Migración de Sistemas Heredados a Cloud Computing

Ana Sofía Zalazar, Silvio Gonnet, Horacio Leone

INGAR (UTN-CONICET), Avellaneda 3657, 3000, Santa Fe, Argentina.
{azalazar,sgonnet,hleone}@santafe-conicet.gov.ar

Abstract. Cloud computing consiste en el aprovisionamiento dinámico de recursos físicos y virtuales por parte de los proveedores, para optimizar al máximo la rentabilidad y la utilización de sus recursos. Los consumidores, contratan estos servicios, negociando los acuerdos de nivel de servicio. Algunos consumidores proyectan migrar las funcionalidades de sus sistemas heredados a los servicios de cloud computing, para minimizar la inversión en infraestructura propia y además adquirir nuevas soluciones informáticas que se adapten rápidamente a los cambios dinámicos del entorno. Por lo tanto, el aporte de este trabajo consiste en clasificar diferentes tipos de migración de sistemas heredados a cloud computing, según las características de estas aplicaciones y los modelos de implementación de cloud computing. También se propone un flujo de trabajo para la migración de funcionalidades, basado en la experiencia en proyectos de conversión de sistemas y las características analizadas de los entornos de cloud computing. Finalmente, se evalúan algunos riesgos de seguridad en el proceso de migración y se proponen algunas recomendaciones contra estos riesgos.

Keywords: Cloud Computing, Sistemas Heredados, Migración.

1 Introducción

Cloud computing, también llamado computación en la nube, se refiere al régimen de externalización, en el cual se contratan servicios de terceros utilizando acuerdos de nivel de servicio ("*Service Level Agreement*", SLA) y a través de protocolos de internet. Esto es posible, porque varias empresas han optado por optimizar la utilización de su infraestructura tecnológica, ofreciendo soluciones de almacenamiento ("*hosting*") y servicios de computación ("*outsourcing*"), por medio de políticas de cobros por suscripción y pago por uso ("*pay-per-use*"), entre otras [1][2].

La migración de los sistemas heredados ("*legacy systems*") de una organización a entornos de cloud computing representa grandes beneficios de costos (pagar sólo por lo utilizado, menos inversiones en hardware y mantenimiento, etc.) y la oportunidad de realizar cambios en el modelo de negocio para adaptarse rápidamente a la demanda del mercado y su entorno dinámico. Del mismo modo, la migración de sistemas ofrece la posibilidad de integrar, en una misma solución informática, las aplicaciones de la organización y crear procesos de colaboración con clientes, socios y diferentes proveedores [3].

La mayoría de los trabajos analizados en el área de ingeniería de software se enfocan en los aspectos funcionales para decidir sobre la migración hacia servicios de cloud computing. Por ejemplo, el trabajo de Andrikopoulos y colaboradores [4] menciona a la migración como una adaptación de las aplicaciones de sistemas heredados, para ser ejecutados en la infraestructura de proveedores de cloud computing. En la contribución [4] no se propone ningún mecanismo o secuencia de pasos para llevar a cabo esta adaptación y se enfoca simplemente en definir los conceptos relacionados a cuatro tipos de migración: reemplazo de componentes, migración parcial de la aplicación, migración total de la aplicación, y transformar la aplicación a cloud computing. En el trabajo [5] también se deja de lados los procesos de migración, y se analizan los aspectos sobre la adquisición, la implementación, los factores económicos, la seguridad y la privacidad, de una clasificación de cuatro tipos de migración: migración de datos, migración de información, migración de servicios, y migración autonómica. Por otro lado, Know y Tilevich [6] presentan el proceso de migración a cloud computing como la refactorización de funcionalidades para ser accedidas de forma remotas por los clientes, y este proceso consiste en transformar porciones de códigos de los sistemas heredados a servicios de cloud computing y configurar la aplicación cliente para la utilización de los servicios creados. Este último trabajo se limita a la reingeniería y refactorización, y no abarca otros tipos de migración que son más simples de llevar a cabo, como el reemplazo de un componente del sistema por la adquisición de servicios ya existentes en Internet.

Sin dudas, la tendencia está en transformar primero las aplicaciones tradicionales, comúnmente estructuradas y basadas en formularios, a aplicaciones basadas en la arquitectura orientada a servicios ("*Software Oriented Arquitecture*", SOA) [7][8][9]. Esta transformación favorece el débil acoplamiento, la reutilización, la integración y la abstracción de la infraestructura tecnológica, que son factores claves en los entornos de cloud computing.

Por ejemplo, en el trabajo [10], Chauhan y Babar analizan las actividades de la migración de sistemas basados en SOA hacia el modelo "software como un servicio" (*SaaS*) de cloud computing y, una vez analizados los requerimientos de calidad, proponen un proceso para esta migración. El proceso presentado en la contribución [10] consiste en: evaluación de la escalabilidad de los componentes, evaluación de la orquestación, identificación de los componentes a ser refactorizados y la evaluación de la solución frente al ambiente de cloud computing destino.

A continuación, se presenta las características de cloud computing y los diferentes tipos de migración de sistemas heredados, según el análisis de las características de estos sistemas y los modelos de implementación de cloud computing. En la Sección 4 se define un flujo de trabajo ("*workflow*") para esta migración, basado en la experiencia en proyectos de migración de sistemas y adaptado estas tareas para ser aplicadas a entornos de cloud computing. Finalmente, en la Sección 6, se presentan algunos riesgos de seguridad y consideraciones a tener en cuenta durante la migración de sistemas heredados a cloud computing. En este trabajo se considera que el análisis de los aspectos de seguridad debe ser integrado a todas las actividades de migración.

2 Características de Cloud Computing

El término cloud computing ha sido utilizado como un término de marketing en varios contextos y representando diferentes ideas [11]. No es una nueva tecnología, sino un nuevo paradigma de negocio basado en tecnologías existentes como: Virtualización: mecanismo de ejecución de aplicaciones y almacenamiento de datos, como si estuvieran aislados y en diferentes servidores, en recursos físicos compartidos; Grid computing: procesamiento en varios servidores; Broadband Internet: redes de transporte rápido para grandes cantidades de datos; Web 2.0: aplicaciones y tecnologías que hacen que la Web sea un medio de colaboración; y SOA: arquitecturas que soporta la construcción de aplicaciones utilizando servicios interconectados.

Existen muchas definiciones de cloud computing [1][2][12], y la más acepta es la ofrecida por Mell y Grace [1] pertenecientes al *National Institute of Standard and Technology* (NIST). Estos autores proponen una definición que abarca los aspectos más generales del modelo de negocio: "*Cloud computing es un modelo que permite acceso a redes bajo demanda, para compartir un conjunto de recursos de computación configurable (es decir, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos o liberados con un mínimo esfuerzo de administración o interacción con los proveedores de servicio*".

Además, el NIST define cinco roles: *Proveedor:* entidad que posee el servicio desplegado en sus servidores, y es el responsable del mantenimiento y la disponibilidad del servicio; *Consumidor:* entidad que utiliza el servicio para completar su proceso de negocio; *Portador:* intermediario que proporciona el transporte de datos y la conectividad de los servicios; *Bróker:* intermediario que se involucra en la relaciones contractuales y de negocio; y *Auditor:* agente externo que se encarga de llevar un control de las operaciones, hacer un seguimiento a los procesos de negocios, notificar fallas y analizar la calidad de los servicios según lo contratado en el SLA.

En base a estas definiciones, podemos explicar las cinco características principales atribuidas a cloud computing [1]: *Autoservicio a demanda*: el consumidor del servicio accede automáticamente a los recursos de computación según sus necesidades; *Amplio acceso a redes:* los recursos están disponibles en la red y el acceso a los recursos se realiza, por medio de diferentes plataformas clientes; *Puesta en común de recursos:* los recursos de un proveedor son compartidos entre múltiples clientes, utilizando mecanismos de virtualización y múltiple tenacidad; *Rápida elasticidad:* los recursos son adicionados y liberados según la demanda de los consumidores; y *Medición de servicios:* los sistemas de cloud computing controlan y miden automáticamente la utilización de los servicios, de forma transparente a los actores.

La mecánica de cloud computing consiste en el aprovisionamiento variable de recursos físicos y virtuales por parte del proveedor, para optimizar al máximo la rentabilidad y la utilización. Los proveedores varían la cantidad de recursos, agregando nuevas unidades, reemplazando o desconectado unidades según el consumo y la demanda de servicios, de manera rápida y no perceptible por los usuarios conectados a los servicios [13].

Esta mecánica de aprovisionamiento de recursos resuelve el problema de los sistemas heredados, que por sí solos no son capaces de mantener la demanda de recursos y el rendimiento necesario que acompañe la evolución de sus procesos del negocio.

2.1 Modelos de Despliegue

Antes de contratar un proveedor y migrar las funcionalidades de los sistemas heredados a los entornos cloud computing, es necesario estudiar los diferentes modelos de despliegues y los requerimientos específicos de la organización. Además, la adopción de determinado modelo de despliegue dependerá de la criticidad de los procesos y la sensibilidad de los datos asociados a estos procesos.

Los modelos de despliegue indican si los servicios de cloud computing han sido desplegados privadamente o en un lugar donde el cliente puede compartirlos con un número limitado de socios de confianza, o bien puede ser almacenados en hardware de una tercera parte y acceder a ellos públicamente. Según la ubicación de los datos, los servicios de cloud computing pueden ser:

- "*On premises*". El despliegue se realiza dentro de la zona de seguridad y los centros de datos ("*data center*") de la organización. El consumidor de servicio puede requerir que los recursos sean de su uso exclusivo, con la protección de contrafuegos corporativos ("*firewall*") y bajo una determinada legislación.
- "*Off premises*". El despliegue se realiza fuera de los servidores del consumidor y la información de la ubicación física del centro de datos puede no ser especificada por el proveedor del servicio. Esta forma de despliegue puede ser muy riesgosa.

Los distintos modelos de despliegue definido por NIST [1] son:

- *Nube Privada*. Los recursos y accesos son de uso exclusivo de una organización con múltiples usuarios internos. Esta nube puede ser controlada por la organización propietaria, por el proveedor o pueden compartir responsabilidades de gestión.
- *Nube Comunitaria.* Los recursos son compartidos por una comunidad de organizaciones que poseen alguna característica especial o fin determinado que la hacen formar parte de esta comunidad. Estas comunidades obligan al proveedor a compartir políticas específicas entre los usuarios de la nube comunitaria.
- *Nube Pública.* La infraestructura de la nube es compartida por varios clientes independientes, utilizando mecanismos de multi-tenacidad reforzados y se debe asegura la independencia entre los entornos de estos clientes. Los servicios se encuentran alocados dentro de los servidores del proveedor o de terceras partes.
- *Nube Híbrida*. Es una combinación de una nube privada, nube pública o nube comunitaria. Se crean generalmente para proteger datos sensibles, resguardar información y aprovechar el rápido aprovisionamiento público cuando existe sobrecarga de trabajo.

Probablemente una organización, consumidora de servicios en cloud computing, deba asegurarse cierto nivel de seguridad y confidencialidad en sus datos, por lo tanto deberá optar por una nube privada, y parte de los servicios del modo "*on-premises*" para

poder auditar las rutinas en los servidores y el mantenimiento de equipos. Sin dudas, la mejor solución es una combinación adecuada de servicios de nube privada y nube pública en un entorno híbrido, para aprovechar el control de los datos en servidores propios y a la vez beneficiarse de las bondades que ofrece la nube pública en la tercerización de servicios, escalabilidad y aprovisionamiento.

2.2 Modelos de Servicio

Podemos considerar cinco capas para la definición de un sistema de información [15]: *Capa de Aplicación*: incluye los componentes de software, los servicios web y los clientes; *Capa de Middleware*: permite la construcción de aplicaciones y lleva a cabo la comunicación con otras aplicaciones, base de datos y sistemas operativos; *Capa de Sistema Operativo:* se encarga de administrar los recursos virtuales o físico donde se alojan las aplicaciones; *Capa de Hypervisor*: es la capa de virtualización de recursos para ser administrados por el sistema operativo; y la *Capa de Infraestructura* que consiste en el almacenamiento, el hardware y la red.

Generalmente, en un sistema heredado la gestión administrativa de todos los componentes se encuentran bajo el control del consumidor del servicio, y cuando se analiza la posibilidad de migrar estos sistemas, la atención se centra principalmente en la capa de aplicación y los repositorios de datos asociados a esta capa.

Los modelos de servicio describen los tipos de servicios que pueden ser obtenidos en cloud computing y dependiendo de estos, el proveedor utilizará mecanismos de abstracción de las capas, administración de recursos y control de accesos. Tres modelos son los principales y cualquier otro puede ser derivado de estos modelos [1]:

- *Software como un Servicio (SaaS)*. El servicio está formado por aplicaciones que los usuarios finales pueden acceder a través de uso de navegadores o interfaces web en los dispositivos utilizando protocolos de Internet. Por otro lado, el proveedor se encarga del mantenimiento de plataforma y los mecanismos de seguridad Los accesos son generalmente llevados a cabo mediante la autenticación de contraseñas y token. Dependiendo de las especificaciones del contrato de servicio, el cliente puede tener permisos de configuración de las aplicaciones.
- *Plataforma como un Servicio (PaaS)*. El servicio ofrecido es un contenedor que posee un entorno de programación, con bibliotecas y herramientas que dan soporte al desarrollo de aplicaciones. El contenedor limita las interacciones del entorno de desarrollo con los otros sistemas que se encuentran en la infraestructura física. El proveedor gestiona los accesos a las redes y a las plataformas, y se encarga de las instalaciones de aplicaciones, bibliotecas y herramientas que den soporte al desarrollo en la plataforma virtual.
- *Infraestructura como un Servicio (IaaS)*. El servicio está dado por máquinas virtuales, capacidad de almacenamiento, servicios de base de datos y componentes de redes. El proveedor se encarga de los detalles administrativos, el personal técnico de soporte, el mantenimiento de los recursos físicos, y dispositivos de Internet. Un servidor físico puede contener varios servidores virtuales y el proveedor puede ofrecer estos servicios en fracciones y a diferentes consumidores.

3 Migración de Sistemas Heredados

Los sistemas heredados son soluciones informáticas que se encuentran en una empresa durante un largo periodo de tiempo [16]. Es probable que estos sistemas hayan sobrevividos en una organización gracias a algún tipo de mantenimiento (correctivo, preventivo, y evolutivo), por las resistencias internas al cambio de tecnología, o porque ejecutan los procesos crítico de una organización.

Habitualmente estos sistemas trabajan en forma aislada y poseen un repositorio de datos (archivos de datos, base de datos, etc.) de uso exclusivo. Por lo tanto, la comunicación de estos sistemas a otras aplicaciones es una tarea difícil, que requiere la definición de interfaces complejas de comunicación y componentes de conversión de datos. Por otro lado, las organizaciones que desean continuar siendo competitivas deben invertir recursos para integrar sus herramientas, adaptar sus funcionalidades a nuevas tecnologías y buscar flexibilidad de sus procesos de negocio.

Actualmente, antes de migrar a cloud computing, se transforma primero las aplicaciones tradicionales a aplicaciones basadas en SOA, ya que esta arquitectura es flexible a la composición de servicios. SOA encapsula la lógica del negocio a través de servicios web (WSs) que se comunican entre sí por medio de métodos y protocolos estándares de intercambio de mensaje, que facilita la composición de servicios.

Las aplicaciones constan básicamente de tres capas: *Capa de Presentación*: donde se encuentra la interfaz de usuario; *Capa de Negocio*: donde se encuentran la lógica del negocio y sus funcionalidades implementadas en algoritmos, componentes de software o WSs; y *Capa de Datos*: donde se encuentra los datos y el esquema de datos de la aplicación. Además estas aplicaciones pueden ser migradas por capas.

En la Fig. 1 se presentan un modelo conceptual de migración a cloud computing con las técnicas para migrar aplicaciones. A continuación se describen estas técnicas que serán aplicadas en el proceso de migración propuesto:

- *Substitución de la aplicación:* consiste en reemplazar la aplicación o parte de ella por alguna solución estándar ofrecida en el mercado. Como resultado, algunas configuraciones y actividades de adaptación a los cambios deberán llevarse a cabo como parte de esta migración. Este reemplazo puede generar pérdidas del control de la información, la necesidad de crear interfaces con otros componentes o aplicaciones, la modificación del flujo de trabajo de la organización y el desconocimiento de la estructura interna de los componentes adquiridos [4].
- *Conversión de la aplicación:* consiste en transformar la aplicación en una solución de cloud computing. A través de algún motor de conversión y mapeo de datos convertidos, se puede realizar estas transformaciones de forma automática, pero se requiere que el sistema heredado se encuentre normalizado y no presente fallas. Además, este tipo de migración puede dividirse en tres tipos de conversión [16]:

  (a) *Conversión de programas:* es la transformación de algoritmos y aplicaciones software, manteniendo la funcionalidad y la estructura, pero modificando los aspectos de programación.

(b) *Conversión de datos:* es la transformación de los datos según el esquema y formato destino.
(c) *Conversión de esquemas:* transformar una estructura de datos a una nueva estructura de base de datos equivalente.

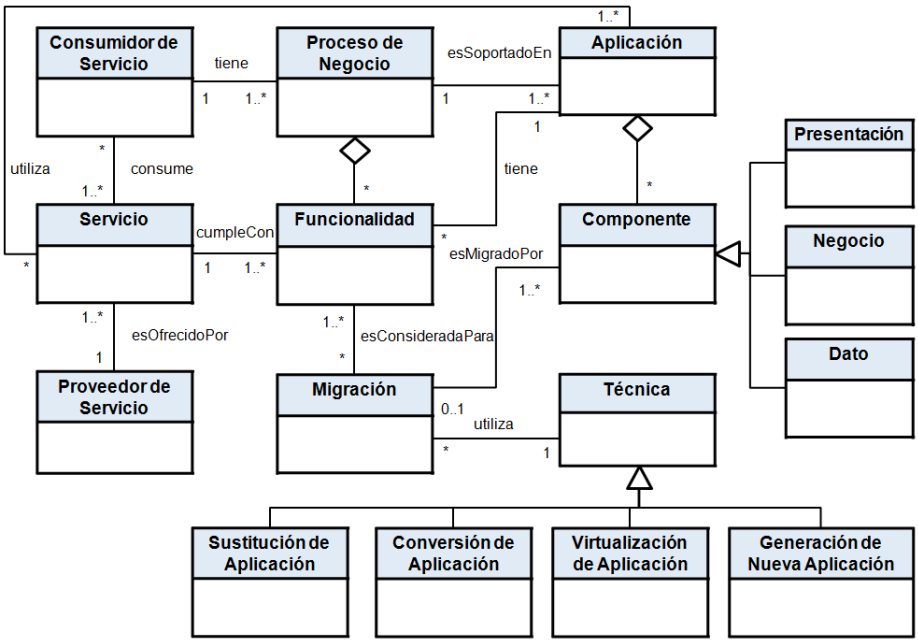

Fig. 1. Modelo Conceptual de Migración a Cloud Computing

- *Virtualización de la aplicación:* consiste básicamente en generar un contenedor virtual de la aplicación y trasladar todos sus componentes sin modificar los códigos fuente y el esquema de datos. Es decir se considera al sistema heredado como una caja negra, donde se encapsulan todas sus capas, y durante la interacción del usuario con el sistema se analizan las entradas y salidas, para generar un "*wrapper*" [9] que pueda ser el nexo el sistema heredado encapsulado y una nueva capa de presentación desplegada en cloud computing.
- *Generación de una nueva aplicación:* se trata de programar una nueva aplicación compatible con los entornos de cloud computing. Esta solución deberá realizar una reingeniería de la aplicación para obtener la definición de sus procesos y funciones, y generar una nueva aplicación para cloud computing. Como parte de esta reingeniería se deberá analizar de aquellas funcionalidades no utilizadas, redundantes, caducadas, con necesidades de mejoras, y que pueden ser consolidadas en otra funcionalidad.

4 Enfoque Propuesto para Migración a Cloud Computing

Una vez comprendido la naturaleza de cloud computing, los sistemas heredados y los factores claves para la migración de estos sistemas, se puede abarcar el enfoque propuesto para la migración de sistemas heredados a una arquitectura del tipo “cloud computing”. En el flujo de trabajo propuesto, no se considera al análisis de seguridad como una tarea independiente, sino integrada a cada una de las tareas involucradas en la migración. Es por esto que el consumidor tiene la responsabilidad de alinear cada actividad de la migración a sus políticas de seguridad y asegurarse que el contrato del proveedor abarque estas políticas.

En la Fig. 2 se encuentra el diagrama propuesto de flujo de trabajo para esta migración. Este esquema incluye 13 procesos que deben ser llevados a cabo por el consumidor, proveedor y desarrollador del servicio. La parte desarrolladora consiste en un equipo de analistas y desarrolladores, que pueden pertenecer al consumidor, proveedor o una empresa consultora. A continuación se analiza cada uno de estos pasos.

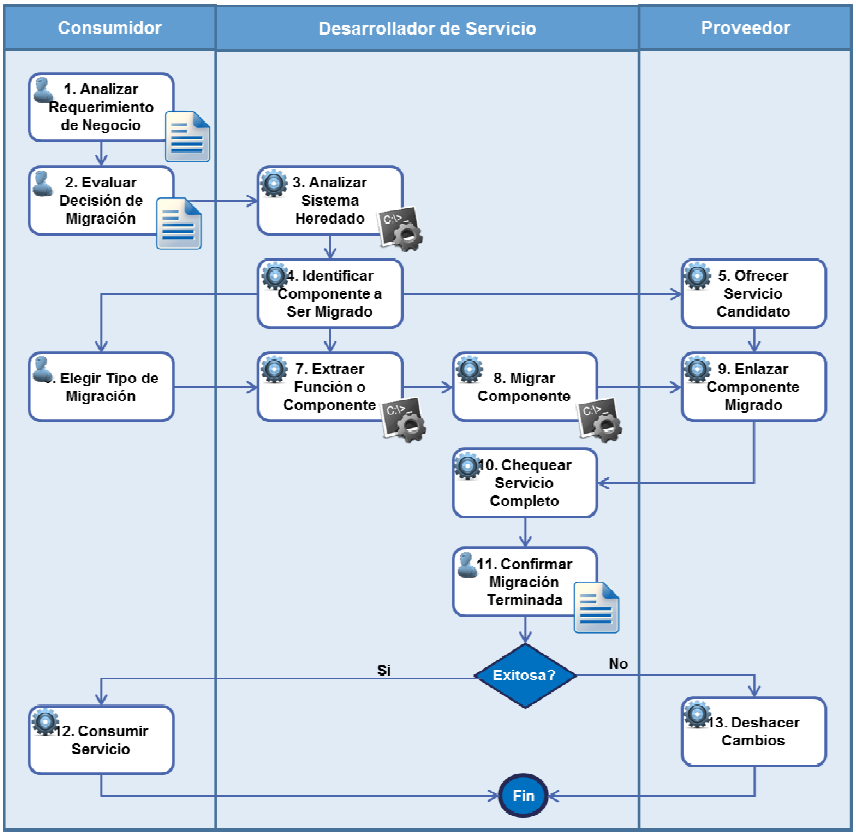

Fig. 2. Workflow para Migración de Aplicaciones a Cloud Computing

1. Analizar Requerimiento de Negocio. El consumidor del servicio debe tener en claro que es lo que desea conseguir al migrar el sistema heredado, una aplicación o un componente a los entornos de cloud computing. Para esto, debe identificar las metas y los objetivos del negocio, y de qué manera esta migración permitirá alcanzarlo. Además debe analizar las características de los datos del negocio, antes de adquirir una modelo de negocio cuyos datos sensibles puedan ser manipulados por otra organización.

2. Evaluar Decisión de Migración. En esta tarea se define el proyecto de migración, la justificación de la migración, las metas, el alcance, y las restricciones. Generalmente, las metas a conseguir con la migración son reducción de costos, ampliar funcionalidades para adaptarse a mercados emergentes, mejorar productividad y seguridad. Se debe analizar estos requerimientos y el impacto de la migración en la organización, y a continuación se define una planificación para la migración.

3. Analizar Sistema Heredado. Esta tarea consiste en entender el sistema actual y para esto se reúne información sobre la implementación, mediante el análisis de componentes. En caso de que el sistema sea una "caja negra" (no haya acceso al código fuente), se analizan las entradas, salidas, y las respuestas obtenidas del sistema. Por otro lado, la ingeniería inversa es útil para sistemas de "caja blanca" (con visibilidad del código fuente) y permite descomponer el sistema en funciones y datos. El análisis final de los diferentes componentes del sistema heredado permitirá dividir las partes de aplicación según el tipo de funciones y alinear estas funciones a las metas del negocio, es decir mapear las funcionalidades a los requerimientos del negocio. También, permitirá descubrir aquellas funcionalidades importantes, que deben conservarse en el sistema migrado.

4. Identificar Componente a Ser Migrado. En este paso, se reconoce el componente a ser migrado, y se extraer su configuración. Según los objetivos de la migración puede ser que el componente a migrar sea una base de datos, una capa de aplicación, una funcionalidad, un algoritmo, o hasta todo el sistema heredado. En este punto se puede considerar una manera de preservar la seguridad de los componentes utilizando algún mecanismo de codificación o encriptación de datos.

5. Ofrecer Servicio Candidato. Esta actividad permitirá identificar los servicios que han sido desplegadas en los entornos de cloud computing, que pudieran contratase para dar solución a la migración. Luego, el consumidor deberá seleccionar los servicios candidatos según el cumplimiento de sus requerimientos y el grado de seguridad que el proveedor garantice en los contratos y SLA. Es posible que los servicios sean ofrecidos directamente por el proveedor de servicio, o también se puede necesitar la participación de un actor bróker, que realice la búsqueda del servicio y el contacto con el proveedor del servicio. Generalmente estos servicios actúan como cajas negras, por lo tanto se deberá analizar la transformación del componente a ser migrado con el

servicio candidato. Es probable que se presente alguno de los siguientes casos: no existe un servicio candidato, el servicio candidato es incompleto, se debe codificar una interfaz para estregar el servicio candidato, o el servicio candidato se ajusta perfectamente a la solución esperada. En la Sección 6 se abordan algunas consideraciones sobre seguridad y contratación que se pueden tener en cuenta en este paso.

6. Elegir Tipo de Migración. Para elegir el tipo se migración se debe validar los componentes identificados, el servicio candidato (en caso de que existiera) y los recursos necesarios para realizar esta migración. El consumidor de servicio deberá indicar qué tipo de migración (presente en la Sección 3) se ajusta a sus objetivos y analizar las políticas necesarios para contratación de servicios, en caso de que un servicio candidato cumpla estos objetivos.

7. Extraer Función o Componente. Una vez identificado y localizado el componente a ser migrado, se procede con su extracción. Para esto se utiliza un mecanismo de débil acoplamiento y alta modularidad, para que este componente sea independiente y no posea rutinas o funciones que puedan ser accedidas desde afuera del componente.

8. Migrar Componente. La primera actividad de esta tarea es realizar una copia de resguardo del sistema funcionando, tanto del código fuente como los datos, en caso de que deba deshacer los cambios realizados durante la migración del componente ("*rollback*"). De acuerdo al tipo de migración seleccionado, en este paso se deberá realizar la programación de las interfaces, la conversión de funciones y adaptación de datos al esquema del nuevo repositorio.

9. Enlazar Componente Migrado. En esta tarea se despliega la solución en los entornos de cloud computing, y se prueban las configuraciones de los servicios del proveedor. Además se establecen las configuraciones necesarias para enlazar los servicios adquiridos a los entornos del consumidor del servicio. Es posible que durante este proceso se necesite la participación de un actor portador, que se encargue de transportar de forma segura todos los componentes migrados a los sistemas del proveedor.

10. Chequear Servicio Completo. Verificar la migración por medio de pruebas, para asegurarse que las funcionalidades necesarias de la antigua implementación se mantienen en la nueva implementación. En esta tarea los analistas de calidad pueden realizar prueba de unidad, prueba de integración, prueba de aplicación y prueba piloto, antes de integrar esta solución a los procesos de la organización.

11. Confirmar Migración Terminada. Después de verificar el correcto funcionamiento del servicio migrado, se deberá evaluar que el servicio cumple con los niveles mínimos de calidad y si está en condiciones de ser incorporado a los proceso de nego-

cios de la organización. Esta confirmación va acompañada de la documentación de la implementación efectuada, la configuración necesaria de los servicios y los cambios realizados durante los pasos del proceso de migración.

12. Consumir el Servicio. El consumidor del servicio deberá estar lo suficientemente preparado para utilizar los servicios y conocer los cambios realizados en la migración del sistema, ya que la migración de funcionalidades a un nuevo paradigma generalmente trae asociado un cambio en los procedimientos de los usuarios.

13. Deshacer Cambios. Este paso se realiza en caso de que la migración haya fallado o no cumple con los niveles mínimos de calidad que necesita el consumidor de servicio, por lo tanto se deberá revertir el proceso de migración utilizando alguna copia de resguardo.

5 Caso de Estudio: Empresa de Distribución de Bebidas

Este caso de aplicación describe brevemente como los pasos presentados en flujo de trabajo son aplicables a una solución de migración de funcionalidades a entornos y servicios de cloud computing.

Se considera a una empresa de distribución de bebidas que debe adaptar su sistema de órdenes de compra, para permitir que sus proveedores de bebidas realicen reportes de demandas diarias, semanales, y mensuales, para la reserva de mercaderías y abastecimiento de pedidos. Además, para lograr competitividad en el mercado de la distribución de bebida, la empresa distribuidora debe asegurarse que su proveedor de bebidas importadas cumpla a tiempo con sus pedidos, y por lo tanto se consideró la instalación de un módulo de compra que permita visualizar el stock y reservar un pedido en tiempo real.

Después de analizar estos requerimiento (*Paso 1. Analizar Requerimiento de Negocio* en Fig. 2), los ejecutivos de la empresa consideraron que su viejo servidor es muy pequeño para realizar los reportes exigidos por sus proveedores de bebidas, y que tener un módulo de compra instalado de otra empresa representaría un riesgo de seguridad informática. Por lo tanto, se evaluó la decisión de migrar estas funcionalidades a cloud computing (*Paso 2. Evaluar Decisión de Migración* en Fig. 2).

La solución encontrada a nivel gerencial fue migrar a un esquema de base de datos (*Paso 4. Identificar Componente a Ser Migrado* en Fig. 2) en cloud computing sólo los datos necesarios para los reportes, evitando poner en riesgo información sensible de sus clientes, y mantener este repositorio actualizado mediante una rutina que actualice los datos regularmente. Esto lo lleva a cabo suscribiéndose un servicio de base de datos de un proveedor de cloud computing y pagando el uso de la red por las transferencias de datos realizadas (*Paso 5. Ofrecer Servicio Candidato*, *Paso 6. Elegir Tipo de Migración*, y *Paso 7. Extraer Función o Componente* en Fig. 2). En definitiva, esta solución es mucho más rentable que adquirir un nuevo servidor. De esta manera, los surtidores y proveedores pueden acceder a la información necesaria, y crear sus repor-

tes de ventas y tendencias del mercado (*Paso 9. Enlazar Componente Migrado* en Fig. 2). Por otro lado, para los pedidos online se decidió adquirir una interfaz del tipo wrapper que interactúe con el módulo de pedidos del sistemas del proveedor de bebidas importadas. De esta manera, un empleado de la distribuidora entra a un formulario online y el *wrapper* se encarga de interactuar con el sistema (*Paso 12. Consumir el Servicio* en Fig. 2) después de un intercambio de certificados de seguridad.

6 Recomendaciones para la contratación en Cloud Computing

La aceptación del empleo de servicios ofrecidos bajo la arquitectura de "cloud computing" depende ampliamente de la manera que los mismos cumplan con los requerimientos funcionales y no funcionales planteados por los consumidores. Sin embargo, la seguridad y los contratos de servicios son los aspectos más criticados de las soluciones de cloud computing. Es por ello que se considero dedicar esta sección para tratar algunos de los aspectos de seguridad más importantes que los consumidores deben tener en cuenta, cuando desean mudar alguna funcionalidad a esta arquitectura.

Generalmente la brecha de seguridad se crea porque los centros de datos de los proveedores de servicio no están ubicados en la misma geografía que el consumidor del servicio, y por lo tanto estos no están obligados a cumplir los mismos aspectos legales. Consecuentemente, el consumidor de servicio debe evaluar las políticas de seguridad ofrecidas en el SLA y asegurarse que se ajustan a las necesidades de su organización.

En el siguiente listado se encuentran los aspectos de seguridad más importantes considerados por la European Network and Information Security Agency (ENISA) [17] y algunas recomendaciones sobre los mismos:

- *Protección, Seguridad de Datos y Propiedad Intelectual*: en este punto se debe analizar aspectos [18] como la autenticidad, la integridad de los datos y servicios, la operatividad durante un periodo de tiempo, y la confidencialidad de la información. Antes de adquirir un servicio, donde se delegue la manipulación de datos sensibles de la organización, se debe analizar que el contrato estipule mecanismos de protección, garantías de tratamiento lícito y compensaciones ante violación de estas cláusulas. Además, el proveedor debe verse obligado a notificar cuando existen amenazas, riesgos o incidentes que afecten la integridad, la confidencialidad y la disponibilidad de la información del cliente.
- *Transferencia de Información*: Garantizar la protección adecuada de los datos, aun cuando el origen/destino de la transferencia sea de diferente jurisdicción.
- *Confidencialidad y no divulgación:* El consumidor del servicio debería analizar las políticas de confidencialidad y no divulgación de sus datos y saber qué información circulará en los entornos de cloud computing, ya que estos datos pueden almacenarse y procesarse sin su consentimiento.
- *Limitación de la responsabilidad:* Considerar los riesgos y los límites de responsabilidad cuando no se cumpla un contrato, además que las compensaciones asociadas sean de la dimensión de los riesgos.

- *Análisis de impacto al cambio de control:* Otorgar responsabilidades y obligaciones contractuales cuando el proveedor realice cambio de control o subcontrataciones sin consentimiento del consumidor.
- *Portabilidad de datos y funcionalidad:* Exigir en los contratos de negocio que la transferencia de datos y documentos entre proveedores del servicio pueda llevarse a cabo sin complicaciones, así el consumidor pueda migrar sus servicios de cloud computing cuando lo requiera necesario.

Estos riesgos de seguridad, no sólo se pueden presentar en los sistemas del proveedor del servicio, sino que también pueden ser riesgos internos de la infraestructura del consumidor y de las redes utilizadas en la contratación de servicios.

7 Conclusiones

En este trabajo inicialmente se abordan las características del empleo de servicios de tipo “cloud computing”, razones por la cual este paradigma de negocio continúa creciendo, y la mecánica que utiliza para el aprovisionamiento de recursos físicos y virtuales. Luego se presentaron los modelos de despliegue, según la ubicación (on premises y off premises) y según el acceso (nube privada, nube pública, nube comunitaria y nube hibrida). También se identificaron las capas físicas y lógicas que tiene un sistema de información y, según el control que el proveedor otorga al consumidor sobre estas capas, se clasificó los modelos de servicio de cloud computing (IaaS, PaaS y SaaS).

Luego se describieron las características de los sistemas heredados, y se explicó la tendencia de transformar estos sistemas a aplicaciones basadas en SOA. A continuación se presentaron las técnicas de migración de los sistemas heredados a cloud computing y un diagrama conceptual de esta migración.

En este trabajo se ha propuesto un workflow preliminar para llevar a cabo la migración de sistemas heredados, el cual consiste en 13 pasos. Este enfoque fue creado según experiencias previas en proyecto de migración de sistema y el análisis de las características de cloud computing. Luego, se presentó un ejemplo ilustrativo de la aplicación de este workflow en una empresa mediana de distribución de bebidas. El proceso propuesto es sencillo y representa un esquema útil para organizar las decisiones y las tareas de adquisición de servicios en cloud computing.

Finalmente, se consideró que el plan de seguridad debe integrarse a todo el proceso de migración, y además se enunciaron algunos puntos y recomendaciones sobre la seguridad y contratación de servicios.

Agradecimientos. Este trabajo ha sido financiado en forma conjunta por CONICET, la Universidad Tecnológica Nacional y la Agencia Nacional de Promoción Científica y Tecnológica. Se agradece el apoyo brindado por estas instituciones.

8 Referencias

1. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. National Institute of Standards and Technology. NIST Special Publication 800-145 (2011)
2. Vaquero, L. M., Rodero-Merino, L., Caceres, J., Lindner, M.: A break in the clouds: towards a cloud definition. SIGCOMM Computer Communication Review 39(1), pp. 50-55. ACM (2008)
3. Mezgar, I., Rauschecker, U.: The challenge of networked enterprises for cloud computing interoperability. Comput. Industry (2014)
4. Andrikopoulos, V., Binz, T., Leymann, F., Strauch, S.: How to adapt applications for the Cloud environment. Computing, 95(6), 493-535 (2013)
5. Kaisler, S. H, Money, W. H.: Service Migration in a Cloud Computing. Proceeding of the 44th Hawaii International Conference on System Sciences. Hawaii (2011)
6. Kwon, Y. W., & Tilevich, E.: Cloud refactoring: automated transitioning to cloud-based services. Automated Software Engineering, 1-28 (2013)
7. Khadka, R., Saeidi, A., Jansen, S., Hage, J.: A structured legacy to SOA migration process and its evaluation in practice. In Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), 2013 IEEE 7th International Symposium on the (pp. 2-11). IEEE (2013)
8. Khadka, R., Saeidi, A., Jansen, S., Hage, J., & Haas, G. P.: Migrating a large scale legacy application to SOA: Challenges and lessons learned. In Reverse Engineering (WCRE), 2013 20th Working Conference on(pp. 425-432). IEEE (2013)
9. Canfora, G., Fasolino, A. R., Frattolillo, G.,Tramontana, P.: Migrating interactive legacy systems to web services. In Software Maintenance and Reengineering, 2006. CSMR 2006. Proceedings of the 10th European Conference on (pp. 10-pp). IEEE (2006)
10. Chauhan, M. A., & Babar, M. A.: Migrating service-oriented system to cloud computing: An experience report. In Cloud Computing (CLOUD), 2011 IEEE International Conference on (pp. 404-411). IEEE (2011)
11. Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), pp. 7-18 (2010)
12. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6), 599-616 (2009)
13. Badger, L., Grance, T., Patt-Corner, R., Voas, J.: Cloud computing synopsis and recommendations. NIST Special
14. Winkler, V. J.: Securing the cloud: Cloud computer security techniques and tactics. Syngress, Boston (2011)
15. Winkler, V. J. Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier (2011)
16. Hainaut, J. L., Cleve, A., Henrard, J., Hick, J. M.:Migration of legacy information systems. In Software Evolution (pp. 105-138). Springer Berlin Heidelberg (2008)
17. Catteddu, D., Hogben, G.: Cloud computing: Benefits, risks and recommendations for information security. European Network and Information Security Agency: Heraklion, Crete, Greece (2009)
18. Cherdantseva, Y., Hilton, J.:A Reference Model of Information Assurance & Security. In Availability, Reliability and Security (ARES) 2013 Eighth International Conference on (pp. 546-555). IEEE (2013)