Congreso Internacional en Ingeniería Electrónica. Mem. Electro 2015, Vol. 37, pp 436-441, Chihuahua, Chih. México
http://depi.itchihuahua.edu.mx/display/memorias_electro/MemoriaElectro2015
ISSN 1405-2172

RIESGOS PARA LA INCORPORACIÓN DE PYMES AL CÓMPUTO EN LA NUBE

Blanca Hilda Castro Morales, Rodolfo Romero Herrera
Instituto Politécnico Nacional – Escuela Superior de Computo
Departamento de Posgrado
Av. Juan de Dios Bátiz esq. Av. Miguel Othón de Mendizábal, Col. Lindavista. Del. Gustavo A. Madero.
México, D. F. C.P. 07738.
Tel. 5729-6000 Ext. 52040
e-mail: whitehilda@yahoo.com.mx, rromeroh@ipn.mx

RESUMEN.

La computación en la nube promete a cualquier empresa que utilice tecnologías; alta disponibilidad, flexibilidad, aumentar la eficiencia, ahorrar dinero, etc; pero genera dudas con respecto a la forma de proteger su información y garantizar el cumplimiento de normas, al considerarse un panorama de riesgo donde se ven involucrados la confidencialidad y la privacidad entre algunos de estos aspectos.

Generalmente en los grandes corporativos la tecnología de la información es resuelta adecuadamente al no tener limitaciones económicas o tecnológicas como las que tiene una PyME, resultando para ellas más complicado adoptar estas prácticas, optando en la mayoría de los casos por no utilizarlas.

Con este trabajo de investigación se busca encontrar los peligros para las PyMES bajo la computación en la nube, de tal manera que disminuya el riesgo de sus operaciones, permitiéndoles mantenerse a la vanguardia en el uso de herramientas informáticas.

Palabras Clave: Computo en la nube, PyMes, Riesgos, Analisis.

1. INTRODUCCIÓN

Para llevar a cabo una implementación bajo computación en la nube es necesario que se haga mediante un proveedor, lo cual no permite a los usuarios tener físicamente los dispositivos para el almacenamiento de sus aplicaciones y mucho menos la administración de estos, dejándole esta responsabilidad a un tercero.

La computación en nube es y ha sido criticada por limitar la libertad de los usuarios y hacerlos dependientes del proveedor de servicios. Así, el periódico de Reino Unido, The Times en el año 2011 realizó una comparación entre la computación en la nube contra los sistemas centralizados que se utilizaban entre los años 50 y 60; este periódico argumenta que la computación en nube es un retorno a esa época y numerosos expertos respaldan la teoría.

De forma similar, Richard Stallman fundador de la Free Software Foundation, cree que la computación en nube pone en peligro las libertades de los usuarios, porque éstos dejan su privacidad y sus datos personales en manos de terceros.

Actualmente un sin número de universidades, institutos, proveedores e instituciones gubernamentales están invirtiendo en computación en la nube:

- En enero de 2011, IRMOS EU financió el desarrollo de una plataforma en la nube en tiempo real, permitiendo aplicaciones interactivas en infraestructuras de la nube.
- En junio de 2011, dos universidades de la India University of Petroleum and Energy Studies y University of Technology and Management introdujeron una asignatura de computación en la nube en colaboración con IBM.
- En diciembre de 2011, el proyecto VISION Cloud financiado por la UE propuso una arquitectura y una implementación para los servicios de uso intensivo de datos con el objetivo de proporcionar una infraestructura de almacenamiento virtualizada.
- En octubre de 2012, el Centro de desarrollo para la Computación Avanzada publicó un software llamado "Meghdoot" de código abierto, de servicio en la nube.
- En febrero de 2013, el proyecto BonFire lanzó un centro de experimentación y pruebas en la nube. La instalación ofrece acceso transparente a los recursos de la nube, con el control y la observabilidad necesaria para diseñar las futuras tecnologías en la nube.

De manera particular, en México continúa en aumento la cantidad de empresas, instituciones y universidades que adoptan la computación en la nube como una herramienta tecnológica.

El intercambio de datos entre las personas y las empresas en la actualidad es de gran volumen en Internet. En los últimos años, se ha generalizado el uso de proveedores de tecnología que ofrecen sus servicios desde la red.

Una de las principales formas de generar confianza, entre proveedores y usuarios (clientes), es ponerse de acuerdo sobre quién obtiene qué derechos, y quién asume responsabilidades de lo que pase con la información en la nube.

La novedad es la misma de siempre: la preocupación; ya que muchos de los asuntos de privacidad en la nube son objeto de constantes inquietudes acerca de:

La manera en cómo las personas y las empresas conforman su postura ante las políticas aplicables, regulaciones estándar, contratos y políticas de intercambio.

• La metodología con la que la información es puesta en la nube y cómo permanece en ella, así como también la certidumbre de

que al borrarla sea realmente borrada por competo de los dispositivos de almacenamiento del proveedor.
• Las palabras clave generadas para mostrar y acceder a la información para modificarla, copiarla u otros usos.
Estas consideraciones deberían llevar a la difusión de mecanismos reguladoresque orienten a los usuarios a un empleo más definido de estos servicios, así como
de las ventajas y desventajas que pueden encontrar en las políticas de privacidad
que los proveedores otorgan.
El correcto establecimiento de políticas de privacidad de la información en este tipo de servicios evita que datos como: nombre, tarjeta de crédito, registros biométricos, etc., puedan ser usados para distinguir o rastrear la identidad de una persona; y éstos se utilicen para cometer fraudes, robos de identidad, envío de correo no deseado, entre otros. No obstante, falta preocupación de los proveedores respecto a las consecuencias de no tener control adecuado sobre la privacidad de la información de sus clientes; un hecho concreto ocurre en la declaración de políticas de Facebook por ejemplo, en las que se aclara a los usuarios que no se respalda la seguridad del servicio, pues éste se ofrece tal cual y sin ningún tipo de garantía.
Los miedos de los usuarios están justificados, pues no existe una figura legal que establezca lineamientos, reglas o leyes sobre cuándo una información puede hacerse pública, cuándo debe estar asegurada, o bien, cuándo es robada.
En México, el avance en cuanto a privacidad y protección de la información ha crecido lentamente, no obstante el 5 de julio de este año se publicó en el Diario Oficial de la Federación la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en la cual se preservan en esencia la privacidad, confinación y auto-determinación de la información de las personas.
En esta ley se hace observación sobre el consentimiento, el cual se entiende como la “manifestación de la voluntad del titular de los datos personales mediante la cual se efectúa el tratamiento de los mismos”.
El criterio de consentimiento aplicado a las políticas de uso de los servicios de cómputo en la nube podría servir para dar contexto y referencia sobre lo que usuarios podrían exigir en caso de presentarse una infiltración o violación a las sesiones privadas en este tipo de servicios, aunque debemos ser conscientes que la amenaza siempre estará presente. Entre los riesgos que más persisten bajo este panorama se pueden mencionar:
• El uso permitido de información por parte del proveedor podría no estar claramente definida en los términos del servicio o contrato, permitiendo al proveedor, por ejemplo, usarla para sus propósitos o venderla a terceros.
• El proveedor podría ser requerido para permitir a autoridades judiciales locales o extranjeras buscar en la información resguarda por éste.
• La información almacenada por el proveedor podría verse comprometida, sin informar a las autoridades competentes o a los usuarios afectados por el incidente.
• El proveedor podría no tomar las medidas necesarias para evitar perder accidentalmente la información.
• Que los proveedores no garanticen al usuario que su información no sea expuesta durante el intercambio de datos con otros usuarios a través de estos servicios.
La computación en nube puede representar una mejora en la privacidad de información de aplicaciones no críticas. Sin embargo la transparencia es crucial, los usuarios deben poder evaluar y comparar las prácticas de seguridad de cada proveedor.
Desde esta perspectiva, las preocupaciones por la privacidad continuarán creciendo, ya que la información, en distintos formatos, procesada y almacenada en la nube, usualmente contiene datos personales o información sensible de las organizaciones, los cuales siempre resultan atractivos para los delincuentes cibernéticos.

2. PLANTEAMIENTO

La computación en la nube ayuda a las empresas de todos los tamaños a transformar sus operaciones y tecnología estableciendo un entorno flexible y adaptable para satisfacer rápidamente los cambiantes requisitos. La necesidad de lograr más con menos se encuentra en la esencia financiera de cada empresa en crecimiento y la naturaleza on-demand de la nuble la convierte en el recurso perfecto de tecnologías de la información para empresas que necesitan operar con un presupuesto estrecho, pero que también necesitan expandir su capacidad a medida que crece.
Para el 55% de las empresas en América Latina, la computación en la nube es una de las tecnologías prioritarias que se implementarán a partir del 2014, de acuerdocon la Encuesta de Prioridades de TI en América Latina 2014 de TechTarget.

2.1. Objetivo

Esta investigación busca poner en contexto los riesgos al implementar Computo en la nube en las PyMES, por lo que propone un análisis de riesgos basados en el método de Montecarlo que permita determinar los puntos finos para su implementación.

2.2. Problematica

Tomando en cuenta el caso de las PyMES, que son organizaciones vulnerables en temas de tecnologías de la información, y debido a que una gran parte de estas prestan u ofrecen sus servicios a sus clientes sin importar su giro particular, resulta fundamental entonces que las empresas conozcan cuál es el modelo de computación en la nube más adecuado para ellas, el cual ayude a disminuir el riesgo en el que se encuentra su información ante los delincuentes cibernéticos.

ISSN 1405-2172

Dentro de la nube, los usuarios tienen una gran variedad de recursos virtuales para sus necesidades de cómputo y no necesitan instalar o configurar una infraestructura compleja, ya que todas las tareas se llevan a cabo fuera de los dispositivos que se estén utilizando.

Las PyMes en su mayoría cuentan con una pequeña o nula infraestructura tecnológica para el procesamiento de los datos involucrados en sus procesos internos. Sin embargo, como en cualquier tecnología de la información, resulta imprescindible la implementación de seguridad a fin de buscar la mayor confiabilidad de los datos que se procesan bajo este esquema, evitando los usos indebidos de estos por usuarios ajenos, todo esto bajo un modelo accesible para las PyMes que les ayude en la reducción del riesgo en el que se encuentra su información al ser "administradas" sus aplicaciones por un tercero.

La característica principal de la computación en la nube es que los recursos y servicios informáticos, tales como infraestructura, plataforma y aplicaciones, son ofrecidos y consumidos como servicios a través de la Internet sin que los usuarios tengan que tener ningún conocimiento de lo que sucede detrás.

Acceder a la información de manera continua y cuando se necesite, facilita a las empresas la toma de decisiones y contribuye a ofrecer mejores servicios, por lo que se puede pensar que la computación en la nube, es una alternativa, para mejorar la disponibilidad y continuidad en los servicios informáticos en las empresas.

Según la definición del NIST (Instituto Nacional de Normas y Tecnología de los Estados Unidos) las computación en la nube tiene las siguientes características:

Autoservicio a demanda. Un consumidor puede proveer unilateralmente capacidades de computación, como almacenamiento en la red y tiempo de servidor, según sea necesario de manera automática sin interacción humana con cada proveedor de servicio.

- Acceso amplio a la red. Existen capacidades disponibles en la red y se puede acceder a ellas a través de mecanismos o estándares que promueven el uso por medio de plataformas de cliente pesado o liviano heterogéneas (p. ej., teléfonos móviles, computadoras portátiles y PDA).
- Agrupación de recursos. Los recursos de computación del proveedor se agrupan para brindar servicio a múltiples consumidores utilizando un modelo de multiempresa, con recursos virtuales y físicos diferentes asignados dinámicamente y reasignados según la demanda del consumidor.
- Hay un sentido de independencia de ubicación ya que generalmente el cliente no tiene control ni conocimiento sobre la ubicación exacta de los recursos proporcionados.
- Elasticidad rápida. Las capacidades se pueden proporcionar de manera rápida y elástica, en algunos casos automáticamente, para expandir y se pueden liberar de manera rápida para reducir. Para el consumidor, las capacidades disponibles para el aprovisionamiento generalmente parecen ser ilimitadas y se pueden comprar en cualquier cantidad en cualquier momento.
- Servicio medido. Los sistemas en nube controlan y optimizan automáticamente el uso de recursos aprovechando la capacidad de medición a cierto nivel de abstracción adecuado para el tipo de servicio. (p.ej., almacenamiento, procesamiento, ancho de banda y cuentas de usuarios activos). El uso de recursos se puede monitorear, controlar y denunciar proporcionando transparencia para tanto el proveedor como el consumidor del servicio utilizado

La computación en la nube puede implementarse con las siguientes capas:

• El software como servicio (en inglés software as a service, SaaS) se encuentra en la capa más alta y se caracteriza por una aplicación completa ofrecida como un servicio, por demanda, que significa una sola instancia del software que corre en la infraestructura del proveedor y sirve a múltiples organizaciones de clientes. Las aplicaciones que suministran este modelo de servicio son accesibles a través de un explorador de internet o de cualquier aplicación diseñada para esto y el usuario no tiene control sobre ellas, aunque en algunos casos se le permite realizar algunas configuraciones.

• La capa del medio, que es la plataforma como servicio (en inglés platforms a service, PaaS), es la encapsulación de una abstracción de un ambiente de desarrollo y el empaquetamiento de una serie de módulos o complementos que proporcionan, normalmente, una funcionalidad horizontal (persistencia de datos, autenticación, mensajería, etc.). De esta forma, un arquetipo de plataforma como servicio podría consistir en un entorno conteniendo una pila básica de sistemas, componentes o APIs preconfiguradas y listas para integrarse sobre una tecnología concreta de desarrollo. Las ofertas de PaaS pueden dar servicio a todas las fases del ciclo de desarrollo y pruebas del software, o pueden estar especializadas en cualquier área en particular, tal como la administración del contenido. En este modelo de servicio al usuario se le ofrece la plataforma de desarrollo y las herramientas de programación por lo que puede desarrollar aplicaciones propias y controlar la aplicación, pero no controla la infraestructura.

• La infraestructura como servicio (infrastructure as a service, IaaS) también llamado en algunos casos hardware as a service, HaaS se encuentra en la capa inferior y es un medio de entregar almacenamiento básico y capacidades de cómputo como servicios estandarizados en la red.

Como producto de este modelo de Computo en la nube y provocado por las capas que lo constituyen se tienen los siguientes inconvenientes:

- La disponibilidad de servicios altamente especializados podría tardar meses o incluso años para que sean factibles de ser desplegados en la red.

- La madurez funcional de las aplicaciones hace que continuamente estén modificando sus interfaces, por lo cual la curva de aprendizaje en empresas de orientación no tecnológica teine unas pendientes significativas, así como su consumo automático por aplicaciones.
- La información de la empresa debe recorrer diferentes nodos para llegar a su destino, cada uno de ellos (y sus canales) son un foco de inseguridad. Si se utilizan protocolos seguros, HTTPS por ejemplo, la velocidad total disminuye debido a la sobrecarga que éstos requieren.

• Escalabilidad a largo plazo. A medida que más usuarios empiecen a compartir la infraestructura de la nube, la sobrecarga en los servidores de los proveedores aumentará, si la empresa no posee un esquema de crecimiento óptimo puede llevar a degradaciones en el servicio.

• Privacidad. La información queda expuesta a terceros que pueden copiarla o acceder a ella. Aún cuando hasta la fecha estas son las desventajas que presenta la implementación de este modelo diversas empresas continuan creando servicios usando esta herramienta.

- Los beneficios de las nubes han sido enumerados por personalidades como Steve Jobs hasta funcionario estadounidenses que aseguran que esta herramienta reduce la piratería. Sin embargo, la seguridad de los servidores y la vulnerabilidad ante ataques y hackeos podría ser la mayor desventaja de esta herramienta.
- Los ataques informáticos a compañías de alto perfil parecen mostrar que internet es un lugar inseguro para la información. Hackeos a la información de empresas como Sony, la consola de juegos de Microsoft y Gmail muestran que incluso las empresas que invierten grandes cantidades de dinero en seguridad pueden ser víctimas de robos de información.
- Otro problema sobre la confianza en la nube es que los proveedores de servicios encargados de almacenar dicha información guardan los datos en servidores remotos (cuya ubicación en la mayoría de los casos permanece en secreto), por lo que los usuarios no pueden saber con seguridad cómo se está manejando su información.

La incertidumbre que genera la adopción de una nueva tecnología es normal. Si regresáramos 10 años en el tiempo y se le dijera a una persona que puede realizar compras por internet al ingresar los datos de su tarjeta de crédito, seguramente no confiaría en hacerlo. Por tal motivo las PyMES deben relizar antes de implementar computo en la nube un análisis de riesgos. Aquí se propone el uso de Mote Carlo.

3. ANÁLISIS DEL RIESGO

Cuando ya se han identificado y clasificados los riesgos, se realiza un análisis de los mismos, es decir, se estudian la posibilidad y las consecuencias de cada factor de riesgo con el fin de establecer el nivel.

El análisis de los riesgos determinará cuáles son los factores de riesgo que potencialmente tendrían un mayor efecto y, por lo tanto, deben ser gestionados por el emprendedor con especial atención.

3.1. Método Montecarlo.

Es un método cuantitativo para el desarrollo de análisis de riesgos. El método fue llamado así en referencia al Principado de Mónaco, por ser “la capital del juego de azar” [ ].

Dicho método busca representar la realidad a través de un modelo de riesgo matemático, de forma que asignando valores de manera aleatoria a las variables de dicho modelo, se obtengan diferentes escenarios y resultados.

El método Montecarlo se basa en realizar un número lo suficientemente elevado de iteraciones (asignaciones de valores de forma aleatoria), de manera que la muestra disponible de resultados, sea lo suficientemente amplia como para que se considere representativa de la realidad. Dichas iteraciones se podrán realizar haciendo uso de un motor informático.

Con los resultados obtenidos de las diferentes iteraciones realizadas se efectúa un estudio estadístico del que se sacan conclusiones relevantes respecto al riesgo del proyecto, tales como, valores medios, máximos y mínimos, desviaciones típicas, varianzas y probabilidades de ocurrencia de las diferentes variables determinadas sobre las que medir el riesgo.

3.2. Modelo de Riesgos

Un modelo de riesgos es un mecanismo que nos permite poner en práctica el método cuantitativo de Montecarlo para el análisis de riesgos.

Es la representación de la realidad a analizar a través de una estructura de cálculos matemáticos, en la cual se detectan las variables significativas de riesgo y se ponen en relación con el resto de variables que afectan a nuestro proyecto, y con las variables económicas sobre las que vamos a medir el nivel de riesgo del mismo, Beneficio y Valor actual neto.

Para la medición de la probabilidad de ocurrencia del riesgo y el impacto que el mismo tendría en nuestro proyecto, este impacto se mide en el Beneficio obtenido por el emprendedor en el ejercicio y el Valor Actual Neto del proyecto empresarial.

De forma adicional, un modelo de riesgos nos permitirá realizar un control y seguimiento sobre el mismo, comparando el valor en riesgo de las variables con el valor real incurrido finalmente en el periodo sujeto a análisis.

Para el desarrollo de un Modelo de Riesgos basado la medición de las probabilidades de ocurrencia los pasos a seguir son mostrados en la figura 1.

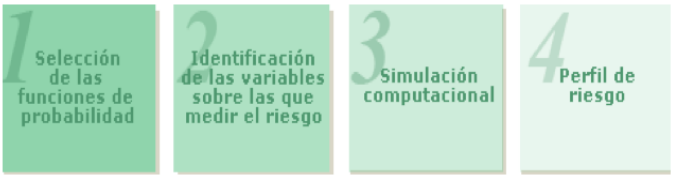

Figura 1. Pasos a seguir para medir los riesgos.

ISSN 1405-2172

Una vez Identificados las variables de riesgo nos interesa conocer cual es el comportamiento de dichas variables, es decir, cual va a ser su rango de variación para cada uno de los periodos de proyección.

Para ello es necesario identificar la función de probabilidad que se asocia a cada uno de las variables afectadas por el riesgo, es decir, la función que explica y refleja el comportamiento de la variable de riesgo definida por el emprendedor.

Basándonos en la determinación del valor de la empresa a través de la estimación de los flujos de dinero que genere en el futuro, consideramos una variable adecuada sobre la cual medir el riesgo el Valor Actual Neto, VAN del proyecto y como variable complementaria a corto plazo el valor del Beneficio Neto.

A modo de resumen:

- El emprendedor realiza un ejercicio de reflexión para identificar los riesgos en función de alguno de los métodos propuestos.
- Selecciona cuales son la variables de su Plan que se ven afectadas por el riesgo.
- Introduce los valores solicitados por la herramienta para cada uno de las variables afectadas por el riesgo.
- Determina cual es la variable de salida donde se va a cuantificar el riesgo total de su proyecto, beneficio o valor actual neto.

En este momento la herramienta comienza el proceso de simulación, es decir, efectúa las iteraciones necesarias, a través de un motor informático. Este paso, se ejecuta de forma automática por parte de la herramienta, el motor de cálculo genera mil iteraciones, con objeto de obtener una muestra que sea representativa de la realidad. La simulación genera de forma aleatoria, mil posibles valores para las variables de riesgo, todos ellos se encuentran entre los intervalos previamente definidos por el usuario y arrojará mil valores de las variables de salida, beneficio o valor actual neto.

Esto permite al emprendedor alcanzar conclusiones del grado de ocurrencia o probabilidad de los diferentes posibles resultados, como cual será el valor más probable del valor de su negocio y beneficio, cual será el valor mínimo o el valor máximo que podría alcanzar, etc.

Los resultados que nos va a mostrar el modelo de riesgo son las posibles conclusiones a alcanzar con la muestra obtenida de las diferentes iteraciones efectuadas, que es representativa de la realidad.

El Histograma muestra los posibles valores del beneficio neto o del VAN del proyecto empresarial que podrán ser alcanzados con un nivel de confianza determinado (probabilidad de ocurrencia asociada al valor).

Mediante un gráfico se expone lo que podría constituir la curva de perfil de riesgo de un determinado activo, empresa, región, etc., respecto de los riesgos que afectan al VAN o al beneficio neto.

La herramienta permite obtener una visión del riesgo que facilita la toma de decisiones más optima en cada momento del ciclo de vida de su proyecto.

4. RESULTADOS.

Siguiendo la metodología propuesta para hallar controles que deben ser considerados de cara al cliente para cada uno de los diferentes modelos de servicios y para los modelos de implementación privado o comunitario, donde la infraestructura física se encuentra alojada en las instalaciones del cliente, se encontró un total de 69 riesgos y 95 controles, que se clasificaron para cada uno de los dominios del modelo de computación en la nube para un caso especifico de una empresa PyME..

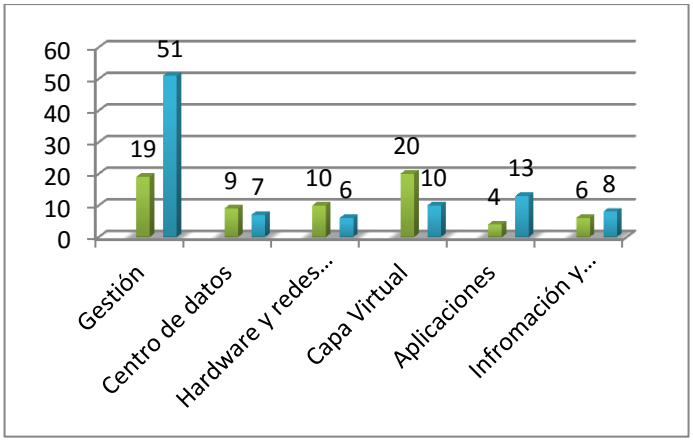

Figura 2. Controles y riesgos para un caso especifico.

Tabla 1Controles y riesgos de la figura 1.

Dominio	Total de Riesgos	Total de Controles
Gestión	19	51
Centro de datos	9	7
Hardware y redes de Computación	10	6
Capa virtual	20	10
Aplicaciones	4	13
Información y servicios	6	8

El dominio de gestión, debido a su complejidad operativa y extensión se subdivide para su clasificación como lo muestra la figura 3 y tabla 2.

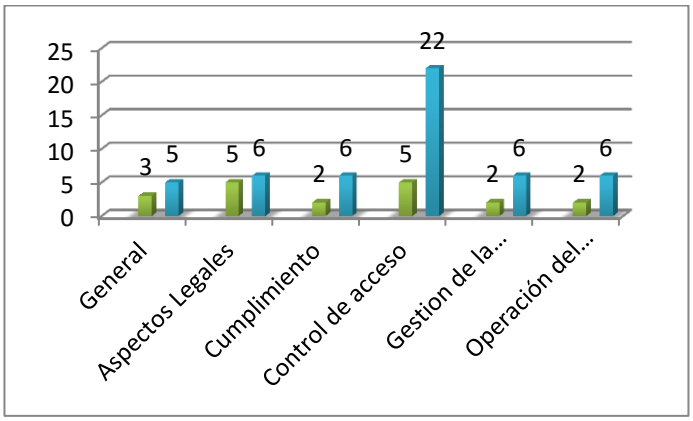

Figura 3. Dominio de gestión

Tabla 2. Dominio de gestión

	Total de Riesgos	Total Controles
General	3	5
Aspectos legales	5	6
Cumplimiento	2	6
Control de acceso	5	22
Gestión de la continuidad del Proyecto	2	6
Operación del servicio	2	6

5. CONCLUSIONES

En términos de seguridad de la información, las economías de escala y la flexibilidad ofrecidas por la computación en la nube privada o comunitaria puede tener impacto positivo en el caso que se requiere menor inversión en medidas de seguridad por que se distribuyen los costos y puede tener impacto negativo a que la concentración masiva de recursos y datos se convierten en un objetivo más atractivo para atacantes.

5.1. Referencias

[1]Michel Ruiz Tejeida, Seguridad de la computación en la nube. México, Distrito Federal : CINVESTAV IPN, 2013.
[2]Andrés Chacón y Juan Hurtado, Definición de un modelo de seguridad de la información en nubes privadas y comunitarias. Santiago de Cali: Facultad de Ingeniería, 2012.
[3]Héctor Poveda, Privacy, La nube de computación móvil: una solución a la demanda de procesamiento de señal en las comunicaciones móviles. Panamá, Panamá: Universidad Tecnológica de Panamá, 2014.
[4]Robert Ramírez Vique, Métodos para el desarrollo de aplicaciones móviles. Catalunya: Universidad Oberta de Catalunya.
[5]Beka Kezherashvili, Computación en la nube. Almeira: Universidad de Almeira.
[6]Oscar Ávila Mejía, Computación en la nube. México, Distrito Federal: UAM-I, 2011.
[7]José Parada Gimeno, Infraestructuras de seguridad en la nube. Madrid, España: Microsoft España, 2011
[8]William F. Pegrin, Cloud Computing, Privacy Recommendations for the Use of Cloud Computing. Masachusets: 2011.
[9]Ko, Ryan K. L. Ko; Kirchberg, Markus; Lee, Bu Sung, From System-Centric Logging to Data-Centric Logging – Accountability, Trust and Security in Cloud
Computing. Singapore:2011.
[10]Ko, Ryan K. L.; Jagadpramana, Peter; Mowbray, Miranda; Pearson, Siani; Kirchberg, Markus; Liang, Qianhui; Lee, Bu Sung. TrustCloud: A Framework for Accountability and Trust in Cloud Computing. Washington DC, USA:2011.
[11]Ko, Ryan K. L.; Jagadpramana, Peter; Lee, Bu Sung. A File-centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments. Washington DC, USA:2011.