Análisis de riesgos antes de adoptar la computación en nube como una estrategia corporativa.

Erick Meneses Cuadros

Universidad Pontificia Bolivariana
Bucaramanga, Colombia
erickmeneses@gmail.com

Resumen

Actualmente, la computación en la nube es la tendencia corporativa con mayor desarrollo, un fenómeno no solo desde el punto de vista tecnológico, sino práctico y financiero que atrae a las empresas al ofrecer recursos teóricamente ilimitados bajo un modelo de pago por consumo. Sin embargo, migrar a la computación en nube implica mover la información asegurada dentro un perímetro local (modelo tradicional) a un ambiente distribuido remoto (modelo nube) que, si bien puede resultar atractivo al generar nuevos beneficios, también puede ser perjudicial generando nuevas vulnerabilidades.

Ante ese dilema de adoptar o no la computación en la nube como una estrategia corporativa, la mayoría de los gerentes prefieren ser conservadores y evitar riesgos, por lo general, debido a que no cuentan con el conocimiento y/o herramientas necesarias para tomar dicha decisión.

En este sentido, el artículo pretende a partir de la metodología NIST 800-30 para la gestión de riesgos y basado en la experiencia vivida por la Cámara de Compensación de Divisas de Colombia migrando uno de sus sistemas de contingencia a la nube, mostrar una forma sencilla para identificar, evaluar y mitigar los riesgos de manera previa a la migración/implementación de un sistema en la nube.

Palabras claves

Computación en nube, análisis de riesgos.

Abstract

Cloud computing is currently the most developed corporate trend, a phenomenon not only from the technological point of view but also practical and financial, a phenomenon that attract enterprises offering theoretically unlimited resources under a pay per use model. However, migrating to cloud computing involves moving information secured within a local perimeter (traditional model) to a remote distributed environment (cloud model) that, can be attractive generating new benefits, but also damaging generating new vulnerabilities
Faced with this dilemma to adopt or not adopt cloud computing as a corporate strategy, most managers prefer to be conservative and avoid risks, usually because they do not have the knowledge and/or tools necessary to take such decision. In this sense, the article seeks the methodology NIST 800-30 for risk management and based in the experience lived by the Currency Clearing House of Colombia migrating one of these contingency systems to the cloud, show a simple way to identify, assess and mitigate risks before one migration/implementation of a system in the cloud.

Keywords:
cloud computing, risks analysis.

1. Introducción

Recientemente se advierten numerosas publicaciones que muestran el impacto positivo de la computación en nube en las organizaciones, ejemplo de esto es la iniciativa presentada por el CIO Council[1] donde el gobierno los estados unidos donde expresa formalmente su apoyo y alienta a la migración de los sistemas convencionales a la nube, mostrando los beneficios a través de 30 casos en entidades a nivel federal, estatal y local [5]. Otro ejemplo es el estudio realizado por Ponemon Institute[2] donde se muestran indicadores de la percepción y los hábitos de 925 compañías usuarias del cloud en Estados Unidos y Europa [4]. Tales indicadores dejan ver de manera general el éxito alcanzado, sin embargo, un indicador revela que del total de aplicaciones en la nube solo un 15% de ellas son críticas, es decir, hay un reconocimiento de las innegables ventajas pero aún no se tiene plena confianza debido a que si bien aparecen documentos que tratan el tema, no se muestra de forma sencilla como realizar un análisis de las consideraciones de seguridad y control de la información requeridas para entrar en este esquema de computación tercerizada y basada en servicios.

2. Computación en la Nube

La computación en nube es un modelo que habilita bajo demanda el acceso a la red para compartir un conjunto de recursos computacionales configurables (ej. redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente suministrados y desplegados con un mínimo de esfuerzo por parte del cliente y del proveedor del servicio, un modelo que promueve la disponibilidad y está definido por un conjunto de características,

[1] Chief Information Officers Council – www.cio.gov
[2] Center dedicated to Information Security - www.ponemon.org

modelos de despliegue y modelos de servicio [8], factores importantes a conocer, que serán explicados a continuación:

Características

Los servicios en la nube se basan en cinco características esenciales que muestran sus similitudes y diferencias con estrategias de computación tradicionales [1]:

- Consumo de servicio por demanda: un cliente puede decidir unilateralmente cuando consumir o no los recursos computacionales de acuerdo a sus necesidades, pagando solo el tiempo que utiliza.
- Amplio acceso a la red: es posible acceder a través de múltiples mecanismos de comunicación estándar sobre plataformas heterogéneas (Ej. PCs, móviles, PDAs, etc.).
- Uso de recursos compartidos: gracias a la virtualización es posible compartir recursos dando al cliente un sentido de independencia al hacer transparenté el sistema y abstraer la complejidad subyacente.
- Rapidez y elasticidad: el cliente cuenta con la posibilidad de realizar despliegues de manera rápida y expandir sus recursos (teóricamente) ilimitados en cualquier momento.
- Servicio supervisado: los sistemas en la nube monitorean y optimizan el uso de recursos de manera automática según el servicio (Ej. ancho de banda, cuentas de usuario, almacenamiento).

Modelos de Servicio

La prestación de servicios en la nube se da a través de tres modelos generales (y sus combinaciones derivadas), estos son:

- Infraestructura Como Servicio – (IAAS) permite al consumidor rentar capacidad y administración sobre procesamiento, almacenamiento y comunicación, representado en máquinas virtuales, dispositivos de almacenamiento y redes. Ej: Amazon [11], Terremark, Dropbox y Rackspace.
- Plataforma Como Servicio – (PAAS) permite al consumidor desplegar aplicaciones propias creadas con lenguajes de programación, servidores de aplicaciones y bases de datos soportadas por el proveedor. Ej: Windows Azure, Google App Engine y Aptana Cloud.
- Software Como Servicio – (SAAS) haciendo uso de una interfaz ligera el cliente utiliza aplicaciones web que se ejecutan en la nube y son suministradas por el proveedor. Ej: Salesforce, Google Docs, Zoho y SlideRocket.

Modelos de Despliegue

Los modelos de despliegue pueden ser divididos en cuatro tipos dependiendo del nivel de apropiación y la arquitectura [6]:

- Nube Pública: es propiedad de una organización que provee diferentes servicios a múltiples clientes.

- Nube Privada: es propiedad de una organización que la administra y la utiliza permitiendo el acceso solo a los miembros de la misma.
- Nube Hibrida: está compuesta por dos o más nubes (una privada y una/varias públicas) que buscan complementarse y compartir recursos definidos a través de tecnologías estándar.
- Nube Comunitaria: se trata de una sola nube compartida por diferentes organizaciones con objetivos y preocupaciones similares.

3. Análisis de Riesgos.

Los sistemas tradicionales se encuentran protegidos detrás de firewalls, NATs, VPNs, y un conjunto de restricciones, de modo que los atacantes deber realizar una exhaustiva labor de inteligencia para saber que ellos existen dice Greg Day – Analista de seguridad de McAfee. Los servicios en la nube en cambio son altamente visibles y están diseñados para ser accedidos desde cualquier parte por cualquier persona, un gran blanco en cuestión [10].

Figura 1. Metodología de Gestión de Riesgos - NIST 800-30

Por tanto, es recomendable evaluar las consecuencias a nivel de seguridad antes de empezar cualquier proceso de migración/implantación de un sistema en la nube. Para alcanzar tal

objetivo es usada la metodología de análisis de riesgos [6] propuesta por NIST[3] (ver figura 1), la cual parte caracterizando el sistema, para luego identificar las amenazas y vulnerabilidades presentes, y en base a ellas determinar los posibles riesgos y la probabilidad e impacto que causaría la materialización de uno de ellos. Finalmente, se proponen controles para mitigar los riesgos aceptados y se presenta un informe claro al respecto.

3.1. Caracterización del Sistema

El sistema en estudio tiene como objetivo apoyar la operación de cambio de divisas entre las entidades financieras en Colombia. Por lo tanto, su disponibilidad es un factor vital a proteger, así como la integridad y confidencialidad de la información que maneja. Por esta razón se propone una arquitectura de alta disponibilidad en cluster.

A nivel de hardware se compone de dos servidores y una unidad de almacenamiento redundante, todo conectado por una red de alta velocidad. El nivel de software se compone de las siguientes capas: sistema operativo (Red Hat), base de datos (MySQL, PostgreSQL), ambiente de aplicación (conjunto de servicios a través de JBoss) y middleware (Red Hat Cluster Suite). Tal arquitectura es representada en la figura 2.

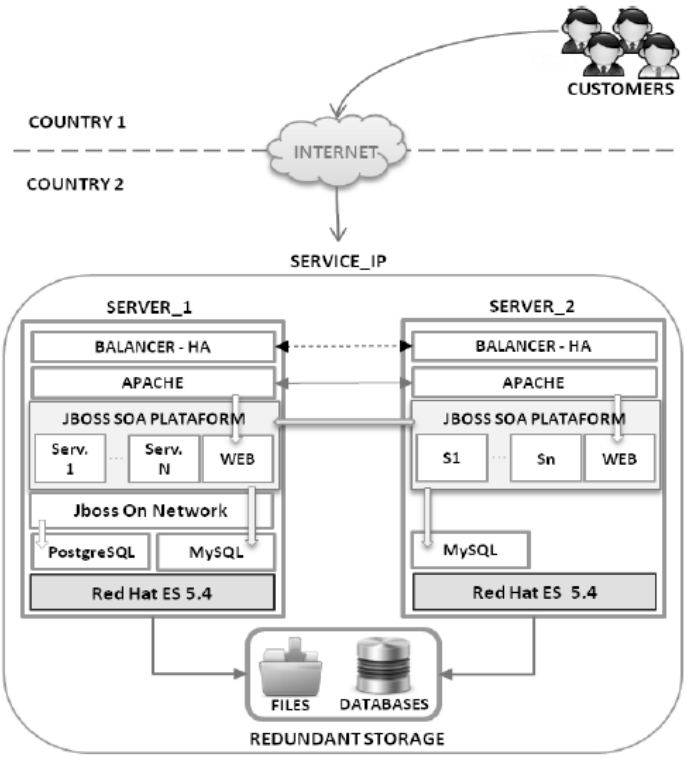

Figura 2. Arquitectura de Alta disponibilidad en Cluster

[3] National Institute of Standards and Technology – www.nist.gov

El modelo de servicio que mejor se adapta a las necesidades es infraestructura como un servicio - (IAAS), ya que el proveedor de cloud se encarga de suministrar y administrar la infraestructura, dejando la gestión de software del lado del cliente. De acuerdo con esto, el modelo de despliegue elegido es la nube pública [6], provista por Amazon Web Services.

3.2. Identificación de Amenazas

Las amenazas que atentan contra la seguridad de un sistema se pueden generalizar analizando cómo se afectan las principales características de la seguridad de la información (confidencialidad, integridad y disponibi-lidad) [3] y aquellas que las complementan (autenticación, autorización y audibilidad). Estas se muestran a continuación en la Tabla 1.

COD.	FUENTE	AMENAZA
A1	Atacante (Interno o Externo)	Espionaje de información sobre datos trasmitidos o almacenados.
A2		Modificación no autorizada de información
A3		Generación de mal funcionamiento o denegación del servicio
A4		Suplantación de identidad o burla de sobre los sistemas de identificación.
A5		Acceso no autorizado sistema e información.
A6		Destrucción de logs, registros y bitácoras
A7		Aprovechar errores en contraltos o acuerdos de nivel de servicio.

Tabla 1. Identificación de Amenazas

3.3. Identificación de Vulnerabilidades

En la identificación de las vulnerabilidades se pueden encontrar tanto aquellas generales a todos los sistemas (vulnerabilidades tradicionales), como aquellas inherentes a los sistemas en la nube [2]. En este trabajo solo se abordan estas últimas por considerarse relevantes (ver tabla 2).

COD.	VULNERABILIDAD
V1	Sistema débil de autenticación y autorización
V2	Acceso remoto a la interfaz de administración
V3	Vulnerabilidades en el hipervisor.
V4	Falta de aislamiento en los recursos del cliente
V5	Limitación a tecnologías dadas por el proveedor
V6	Error en algoritmos de asignación de recursos
V7	Fallas de red: interna (proveedor) o externa (internet)
V8	Falta de certificación en procedimientos o normas internacionales (gobierno, calidad y seguridad).
V9	Ausencia o deficiencia en procesos recuperación.
V10	Ausencia de procedimientos forenses en la nube.
V11	Debilidades en sincronización de responsabilidades y acuerdos de nivel de servicio.
V12	Débil cifrado en el almacenamiento y trasmisión de datos
V13	Ausencia o debilidad en procedimientos para la generación y administración de claves

Tabla 2. Identificación de Vulnerabilidades

Una vez identificadas las amenazas y vulnerabilidades presentes en el sistema, se confrontan y mediante análisis se identifican un conjunto de riesgos [2] [3]. A continuación cada uno de ellos será definido e ilustrado a través de un caso real donde el riesgo fue materializado.

AMENAZA	VULNERAB.	RIESGO
A3	V5	R1: Alta Dependencia del Proveedor
A7	V11	R2: Perdida de Control y Gobernabilidad
A3	V8	R3: Problemas Cumplimiento
A1 A2 A3	V1 V3 V4 V6	R4: Falta de Aislamiento
A1 A4 A5	V1 V2 V13	R5: Sistemas Débiles de Autenticación y Autorización
A1 A2 A3	V4 V12	R6: Errores en Aseguramiento de datos
A3	V5 V7 V8 V9	R7: Denegación del Servicio
A1 A2 A3	V3	R8: Vulnerabilidades en el Hipervisor
A7	V11	R9: Problemas Jurisdicción y Políticas
A6 A7	V10	R10: Dificultades para efectuar Análisis Forense
Todas	Todas	R11: Vulnerabilidades en el Proveedor

Tabla 3. Relación entre Amenazas, Vulnerabilidades y Riesgos

R1: Alta Dependencia del Proveedor

Actualmente cada proveedor en la nube genera y ofrece herramientas, procedimientos, formatos de datos e interfaces propias, pero no existen estándares claros para operar en la nube, y en el caso en que un cliente desee realizar una migración a su infraestructura local u otro proveedor de la nube se enfrenta a una tarea difícil pues de cierta forma está atado al proveedor inicial, y pareciera que el modelo fue diseñado con esta intensión. Tal nivel de dependencia implicaría que si el proveedor va a la quiebra el cliente puede, en el mejor de los casos realizar una migración lenta y costosa, y en el peor quebrar también. Coghead [19] es ejemplo de una plataforma en la nube cuyo cierre dejo a sus clientes luchando por migrar sus datos y aplicaciones.

R2: Perdida de Control y Gobernabilidad

Al migrar a la nube se dividen responsabilidades entre cliente y proveedor, sin embargo, el no tener claro cuales corresponden a cada quien da pie a omisión y no tener responsable en caso de un evento negativo. Más aun, es frecuente que el ceder obligaciones tranquilice al cliente pero esto no lo exime de realizar un monitoreo de las actividades efectuadas por el proveedor, quien podría generar un agujero de seguridad si toma alguna de las siguientes acciones: no realizar los procedimientos, realizarlos inadecuadamente, o delegarlos a empresas desconocidas, lo cual no ofrece garantías desde el punto de vista legal. Ejemplo de este último es lo sucedido a Carbonite [20] quien entabla una demanda contra sus proveedores de hardware por venta de equipos defectuosos que ocasionaron perdida de información a sus clientes.

R3: Problemas de Cumplimiento

Algunas empresas realizan esfuerzos para cumplir normas o estándares para gestión de la calidad, seguridad u otros, tales certificaciones son necesarias o simplemente dan una ventaja competitiva en el mercado. La transición a la nube puede poner el riesgo las certificaciones adquiridas si el proveedor de servicios no cumple con los estándares o no permite una auditoría externa. Un ejemplo claro se da en el sector financiero ya que estas empresas no pueden usar el servicio EC2 de Amazon al no dar cumplimiento con el estándar de seguridad PCI [21], requisito indispensable para entidades que soportan transacciones con tarjetas de crédito.

R4: Falta de Aislamiento

El hecho de compartir recursos distribuidos a través de tecnologías de virtualización es una de las características más importantes a la hora de definir la computación en nube, y es la que posibilita en gran parte la reducción de costos y flexibilidad de la infraestructura, no obstante, el hecho de compartir recursos tales como almacenamiento, procesamiento o comunicación, genera un riesgo en caso de que los mecanismos de aislamiento no funcionen correctamente y un usuario se aproveche esto para violar la confidencialidad, integridad o disponibilidad de los sistemas de sus vecinos, tal como paso a Zoho cuando implanto su nuevo sistema de indexación, con un error que permitía a un usuario leer los documentos de otros [10].

R5: Sistemas Débiles de Autenticación y Autorización

Cuando las organizaciones migran a la nube tienen la necesidad de conservar sus mecanismos, políticas y procedimientos de autenticación y autorización, sin embargo es visto que tal extensión no es posible pues se restringe a lo que ofrece el proveedor. Un ataque a este nivel podría ser llevado a cabo a través de los clientes livianos que permiten el acceso remoto a consolas de administración. Si un atacante lograra por medio de fuerza bruta u otro tipo de ataque burlar la seguridad y autenticarse, los daños serian desbastadores, como ocurrió a Google al mostrar fallas en los sistemas de autenticación que usaban SAML [22].

R6: Errores en el Aseguramiento de los Datos

Actualmente las infraestructuras almacenan grandes cantidades de datos tal como lo hace Google con aplicaciones como Google Docs o Gmail. El tratamiento de estos es uno de los ítems más complicados pues se debe garantizar por un lado la disponibilidad e integridad de la información y por otro el correcto uso de la misma, evitando así ataques de acceso o robo información como le ocurrió a Facebook [23], o la utilización indebida como es el caso de empresas que realizan minería de datos para explorar perfiles y vender esta información.

R7: Denegación del Servicio

Este es un riesgo al que contribuye la infraestructura misma pues al tratarse de una plataforma distribuida aumentan los puntos de fallo y es más difícil realizar un correcto aseguramiento. Aumenta el problema la ausencia de procedimientos de recuperación de desastres que definan correctamente los tiempos y puntos de recuperación. La materialización de este riesgo podría

causar pérdidas millonarias tal como lo sucedido en 2008 a Google [24], Amazon [25] y FlexiScale [26] al interrumpir sus operaciones durante 24, 7 y 18 horas respectivamente.

R8: Vulnerabilidades en el Hipervisor

La arquitectura de la nube se basa en el concepto de virtualización que permite alojar múltiples maquinas sobre el mismo hardware, realizando un mayor aprovechamiento de los recursos. Existen múltiples técnicas para esto, sin embargo las más aceptadas (paravirtualización y virtualización nativa) gestionan y distribuyen los recursos de hardware entre las máquinas virtuales a través de una capa intermedia denominada hipervisor [15]. Las vulnerabilidades en este punto representan un riesgo enorme pues se concede acceso a todo el recurso hardware bajo él y todo el contenido de las maquinas virtuales sobre él. Se han registrado vulnerabilidades en las aplicaciones de virtualización más importantes: VMWare [27], Xen [28] y Microsoft Virtual PC [29] entre otros. Y la prueba de concepto se pudo apreciar en la conferencia Black Hat de 2008 donde una hacker hizo uso de un código para tomar control del hipervisor Xen y desde el tener acceso a datos, aplicaciones y todo lo que estuviera a su alcance [14].

R9: Problemas de Jurisdicción y Políticas

La relación que crea un servicio entre el cliente y el proveedor en la nube es buena hasta que se presenta una falla (interna o externa), pues en la mayoría de los casos acarrea perdidas dependiendo de la criticidad del sistema. En tales casos la primera acción es recurrir a las políticas de operación y acuerdos de nivel de servicio del proveedor para entablar una solicitud de reclamación fundamentada, sin embargo, es posible que tales políticas y acuerdos de servicio no hayan sido adecuadamente inspeccionadas antes de firmar el contrato, lo que se convierte en un problema fuerte pues no hay punto de reclamación, y en tal caso la segunda instancia es acudir a políticas y leyes de estado, pero dado que la infraestructura del cloud se haya distribuida en zonas geográficamente distantes (países o continentes), las políticas de estado son diferentes y es posible que lo que se entiende como falta en un lugar no lo sea en otro, dejando al cliente sin argumentos para reclamar sus derechos. Una muestra es el incidente ocurrido en 2003 cuando el gobierno de Francia demanda a Yahoo porque en su portal en francés anunciaba publicidad nazi, a lo que Yahoo replicó aludiendo que los servidores que albergaban el portal se encontraban ubicados en Estados Unidos, lo cual generó un problema de jurisdicción [30].

R10: Dificultades para Realizar Análisis Forense

Frecuentemente la preocupación del cliente es como prepararse para migrar a la nube, esto es lógico dado que cronológicamente es el primer paso dentro del proceso, pero pocas veces se detiene a pensar que debe hacer si alguno de los riesgos se materializa y se quiere encontrar el que, como, quien y porque del ataque? Los procedimientos forenses habituales no encajan adecuadamente en el cloud, pues… ¿Cómo se realiza un análisis en el lugar, si tal lugar es un conjunto de lugares, un sistema distribuido dinámico en el que entran y salen recursos utilizados por muchos usuarios repartidos en todo el mundo? [17] [18] Al momento solo se

encuentran algunas referencias al tema pero no ha sido ampliamente abordado y su tratamiento es incierto lo que lo convierte en un riesgo.

R11: Vulnerabilidades en el Proveedor

La confianza es un factor que genera relaciones fuertes y duraderas, pero hasta qué punto se debe confiar en un proveedor de servicios si de su buen desempeño depende el desempeño de una organización? Las vulnerabilidades a nivel de proveedor pueden afectar cualquiera de los servicios y es importante saber hasta qué punto tiene responsabilidad, pues se encarga de la infraestructura hardware en IaaS, añade la capa de integración en PaaS y finalmente asume la capa de aplicación en SaaS. La caída de la red, una falla en el servidor de aplicaciones, o un error de programación en una aplicación son ejemplos de vulnerabilidades en cada caso. Algunos ejemplos son las vulnerabilidades de SQL-injection y cross-site scripting presentadas por Google Docs [31] [32].

3.4. Análisis de Controles

En este punto se identifican los controles existentes, y después de un análisis de riesgos se determina si es necesario implementar más controles o mejorar los actuales. Ahora, de acuerdo al proveedor de servicios tomado en el caso de estudio (Amazon Web Services) se hace una revisión de los controles de seguridad que implementa, estos son:

AREA	CONTROLES EXISTENTES
Certificaciones	Evaluaciones cada seis meses, de conformidad con la Declaración de Normas de Auditoría N ° 70
Administración de Riesgos	Marco de seguridad y de política basado en el COBIT y recientemente certificados en ISO 27001.
Monitoreo	Sistemas automatizados de control para proporcionar un alto nivel de rendimiento y disponibilidad
Almacenamiento	La redundancia es proporcionada por los servicios en S3 y EBS, y la integridad a través de sumas de comprobación y los procedimientos de destrucción de datos con NIST 800-88.
Autenticación y Autorización	Autenticación múltiple factor (usuario/contraseña, certificados digitales y llaves pares en SSH), y la independencia de los usuarios a través de ACLs.
Aislamiento	Entre máquinas virtuales se hace a través del hipervisor Xen. EC2 proporciona seguridad a nivel de sistema operativo de base y maquina virtual.
Continuidad de Negocio	Los centros de datos están diseñados para mantener el nivel de servicio y responder a incidentes con 24x7x365 de cobertura y apoyo continuo en el BCP
Seguridad en la Red	Firewalls para prevenir ataques comunes como DDoS, MITM, etc. Se provee el servicio de VPN para crear un puente seguro entre la compañía y la nube. Trasporte de datos basado en protocolo SSL.

Tabla 4. Identificación de los Controles Existentes

3.5. Determinación de la Probabilidad

En este análisis se utilizaran los criterios estándar para definir los niveles de probabilidad bajo los cuales una amenaza puede aprovechar una vulnerabilidad generando la materialización de un riesgo (Ver tabla 5).

NIVEL	DEFINICIÓN PROBABILIDAD
ALTO	La fuente de la amenaza está altamente motivada y es capaz de realizar el ataque, y los controles aplicados para prevenir la vulnerabilidad no son efectivos.
MEDIO	La fuente de la amenaza está motivada y es capaz de realizar el ataque, pero los controles podrían impedir el éxito del mismo.
BAJO	La fuente de la amenaza carece de motivación o capacidad, o los controles implementados impiden que la vulnerabilidad sea aprovechada.

Tabla 5. Niveles de Probabilidad

RIESGO	NIVEL PROB.
R1: Alta Dependencia del Proveedor	Alto
R2: Perdida de Control y Gobernabilidad	Alto
R3: Problemas de Cumplimiento	Alto
R4: Falta de Aislamiento	Bajo
R5: Debilidad en Autenticación y Autorización	Bajo
R6: Errores Aseguramiento de los Datos	Medio
R7: Denegación del Servicio	Medio
R8: Vulnerabilidades en el Hipervisor	Bajo
R9: Problemas de Jurisdicción y Políticas	Medio
R10: Dificultad Realizar Análisis Forense	Medio
R11: Vulnerabilidades en el Proveedor	Medio

Tabla 6. Determinación de la Probabilidad

3.6. Determinación del Impacto

Del mismo modo se utilizan los criterios estándar y se definen tres niveles posibles de impacto, para a partir de estos clasificar cada uno de los riesgos (ver tabla 7 y 8).

NIVEL	DEFINICION DE IMPACTO
ALTO	La materialización podría generar pérdidas materiales altas y ocasionar la muerte o serios daños en las personas. Impedir el cumplimiento de la misión y afectar la reputación e intereses de la organización.
MEDIO	La materialización del riesgo podría generar pérdidas materiales bajas y ocasionar lesiones en las personas; o afectar el cumplimiento de la misión, la reputación e intereses de la organización.
BAJO	La materialización del riesgo puede ocasionar la perdida de algunos bienes o afectar ligeramente el cumplimiento de la misión, la reputación y los intereses de la organización.

Tabla 7. Niveles de Impacto

RIESGO	NIVEL IMPACTO
R1: Alta Dependencia del Proveedor	Medio
R2: Perdida de Control y Gobernabilidad	Alto
R3: Problemas Cumplimiento	Alto
R4: Falta de Aislamiento	Alto
R5: Sistemas Débiles de Autent. y Autoriz.	Alto
R6: Errores en el Aseguramiento de los Datos	Alto
R7: Denegación del Servicio	Alto
R8: Vulnerabilidades en el Hipervisor	Alto
R9: Problemas de Jurisdicción y Políticas	Alto
R10: Dificultades realizar Análisis Forense	Medio
R11: Vulnerabilidades en el Proveedor	Alto

Table8. Determinación del Impacto

3.7. Determinación del Riesgo

Finalmente los riesgos son mapeados en una matriz, de acuerdo a los valores obtenidos de impacto (eje x) y probabilidad (eje y). Se crean entonces tres posibles niveles de riesgo para los cuales se define como actuar.

	IMPACTO		
PROBABILIDAD	BAJO	MEDIO	ALTO
BAJO			R4, R5, R8
MEDIO		R10	R6, R7, R9, R11
ALTO		R1	R2, R3

Tabla 9. Matriz de Riesgos

NIVEL	DESCRIPCIÓN DEL RIESGO Y ACCIONES A TOMAR
ALTO	Si un riesgo alto es encontrado en un sistema este puede seguir operando, pero es necesario generar un plan de acciones correctivas y ponerlo en marcha tan pronto como sea posible.
MEDIO	Se deben proponer acciones correctivas e implementarlas dentro de un periodo de tiempo razonable
BAJO	Respecto a riesgos de nivel bajo, es la dirección quien determina si se aceptaran o mitigaran los mismos, y dentro de que plazo.

Tabla 10. Niveles de Riesgo

3.8. Controles Recomendados

En este punto se proponen los controles orientados a mitigar o eliminar cada uno de los riesgos encontrados. Sin embargo, es al final la dirección quien determina de acuerdo a unos objetivos y el estudio de la relación costo-beneficio, si un riesgo es tratado, transferido o aceptado.

De otra parte, en la aplicación de controles es importante que mantener la relación con el sistema de gestión de seguridad de la información y estándares usados en la organización (COBIT, ISO27002, NIST SP8000-53, PCI, etc.). De acuerdo a esto, es utilizada la matriz de control propuesta por Cloud Security Alliance [16], que presenta un conjunto de controles para

cada uno de los dominios de seguridad definidos en cloud, mostrando la relación de cada uno con los sistemas de gestión y estándares más importantes del mercado. Dichos controles son enunciados a continuación:

Alta Dependencia del Proveedor
• Utilizar en la medida de lo posible componentes con APIs y estándares abiertos. Por ejemplo open virtualization format. • Determinar un segundo proveedor que cumpla con los requisitos establecidos. • Identificar los componentes y sus relaciones dentro del sistema, estableciendo para cada uno de ellos la dependencia que tiene con formatos de archivos, hardware o software. • Realizar copias de seguridad periódicas a un lugar remoto usando formatos que sean reutilizables.
Pérdida de Control y Gobernabilidad
• Analizar las implicaciones legales considerando las dimensiones funcionales, jurisdiccionales y contractuales • Establecer claramente las funciones y responsabilidades de cliente y proveedor dentro del servicio. • Cerciorar que el contrato estipule debida diligencia en el monitoreo, mantenimiento y recuperación del sistema. • Asegurar que la organización mantiene la propiedad intelectual de su información, en formato original.
Problemas de Cumplimiento
• Analizar el alcance del cumplimiento normativo y si este se verá afectado y de qué forma, al migrar a la nube. • Revisar que los posibles proveedores cumplan con las certificaciones o controles requeridos. • Crear una clausula que especifique el derecho a auditar. • Recabar evidencias de cumplimiento para cada requisito.
Problemas de Aislamiento
• Exigir mecanismos y procedimientos claros de separación para la información y control de acceso. • Realizar monitoreo sobre los procedimientos y validar sistemas de acceso e integridad de la información.
Debilidades en Sistemas Autenticación y Autorización
• Tratar de mantener el sistema de autenticación que posee la empresa, de no ser posible, usar estándares abiertos. • Contar con sistemas de autenticación de múltiple factor haciendo uso de recursos como tokens, certificados, contraseñas de un solo uso, biométricas, entre otros. • Tratar de mantener una conexión entre la organización y la nube, tal vez a través de una VPN o usar aserciones (SAML, WS-F) en las aplicaciones, combinado con SSL • Usar un mecanismo de autorización que permita una granularidad fina y sea dinámico permitiendo implementar todas las políticas establecidas.
Errores en el Aseguramiento de Datos
• Realizar una clasificación de toda la información determinando su grado de sensibilidad frente a la integridad, confidencialidad y disponibilidad. • Generar una política para el cuidado de la información: acceso, modificación, respaldos, eliminación, etc. • Establecer mecanismos de redundancia de información. • Utilizar mecanismos de cifrado en transmisión y almacenamiento, y tal vez a futuro en su procesamiento con la evolución de la criptografía homomórfica.

Denegación de Servicio
• Verificar que el proveedor cuente con un plan de continuidad del negocio certificado por estándares internacionales como BS 25999. • Determinar si el proveedor tiene recursos (humanos y tecnológicos) dedicados al cumplimiento del plan de continuidad. • Cerciorar que el acuerdo de nivel de servicio especifique la tasa de disponibilidad de los sistemas, tiempos y puntos de restauración (RTO y RPO) y la respectiva indemnización en caso de un incidente o el no cumplimiento de lo pactado. • Se recomienda a nivel de cliente realizar un análisis de impacto del negocio (BIA) para en base a este determinar acciones que permitan mantener la continuidad de los procesos críticos.

Vulnerabilidades en el Hipervisor
• Identificar el tipo de virtualización usado por el proveedor y comprobar la actualización del software de acuerdo a vulnerabilidades publicadas. • Comprender, configurar y activar los mecanismos de seguridad propios de las maquinas virtuales alojados en los APIs del hipervisor. • Disponer de mecanismos de generación de informes y alertas en caso de una violación del aislamiento.
Problemas de Jurisdicción y Políticas
• Revisar la ubicación geográfica de la información y asegurarse que las leyes que gobiernan los datos no entran en conflicto con las leyes del país. • Un sistema puede incluir: datos, aplicaciones, equipos, etc. Cada elemento debe ser asignado un dominio y jurisdicción legislativa para facilitar el mapeo adecuado de cumplimiento.
Dificultad para Realizar Análisis Forense
• De ser posible solicitar al proveedor el mapa de la arquitectura donde se encuentran sus recursos a fin de saber física y lógicamente cuales deben ser los escenarios a analizar. • Contar con la especificación de roles internos/externos y relacionarlos con las etapas de flujo de información. • Contar con procedimientos adecuados que garanticen la cadena de custodia para la recolección, conservación y presentación de pruebas en apoyo de una acción legal.

Vulnerabilidades de parte del Proveedor
• Realizar revisiones y evaluaciones independientes al menos una vez al año, o en intervalos planificados, para asegurar que la organización cumple con las políticas, procedimientos, normas y los requisitos aplicables (internos/externos auditorías, certificaciones, pruebas de vulnerabilidades y de penetración)

4. Conclusiones y Trabajo Futuro

La migración/implementación de un sistema en la nube es un proceso que debe adelantarse gradualmente pasando etapas como el levantamiento de requisitos, selección del proveedor, análisis de riesgos, implementación de controles, migración del sistema y pruebas de validación sobre el mismo, teniendo en cuenta siempre la alineación con los objetivos del negocio.

La computación en la nube es una tendencia formal con fuertes ventajas que promete rediseñar el concepto de servicios computacionales, sin embargo es deber del consumidor realizar un estudio de las implicaciones en seguridad no solo antes de la migración sino durante y después de ella, siendo la forma más recomendable el uso de un sistema de gestión de seguridad de la información.

Es visto que la metodología 800-30 propuesta por NIST es un instrumento útil y sencillo para la gestión de riesgos de manera cualitativa, que brinda el marco estructural a partir de una serie de etapas que si bien son especificadas están abiertas para ser complementadas con otras metodologías o estudios.

5. Trabajo Futuro

Normalmente una solución en la nube tiene mucho menor costo que una solución interna, sin embargo, tal cambio puede implicar nuevos controles que afectan el balance haciendo más costosa una solución externa. De acuerdo a esto es importante crear una metodología o herramienta que permita hacer una evaluación cuantitativa de los controles y una comparación a nivel de costos entre las dos opciones.

6. Agradecimientos

Agradecimientos a la Cámara de Compensación de Divisas de Colombia (CCDC) por permitirme trabajar en la iniciativa de adopción de la computación en nube en la empresa, y su gran cooperación durante el desarrollo de este proyecto.

7. Referencias

[1] Cloud Security Alliance. (2009, Nov). Security Guide: Critical Areas in Cloud Computing, Version 2 [En línea]. Disponible en: http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[2] European Network and Information Security Agency. (2009, Nov). Cloud Computing: Benefits, Risks and Recommendations for Information Security [En línea]. Disponible en: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-riskassessment/at_download/fullReport

[3] Centre for Protection of National Infrastructure (2010, Mar). Information Security Briefing Cloud Computing [En línea]. Disponible en: http://www.cpni.gov.uk/Docs/cloud-computing-briefing.pdf

[4] Ponemon Institute. (2010, May). Security of Cloud Computing Providers Study. [En línea]. Disponible en: http://www.ca.com/files/industryresearch/security-cloud-computing-users_235659.pdf

[5] V. Kundra. (2010, May). State of Public Sector Cloud Computing [En línea]. Disponible en: http://cio.gov/documents/StateOfCloudComputingReport-FINALv3_508.pdf

[6] Stoneburner G, Goguen A, Feringa A. Risk Management Guide for Information Technology Systems. SP 800-30. Nist Special Publications. 2002.

[7] J. Cano. (2010, May). Cumplimiento, seguridad y control en la nube. [En línea]. Disponible en: http://www.acis.org.co/fileadmin/Revista_112/uno.pdf

[8] National Institute of Standards and Technology. (2009, Oct). "The NIST Definition of Cloud Computing [En línea]. Disponible en: http://csrc.nist.gov/groups/SNS/cloud-computing/

[9] T. Mather, S. Kumaraswamy and S. Latif. Cloud Security and Privacy. Ed. O'reilly, 2009.

[10] S. Mansfield, "Danger in the clouds". Network Security Review, vol. 2008, pp. 9-11, Dec. 2008.

[11] Amazon. (2010, Aug). Amazon Web Services: Overview of Security Processes [En línea]. Disponible en: http://aws.amazon.com/security

[12] J. Heiser and Mark Nicolett. (2008, Jun). Assessing the security risks of cloud computing [En línea]. Disponible en: www.gartner.com/DisplayDocument?id=685308

[13] M. Christodorescu, R. Sailer, D. Schales, D. Sgandurra, D. Zamboni, "Cloud Security Is Not (Just) Virtualization Security", in ACM Cloud Computing Security Workshop, 2009.

[14] J. Rutkowska. (2008). Security Challenges in Virtualization Environments [En línea]. Disponible: http://www.invisiblethingslab.com/bh08/part{1,2,3}.pdf

[15] R. Ray and E. Schultz, "Virtualization Security", in ACM 5th Workshop on Cyber Security and Information Intelligence, 2009.

[16] Cloud Security Alliance. (2010, May). Controls Guide Cloud Computing [En línea]. Disponible en: http://www.cloudsecurityalliance.org/guidance/CSA-ccm-v1.00.xlsx

[17] S. Biggs and S. Vidalis, "Cloud Computing: The Impact on Digital Forensic Investigations". IEEE, 2009.

[18] S. Wolthusen, "Overcast: Forensic Discovery in Cloud Environments", in IEEE Fifth International Conference on IT Security Incident Management and IT Forensics, 2009.

[19] Cloud Bursts as Coghead Calls It Quits.http://www.zdnet.com/blog/collaboration/cloud-bursts-as-coghead-calls-it-quits/349

[20] Latest cloud storage hiccups prompts data security questions. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130682&source=NLT_PM

[21] Industria de Tarjetas de Pago – PCI. (2009, Jun), Requisitos y Procedimientos de Evaluación de Seguridad [En línea]. Disponible en: http://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/doc/pci_dss_v1-2.pdf

[22] Google (2008, Oct), SAML Single Sign on vulnerability. [En línea]. Disponible en: www.kb.cert.org/vuls/id/612636

[23] BBC News (2009, Mar), Facebook users suffer viral surge. [En línea]. Disponible en: http://news.bbc.co.uk/2/hi/technology/7918839.stm

[24] ComputerWorld (2008, Oct), Extended Gmail outage hits Apps admins [En línea]. Disponible en: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117322.

[25] Amazon (2008, Jul), Amazon S3 Availability Event [En linea]. Disponible en: http://status.aws.amazon.com/s3-20080720.html.

[26] The Whir (2008, Oct). FlexiScale Suffers 18-Hour Outage [En línea]. Disponible en: http://www.thewhir.com/web-hosting-news/103108_FlexiScale_Suffers_18_Hour_Outage

[27] Security Tracker (2008, Feb). VMWare vulnerability. http://securitytracker.com/alerts/2008/Feb/1019493.html

[28] Xen Vulnerability (2007, Oct) http://secunia.com/advisories/26986

[29] Microsoft (2007, Ago) Virtual PC vulnerability. http://www.microsoft.com/technet/security/bulletin/ms07-049.mspx

[30] Out Law (2003, Feb) French court acquits Yahoo! of criminal charges for Nazi sales [En línea]. Disponible en: http://www.out-law.com/page-3319

[31] Google Docs Glitch Exposes Private Files. http://www.pcworld.com/article/160927/google_docs_glitch_exposes_private_files.html

[32] Security issues with Google Docs. http://peekay.org/2009/03/26/security-issues-with-google-docs

Erick Ramón Meneses Cuadros es ingeniero y magister en Informática de la Universidad Industrial de Santander, y actualmente se desempeña como investigador en doctorado para la Universidad Joseph Fourier y los Laboratorios Orange-Francia. Dentro de sus intereses se encuentran los sistemas distribuidos, la seguridad informática y la astronomía, áreas en las cuales cuenta con conocimiento y experiencia a nivel académico y empresarial.