Identificación de Riesgos vinculados con el uso de *Cloud Computing* en la Gestión Organizacional. Aplicación de la *Risk Breakdown Structure* a Entidades Financieras de la República Argentina

Autoria: María de los Ángeles López, Diana Ester Albanese, Marisa Analía Sánchez

RESUMEN

La tecnología de información es en la actualidad una herramienta indispensable en la actividad de cualquier organización, lo cual justifica su continuo desarrollo con el objeto de satisfacer necesidades en un contexto complejo. En esta evolución surgen nuevas opciones como las infraestructuras tecnológicas dinámicas.

Entre ellas, c*loud computing* se presenta como una nueva herramienta para la gestión de negocios basada en la virtualización. Siendo que brinda múltiples facilidades para el desarrollo de las actividades, las entidades han comenzado a evaluar la posibilidad de su aplicación. Sin embargo, los beneficios proporcionados por estas tecnologías son acompañados por una modificación en las estructuras de riesgos asociados.

Cualquier proyecto de implementación de *cloud computing* debe prever la gestión de dichos riesgos, de modo de prevenir aquellos que pudieran atentar contra el éxito del proyecto y de la organización. En la primera fase de dicho proceso se debe realizar una identificación y comprensión acabada de cada fuente de riesgos para garantizar el desarrollo de estrategias efectivas y la revisión del diseño de los controles relacionados.

Lo expuesto adquiere especial relevancia en aquellas entidades en las que se procesa información sensible, como es el caso de las entidades financieras.

El presente trabajo tiene como objetivo diseñar una *Risk Breakdown Structure* (RBS) para la identificación y descripción jerárquica de las fuentes de riesgos vinculados con la implementación de *cloud computing* en una entidad financiera de la República Argentina

Para ello se realizó un relevamiento de riesgos identificados por diversos autores, analizando específicamente aquellos definidos en las disposiciones que el Banco Central de la República Argentina en su carácter de organismo de contralor ha emitido en relación con la utilización de tecnología de información (TI) y tercerización de los servicios.

El resultado es una estructura de desglose orientada a la industria mediante la cual se exponen cuatro categorías de fuentes de riesgos – reputacional, cumplimiento, legales y operativos – exponiéndose una descripción de los eventos incluidos en cada una de ellas.

De acuerdo a la cantidad y variedad de subcategorías surge que los riesgos operativos resultan críticos y merecen especial atención. La exposición se realiza con diferentes grados de detalle, en función de la naturaleza de los riesgos, ejemplificando la utilidad para el reporte de riesgos a personal de diferentes niveles dentro de una organización. En una próxima investigación se pretende evaluar el impacto y probabilidad de ocurrencia de los riesgos identificados.

Se espera que la herramienta sirva a los managers como base para definir sus propias estructuras aplicadas a proyectos de sus organizaciones, tomar decisiones entre distintas alternativas, crear bases de datos útiles, y diseñar estrategias de gestión de riesgos que promuevan el éxito en la implementación de *cloud computing* promoviendo el máximo aprovechamiento de la tecnología en pos de los objetivos organizacionales.

1. INTRODUCCION

El permanente desarrollo de los servicios informáticos pretende dar satisfacción a las necesidades cada vez más exigentes de los usuarios. En esta evolución, hay intentos de reemplazar algunos sistemas tradicionales de tecnologías de información por modelos de infraestructuras tecnológicas dinámicas, entre ellos, *cloud computing*.

Esta herramienta consiste en un modelo de distribución de recursos informáticos a través de Internet, mediante la cual los usuarios acceden a aplicaciones y datos en el momento en que lo necesitan, durante el tiempo en que son requeridos y desde cualquier lugar. Desde la perspectiva empresarial, se obtienen múltiples beneficios mediante la gestión de los negocios a través de estos nuevos paradigmas.

Sin embargo, resulta imprescindible realizar análisis adecuados de los riesgos asociados a su implementación para garantizar buenos resultados en el desarrollo de un proyecto o proceso en particular y la sostenibilidad de una organización en el tiempo (Holzmann & Spiegler, 2010).

La gestión de riesgos emerge como un proceso esencial destinado a tomar acciones tempranas, efectivas y ofensivas contra los hechos contingentes que amenazan un proyecto, a la vez que busca aumentar la probabilidad de éxito que permita la supervivencia y la rentabilidad en un ambiente de negocios competitivo (Nguyen, 1998).

Al momento de planificar la utilización de *cloud computing* en la gestión de las actividades de una empresa se requiere una adecuada identificación y evaluación de los riesgos asociados, pero fundamentalmente una comprensión de los mismos y una visión en conjunto que permita detectar patrones de exposición a eventos contingentes que pueden afectar al proyecto (Hillson, 2002b).

Como respuesta a dicha necesidad, la *Risk Breakdown Structure* (RBS – Estructura de Desglose de Riesgos) se presenta como un método de identificación de riesgos estructurado que permite el reconocimiento de aquellos eventos que podrían afectar el status del proyecto. Los mismos son categorizados de acuerdo a su fuente, realizándose una descripción jerárquica que facilita el diseño de controles orientados a gestionar aquellas que resultan recurrentes o críticas.

Lo expuesto adquiere especial relevancia en sectores que hacen un uso intensivo de la información, como lo es el caso de las entidades financieras. Los avances tecnológicos, en especial las propuestas de servicios recientes, han llevado a cambios en el entorno, con mayor participación de servicios tercerizados, convirtiéndose en una potencial fuente de riesgos que implican constantes adecuaciones de la normativa vigente y la implementación de controles especiales (Estupiñán Gaitán, 2006).

El presente trabajo tiene como objetivo diseñar una RBS para la identificación y descripción jerárquica de las fuentes de riesgos vinculados con la implementación de *cloud computing* en una entidad financiera de la República Argentina.

Para ello se realizó el análisis de los riesgos teniendo en cuenta las disposiciones que el Banco Central de la República Argentina en su carácter de organismo de contralor ha emitido en relación con la utilización de tecnología de información (TI) y tercerización de los servicios.

El trabajo se estructuró en cuatro partes: en primer lugar, se realiza una revisión de las referencias bibliográficas; luego se expone la metodología implementada para la elaboración de la RBS. A continuación se presentan los resultados, y por último, se exponen las consideraciones finales y las propuestas para futuras investigaciones.

2. REFERENCIAL TEÓRICO

2.1. *Cloud Computing* como herramienta de gestión para las organizaciones

En la actualidad, y cada vez con mayor frecuencia, la gestión de las organizaciones depende de las facilidades que la tecnología de la información les brinda. Así existen entes que crean áreas y disponen de recursos destinados al desarrollo y mantenimiento interno del software y de las aplicaciones.

Sin embargo, no todas las organizaciones incorporan el desarrollo y mantenimiento de TI como proceso propio, sino que prefieren concentrar los recursos disponibles en sus principales capacidades competitivas y contratar servicios de apoyo informático. Es así que varios de los servicios proporcionados históricamente por los departamentos internos de informática actualmente suelen subcontratarse.

Una alternativa para el reemplazo de los modelos tradicionales de provisión de servicios informáticos son los modelos de infraestructuras tecnológicas dinámicas, los cuáles maximizan el valor para la organización y reducen costos. Éstas involucran el concepto de virtualización, referido al desacople de los recursos lógicos de los elementos físicos, permitiendo que los mismos puedan asignarse en forma más eficiente y efectiva, de acuerdo a los niveles de demanda de la organización.

Desde el punto de vista de la entidad, la virtualización ayuda a crear un cimiento para el crecimiento, brinda mayor flexibilidad y facilita el desarrollo de nuevas estrategias empresariales. Ejemplos de ello, son los servidores virtuales, el almacenamiento virtual de datos y el servicio de *cloud computing*, entre otros.

El caso particular de *cloud computing* representa un modelo de infraestructura dinámica que surgió en un momento de recesión global con una importante contracción al crédito, brindando soluciones de tecnología de información focalizadas en disminución de costos e incremento de eficiencia en los recursos, constituyendo un componente adecuado para la gestión de muchos negocios (Joint, Baker & Eccles, 2009).

Según *The National Institute of Standards and Technology*, *cloud computing* es un modelo que permite un acceso en red, conveniente y según las necesidades de la demanda, a un conjunto de recursos informáticos configurables compartidos, que pueden ser provistos rápidamente y con un mínimo esfuerzo de gestión o interacción por parte del prestador del servicio. Dichos recursos pueden ser, por ejemplo, redes, servidores, almacenamiento, correo electrónico, aplicaciones y servicios (NIST, 2010).

Cloud computing representa una forma diferente de infraestructura de TI. La información, el *software* o cualquier otro servicio, es almacenado y utilizado en los servidores de un tercero, a través de Internet, y no en la computadora personal o en los servidores privados.

El crecimiento en su utilización es notorio, convirtiéndose en una realidad innegable tanto para usuarios individuales como corporativos.

El beneficio más significativo que brinda esta estructura radica en la eficiencia lograda mediante la tercerización de parte de la gestión de la información y de las operaciones de TI. De ese modo, los miembros de las empresas pueden ocuparse de cuestiones estratégicas, mejorando procesos, aumentando la productividad e innovando, mientras el proveedor de la nube se encarga de las actividades operativas de TI de modo más inteligente, rápido y económico (ISACA, 2009).

El pago en función del nivel de uso del servicio permite obtener importantes reducciones de costos. Asimismo se evitan las grandes inversiones iniciales en recursos de *hardware* y *software* al momento de emprender un nuevo negocio o proyecto.

Otros beneficios relevantes se dan a nivel operativo y se refieren al poder de respuesta satisfactoria frente a las necesidades de *backups* y recuperación de desastres mediante el uso de sitios redundantes para el almacenamiento de la información, así como la seguridad de la misma en función de las grandes inversiones que realizan los proveedores de *cloud computing* en el desarrollo de soluciones y de la disponibilidad de recursos humanos expertos dedicados a ello (López, Sánchez & Albanese, 2010).

Como toda nueva tecnología, si bien brinda múltiples beneficios, también genera riesgos que deben ser considerados por los usuarios antes de su implementación.

Se debe tener en cuenta fundamentalmente el tipo de servicio – software, plataforma o infraestructura como un servicio - y el modelo de distribución adoptado – nubes públicas, privadas, comunitarias o híbridas.

En oposición a quienes consideran el incremento en la seguridad como uno de los beneficios del uso de *cloud computing*, hay quienes lo consideran como uno de los mayores obstáculos debido a que las complicaciones sobre la protección y confidencialidad de los datos preocupa al mercado (Joint et al., 2009), especialmente en sectores en los cuales se manejan importantes volúmenes de información sensible o confidencial.

Aún cuando el proveedor del servicio tercerizado garantice la seguridad de la información, la organización continúa siendo responsable de los datos que se proporcionan y de cualquier daño que pudieran generarse a terceros. Es por ello que resulta fundamental la evaluación de los riesgos asociados a la utilización de servicios tipo *cloud computing* (Gartner, 2009) y la delimitación de responsabilidades que le puedan caber a los proveedores del servicio.

En contextos donde las transacciones diarias se procesan en entornos de cl*oud computing*, la dirección de las organizaciones necesitan certezas sobre la calidad de su sistema de control interno (Senft & Gallegos, 2009) y su eficiencia para reducir el posible impacto negativo de los riesgos mencionados.

2.2. Sistema de control interno y gestión de riesgos

Avances tecnológicos como el descripto en el apartado anterior generan numerosos riesgos que requieren una adecuación de los controles internos vinculados. Se produjo a nivel mundial un cambio en los paradigmas de control surgiendo estructuras de control interno como las propuestas por los modelos COSO y COSO ERM.

Para lograr un uso apropiado de las nuevas tecnologías, se requiere una adecuada comprensión por parte de los usuarios de los riesgos que generan. Ello resulta fundamental para el desarrollo de estrategias que permitan gestionarlos. Éstas últimas en general no permiten su completa eliminación, pero al menos facilitan la reducción significativa de sus efectos, o su transferencia a un tercero (López et al., 2010).

Un sistema de control interno basado en el modelo COSO ERM pone énfasis en la gestión de riesgos, entendiéndose como tal un proceso llevado a cabo por el directorio, los gerentes y el resto del personal, destinado a establecer estrategias para toda la empresa, diseñado para identificar eventos potenciales que pudieran afectar a la entidad, y administrar los riesgos para que estén dentro de los límites de su aversión al riesgo, a fin de proporcionar una razonable seguridad respecto al logro de los objetivos de la organización (Estupiñan Gaitán, 2006).

Desde el punto de vista de la administración de proyectos se hace referencia a lo que se conoce como Gestión de Riesgos de un proyecto, identificada como una de las principales áreas del *Project Management Body of Knowledge* (PMBOK) desarrollado por el *Project Management Institute*, la organización profesional más importante dedicada al campo de la

gestión de proyectos. La misma pretende identificar y evaluar los riesgos a efectos de que puedan ser comprendidos y administrados de forma eficiente (Hillson, 2002a, 2002b).

Los objetivos de la gestión de los riesgos de un proyecto consisten en incrementar la probabilidad y el impacto de los eventos positivos y disminuir la de los eventos negativos que pueden afectar a un proyecto (PMI, 2008).

Según Nguyen (1998), consiste en una técnica de *management* que identifica un problema crítico o incertidumbre que amenaza el éxito de un proyecto, focaliza la atención en él, toma acciones ofensivas para evitarlo, e implementa planes para neutralizar o minimizar su impacto, incluyendo planes para incrementar los resultados de eventos positivos.

Dichas etapas son reflejadas en el proceso descripto por el PMI (2008). En primer lugar se debe realizar la Planificación de la Gestión de Riesgos, proceso por el cual se define la forma de llevar a cabo las actividades de gestión de riesgos. Posteriormente se realiza la Identificación de los Riesgos, en la cual se determinan los eventos legítimos y manejables que se oponen al proyecto y se documentan sus características para luego realizar el Análisis Cualitativo de Riesgos, que consiste en establecer un orden de prioridad para posteriormente realizar acciones de evaluación y análisis de probabilidad de ocurrencia e impacto de los mismos.

En dicho proceso los riesgos se pueden identificar y describir a varios niveles de detalle, dependiendo de las necesidades del usuario de la información y las decisiones que deba adoptar. Puede existir una variación considerable entre proyectos u organizaciones distintas.

Una herramienta útil para guiar la definición del grado de detalle a utilizar en la descripción de riesgos es la *Risk Breakdown Structure.*

2.3. Conceptualización de la *Risk Breakdown Structure*

La RBS busca el agrupamiento y organización de los riesgos a los que está expuesto un proyecto de acuerdo a su fuente. Cada nivel inferior dentro de la estructura representa una definición con un creciente grado de detalle (Hillson, 2002a).

El PMI (2008) la define como una descripción jerárquica de los riesgos del proyecto, organizados por categorías y subcategorías que identifican las distintas áreas de posibles riesgos. La estructura de desglose del riesgo a menudo suele adaptarse para tipos de proyectos específicos.

Las categorías de riesgos incluyen grupos de posibles causas de riesgo tales como técnica, externa, de la organización, ambiental o de dirección de proyectos. Una categoría puede incluir subcategorías como madurez técnica, clima o estimación agresiva.

La visualización de los riesgos a un solo nivel puede no brindar información lo suficientemente útil para satisfacer toda necesidad. Es por ello que la ubicación de los riesgos en una estructura como la descripta otorga valor al proyecto.

Mediante el ordenamiento de los riesgos en tantos niveles como sean necesarios permite a la RBS proveer la flexibilidad necesaria para realizar distintos tipos de análisis y tomar diferentes decisiones.

Facilita así las tareas de comprensión, identificación y evaluación de los riesgos, asegurando la cobertura de la totalidad de fuentes de riesgo, indicando aquellas que resultan críticas para el proyecto y brindando una base de datos para futuros proyectos. En base a ello, es posible desarrollar planes de respuesta robustos basados en las verdaderas causas que los desencadenan (Hillson, 2002a, 2002b; PMI, 2008).

En lo que respecta a la elaboración de una RBS, Holzmann et al. (2010) proponen utilizar una metodología *bottom-up*, agrupando los ítems de riesgo en áreas. En contraposición existe

el método tradicional de *top-down*, en el cual en primer lugar se definen las áreas de riesgo y luego a ellas se les asignan ítems cada vez más específicos.

La identificación puede realizarse a partir de supuestos, escenarios hipotéticos o predicciones a los que un proyecto u organización podría verse expuesto, o bien a partir de experiencias reales y actuales que en base a información del pasado permitan definir áreas de riesgo a los que una organización está sujeta en función de los proyectos y actividades que ejecuta.

En la categorización, al nivel superior (Nivel Cero), todo riesgo es simplemente "Riesgo del Proyecto". Luego se puede dividir en fuentes de riesgo relevantes al Nivel Uno, tales como riesgo técnico, riesgo comercial, riesgo de gestión, riesgo externo y así sucesivamente en niveles inferiores. Cada uno de ellos puede a su vez subdividirse en categorías con mayor grado de detalle

Existen dos alternativas en relación con la aplicación de esta herramienta, que son la RBS Genérica y la RBS aplicada a una industria.

La primera aplica a cualquier tipo de organización o proyecto y consiste en una categorización de riesgos internos y externos al ente. Cada uno de ellos puede subdividirse en diversas áreas, como ser riesgos económicos, físicos, políticos y tecnológicos en el caso de los externos. Los internos suelen dividirse de acuerdo a los *work package o categoría.* Luego están los riesgos globales no asociados a ninguna categoría en particular. Asimismo se han propuesto clasificaciones de acuerdo a los riesgos inherentes a las etapas del ciclo de vida de un proyecto (Holzmann et al., 2010).

Como caso particular se puede citar al trabajo realizado por el R*isk Management Specific Interest Group* del *Proyect Management Institute* (PMI Risk SIG) en conjunto con el *Risk Management Working Group* del *International Council On Systems Engineering* (INCOSE RMWG), quiénes formularon un Proyecto Universal de Riesgos, que contempla una lista global de áreas de riesgos que pueden aplicar a cualquier tipo de proyecto de cualquier sector de actividad industrial, gubernamental o comercial (Hillson, 2002a; Holzmann et al., 2010).

Dada la variedad de objetivos y características de los proyectos, cada RSB es diferente y posee la cantidad de niveles de riesgo considerada adecuada para el caso en particular. Las versiones de RBS genéricas suelen utilizarse como puntos de partida, pero no representan un enfoque completo de los riesgos de un proyecto en particular, de modo que deben ser adecuadas en cada caso (Hillson, 2002a, 2002b; Holzmann et al., 2010).

Las RBS Orientadas a una Industria son casos particulares de aplicación de la herramienta a un tipo de proyecto determinado. Existen diversos casos de desarrollo de la RBS en áreas muy variadas, como ser proyectos de construcción suministro de energía, desarrollo de vacunas farmacéuticas, telecomunicaciones, entre otros (Tummala & Burchet, 1999; Chapman, 2001; Miller & Lessard, 2001; Dey, 2002 citados por Hillson 2002a).

Distinto de los casos anteriores es la alternativa implementada por algunas organizaciones, la cual consiste en la elaboración de una única estructura de desglose general que abarca la totalidad de sus proyectos. Si bien resulta útil para tener una visión del conjunto de riesgos a los que el ente se encuentra expuesto, los proyectos complejos que se encuentre ejecutando podrían requerir la aplicación de RBS específicas (Hillson, 2002b).

2.4. RBS aplicada a la industria de tecnología de información

En el caso particular de la industria del *software* y la tecnología de información existe el antecedente de una RBS conocida como *risk taxonomy* o *Taxonomy-Based Risk Identification*,

del *Software Engineering Institute* (Carr, Konda, Monarch, Ulrich & Walker, 1993; Williams et al., 1999, citados por Holzmann et al., 2010; Hillson, 2002a; Dorofee et al., 1996).

La misma describe el proceso por el cual los riesgos de cada proyecto específico de desarrollo de *software* son identificados y agrupados en tres categorías: ingeniería de producto - referidos a requerimientos, diseño, *code* y *unit test*, tests de integración y especialidades de ingeniería-, ambiente de desarrollo – incluye los elementos de procesos de desarrollo, sistemas de desarrollo, procesos de *management*, métodos de *management* y ambiente de trabajo- y por último, limitaciones del programa, que incluyen recursos, contratos e interfaces del programa.

Otro caso es el de Holzmann et al. (2010), quiénes desarrollaron una RBS para una empresa de tecnología de información de Israel. Su metodología en particular se basó en la identificación de los riesgos mediante el estudio de la documentación que le proporcionó la empresa, y a partir de los códigos de riesgos encontrados utilizaron el método de *clustering* para elaborar la RBS. Los *managers* de la organización consideraron apropiada la metodología utilizada, prefiriendo la utilización de la experiencia pasada en lugar de escenarios y suposiciones para la identificación de los riesgos a los que están sujetos.

El resultado encontrado fue que los dos niveles más amplios de riesgos estaban dados por las especificaciones de producto y definición del trabajo, y por la participación del cliente y la comunicación. Se concluyó que la principal fuente de riesgo en este tipo de organización son los recursos humanos.

3. METODOLOGÍA

El presente estudio de carácter exploratorio y descriptivo se enfoca en identificar características del tema de estudio, comprendiendo y profundizando el conocimiento del fenómeno dentro de su contexto (Hernández Sampieri, Fernandez Collado & Baptista Lucio, 2010; Mendez Alvarez, 2000), pretendiendo crear interrogantes a ser respondidos en futuras investigaciones.

Se pretende indagar y conocer acerca de los riesgos asociados a proyectos de implementación de infraestructuras tecnológicas dinámicas en una organización, en particular el caso de *cloud computing* para la gestión de actividades en entidades financieras de la República Argentina, considerando la aplicación de un modelo de Infraestructura como un Servicio, donde la entidad desarrolla las aplicaciones a ser ejecutadas en la nube.

Los conceptos desarrollados en el marco teórico son aplicados para la elaboración de una RBS aplicada a dicha situación, brindando una herramienta para la identificación y estructuración de riesgos.

Para cumplir el objetivo planteado se analizaron las disposiciones del Banco Central de la República Argentina, en su calidad de organismo de contralor de las entidades financieras, relacionadas con la implementación de estructuras de tecnología informática en dichos entes y con la tercerización del servicio de TI, elaborando la RBS para la implementación de *cloud computing* sólo para aquellos servicios que se admite sean prestados por un tercero.

Se utilizó un enfoque de RBS orientada a una industria, elaborando un modelo genérico (Holzmann et al., 2010), de modo que la estructura aquí presentada debe ser analizada en cada caso de aplicación particular, considerando las características de la entidad, el proyecto de implementación de *cloud computing*, los objetivos específicos y el ambiente de control del ente, entre otras cuestiones.

Los datos que constituyen la base para la elaboración del modelo han sido obtenidos de listas de riesgos desarrolladas por múltiples organismos y autores que estudian acerca de *cloud computing*. El principal aporte fue el trabajo de la *European Network and Information Security Agency* (ENISA, 2009), una agencia de la Unión Europea cuyo objetivo consiste en brindar recomendaciones e información sobre buenas prácticas relacionadas a seguridad de la información.

Se utilizó también la estructura conocida como *Taxonomy-Based Risk Identification,* método para la identificación recurrente de riesgos asociados a proyectos de desarrollo de *software* elaborado por el *Software Engineering Institute* (Carr et al., 1993). Se consideró útil en la medida en que ha sido presentado con un formato de RBS por autores como Hillson (2002b) y Dorofee et al. (1996).

Los riesgos allí identificados fueron corroborados y complementados por otros autores que los respaldan (NIST, 2010; Montahari, Stephenson & Singhal, 2009; ISACA, 2009; Armbrust et al., 2009; Svantesson & Clarke, 2010; Mowbray, 2009; CSA, 2010; Holzmann et al., 2010; entre otros).

Una vez obtenidos los datos fueron confrontados con la normativa emanada del BCRA en lo referente a riesgos relacionados con la utilización de TI y tercerización de servicios. Específicamente se consideró como fuente de datos las Comunicaciones A 2529 y A 5042 sobre normas mínimas sobre control interno para entidades financieras y la Comunicación A 4609 que se ocupa específicamente de la regulación de riesgos relacionados a TI, sistemas de información y recursos asociados para las entidades financieras.

Una vez identificados los riesgos y analizados los mismos dentro del marco y normativa mencionada vigente en la Argentina, se elaboró una *Risk Breakdown Structure* que pretende servir como herramienta para la gestión de riesgos a ser utilizada por los profesionales y gerentes de entidades financieras para la ejecución de proyectos de esta índole.

4. RESULTADOS

4.1. Aplicación de *cloud computing* en entidades financieras

Siendo que las entidades financieras realizan un significativo uso de la información, *cloud computing* puede brindarles importantes beneficios para mejorar su gestión. El banco australiano Commonwealth Bank es un ejemplo, habiendo iniciado tratativas en el año 2009 con diversos proveedores con el objetivo de superar los servicios básicos brindados por las entidades financieras (Foo & Sharma., 2009; Foo, 2010).

Las principales ventajas que otorgan las infraestructuras dinámicas a estas organizaciones se refieren a la posibilidad de utilizar los servicios computacionales – almacenamiento, capacidad, ancho de banda, etc. – en función de las necesidades de cada momento y con un precio de acuerdo al nivel de uso, generando reducciones de costo y mayor agilidad en el aprovisionamiento y uso de recursos de *hardware* y *software.* La mayor eficiencia les permite focalizarse en el desarrollo de productos y servicios, y en el caso de entes pequeños, el acceso a facilidades que no podrían crear *in house* dadas sus restricciones de recursos.

Sin embargo, a pesar de los beneficios que puede reportar a la industria de las entidades bancarias y similares, se espera una adopción lenta de la computación en nube (Jaworski, 2009), al igual que en el resto de los sectores de la economía.

La principal barrera a la aplicación de esta tecnología para la gestión en un sector como el financiero es la seguridad del significativo volumen de datos sensibles que se manejan. Los

bancos que deben utilizar aplicaciones basadas en normativas y marcos de referencia fuertes son los que enfrentan las mayores restricciones para la implementación, dado que muchos de sus requerimientos pueden no ser cumplidos, debido a que las cuestiones de regulación y seguridad son más rigurosas.

El interés por su implementación ha llevado a que se realicen esfuerzos para aprovechar su potencial en la industria, habiéndose comenzado a experimentar con la herramienta para uso en el sector financiero (Cohen, 2008).

Ante las importantes ventajas que *cloud computing* puede brindarle al sector financiero, y siendo la evaluación de los riesgos asociados una tarea indispensable para su implementación, se hace necesario desarrollar herramientas que colaboren con la identificación de los mismos de manera que puedan ser correctamente gestionados (sea reduciéndolos, eliminándolos, transfiriéndolos a terceros o aceptándolos).

4.2. Diseño de *Risk Breakdown Structure* propuesto

El trabajo en un ambiente computarizado otorga beneficios a la hora de llevar a cabo el procesamiento de la información. Sin embargo, los riesgos van variando en dicho proceso, y se requiere una redefinición de los mismos, los controles y la legislación acorde al nuevo contexto.

El BCRA establece en su normativa que las autoridades de cada entidad deben procurar y observar la existencia de políticas y procedimientos para administrar el riesgo relacionado a los sistemas de información y la tecnología informática implementada por la organización. Deben tomar conocimiento de los análisis de riesgos realizados para estar en condiciones de de gestionar las debilidades que expongan a la entidad a niveles de riesgo alto o inaceptable y sean corregidas a niveles aceptables.

Este tipo de exigencias requiere herramientas que permitan una adecuada identificación y exposición de los mencionados riesgos, a efectos de facilitar el análisis y gestión por parte de las autoridades de la entidad, así como el reporte de los mismos a los organismos de contralor.

El presente trabajo propone en consecuencia una RBS aplicada a dichos proyectos. La organización de los riesgos se realizó sobre la base de la *Risk Breakdown Structure* expuesta en la **Figura 1**. El Nivel Cero de riesgos representa el conjunto de riesgos asociados al proyecto de implementación de *cloud computing* por una entidad financiera.

El Nivel Uno describe una serie de fuentes de riesgo que coinciden con la clasificación que deben utilizar las entidades financieras para elaborar sus informes de riesgos destinados al ente de contralor, incluyendo en este caso riesgos reputacionales, de cumplimiento, legales y operativos. Dentro de cada una de las fuentes se ejemplifican riesgos asociados.

En primer lugar se exponen los riesgos reputacionales, referidos a la publicidad negativa relacionada con las políticas y prácticas la entidad, sean ciertas o no, que tenga como consecuencia un impacto adverso en los clientes de la misma, en acciones legales o disminución de ingresos

En el caso de la implementación de *cloud computing*, al compartir recursos con múltiples usuarios puede suceder que las actividades maliciosas desarrolladas por uno de ellos afecte la reputación de los demás. En el sector financiero donde se procesan datos especialmente sensibles acerca de los clientes este tipo de riesgos es de alto impacto necesitando controles eficientes para gestionarlos.

Los riesgos de cumplimiento se refieren a las leyes y normas aplicables a la industria. A pesar del uso de *cloud*, la responsabilidad última de cumplimiento es del usuario, siendo las sanciones por incumplimiento aplicadas sobre la entidad financiera.

En el proyecto aquí analizado, resulta indispensable el cumplimiento de las normas dictadas por el BCRA referidas a los requisitos mínimos de TI y de sistemas de información, que deben ser cumplidos no solo por la entidad financiera, sino también por el proveedor de *cloud computing* o cualquier tercero a quien se le delegue alguna actividad vinculada.

El incumplimiento genera el riesgo de que la autoridad de contralor cancele la autorización para la tercerización del servicio debiendo ser nuevamente gestionados por el ente perdiéndose los beneficios de las infraestructuras tecnológicas dinámicas.

Figura 1:
RBS - Implementación de *cloud computing* en entidades financieras.

NIVEL 0	NIVEL 1	NIVEL 2	NIVEL 3
Riesgo del Proyecto: Implementación de *cloud computing* por una entidad financiera	**Reputacional**	Efecto del uso de recursos compartidos en la reputación de la entidad financiera	
	Cumplimiento	Normas BCRA de requisitos mínimos de los sistemas informáticos y de información	
		Normativa sobre tratamiento de datos de clientes	
		Cumplimiento de requisitos de certificaciones	
	Legales	Demandas o juicios adversos	Divulgación de datos personales
			Cambios de jurisdicción
		Contratos	Contenido del contrato
			Incumplimiento del acuerdo por el proveedor de *cloud computing*
			Adquisición del proveedor de *cloud computing*
	Operativos	Proceso de management	Planeamiento
			Organización del proyecto
			Experiencia de management
			Interfaces del programa
			Lock In
		Requerimientos al sistema	Eficacia
			Eficiencia
			Confiabilidad
			Integridad
			Disponibilidad
			Estabilidad de los requerimientos legales
			Verificacion del sistema
		Seguridad Lógica y de acceso a los datos	Empleado malicioso
			Fallas de aislamiento de la información
			Interceptación de datos en tránsito y fuga de datos
			Eliminación de datos insegura o no efectiva
			Gestión de la identidad
			Software malicioso
			Programas y usuarios privilegiados y de contingencia
			Administración de las bases de datos
		Seguridad física	Accesos no autorizados a las instalaciones
			Pérdida o robos de *back-ups*
			Robo de computadoras
			Desastres naturalse
			Condiciones ambientales
		Disponibilidad del servicio	Falla de la cadena de suministro
			Falla de internet
			Gestión de la red
			Tráfico de la red
		Continuidad del procesamiento electrónico de datos	Planificación de continuidad de la operatoria delegada
			Análisis de impacto
			Instalaciones alternativas de procesamiento de datos
		Ambiente de trabajo	Cooperación y comunicación del personal
			Actitud orientada a la calidad
			Moral
			Connivencia del personal
			Desconocimiento de la tecnología por el personal

Nota: Fuente: Elaboración propia

Se incluyen también los riesgos referidos al incumplimiento por parte del proveedor de requerimientos sobre el tratamiento legal de los datos de los clientes, de protección de propiedad intelectual por las aplicaciones creadas y ejecutadas en la nube, entre otras.

En tercer lugar, dentro del Nivel Uno, se incluyen los riesgos legales, que comprenden aquellos relacionados a contratos incumplidos, demandas o juicios adversos que puedan afectar en forma negativa a las operaciones o a la entidad y sus responsables, separándose en dos grupos en el Nivel Dos.

Los datos del cliente pueden almacenarse en múltiples jurisdicciones, pudiendo ser algunas de ellas de alto riesgo según el marco jurídico vigente en cada estado. En un país donde rige un conjunto de normativas impredecibles, los datos pueden quedar sujetos a divulgación forzada o secuestro o los proveedores pueden utilizarlos con fines ilícitos. Ello genera el riesgo de situaciones litigiosas contingentes por parte de los clientes contra las entidades financieras con alta probabilidad de impactos negativos en los resultados de las mismas.

Los incumplimientos de pautas contractuales o la existencia de cierta informalidad en los acuerdos para la prestación de servicios a través de Internet, junto con modificaciones de las condiciones que suelen adoptar los proveedores de manera unilateral, generan riesgos muy costosos que ninguna entidad financiera puede dejar librado a decisiones del proveedor.

En caso que el proveedor sea adquirido por un tercero implica la probabilidad de un cambio estratégico que puede generar el incumplimiento de ciertas pautas contractuales o de acuerdos no vinculantes - por ejemplo, las interfaces de software, las inversiones en seguridad, los controles de seguridad no contractual - generando incumplimientos en los requisitos de seguridad preestablecidos y acordados. El impacto final podría darse sobre activos esenciales como la reputación de la organización, la confianza de clientes y la lealtad de los empleados.

La última fuente identificada dentro del Nivel Uno es la de riesgos operativos. Con una definición amplia, incluye todos aquellos riesgos de pérdidas directas o indirectas que resulten de procedimientos internos, recursos humanos o fallas o inadecuación de los sistemas.

Dentro de ella se definieron siete sub-categorías, donde la primera reúne los posibles eventos desfavorables asociados al proceso de *management* del proyecto. Por ejemplo, la inexistencia de una planificación adecuada implica el riesgo de que los sistemas de información y tecnologías asociadas no respondan a las necesidades de la entidad financiera o no se alineen con los planes estratégicos de la misma.

La definición previa de la estructura organizativa, con una identificación clara de los roles y responsabilidades, resulta fundamental, dado que una incorrecta separación y definición de funciones pueden llevar al fracaso del proyecto. Según el BCRA es obligatoria la creación de áreas dedicadas a la gestión de la seguridad y al soporte, registro y seguimiento de los incidentes que surjan con los sistemas, la tecnología informática y los recursos asociados, sumamente importantes en el tipo de proyecto aquí descripto.

La falta de experiencia de los gerentes en relación con la gestión de proyectos de implementación de software, más aún de *cloud computing* – dado su reciente desarrollo – puede ser una fuente de riesgos relevante si no se realiza una adecuada capacitación de la dirección. También se incluyen aquí los riesgos asociados a las interrelaciones de los gerentes de diferentes niveles y áreas con el personal encargado del proyecto de implementación de *cloud computing*, así como sus relaciones con personas ajenas a la organización implicadas en el mismo.

Una cuestión particular a tener en cuenta en la etapa de selección del proveedor del servicio es el riesgo de *lock in*, cuestión que debe ser considerada en el proceso de gestión del proyecto dentro de la administración de relaciones. Una vez contratado un servicio, se genera

cierta dependencia con el proveedor elegido, existiendo dificultades para poder migrar de un prestador a otro, o volver al entorno de TI interno, propio de la entidad.

La Comunicación A 4609 anteriormente mencionada establece un conjunto de normas a ser respetados por los recursos intervinientes en los procesos de tecnología informática, a saber: datos, sistemas de aplicación, tecnología, instalaciones y personas. En el modelo son agrupados en una categoría de riesgos que se ha denominado requerimientos del sistema.

La norma requiere que el procesamiento en la nube resulte eficiente, brindando información relevante, pertinente, correcta, coherente, completa y que pueda ser utilizada en forma oportuna para la toma de decisiones. La eficiencia en este caso puede verse afectada por dos riesgos: el uso excesivo de recursos para el desarrollo, implementación, mantenimiento y actualización de los sistemas, de modo que se vea vulnerada la relación costo-beneficio derivados de la utilización de *cloud computing*, y la escasez de recursos, lo cual no permitiría el adecuado desarrollo de las actividades asociadas a esas etapas, de modo que los buenos resultados no se alcanzarían por falta de personal, de tiempo, de dinero, etc.

La integridad, disponibilidad y confiabilidad son requisitos que debe cumplir la información obtenida de las aplicaciones ejecutadas en la nube, donde los sistemas deben cumplir con las expectativas del usuario y facilitar la toma de decisiones así como la presentación de informes al Banco Central de la República Argentina y demás organismos reguladores.

Por último se incluyen la estabilidad de requerimientos legales y la posibilidad de verificación del sistema. En caso de no cumplirse pueden llevar a la falla en la detección de errores así como a modificaciones permanentes del sistema creado, con aplicaciones obsoletas en el corto plazo, modificaciones incompatibles con el desarrollo en el sistema de *cloud*, imposibilidad de realizar evaluaciones de la robustez y de penetración al encontrarse dentro de la plataforma de un tercero, etc.

Las dos categorías que siguen se refieren a los riesgos vinculados a la seguridad, en sus dos versiones, lógica y física. El BCRA exige que los proyectos informáticos contemplen sus requerimientos desde sus etapas iniciales, con el objetivo de asegurar el diseño y la implementación de apropiados controles y registros, como así también la correcta selección de tecnología que haga a la solución integral de la misma.

En cuanto a la seguridad lógica, se incluyen los riesgos asociados al acceso privilegiado que poseen los empleados del proveedor de *cloud* a información confidencial; el fracaso de los mecanismos de separación de la información debido a que los recursos en nube son compartidos por múltiples usuarios; la interceptación de datos en tránsito entre el cliente y el proveedor y dentro de la nube en sí misma – requiriendo técnicas de encriptación efectivas –; así como el riesgo de que los datos puedan estar disponibles más allá de la vida útil especificada en la política de seguridad del usuario en el caso en que la eliminación por él solicitada no sea respetada por el proveedor de la nube.

La necesidad de uso de contraseñas para el acceso a aplicaciones y datos genera un riesgo adicional. Se incluye la pérdida de contraseñas, la transferencia de las mismas entre usuarios, o los accesos no autorizados por técnicas más sofisticadas como es el caso de *hackers* y delincuentes de la *web*.

El resto de las fuentes de riesgo incluidas podrían ocasionar, en forma intencional o no, la modificación no autorizada, la destrucción o exposición de datos. Las mismas deben ser analizadas y gestionadas adecuadamente mediante la creación de controles específicos.

Los riesgos vinculados a la seguridad física se refieren a las necesidades de resguardo de la información y continuidad del procesamiento. Incluyen accesos no autorizados a las instalaciones, pérdidas o robos de *back ups*, robos de computadoras, desastres naturales,

condiciones ambientales desfavorables. La redundancia de sitios de almacenamiento de la información exigida por el BCRA, y provista como un servicio por *cloud computing* es un modo de evitar las consecuencias de este tipo de riesgos, sin embargo deben ser tenidos en cuenta, principalmente aquellos que implican la posibilidad de robo y divulgación de información.

Todas estas cuestiones de seguridad aplican no sólo a la entidad financiera, sino también al proveedor de *cloud computing*.

Al decidir implementar infraestructuras tecnológicas dinámicas, las entidades deben contemplar las cuestiones relacionadas con la disponibilidad de los servicios informáticos. Su actividad se desarrolla en un horario acotado y, en gran medida, mediante la atención al público. En este ámbito, la interrupción de sistema seguido de la insatisfacción de las demandas de los clientes puede generar daños económicos y en la imagen de la empresa.

Al utilizar un servicio basado en Internet, se suman riesgos tales como la falta de conexión y la congestión de la red que pueden generar interrupciones, errores o dificultades para el procesamiento de las operaciones.

También se han incluido en esta categoría riesgos asociados a las fallas en la cadena de suministro, que se dan en aquellos casos en los que el proveedor de *cloud computing* hubiera externalizado ciertas tareas especializadas de la prestación del servicio a terceros.

La continuidad es considerada como un proceso que se inicia con la recuperación durante una contingencia y concluye con el regreso a la normalidad una vez controladas las causas que la generaron. El BCRA establece un conjunto de pautas a ser respetadas, en las que se incluye la responsabilidad de la entidad de controlar su aplicación por parte de los terceros a fin de garantizar la continuidad de las actividades delegadas.

La inexistencia de un adecuado análisis de impacto de las eventualidades, la falta de un plan de recuperación del procesamiento de datos actualizado, coordinado entre la entidad y el proveedor de *cloud computing* y acorde a los requerimientos de negocio de la entidad y los niveles de riesgos asumidos por la misma, y la falta de pruebas periódicas sobre los planes existentes, generan el riesgo de que ante una eventualidad no se logre volver a una situación operativa en los tiempos considerados adecuados, exponiéndose a la perdida de información y a reclamos de los clientes.

El último grupo de riesgos considerado dentro de la fuente de riesgos operativos es el vinculado al ambiente de trabajo. Aquí se ven reflejados todos aquellos aspectos relacionados a las características de las personas que participan en el proyecto y la naturaleza de sus funciones en este caso en particular.

Las fallas en la comunicación, la cooperación y el compromiso con la calidad representan un riesgo importante. Sin un conocimiento adecuado de los objetivos del proyecto, de la importancia y el impacto que tiene para la entidad financiera la implementación de este tipo de herramientas, así como en la colaboración del los integrantes, difícilmente podrán obtenerse buenos resultados.

La moral de los empleados, incluye la motivación, performance, productividad y creatividad. Las posibilidades de connivencia entre el personal en detrimento de los objetivos organizacionales son riesgos que se asocian al hecho de que son conocedores privilegiados de información relevante que pueden utilizar en su propio beneficio comprometiendo la actividad de la entidad.

Finalmente, la falta de conocimientos adecuados pone en riesgo cualquier proyecto, en especial uno de implementación de *cloud computing* en un sector fuertemente regulado como lo es el sector financiero argentino, en donde hacen falta conocimientos técnicos y legales para garantizar el cumplimiento de los objetivos organizacionales.

Tal como lo expusieron Holzmann et al. (2010), los principales focos de riesgo en las organización y proyectos dedicados a la tecnología de información son los recursos humanos, de modo que debe prestarse especial atención.

La presente definición de la RBS es un punto de partida para la posterior evaluación de riesgos y el diseño de controles que permitan minimizar sus efectos y garantizar el cumplimiento de los objetivos organizacionales.

5. CONSIDERACIONES FINALES

Avanzar en un proyecto sin adoptar un enfoque proactivo en materia de gestión de riesgos aumenta la probabilidad de que la materialización de alguno de ellos pueda conducir al fracaso.

En consecuencia son necesarias herramientas que faciliten la identificación, comprensión y evaluación de riesgos para guiar el diseño de estrategias adecuadas.

Este trabajo propone el diseño de una estructura de riesgos basada en el modelo denominado *Risk Breakdown Structure* con enfoque orientado a una industria, aplicada a la implementación de *cloud computing* en entidades financieras reguladas por el Banco Central de la República Argentina. Para su desarrollo se adoptaron las fuentes propuestas por el mencionado organismo para la presentación de reportes de riesgos al BCRA, clasificándolos en riesgos reputacionales, de cumplimiento, legales y operativos, logrando una amplia cobertura de las eventualidades asociadas al proyecto.

El desarrollo realizado permitió ejemplificar el uso de distintos niveles de acuerdo a las características de las fuentes y las necesidades de los usuarios. En el caso de los riesgos reputacionales y de cumplimiento sólo se definieron tres niveles, utilizándose cuatro en el caso de los legales y operativos. Cuanto mayor sea la cantidad de niveles, mayor será el detalle de riesgos asociados a cada fuente, pudiendo generarse distintos reportes de riesgos, informando a los estratos más altos de la compañía aquellos niveles de riesgo superiores y los de mayor detalle a quienes ejecutan los planes de acción.

En el modelo se puede apreciar que la fuente de riesgos operativa es sin duda una categoría crítica, con un amplio espectro de posibles eventos a ser tenidos en cuenta y por ende mayor cantidad de apertura. Ello denota la necesidad de prestarle especial atención al momento de definir las acciones de gestión de riesgos asociadas.

A efectos de maximizar el objetivo de gestión de riesgos, en una futura investigación se incorporará al modelo propuesto un análisis de riesgo considerando la probabilidad de ocurrencia e impacto. Su cuantificación permitirá disminuir el nivel de subjetividad en la evaluación de los riesgos asociados al proyecto.

A partir de la herramienta propuesta, los *managers* del proyecto podrán realizar una comparación con otros servicios informáticos de modo de seleccionar la mejor opción entre las alternativas posibles. A modo de ejemplo se puede mencionar la adopción de estructuras del tipo *cloud computing* o el desarrollo y ejecución *in house* de los procesos, siempre dentro del marco de la normativa vigente. Las bases de datos creadas sobre riesgos y actividades de gestión para un proyecto particular, junto con los resultados de las decisiones, podrán ser utilizadas como soporte de futuras decisiones.

La principal limitación encontrada consiste en que es incipiente la implementación de esta tecnología en las organizaciones argentinas, más aún en el sector financiero.

Se pretende que la propuesta realizada sirva a los directivos de las entidades financieras como punto de partida para sus análisis, en la medida en que este tipo de tecnologías surgen y

se posicionan en el mercado como una alternativa fuerte que puede brindar múltiples beneficios en el procesamiento de la información.

6. BIBLIOGRAFÍA

1. Armbrust M., Fox A., Griffith R., Joseph A. D., Katz R., Konwinski A., et al. (2009). Above the clouds: a Berkeley view of Cloud computing. *UC Berkeley Reliable Adaptive Distributed Systems Laboratory.* Consultado el 06 de Septiembre de 2010 en http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

2. Banco Central de la República Argentina (1997a). Comunicación A 2529 - Normas Mínimas sobre Controles Internos. Complemento. Disponible en http://www.bcra.gov.ar/pdfs/comytexord/A2529.pdf

3. ____ (1997b). Comunicación A 4609. Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información. Disponible en http://www.bcra.gov.ar/pdfs/comytexord/A4609.pdf

4. ____ (2004). Comunicación A 4192 - Requisitos Operativos Mínimos de Tecnología y Sistemas de Información para las Casas y Agencias de Cambio. Disponible en http://www.bcra.gov.ar/pdfs/comytexord/A4192.pdf

5. ____ (2010). Comunicación A 5042. Normas Mínimas sobre Auditorías Externas y Controles Internos para Entidades Financieras. Texto Ordenado. Disponible en http://www.bcra.gov.ar/pdfs/comytexord/A5042.pdf

6. Carr M. J., Konda S. L., Monarch I., Ulrich F. C., & Walker C. F. (1993). *Taxonomy-Based Risk Identification.* Software Engineering Institute - Carnegie Mellon University. Pittsburgh, Pennsylvania, USA.

7. Cellary W. & Strykowski S. (2009). E-Government Based on Cloud Computing and Service-Oriented Architecture. ICEGOV2009.

8. Cloud Security Alliance – CSA (2010). *Top Threats to Cloud Computing V1.0.* Consultado el 17 de Septiembre de 2010 en http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

9. Cohen R. (2008/07/25). Cloud Computing – Morgan Stanley is Banking on the Cloud. SYS-CON Media, Inc. Consultado el 16 de Marzo de 2011 en http://weblogic.sys-con.com/node/589951

10. Crosman P. (2010/08/16). BS&T Survey: Banks Take to Cloud Computing. Bank Systems and Technology. Consultado el 16 de Marzo de 2011 en http://banktech.com/architecture-infrastructure/226100004.

11. Dorofee A. J., Walker J. A., Alberts C. J., Higuera R. P., Murphy R. L., & Williams R. C. (1996). *Continuous risk management guidebook.*USA: Carnegie Mellon University – Software Engineering Institute.

12. European Network and Information Security Agency - ENISA (2009). *Cloud Computing - Benefits, risks and recommendations for information security.* Consultado el 20 de Enero de 2010 en http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

13. Estupiñán Gaitán, R. (2006). *Control Interno y Fraudes* (2da ed.). Bogotá: Ecoe Ed.

14. Federación Argentina de Consejos Profesionales en Ciencias Económicas (2007), CECyT *Informe 15. Área Auditoría. Auditoría en ambientes computarizados.* Buenos Aires.

15. Foo F. (2010/05/11). Commonwealth Bank works with Amazon to set up cloud-based operation in Australia. Consultado el 17 de Marzo de 2011 en

http://www.theaustralian.com.au/australian-it/commonwealth-bank-works-with-amazon-to-set-up-cloud-based-operation-in-australia/story-e6frgakx-1225864730999

16. Foo F., & Sharma M. (2009/10/06). Banks looks to cloud to blow away licence costs. The Australian. Consultado el 16 de Marzo de 2011 en http://www.theaustralian.com.au/australian-it/cba-banks-on-cloud-computing/story-e6

17. Gartner Group. Consultado el 12 de Agosto de 2009. Disponible en http://www.gartner.com/technology/home.jsp.

18. Hernández Sampieri R., Fernandez Collado C. & Baptista Lucio P. (2010). *Metodología de la investigación* (5ta ed.). México: Grupo Infagon.

19. Hillson, D. (2002a). Use a Risk Breakdown Structure (RBS) to Understand Your Risks. *Proceedings of the Project Management Institute Annual Seminars & Symposium*. 3 al 10 de Octubre de 2002. San Antonio, Texas, USA.

20. ____ (2002b). The Risk Breakdown Structure (RBS) as an aid to effective risk management. *Fifth European Project Management Conference, PMI Europe 2002*. 19 al 20 de Junio de 2002. Cannes, Francia.

21. Holzmann V., & Spiegler I. (2010). Developing risk breakdown structure for information technology organizations. *International Journal of Proyect Management*, doi: 10.1016/j.ijproman.2010.02.002.

22. Information Systems Audit and Control Association - ISACA (2009). Cloud computing – Business Benefits with security, governance and assurance perspectives. White paper. Consultado el 19 de Enero de 2010 en http://www.isaca.org/Knowledge-Center/Research/Documents/Cloud-Computing-28Oct09-Research.pdf.

23. Jaworski A. (2009). Survey: Banks Slow to Adopt Cloud Computing. *Information Management Online*. Consultado el 16 de Marzo de 2011 en http://www.information-management.com/news/cloud_computing_financial_services_bank-10015811-1.html?zkPrintable=true

24. Joint A., Baker E., & Eccles E. (2009). Hey, you, get off of that cloud?. *Computer and security review*, *25*, 270-274.

25. Kangarloo K. (2010/03/09). More small-to mid-size Banks embrance cloud computing. Consultado el 16 de Marzo de 2011 en http://www.fiercecomplianceit.com/story/more-small-mid-size-banks-embrace-cloud-computing/2010-03-09

26. Leem C. S., & Lee H. (2004). Development of certification and audit processes of application service provider for IT outsourcing. *Elsevier, Technovation, 24*, 63-71.

27. López M. A., Sánchez M. A., & Albanese D. E. (2010). Impacto del uso de Soluciones Informáticas basadas en *Cloud Computing* para el procesamiento de la Información Contable en la Auditoría Financiera. 16° Encuentro Nacional de Investigadores Universitarios del Área Contable ISSN 1853-4155 y 6° Simposio Regional de Investigaciones Contables ISSN 1852-8511. Universidad Nacional de La Plata. 02 y 03 de Diciembre de 2010. La Plata, Buenos Aires, Argentina.

28. Mendez Alvarez, C. E. (2000). *Metodología. Guía para elaborar diseños de investigación en Ciencias Económicas, Contables y administrativas*. Colombia: McGraw-Hill.

29. Montahari-Nezhad H., Stephenson B., & Singhal S. (2009). Outsourcing Business to Cloud Computing Services: Opportunities and Challenges. HP. *IEEE Internet Computing, Special Issue on Cloud Computing.*

30. Mora, C. A.V., Mauro J. C., & Villacorta Cavero A. (2001). *La auditoría ante las operaciones con evidencias virtuales*. XXIV Conferencia Interamericana de contabilidad. Punta del Este – Uruguay. 18 al 21 de Noviembre de 2001.

31. Mowbray M. (2009). The Fog over the Grimpen Mire: Cloud Computing and the Law. *Scripted Journal of Law, Technology and Society, 6* (1).

32. National Institute of Standards and Technology – NIST (2010). www.nist.gov

33. Nguyen N. M. (1998). Effective Risk Management for Proyect Managers: A 21st Century Approach. *29th Annual Project Management Institute 1998 Seminars & Symposium.* Long Beach, California, USA. 9 al 15 de Octubre de 1998.

34. Proyect Management Institute - PMI (2008). *Guía de los Fundamentos para la Dirección de Proyectos* (Guía del PMBOK®) (4ta ed.). Pennsylvania: Project Management Institute, Inc.

35. Senft S. & Gallegos F. (2009). *Information Technology Control and Audit* (3era ed.). USA: Auerbach Publications

36. Smith J. A., Morris J., & Ezzamel M. (2005). Organizational change, outsourcing, and the impact on management accounting. *The British Accounting Review*, *37* (4), Pages 415-441.

37. Svantesson D., & Clarke R. (2010). Privacy and consumer risks in cloud computing. *Computer and security review, 25*, 397-397.

38. Winterford B. (2010/07/06). Interview: Inside the Commonwealth Bank's cloud. iTnews for australian business. Consultado el 17 de Marzo de 2011 en http://www.itnews.com.au/Tools/Print.aspx?CIID=218889