internacional, derecho a realizar auditorias, testear rendimiento y vulnerabilidades.

4.5 Gestión de la información

Es esencial que la información esté correcta y precisamente clasificada, para poder identificar plenamente los usuarios que deben tener acceso a ella [28]. En este caso se pretende adoptar el ciclo de vida seguro de los datos (Fig. 6), compuesto de seis etapas: crear, almacenar, utilizar, compartir, archivar y destruir.

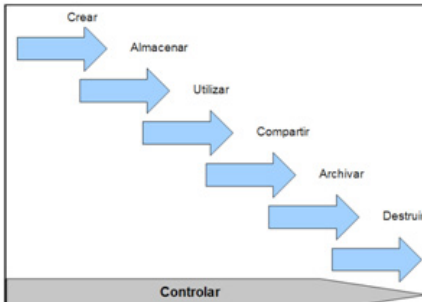

Fig. 6. Ciclo de vida seguro de los datos.

La función de cada uno de sus componentes es la siguiente:

- **Crear:**
- Clasifica y etiqueta los datos de la organización, de acuerdo con la relevancia revestida.
- Asignación de privilegios.

- **Almacenar:**
- Establece e implementa controles de acceso.
- Ejecuta soluciones de cifrado en puntos vulnerables como son transporte en la red, bases de datos, y archivos almacenados.
- Define e implementa procesos de auditoria de acuerdo con las políticas y necesidades de la organización consumidora.

- **Utilizar:**
- Incluye políticas de seguimiento y análisis a los archivos de registro (logs).
- Establece controles dentro de los sistemas manejadores de bases de datos.

- **Compartir:**
- Controla privilegios sobre los datos.
- Verifica los archivos de registro (logs).
- Cifra los datos en el proceso de transporte de información.

- **Archivar:**
- Encripta información en los medios donde se almacenan las copias de seguridad.
- Hace seguimiento a los registros de backup.

- **Destruir:**
- Implementa técnicas de borrado seguro.
- Asegura la destrucción de las claves de cifrado.

4.6 Virtualización. Cloud Computing a nivel de infraestructura

Plataforma o software, requiere virtualizar sus capacidades de prestación para asignar a cada cliente la cantidad de recurso contratado "crear una versión virtual de un sistema operativo, un servidor, un dispositivo de almacenamiento o un recurso de red mediante la utilización software, posibilitando que un recurso físico pueda ejecutar múltiples máquinas virtuales aisladas" [29]. El uso de tecnologías de virtualización genera nuevas vulnerabilidades a intervenir dentro de la arquitectura que soporta la nube, pero también ofrece la posibilidad de introducir e integrar controles de seguridad directamente en la capa virtual [30]. Algunos puntos clave respecto de la virtualización pueden ser:

- Exigir información detallada de los sistemas de virtualización que se usarán para cumplir el objeto del contrato.
- Aplicar controles de seguridad como detección y prevención de intrusiones, antivirus, actualizaciones automáticas de sistema operativo y aplicaciones, escaneo de vulnerabilidades, tanto en la capa virtual como la capa física.
- La administración y acceso a los sistemas operativos virtualizados debe incluir la autenticación fuerte, gestión de identidad y registros de transacciones
- Solicitar al proveedor informes permanentes que evidencien el aislamiento y alerte la ocurrencia de violaciones.

5. CONCLUSIONES

Es indispensable para las empresas que inician o piensan ingresar al uso de esta nueva prestación de servicios en la red, que evalúen objetivamente la relación del beneficio económico contra los riesgos adicionales en los que se incurre al tercerizar en este tipo de computación.

El manejo de la seguridad de la información en Cloud Computing debe ser complementario al tratamiento de estas temáticas dentro de las corporaciones, por lo que los profesionales de TI deben continuar con los planes y programas vigentes, pero adicionalmente vinculando a estos los nuevos riesgos y posibles problemas de seguridad. Es fundamental que la empresa cree o disponga de equipos multidisciplinarios conformados por especialistas legales y de tecnología, a fin de solventar favorablemente los desafíos relacionados con la seguridad y privacidad.

Referencias Bibliográficas

[1] Hardvard business review sponsored by microsoft, achieving competitive advantage in the age of Cloud Computing, Septiembre de 2010, [en línea]. Consultado en Septiembre 8 de 2010, disponible en: http://download.microsoft.com/download/1/4/4/1442E796-0 0 D 2 - 4 7 4 0 - A C 2 D - 782D47EA3808/16700%20HBR%20 Microsoft%20Report%20LONG%20 webview.pdf.

[2] D. David, S. Tamim, Captar el verdadero valor del cloud computing. The Boston consulting group. Ref 3553, [en línea]. Consultado en Agosto 1 de 2010, disponible en: http://www.gestiondeclinica.es/pdf/cloud%20computing.pdf.

[3] ORIOL. Mercedes, Especial Tendencias 2011, Red Seguridad, No. 50, p. 30, Febrero 2011, ISSN 1695-3991.

[4] K. Vivek, Federal cloud computing strategy, Febrero 2010 [en línea]. Consultado en Mayo de 2010, disponible en: www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf.

[5] M. Ramón, Cloud computing y protección de datos.VI Congreso Internet, Derecho y Política, Revista de los Estudios de Derecho y Ciencia Política de la UOC, No. 11, 2010, ISSN 1699-8154.

[6] H. Angel, El SaaS y el cloud-computing: una opción innovadora para tiempos de crisis, Revista Española de Innovación, Calidad e Ingeniería del Software, Vol. 5, No. 1, 2009, ISSN: 1885-4486.

[7] M. Jorge, En busca de una orientación disciplinar para el Cloud Computing, mediaciones sociales. Revista de ciencias sociales y de la comunicación, No 6, 2010, pp. 3961. ISSN 19890494, Universidad Complutense de Madrid.

[8] CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.

[9] ORACLE, Achieving the Cloud Com-

puting Vision, Octubre de 2010, [en línea]. Consultado en Mayo de 2011, disponible en: http://www.oracle.com/technetwork/topics/entarch/architectural-strategies-for-cloud--128191.pdf.

[10] M. Peter, G. Timothy, "The NIST definition of cloud computing", National Institute of Standards and Technology, special publication 800-145, Enero de 2011.

[11] T. Jordi, El cloud computing y las empresas, Business BCN, No. 9, p. 22, Febrero – Abril 2011, ISSN 2013357X.

[12] SUN Microsystems, Cloud Computing at a higher level, [en línea], Consultado en Septiembre 13 de 2010, disponible en: http://www.oracle.com/Sun_Cloud.

[13] NIST, Presentation on effectively and securely using the cloud computing paradigm v26, [en línea]. Consultado en Septiembre 18 de 2010, disponible en: csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt.

[14] Estándar Internacional ISO/IEC 27002 – 2005, Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

[15] A. Michael, F. Armando, G. Rean, J. Anthony, K. Randy, K. Andy, L. Gunho, P. David, R. Ariel, S. Ion, Z. Matei, A view of cloud computing, 2009.

[16] ENISA, Cloud computing information assurance framework, Noviembre de 2009, [en línea]. Consultado en de Octubre 2 de 2010, disponible en: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport.

[17] Estándar Internacional ISO/IEC 27000 – 2009, Tecnología de la Información – Técnicas de seguridad – Información general y vocabulario.

[18] Estándar Internacional ISO/IEC 27001 – 2005, Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.

[19] MICROSOFT, Securing microsoft's cloud infrastructure, Mayo de 2009, [en línea]. Consultado en Mayo 22 de 2010. Disponible en http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloud-May09.pdf.

[20] B. Jorge, C. Pedro G, Modelo para seguridad de la información en TIC, Actas 2do encuentro informática y gestión, Temuco, Chile, Noviembre 2008, [en línea]. Consultado en Mayo 22 de 2010, disponible en http://ceur-ws.org/Vol-488/paper13.pdf.

[21] A. Javier, Protección del cloud computing en seguridad y privacidad, Revista Española de Electrónica, No. 666, p. 42, Mayo 2010, ISSN 0482 -6396.

[22] Sun Microsystems, Optimizing aplications for cloud computing enviromentes, Noviembre de 2009, [en línea]. Consultado en Diciembre 2009, disponible en: http://www.oracle.com/Sun_Cloud.

[23] ISACA, Cloud computing: business benefits with security, Governance and assurance perspectives, Octubre de 2009.

[24] RSA Security Inc, La función de la seguridad en cloud computing de confianza, Mayo de 2009, [en línea]. Consultado en Junio 29 de 2010, disponible en:http://www.rsa.com/solutions/business/wp/11021_CLOUD_WP_0209_SP.pdf.

[25] VMWARE – SAVVIS, Securing the cloud a review of cloud computing, security implications and best practices, 2009, [en línea]. Consultado en Agosto 14 de 2010, disponible en: http://www.savvis.com/en-US/Info_Center/Documents/Savvis_VMW_whitepaper_0809.pdf.

[26] C. Richard, G. Philippe, J. Markus, M. Ryusuke, M. Jesus, S. Elaine, S. Jessica, Controlling data in the cloud: outsourcing computation without outsourcing control, PARC - Fujitsu Laboratories of America, [en línea].

Consultado en Septiembre 19 de 2010 disponible en: http://www.parc.com/content/attachments/ControllingDataInTheCloud-CCSW-09.pdf.

[27] C. Agustin, Cloud computing: el derecho y la política suben a la nube, Revista de los Estudios de Derecho y Ciencia Política de la UOC, No. 11, 2010, ISSN 1699-8154.

[28] JERICHO Forum, Information Lifecycle Management, Ver. 1.0, Enero 2009.

[29] M. Pablo, (2009) Ejecución de una base de datos distribuida sobre un entorno de Cloud Computing, Tesis Final Máster en Investigación en Informática, Universidad Computlense, Madrid 2009, [en línea]. Consultado en Julio 12 de 2010, disponible en: http://eprints.ucm.es/9889/1/Memoria.pdf.

[30] L. Roberto, Virtualización y cloud grandes desafíos, Red Seguridad, No 50. p 50 Febrero 2010, ISSN 1695-3991.