López, María de los Ángeles; Albanese, Diana; Sánchez, Marisa Analía

GESTIÓN DE RIESGOS PARA LA ADOPCIÓN DE LA COMPUTACIÓN EN NUBE EN ENTIDADES FINANCIERAS DE LA REPÚBLICA ARGENTINA

Contaduría y Administración

2014, vol. 59, no. 3, p. 61-88

López, M. A., Albanese, D., Sánchez, M. A. (2014). Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina. Contaduría y Administración. En RIDCA. Disponible en: http://repositoriodigital.uns.edu.ar/handle/123456789/4245

Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina

Fecha de recepción: 11.09.2012 Fecha de aceptación: 12.04.2013

María de los Ángeles López
Universidad Nacional del Sur
angeles.lopez@uns.edu.ar

Diana Ester Albanese
Universidad Nacional del Sur
dalbanese@uns.edu.ar

Marisa Analía Sánchez
Universidad Nacional del Sur
mas@uns.edu.ar

Resumen

Las infraestructuras tecnológicas dinámicas, entre ellas la computación en nube, representan una nueva alternativa de tecnología de información disponible para administrar las actividades de las organizaciones, en particular en aquellas que hacen un uso intensivo de la información, como las entidades financieras. Al analizar la utilización de estas arquitecturas es fundamental considerar los nuevos riesgos a los que se exponen los entes; esto permite desarrollar estrategias de gestión destinadas a identificarlos, evaluarlos y buscar el modo de minimizar sus efectos. En este sentido son útiles herramientas como la *risk breakdown structure* (RBS), una estructura de jerarquización de fuentes de riesgos que simplifica y sistematiza el análisis. En este trabajo se pretende diseñar una RBS para la identificación y descripción jerárquica de las fuentes de riesgos vinculados a la implementación de la computación en nube en entidades financieras, basándose en la normativa del Banco Central de la República Argentina.

Palabras clave: gestión de riesgos, computación en nube, entidades financieras, *risk breakdown structure*

Cloud computing risk management in Argentine financial institutions

Abstract

Dynamic technological infrastructures, including cloud computing, represent a new alternative of information technology available to manage organizational functions, particularly for those that make intensive use of information such as financial institutions. In the assessment of these architectures, it is essential to consider new risks to which institutions are exposed. This allows developing management strategies to identify and evaluate risks and find ways to minimize their effects. The risk breakdown structure (RBS) is a useful tool to structure hierarchical sources of risks and simplify and systematize the analysis. This work aims to design an RBS for the identification and hierarchical description of sources of risks associated with the implementation of cloud computing in financial institutions based on regulations from Banco Central de la República Argentina.

Keywords: risk management, cloud computing, financial institutions, *risk breakdown* structure

Introducción

Las organizaciones cuentan en la actualidad con una herramienta de suma utilidad para el desarrollo de sus actividades como lo es la tecnología de la información (TI). Al diseñar los ambientes de TI deben seleccionar aquellas alternativas disponibles en el mercado que mejor satisfagan sus necesidades. Una de las oportunidades que hoy en día encuentran es la de las infraestructuras tecnológicas dinámicas, entre ellas la computación en nube —conocida por su nombre en ingles *cloud computing*— que está siendo evaluada para su implementación en diversas industrias.

Esta infraestructura consiste en un modelo de distribución de recursos informáticos a través de Internet, mediante la cual los usuarios acceden a sus aplicaciones y datos en el lugar, momento y durante el tiempo que los necesitan. Desde la perspectiva empresarial, estas nuevas arquitecturas ofrecen múltiples beneficios para la gestión de los negocios; en particular, en sectores en los que se hace un uso intensivo de la información, como es el caso de las entidades financieras. Las nuevas soluciones de TI resultan útiles para procesar, gestionar y utilizar estratégicamente la información para crear nuevos productos y servicios basados en la tecnología, racionalizar costos, cumplir la normativa de entes reguladores, entre otras.

Al momento de considerar la utilización de la computación en nube u otras infraestructuras y tecnologías de información resulta imprescindible realizar un análisis adecuado de los riesgos asociados a su implementación para garantizar resultados satisfactorios como consecuencia de su uso y la sostenibilidad de su utilización dentro de una organización en el tiempo (Holzmann y Spiegler, 2011).

La gestión de riesgos y el diseño e implementación de un sistema de control interno efectivo permiten tomar acciones oportunas frente a hechos contingentes que pudieran afectar el éxito y la rentabilidad organizacional en un ambiente de negocios competitivo (Nguyen, 1998).

Una herramienta útil para la identificación, evaluación y comprensión global de los riesgos es la *risk breakdown structure* (RBS) (Hillson, 2002a, 2002b; PMI, 2008; (Holzmann y Spiegler, 2011), conocida en español como estructura de desglose de riesgos; consiste en un método de identificación de riesgos estructurado que permite el reconocimiento de patrones de exposición a eventos contingentes que podrían afectar a una organización en el cumplimiento de sus objetivos o proyectos. Los mismos son categorizados de acuerdo con sus fuentes, realizándose una descripción jerárquica que facilita el diseño de controles orientados a gestionar aquellas que resultan recurrentes o críticas.

Ante las importantes ventajas que la computación en nube puede brindar al sector financiero —y siendo la evaluación de los riesgos una tarea indispensable para su implementación— resulta útil el desarrollo de una RBS que facilite su identificación para una adecuada gestión, ya sea para reducirlos, eliminarlos, transferirlos a terceros o aceptarlos. De igual forma, facilita y estructura la preparación de informes sobre riesgos que las entidades financieras deben elaborar para uso interno y para su presentación ante las autoridades de contralor, como lo es el Banco Central de la República Argentina, así como para aquellas entidades que operan en este país.

Por lo anteriormente expuesto, 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 la computación en nube en entidades financieras de la República Argentina.

El artículo se encuentra organizado de la siguiente forma: en primer lugar se presenta una revisión de la literatura; luego se expone la metodología aplicada para la elaboración de la RBS, en la cual se indica la estructura propuesta con una descripción detallada de las fuentes y los riesgos identificados; por último, se incluyen las consideraciones finales.

Referencial teórico

La computación en nube como herramienta de gestión para las organizaciones

Al momento de implementar nuevas tecnologías de información para mejorar su gestión, muchas organizaciones optaron por la subcontratación de servicios informáticos, tercerizando —total o parcialmente— las funciones previamente desarrolladas por los departamentos internos de TI.

Las infraestructuras tecnológicas dinámicas son una opción para ello; éstas se basan en la virtualización, que supone el desacople de los recursos lógicos de los elementos físicos, permitiendo que los mismos puedan asignarse en forma más eficiente y efectiva de acuerdo con los niveles de demanda de la organización, brindando mayor flexibilidad y facilitando el desarrollo de nuevas estrategias empresariales.

La computación en nube es un caso particular de aplicación de la virtualización. Según The National Institute of Standards and Technology (NIST) es un modelo que permite el acceso a un conjunto de recursos informáticos configurables compartidos, desde cualquier lugar, a través de una red y según las necesidades de la demanda. Estos recursos pueden ser aprovisionados y liberados rápidamente y con un mínimo esfuerzo de gestión o interacción por parte del prestador del servicio; incluyen, por ejemplo, redes, servidores, almacenamiento, correo electrónico, aplicaciones y servicios (NIST, 2011). Dicha arquitectura comprende las aplicaciones provistas como servicios a través de Internet, el *hardware* y los sistemas de *software* en los *data centers* que brindan dichos servicios (Armbrust *et al*., 2010).

Existen diversos modelos de servicios que la caracterizan, entre los cuales una organización puede elegir según su conveniencia: a) el *software* como un servicio (*software as a service*, SaaS) en el que las aplicaciones de *software* son ofrecidas y utilizadas en Internet, constituyendo una alternativa frente a las adquisición y ejecución de paquetes para uso propio en forma local. El usuario no controla

ni manipula la infraestructura subyacente ni las aplicaciones individuales. Como ejemplo se pueden citar los servicios de procesadores de texto y planillas de cálculo *on line*, como los provistos por google docs, adobe photoshop y adobe premiere en la *web*, entre otros; b) la plataforma como un servicio (*platform as a service*, PaaS) provee facilidades para el desarrollo de aplicaciones, incluyendo el diseño, implementación, testeo, operación y soporte de aplicaciones *web* y servicios en Internet adquiridos o creados por el usuario, utilizando el lenguaje de computación y las herramientas provistas por el proveedor en forma remota. Si bien el usuario no controla la infraestructura subyacente, sí tiene control sobre el desarrollo de aplicaciones y, posiblemente, sobre las configuraciones del entorno; ejemplos de ello son el google apps engine, la plataforma de servicios microsoft azure y la plataforma Salesforce.com Internet application development; c) en la infraestructura como un servicio (*infraestructure as a service,* IaaS) los recursos de *hardware*, de almacenamiento y de *computing power*, incluyendo CPU y memoria, son ofrecidos como un servicio para los usuarios, que los alquilan en vez de invertir en la adquisición de servidores y equipamiento de redes, en los cuales pueden ejecutar sus programas. El usuario puede desplegar y ejecutar *software*, incluyendo sistemas operativos y aplicaciones. Si bien no controla la infraestructura subyacente, tiene el control sobre los sistemas operativos, y posiblemente control limitado en la selección de componentes para la creación de redes. Como ejemplos existen Amazon EC2 para *computing power*, S3 para almacenamiento y SQS para comunicación en red para pequeños negocios y consumidores individuales.

La utilización de la computación en nube es una realidad innegable tanto para usuarios individuales como corporativos. El interés por su implementación ha llevado a que se realicen esfuerzos para aprovechar su potencial en diversas industrias, entre ellas la actividad financiera, en la cual ya se ha comenzado a experimentar para su uso (Cohen, 2008).

El beneficio más significativo radica en la eficiencia lograda mediante la tercerización de parte de la gestión de la información y de las operaciones de TI, permitiendo que los directivos y personal de las empresas se focalicen en cuestiones estratégicas mientras el proveedor de la nube se encarga de las actividades operativas de TI de modo más inteligente, rápido y económico (ISACA, 2009).

En las entidades financieras, donde se realizan un significativo uso de la información, *cloud computing* puede brindarles importantes ventajas para mejorar su gestión, tales como la posibilidad de utilizar los servicios computacionales —al-

macenamiento, capacidad, ancho de banda, etc.— en función de las necesidades de cada momento, otorgando mayor agilidad mediante la expansión o reducción en el aprovisionamiento y uso de recursos de *hardware* y *software* atendiendo los picos operacionales.

El pago de un precio de acuerdo con el nivel de uso de los recursos informáticos y los importantes ahorros en el uso de energía generan reducciones de costos operacionales, evitando además grandes inversiones iniciales en recursos de *hardware* y *software* al momento de emprender un nuevo negocio (Armbrust *et al*., 2009 y 2010; Capellozza, Sánchez y Albertin, 2011).

A nivel operativo se obtiene un nivel 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 un incremento en la seguridad de la información. Ello se debe a las grandes inversiones que realizan los proveedores de la computación en nube en el desarrollo de soluciones y a la disponibilidad de recursos humanos expertos dedicados a ello.

A pesar de lo expuesto, se espera una adopción lenta de la computación en nube tanto en la industria de las entidades bancarias y similares como en el resto de los sectores de la economía (Jaworski, 2009).

No obstante los beneficios que brinda esta estructura, genera riesgos que deben ser considerados por los usuarios antes de su implementación. En su evaluación se debe tener en cuenta el tipo de servicio – *software*, plataforma o infraestructura como un servicio - y el modelo de distribución adoptado – nubes públicas, privadas, comunitarias o híbridas (ENISA, 2009; Montahari, Stephenson y Singhal, 2009; Vaquero, Rodero-Merino, Caceres y Linder, 2009; Chen, Paxson y Katz, 2010; CSA, 2010 NIST, 2011).

La principal barrera a la aplicación de esta tecnología en el sector financiero es la seguridad del significativo volumen de datos sensibles que se manejan. Los bancos obligados a utilizar aplicaciones basadas en normativas y rigurosos marcos de referencia son los que enfrentan las mayores restricciones para su utilización. Hay quienes consideran este riesgo como uno de los principales obstáculos para su utilización debido a que las complicaciones sobre la protección y confidencialidad de los datos preocupa al mercado (Joint, Baker y Eccles, 2009).

Existen además otros riesgos propios de la utilización de la computación en nube que demoran su aplicación de modo generalizado: riesgos de política y organización, riesgos técnicos, riesgos legales y otros propios de cualquier ambiente de TI, pero que deben igualmente ser considerados (ENISA, 2009). Este conjunto de eventos contingentes deben ser analizados, procurando que los efectos negativos de los mismos sobre el desarrollo de las actividades de la organización sean minimizados. Ello es lo que se conoce como gestión de riesgos, según se describe a continuación.

La gestión de riesgo empresarial para la implementación de nuevas infraestructuras de TI

A partir de la identificación y análisis de los riesgos y su comprensión por parte de los usuarios puede lograrse un uso apropiado de las nuevas tecnologías, adoptando estrategias que permitan la gestión de los riesgos y la adecuación de los controles internos, que si bien no permiten su eliminación, facilitan la reducción significativa de sus efectos, o su transferencia a terceros.

El marco integrado por gestión de riesgo empresarial (*enterprise risk management,* ERM) desarrollado por el Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2004), mejor conocido por la sigla COSO–ERM, consiste en un proceso estructurado, consistente y continuo implementado a través de toda la organización —directorio, gerentes y resto del personal—, diseñado para identificar, evaluar, medir y reportar eventos potenciales —sean amenazas u oportunidades— que pudieran afectar a la entidad y administrar los riesgos para que estén dentro de los límites de su aversión al riesgo con el fin de proporcionar una razonable seguridad con respecto al logro de los objetivos de la organización (Estupiñan, 2006).

Dicho proceso pretende comprender y administrar los riesgos de forma eficiente de manera de aumentar la probabilidad y el impacto de los eventos positivos y disminuir la de los eventos negativos (Hillson, 2002a y 2002b; PMI, 2008).

La primera etapa del proceso de gestión de riesgos comprende la planificación en la que se define la forma en que se han 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 a los objetivos organizacionales —o en su caso a los de un proyecto de la organización en particu-

lar— 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 (PMI, 2008).

En dicho proceso los riesgos se pueden identificar y describir utilizando diferentes niveles de detalle, dependiendo de las necesidades de los usuarios de la información y de las decisiones que se deban adoptar; cabe aclarar que puede existir una variación considerable entre proyectos u organizaciones distintas. Una herramienta útil para guiar dicha descripción de riesgos es la *risk breakdown structure* (RBS).

Conceptualización de la risk breakdown structure

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

El Project Management Institute (2008) la define como una descripción jerárquica de riesgos, organizados por categorías y subcategorías que identifican las distintas áreas de posibles eventos contingentes. Ejemplos de categorías de riesgos comprenden las fuentes técnica, externa, de la organización, ambiental o de dirección de proyectos.

En algunos casos la visualización de los riesgos a un solo nivel —en un listado, por ejemplo— no brinda información útil para la toma de decisiones. Es por ello que el ordenamiento en tantos niveles como sean necesarios siguiendo una estructura como la descripta brinda la flexibilidad necesaria para realizar distintos tipos de análisis.

El uso de la RBS facilita las tareas de comprensión, identificación y evaluación de los riesgos, asegurando la cobertura de la totalidad de fuentes, indicando aquellas que resultan críticas para que sean gestionadas. A su vez, brinda una base de datos sobre los riesgos a un momento y en un contexto determinado, la cual puede ser revisada periódicamente para evaluar los cambios que se produzcan, permitiendo desarrollar planes de respuesta robustos y flexibles basados en las verdaderas causas que los desencadenan (Hillson, 2002a y 2002b; PMI, 2008).

Por lo que respecta a la elaboración de una RBS, Holzmann *et al*. (2011) proponen utilizar una metodología *bottom-up*, agrupando los riesgos individuales en áreas que incluyan los que corresponden a una misma fuente. En contraposición existe el método tradicional de *top-down*, en el cual en primer lugar se definen las fuentes de riesgos y luego se les asignan tipos de riesgos cada vez más específicos.

La identificación de la problemática puede realizarse a partir de supuestos, escenarios hipotéticos o predicciones de los riesgos potenciales, o bien a partir de experiencias reales basadas en información del pasado.

En el proceso de categorización, existe un nivel superior —el nivel cero— en el cual todo riesgo es simplemente riesgo del proyecto; luego, en el nivel uno, se determinan las categorías de fuentes de riesgo relevantes, tales como riesgo técnico, riesgo comercial, riesgo de gestión, riesgo externo, etc. Cada una de ellas puede a su vez subdividirse en subcategorías con mayor grado de detalle en el nivel dos y así sucesivamente en niveles inferiores.

Existen diversas alternativas en relación con la aplicación de esta herramienta. Una de ellas es la estructura conocida como RBS genérica, cuyo nombre se debe a que aplica a cualquier tipo de organización. Las categorías en el nivel uno comprenden riesgos internos al ente, riesgos externos —que pueden subdividirse en diversas áreas, como económico, físico, político y tecnológico— y riesgos globales —no asociados a ninguna categoría en particular. Una aplicación de este tipo es el trabajo realizado por el *risk 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), quienes formularon un proyecto universal de riesgos, que contempla una lista global de áreas de riesgos comunes a organizaciones de cualquier sector de actividad industrial, gubernamental o comercial (Hillson, 2002a; Holzmann *et al*., 2011).

Es importante señalar que las versiones de RBS genéricas suelen utilizarse como puntos de partida en la elaboración de las específicas de una organización en particular, pero no representan un enfoque completo de riesgos, de modo que deben ser adecuadas a cada situación.

Otro caso es el de la estructura conocida como RBS orientada a una industria; este tipo de caso particular es para la aplicación de la herramienta a una organización o tipo de proyecto determinado. Ha sido elaborada en diversas áreas; por ejem-

plo, para proyectos de construcción, suministro de energía, desarrollo de vacunas farmacéuticas, telecomunicaciones, entre otros (Tummala y Burchet, 1999; Chapman, 2001; Miller y Lessard, 2001; Dey, 2002, citados por Hillson 2002a).

Una tercera alternativa es la utilizada por algunas organizaciones, en donde se elabora una única estructura de desglose general que identifica los riesgos de la totalidad de sus actividades, otorgando una visión en conjunto de las áreas de riesgo a las que se encuentra sujeta; después para actividades, sectores o proyectos particulares y complejos se elaboran RBS más específicas con identificación de eventos particulares que quizás no pudieron verse reflejados en la estructura organizacional, facilitando el trabajo y la toma de decisiones de las personas que están involucrados en ellos (Hillson, 2002b).

RBS aplicada a la industria de tecnología de información

En el caso particular de la industria de la tecnología de información existe el antecedente de una RBS conocida como *risk taxonomy* o *taxonomy-based risk identification*, del Software Engineering Institute (Carr *et al*., 1993; Williams *et al*., 1999, citados por Holzmann y Spiegler, 2011; 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, ambiente de desarrollo y limitaciones del programa. La primera de ellas está referida a requerimientos, diseño, *testing* de unidad y *tests* de integración; la segunda incluye los elementos de procesos de desarrollo, desarrollo de sistemas, procesos de gestión, métodos de gestión y ambiente de trabajo; por último, las limitaciones del programa comprenden cuestiones asociadas a recursos, contratos e interfaces del programa.

Otro caso es el de Holzmann y Spiegler (2011), quienes elaboraron 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 descriptiva de experiencias pasadas que le proporcionó la empresa. Mediante un análisis cuali y cuantitativo de dichos documentos les asignaron códigos de riesgos a cada uno, obteniéndose un set de datos de riesgos de la organización. A través de un análisis de agrupamiento de los mismos se generó la estructura jerárquica organizacional. Los administradores del ente encontraron que la metodología implementada era apropiada, prefiriendo la utilización de la experiencia pasada en lugar

de escenarios y suposiciones para la identificación de los eventos contingentes a los que están sujetos.

A partir del agrupamiento de riesgos resultó que los dos niveles más amplios eran el de especificaciones de producto y definición del trabajo, y el de la participación del cliente y la comunicación. Se concluyó que la principal fuente de riesgo en este tipo de organización eran los recursos humanos.

Metodología

El alcance de la RBS propuesta comprende a potenciales entidades financieras interesadas en adoptar *cloud computing* bajo el modelo conocido como infraestructura como un servicio. En principio, resulta válido aplicar la RBS únicamente a entidades sujetas a la normativa del Banco Central de la República Argentina, dado que en su elaboración se han considerado los riesgos que pueden surgir a partir de esta regulación; por ejemplo, el BCRA indica que no se pueden descentralizar las actividades que tengan exteriorización al público; por lo tanto, en esta propuesta no se describen los riesgos que podrían emerger si la normativa fuera diferente.

Se utilizó un enfoque de RBS orientada a una industria, elaborando un caso genérico. Ello implica que la estructura aquí presentada sirve como punto de partida para la identificación y evaluación de riesgos en un proceso de implementación de *cloud computing* en una entidad financiera; sin embargo, debe ser adaptada en cada caso de aplicación particular, considerando las características de la entidad, el proyecto de implementación, los objetivos específicos y el ambiente de control vigente en la organización, entre otras cuestiones.

Para elaborar el modelo se realizó una revisión bibliográfica a partir de la cual han sido obtenidas listas de riesgos desarrolladas por múltiples organismos y autores. Los principales aportes se obtuvieron del 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 la seguridad de la información— y de la estructura conocida como *taxonomy-based risk identification* (Carr *et al*., 1993) mencionada anteriormente. Los riesgos allí identificados fueron corroborados y complementados por otros autores que los respaldan (Armbrust *et al*., 2009; ISACA, 2009; Montahari *et al*., 2009; Mowbray, 2009; CSA, 2010; Svantesson y Clarke, 2010; Holzmann y Spiegler, 2011; NIST, 2011; entre otros).

Una vez definidos los riesgos, éstos fueron confrontados con la normativa emanada del Banco Central de la República Argentina, en su calidad de organismo de contralor de las entidades financieras. Se analizaron las normas relacionadas con la implementación de estructuras de tecnología informática y tercerización del servicio de TI aplicable a dichos entes y se diseñó una RBS para el uso de *cloud computing* sólo para aquellos servicios que se admite sean prestados por un tercero. En la Comunicación A 3149 se establece que las entidades pueden descentralizar actividades de tipo administrativas o no operativas —que no tengan exteriorización al público— (BCRA, 2000).

En particular se consideraron 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; asimismo la Comunicación A 4793 sobre riesgos operacionales fue de utilidad para la definición de las categorías de riesgos que debían ser consideradas.

Después de haber identificado y analizado los riesgos dentro del marco y normativa mencionada vigente en Argentina se elaboró una *risk breakdown structure* que se presenta a continuación.

Propuesta de la risk breakdown structure

El Banco Central de la República Argentina establece en su normativa que las autoridades de cada entidad financiera deben asegurarse que existan 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 por los diferentes sectores y gestionar las debilidades que expongan a la entidad a niveles de riesgo alto o inaceptable, de modo de que sean corregidos a niveles aceptables.

Cumpliendo con el objetivo del trabajo, se expone a continuación la RBS que permite dar cumplimiento a este tipo de exigencias mediante una adecuada identificación y exposición de los riesgos para 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.

La organización de los riesgos se realizó sobre la base de la *risk breakdown structure* expuesta en el cuadro 1. El nivel cero de riesgos representa el conjunto de riesgos asociados al proyecto de implementación de computación en nube por una entidad financiera. El nivel uno describe una serie de fuentes de riesgo que coinciden con la clasificación mencionada en la Comunicación A 4793 del BCRA, incluyendo los riesgos estratégicos, reputacionales, legales y operacionales. Dentro de cada una de las fuentes se ejemplifican riesgos asociados en los niveles dos y tres.

a) Riesgos estratégicos

La primera fuente de riesgos expuesta en el nivel uno es la de los riesgos estratégicos; es decir, aquellos procedentes de una estrategia de negocios inadecuada o de un cambio adverso en las previsiones, parámetros y objetivos que respaldan la estrategia de la entidad (BCRA, 2008).

Tal como se puede visualizar en el cuadro 1, se han definido dos subcategorías de riesgos en el nivel dos: los relacionados al proceso de gestión y los derivados de los requerimientos para el sistema. La primera de ellas comprende riesgos, mencionados en el nivel tres, asociados a la planificación del proceso de implementación de la computación en nube, la adecuación de la estructura organizacional, la experiencia de la gerencia en la implementación y uso de estas infraestructuras, así como las interfaces entre personas internas y ajenas a la organización involucradas en el proceso de implementación.

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 encuentren alineados con los planes estratégicos de la misma (BCRA, 1997b). Sin planes definidos que respondan a las contingencias y los objetivos de largo plazo de la organización, con aporte y consentimiento de los sujetos involucrados y adecuados presupuestos y cronogramas de ejecución, es muy difícil que se logre aprovechar el potencial de la arquitectura para la gestión de la información.

Es fundamental la definición previa de la estructura organizativa, con una identificación clara de los roles y responsabilidades involucrados en el proceso. Una incorrecta separación y definición de funciones, las incompatibilidades entre ellas y la inexistencia de controles por oposición de intereses pueden llevar al fracaso del proceso de implementación.

Es importante señalar que mínimo debieran existir dos áreas diferenciadas, una de ellas dedicada a la gestión de la seguridad; y, la otra, al soporte, registro y seguimiento de los incidentes que surjan con los sistemas, la tecnología informática y los recursos asociados. Ambas resultan relevantes en un proceso de implementación de nuevos sistemas de TI para registrar las fallas, reducirlas y promover la integridad y confidencialidad de la información procesada.

La falta de experiencia de los gerentes en relación con la gestión de proyectos de implementación de TI, más aún de *cloud computing* —dado su reciente desarrollo—, puede ser una fuente de riesgos significativa si no se realiza una adecuada capacitación de la dirección.

Finalmente, 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, así como sus relaciones con personas ajenas a la organización implicadas en el mismo.

Cuadro 1
RBS , Riesgos de la utilización de computación en nube en entidades financieras

Nivel 0	Nivel 1	Nivel 2	Nivel 3
Riesgo del proyecto: Implementación de *cloud computing* por una entidad financiera	Riesgos estratégicos	Proceso de gestión	Planificación
			Estructura organizacional
			Experiencia de la gerencia
			Dependencias (*lock in*)
		Requerimientos para el sistema	Eficacia
			Eficiencia
			Confiabilidad
			Integridad
			Disponibilidad
			Estabilidad de las disposiciones legales
			Verificación del sistema
	Riesgos reputacionales	Utilización de recursos compartidos	
	Riesgos legales	Incumplimiento de normas	Normas del BCRA sobre requisitos mínimos de los sistemas informáticos y de información
			Normativa sobre el tratamiento de datos de clientes
		Incumplimiento de obligaciones contractuales	Contenido del contrato
			Incumplimiento del acuerdo por el proveedor
			Cambios de jurisdicción
			Adquisición del proveedor
	Riesgos operacionales	Fraude externo	Empleado malicioso
			Fuga/Interceptación de datos en tránsito
			Eliminación de datos insegura o no efectiva
			Gestión de la identidad
			Software malicioso
			Accesos no autorizados a las instalaciones
			Pérdidas o robos de *back-up*
			Robo de computadoras
		Fraude interno	Moral
			Connivencia del personal
			Programas y usuarios privilegiados y de contingencia
			Prácticas con clientes, productos y negocios
		Relaciones laborales y seguridad en el puesto de trabajo	Cooperación y comunicación del personal
			Actitud orientada a la calidad
			Desconocimiento de la tecnología por el personal
		Daños a activos físicos	Desastres naturales
			Condiciones ambientales
		Alteraciones en la actividad y fallas tecnológicas	Falla de Internet
			Gestión de la red
			Tráfico de la red
			Fallas de la cadena de suministro
		Ejecución, gestión y cumplimiento del plazo de los procesos	Planificación de la continuidad de la operatoria delegada
			Análisis de impacto
			Fallas en el cambio de ambiente operativo
			Instalaciones alternativas para el procesamiento de datos
			Fallas en el aislamiento de la información

En cuanto al vínculo con terceros, merece especial atención la relación con el proveedor del servicio que puede generar el riesgo de *lock in*. Implica que 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. Ello hace que el usuario, en este caso la entidad financiera, se vuelva vulnerable a aumentos de precios, problemas de confianza, o inclusive proveedores que abandonen el negocio dejando de prestar el servicio (ENISA, 2009; Armbrust *et al*., 2010), dificultando la continuidad de las operaciones.

La segunda subcategoría dentro de los riegos estratégicos es la de los requerimientos para el sistema. La Comunicación A 4609 establece un conjunto de normas para ser respetados por los recursos intervinientes en los procesos de tecnología informática, a saber: datos, sistemas de aplicación, tecnología, instalaciones y personas.

La norma requiere que el procesamiento en la arquitectura de la nube resulte eficaz, brindando información relevante, pertinente, correcta, coherente y completa. La oportunidad de la información también deberá ser respetada por los procesos, no sólo para facilitar la toma de decisiones, sino además para respetar la normativa vinculada con los plazos de presentación de informes a los organismos de control. En el caso particular del BCRA, exige la presentación de información en fechas determinadas que deben generarse de manera automática por el sistema con intervención mínima del personal de la entidad.

La información obtenida de las aplicaciones ejecutadas en la nube debe cumplir con los requisitos de integridad, disponibilidad y confiabilidad. Se deben satisfacer las expectativas de los usuarios y facilitar la toma de decisiones mediante información exacta, completa y válida, acorde a las pautas fijadas por la regulación, disponible en tiempo y forma. Ello implica que las aplicaciones deberán incluir controles adecuados para su cumplimiento.

El riesgo de inestabilidad en las disposiciones legales implica la posibilidad de cambios que conlleven continuas modificaciones en los sistemas. Las aplicaciones desarrolladas por la entidad y ejecutadas en la nube, así como las pautas establecidas con el proveedor para la prestación del servicio, se volverían obsoletas en el corto plazo, pudiendo generarse alteraciones no compatibles con el nuevo entorno. Así un servicio que en un momento resulta factible, puede luego dejar de serlo.

Otro requerimiento es que los sistemas sean verificables; su incumplimiento puede implicar la imposibilidad de realizar evaluaciones de confiabilidad y *tests* de penetración por encontrarse dentro de la plataforma de un tercero.

Además, existen riesgos de que no se puedan ejecutar los controles y monitoreos exigidos por el BCRA cuando se realiza la tercerización de actividades. Dichos controles deben realizarse sobre el cumplimiento de los niveles de los servicios acordados, el mantenimiento de la confidencialidad de la información y demás aspectos establecidos por la normativa. El incumplimiento de los mismos es responsabilidad del directorio de la entidad financiera (BCRA, 1997b).

Los requerimientos referidos a confidencialidad y cumplimiento son tratados más adelante.

b) Riesgos reputacionales

La segunda categoría de riesgos incluida en el nivel uno de la RBS abarca los riesgos reputacionales. Se refieren a las eventuales pérdidas ocasionadas como consecuencia de la formación y difusión de una opinión pública negativa —fundada o infundada— sobre los servicios prestados por la entidad financiera que fomente la creación de una mala imagen o un posicionamiento negativo, resultando en una disminución en el volumen de clientes, caída de ingresos, de depósitos, etcétera (BCRA, 2008).

En este caso se utilizó una menor cantidad de niveles para la exposición de los riesgos. Como se puede apreciar, se incluye el nivel cero —riesgo total del proyecto— y el nivel uno. La estructura de desglose no necesariamente debe cubrir una cantidad amplia de categorías. La necesidad de mayor o menor información y claridad será la que determine el grado de detalle por utilizar.

En el caso de la implementación de la computación en nube, este riesgo se ve incrementado por la particularidad de los recursos compartidos; es decir que sirven a múltiples usuarios a partir de una dinámica asignación y reasignación de los recursos físicos y virtuales entre ellos en función de su nivel de demanda. De este modo, es posible que actividades maliciosas desarrolladas por uno de los usuarios afecte la reputación de los demás. Podría ocurrir, por ejemplo, que uno de ellos accediera a datos de otro almacenados o procesados en el mismo servidor, pudiendo hacer un uso ilegítimo de los mismos (venta de datos, divulgación de información confidencial, etcétera).

En el sector financiero —donde se procesan datos especialmente sensibles sobre clientes y transacciones, cuya publicidad o usos inadecuados pueden generar daños irreversibles— es necesario implementar controles eficientes que permitan gestionar este tipo de riesgos.

c) Riesgos legales

Los riesgos legales —que pueden ser considerados dentro de los operacionales, pero que en este trabajo se incluyen como la tercera fuente de riesgos en el nivel uno— comprenden, entre otros aspectos, la exposición a sanciones, penalidades u otras consecuencias económicas y de otra índole por incumplimiento de normas y obligaciones contractuales (BCRA, 2008). Estas sanciones podrían provenir de las mismas normas incumplidas, de las pautas de contratos o de sentencias dictaminadas por jueces frente a demandas o juicios que se hubieran iniciado en contra de la entidad y cuyas resoluciones hubieran resultado adversas a sus intereses.

A pesar de la implementación de la computación en nube, la responsabilidad última de cumplimiento de las leyes y normas es del usuario, aunque las sanciones por incumplimiento son aplicables a la entidad financiera.

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 sólo por la entidad financiera, sino también por el proveedor de los servicios de computación en nube 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, de modo que la TI debería ser gestionada nuevamente por el ente en su totalidad, perdiéndose en consecuencia los beneficios de la arquitectura implementada.

Asimismo, se incluyen 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.

Las cuestiones relacionadas a la eventual divulgación de datos personales, sea por negligencia o dolo del proveedor, generan el riesgo de situaciones litigiosas contingentes que deberían afrontar las entidades financieras, con alta probabilidad de impacto negativo en los resultados de la misma.

Un riesgo de alto impacto económico es el relacionado con los incumplimientos de pautas contractuales por parte del proveedor del servicio. Muchas veces los mismos podrían verse asociados a la informalidad en los acuerdos para la prestación de servicios a través de Internet o a las modificaciones unilaterales de las condiciones pautadas.

Si el proveedor se fusiona o es absorbido por un tercero, surge la probabilidad de un cambio estratégico que puede generar el incumplimiento de ciertas cláusulas o de acuerdos no vinculantes, como por ejemplo la definición de interfaces del *software*, las inversiones en seguridad acordadas o los controles de seguridad, afectando los requisitos preestablecidos. El impacto final podría darse sobre activos esenciales como la reputación de la organización, la confianza de clientes y la lealtad de los empleados.

Si bien una de las características del almacenamiento y procesamiento de la información en la nube es la independencia de localización que implica que el usuario normalmente desconoce la ubicación exacta de los recursos, éste puede mediante los contratos o acuerdos de nivel de servicios —conocidos como *service level agreements* (SLAs)— determinarla en un nivel superior de abstracción, indicando el país, estado o centro de datos donde pretende que su información sea almacenada y procesada. La inobservancia de este tipo de cláusulas por parte del proveedor genera el riesgo de que los datos se encuentren en jurisdicciones con marcos jurídicos inestables y normativas impredecibles, pudiendo quedar sujetos a divulgación forzada o secuestro.

d) Riesgos operacionales

La última fuente identificada dentro del nivel uno es la de riesgos operacionales. Incluye aquellos riesgos de pérdidas resultantes de fallas en los procesos internos, actuación del personal o de los sistemas, o bien producto de eventos externos (BCRA, 2008). Dentro de esta categoría se han definido en el nivel dos siete subcategorías que se describen a continuación.

*Fraudes externos***:** aquellos originados fuera de la organización, que no dependen de las decisiones adoptadas por sus miembros (BCRA, 2008). Sobre ellos se posee un menor nivel de control respecto de los de origen interno.

En primer lugar se incluyen algunos riesgos asociados a la vulneración de las medidas de protección de *software* e información sensible, conocidas como seguridad lógica. En las etapas iniciales de los proyectos informáticos, estas cuestiones debieran ser contempladas de modo de promover una correcta selección de tecnología y asegurar el diseño e implementación adecuados de registros de seguridad (BCRA, 1997b). Se deben tener en cuenta diversos riesgos, entre ellos el denominado del "empleado malicioso", basado en el posible abuso de una situación de privilegio por parte de los empleados del proveedor de *cloud computing*, los administradores del sistema de la nube, los auditores, los proveedores de servicios de seguridad, entre otros.

Debido a que la computación en nube es una arquitectura distribuida, esto implica que existe una mayor cantidad de datos en tránsito que en las infraestructuras tradicionales para que puedan ser transferidos ente los servidores de la nube y los clientes *web* remotos. Tal nivel de movilización incrementa los riesgos de interceptación de datos en tránsito y la fuga de datos. A su vez, la eliminación de datos insegura o no efectiva implica que los datos podrían estar disponibles mas allá de la vida útil especificada en la política de seguridad del usuario. Otro tipo de riesgos comunes para ser considerados, si bien no son propios de estos contextos arquitectónicos, son los problemas de gestión de la identidad (como el robo o pérdida de contraseñas) y los conocidos *software* maliciosos (tales como virus informáticos).

De igual manera, corresponden a esta categoría los riesgos asociados a la seguridad física, referidos a cualquier tipo de acceso no autorizado a instalaciones que implique destrucción o robo, ya sea de equipamiento, *software*, información, *backups*, etc. Si bien los proveedores del servicio concentran los recursos en grandes centro de datos cuyos perímetros están fuertemente controlados, el impacto que puede tener la violación a dichos controles es mayor al que tendría en el caso de sistemas domésticos, dado que se resguarda información de múltiples usuarios que poseen una capacidad limitada de verificación de las medidas de seguridad implementadas; sin embargo, la implementación de la computación en nube otorga cierta seguridad en el resguardo de la información dada la redundancia para su almacenamiento.

Fraudes internos: comprenden la elaboración y divulgación de información falsa sobre posiciones, propias o de clientes, robos por parte de empleados o utilización de información confidencial de la entidad financiera en su beneficio, entre otras (BCRA, 2008).

Según Carr *et al*. (1993) en los proyectos asociados a desarrollo de TI, los riesgos que resultan de un nivel bajo de moral comprenden la falta de compromiso con los programas de desarrollo e implementación de la tecnología y pobre performance, productividad y creatividad por parte del personal. La falta de valores y el descontento, junto con la búsqueda del beneficio propio a costa de los demás, pueden derivar en daños intencionales al proceso de mejora de los sistemas de la entidad financiera (boicot) o llevar a éxodos masivos del personal relacionado al mismo.

Debe evaluarse además la posibilidad de connivencia entre el personal en detrimento de los objetivos organizacionales, en la medida en que siendo conocedores privilegiados de información sensible y del funcionamiento de los sistemas de procesamiento y seguridad pueden poner en riesgo la actividad de la entidad. Ello adquiere especial relevancia en el caso de los usuarios privilegiados, con capacidades de administración que podrían dar de alta, de baja o modificar datos y sistemas, respecto de los cuales deberían establecerse controles especiales.

Finalmente, los riesgos de prácticas con los clientes, productos y negocios incluyen el abuso de información confidencial, la negociación fraudulenta en las cuentas de la entidad financiera, el lavado de dinero, la venta de productos no autorizados, entre otros.

Relaciones laborales y seguridad en el puesto de trabajo: esta subcategoría prevista en la Comunicación A 4793 del BCRA incluye, entre otros, el problema de las fallas en la comunicación y cooperación, en la medida en que si hay un desconocimiento de los objetivos perseguidos con la implementación de la computación en nube para la gestión de operaciones, los requerimientos y diseño de los sistemas y de la importancia y el impacto que tiene para la entidad, difícilmente podrán obtenerse buenos resultados.

La falta de experiencia o capacitación del personal en la utilización de la tecnología también es un riesgo que debe ser considerado. El personal operativo necesita ser capacitado para comprender el manejo de las nuevas herramientas, lo cual requiere además actitud y voluntad de los trabajadores en aprender y realizar consultas. Hasta el momento en que se esté seguro de que la planta de personal ha comprendido la gestión del nuevo sistema informático adaptado a la nube no debería autorizarse su implementación.

Los riesgos mencionados en esta subcategoría son relevantes en la medida en que los principales focos de riesgo en proyectos dedicados a la tecnología de información son los recursos humanos, tal como lo expusieron Holzmann y Spiegler *et al*. (2011) en su trabajo.

Daños a los activos físicos: se refiere a los riesgos derivados de actos de terrorismo y vandalismo, terremotos, incendios, inundaciones y otro tipo de eventualidades de naturaleza similar.

En general, se entiende que los riesgos de desastres naturales cuando se implementa *cloud computing* son menores comparados con las infraestructuras tradicionales porque los proveedores ofrecen sitios redundantes para las aplicaciones y el almacenamiento de información.

Las condiciones ambientales inadecuadas, dadas por las características de la construcción y la localización de las instalaciones, equipos de aire acondicionado, grupos generadores, baterías, tableros de distribución de energía y de telecomunicaciones, estabilizadores, etc., son fuentes de potenciales daños y pueden afectar la integridad de los activos físicos.

Alteraciones en la actividad y fallas tecnológicas: incluye, según la normativa, fallas del *hardware* o del *software*, problemas en las telecomunicaciones, interrupción en la prestación de servicios públicos, etcétera.

La actividad de las entidades financieras se desarrolla en un horario acotado y, en gran medida, mediante la atención al público. En este ámbito, la interrupción de los servicios como electricidad o las fallas en el funcionamiento de los sistemas informáticos, seguidos de la insatisfacción de las demandas de los clientes puede generar daños económicos y en la imagen de la empresa.

Un prerequisito para la implementación de las infraestructuras tecnológicas dinámicas es la disponibilidad del servicio de Internet. Así 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. Todos ellos son riesgos de muy alto impacto, en la medida que sin una conexión adecuada a la red no hay servicio posible.

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 computación en nube hubiera externalizado ciertas tareas especializadas de la prestación del servicio a terceros. La entidad pasa a depender de más de un proveedor en cuanto al nivel de seguridad y la calidad del servicio obtenido.

Ejecución, gestión y cumplimiento del plazo de los procesos: esta última subcategoría en el nivel dos dentro de los riesgos operacionales se refiere a errores en la introducción de datos, fallas en la administración de garantías, documentación jurídica incompleta, concesión de acceso no autorizado a las cuentas de los clientes, litigios con proveedores, entre otros (BCRA, 2008).

Muchos son riesgos de tipo operativo que no se relacionan específicamente con un ambiente de computación en la nube, y que podrían ser solucionados por mecanismos de control similares a los utilizados en un contexto de TI tradicional; no obstante, se ha considerado adecuado incluir en esta categoría las eventuales fallas que pudieran producirse cuando se realizan cambios en el ambiente operativo, al realizar el traspaso —sea éste total o parcial— de las operaciones en un ambiente de TI tradicional a uno de *cloud computing*. La transición de una infraestructura a otra no debiera interrumpir las transacciones, el cumplimiento de contratos, el almacenamiento de la información. Es por ello que la implementación debe iniciarse a partir de un proceso debidamente planificado con una adecuada separación entre el ambiente informático de procesamiento operativo y el de prueba del nuevo sistema.

También se debe tener en cuenta como situación riesgosa la inexistencia de procedimientos adecuados para garantizar la continuidad de las operaciones y el cumplimiento de plazos de las transacciones y presentación de informes cuando se producen contingencias. El BCRA establece la responsabilidad de la entidad de controlar la aplicación de la normativa por parte de los terceros con el fin de garantizar la continuidad de las actividades delegadas, por lo que en este caso se deberá controlar los procedimientos de contingencias desarrollados por el proveedor de la nube.

La inexistencia de un adecuado análisis de impacto de los eventos contingentes, la falta de un plan actualizado de recuperación del procesamiento de datos —coordinado entre la organización 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 pérdida de información y a reclamos de los clientes.

Los planes de contingencia deben prever que el equipamiento de procesamiento alternativo posea la capacidad de administración y gestión de todos los procesos de negocios clasificados como críticos para asegurar la continuidad de las actividades de la entidad financiera. La localización de las instalaciones alternativas deberá ser tal que en caso de un siniestro o suceso contingente que torne inoperables las instalaciones principales no se vean afectadas las sustitutas.

Otra falla tecnológica incluida en esta categoría es la del fracaso de los mecanismos de aislamiento de la información; esto significa que al existir el almacenamiento de datos de diversos usuarios en un mismo lugar, alguna falla lógica produjera la confusión de la información de ellos.

Conclusiones

El aporte del presente trabajo consiste en el diseño de una *risk breakdown structure* con un enfoque orientado a la industria que facilita la identificación, comprensión y evaluación de riesgos asociados a la implementación de la computación en la nube por entidades financieras de la República Argentina. Este modelo permite guiar la elaboración de estrategias adecuadas con el propósito de minimizar los efectos de los eventos contingentes negativos.

Para su elaboración se consideraron fuentes de riesgos identificadas por diversos autores que estudian esta infraestructura y la normativa propia del organismo de contralor que las regula que es el Banco Central de la República Argentina, por lo que se les clasificó en riesgos estratégicos, reputacionales, legales y operativos, logrando una amplia cobertura de las eventualidades asociadas.

La estructura definida permite ejemplificar y obtener una visión clara de los diferentes niveles de riesgos que pueden afectar a una entidad del tipo seleccionado en la implementación de esta arquitectura. Se puede observar que cuanto mayor sea la cantidad de niveles utilizados, mayor será el detalle de riesgos asociados a cada fuente, pudiendo generarse distintos reportes de riesgos destinados a los diferentes niveles de mando organizacionales.

Del modelo desarrollado surge la idea de que la fuente de riesgos operacionales es sin duda una categoría crítica, con una importante apertura que comprende un amplio espectro de posibles eventos que deben ser tenidos en cuenta. Ello denota la necesidad de monitoreo continuo y especial atención al momento de definir las acciones de gestión de riesgos.

A partir de la herramienta propuesta, los administradores de la entidad podrían realizar una comparación con otros modelos de servicios informáticos a efectos de seleccionar la mejor opción entre las alternativas posibles; por ejemplo, se pueden comparar los riesgos de la implementación de infraestructuras de computación en nube con el desarrollo y procesamiento propio de arquitecturas de TI, o una combinación de ambas opciones, siempre dentro del marco de la normativa vigente.

En la medida que este tipo de tecnologías surgen y se posicionan en el mercado como una alternativa importante que puede brindar múltiples beneficios en el procesamiento de la información, esta propuesta servirá a los directivos de las entidades financieras como punto de partida para el análisis de riesgos, el diseño de controles que minimicen sus efectos y la búsqueda de garantías del cumplimiento de los objetivos organizacionales.

Referencias

Armbrust M. *et al*. (2009). Above the clouds: a Berkeley view of cloud computing. *Technical Report Nro*. *UCB/EECS-2009-28*, *Electrical Engineering and Computer Sciences*. Universidad de California en Berkeley.

——————— (2010). Above the clouds: a Berkeley view of cloud computing. *Communications of the ACM* 53 (4): 50-58.

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

——————— (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

——————— (2000). Comunicación A 3149. Requisitos mínimos del área de Sistemas de Información de las Entidades Financieras. Disponible en http://www.bcra.gov.ar/pdfs/comytexord/A3149.pdf

——————— (2008). Comunicación A 4793. Lineamientos para la gestión del riesgo operacional en las entidades financieras. Disponible en http://www.bcra.gov.ar/pdfs/comytexord/A4793.pdf

——————— (2010). Comunicación A 5042. Normas mínimas sobre auditorías externas y controles internos para entidades financieras. Disponible en http://www.bcra.gov.ar/pdfs/comytexord/A5042.pdf

Capellozza A., O. P. Sanchez y A. L. Albertin (2011). Estudo da Influência da infra-estrutura de tecnologia de informação à mobilidade computacional dos usuários e utilização da computação em nuvem, aplicado em empresas do setor de serviços. III Encontro de Administração da Informação, Anpad, Porto Alegre, Rio Grande do Sul, Brasil. En ADI 2011. 1:1-16.

Carr M. J., S. L. Konda, I. Monarch, F. C. Ulrich y C. F. Walker (1993). Taxonomy-Based Risk Identification. *Technical Report CMU/SEI-93-TR-6 ESC-TR-93-183*, Software Engineering Institute. Universidad de Carnegie Mellon.

Chen Y., V. Paxson y R. H. Katz (2010). What´s new about cloud computing security *Technical Rep ort No. UCB/EECS-2010-5*, Electrical Engineering and Computer Sciences, Universidad de California en Berkeley.

Cloud Security Alliance (CSA) (2010). *Top Threats to Cloud Computing Version 1.0*. Disponible en: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cohen R. (2008/07/25). Cloud computing. Morgan Stanley is banking on the cloud. SYS-CON Media, Inc. Disponible en: http://weblogic.sys-con.com/node/589951

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004). *Enterprise Risk Management - Integrated Framework*.

Dorofee A. J., J. A. Walker, C. J., Alberts, R. P. Higuera, R. L. Murphy y R. C. Williams (1996). *Continuous risk management guidebook*. Universidad de Carnegie Mellon, Software Engineering Institute.

European Network and Information Security Agency (ENISA) (2009). *Cloud computing, benefits, risks and recommendations for information security*. Disponible en: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Estupiñán Gaitán, R. (2006). *Control interno y fraudes*. 2da. ed. Bogotá: Ecoe Ed.

Hillson, D. (2002a). Use a risk breakdown structure (RBS) to understand your risks. *Proceedings of the Project Management Institute Annual Seminars y Symposium,* San Antonio, Texas.

———— (2002b). The risk breakdown structure (RBS) as an aid to effective risk management. *Fifth European Project Management Conference, PMI Europe 2002,* Cannes, Francia.

Holzmann V. y I. Spiegler (2011). Developing risk breakdown structure for information technology organizations. *International Journal of Project Management* 29 (5): 537-546.

Information Systems Audit and Control Association (ISACA) (2009). Cloud computing. Business benefits with security, governance and assurance perspectives. White paper.

Jaworski A. (2009). Survey: banks slow to adopt cloud computing. *Information Management Online*. Disponible en: http://www.information-management.com/news/cloud_computing_financial_services_bank-10015811-1.html?zkPrintable=true

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

Montahari-Nezhad H., B. Stephenson y S. Singhal (2009). Outsourcing business to cloud computing services: opportunities and challenges, HP. *Special Issue on Cloud Computing,* IEEE Internet Computing.

Mowbray M. (2009). The fog over the grimpen mire: cloud computing and the law. *Scripted Journal of Law, Technology and Society* 6 (1).

National Institute of Standards and Technology (NIST) (2011). The NIST definition of cloud computing. *Special Publication 800-145*, National Institute of Standards and Technology U.S. Department of Commerce.

Nguyen N. M. (1998). Effective risk management for proyect managers: A 21st Century Approach. *29th Annual Project Management Institute 1998 Seminars y Symposium*. Long Beach, California, USA.

Proyect Management Institute (PMI) (2008). *Guía de los fundamentos para la dirección de proyectos* (Guía del PMBOK®), 4ta ed. Pennsylvania: Project Management Institute, Inc.

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

Vaquero L. M., L. Rodero-Merino, J. Caceres y M. Lindner (2009). A break in the clouds: towards a cloud definition. *ACM Sigcomm Computer Communication Review* 39 (1).