Cloud Computing. Su aplicación en la banca privada argentina.

Hector Noceti[1], Anibal Freijo[1]
[1] Universidad Argentina de la Empresa (UADE), Facultad de Ingeniería y Ciencias Exactas
Buenos Aires, Argentina
{hnoceti, afreijo}@uade.edu.ar

Resumen. Cloud Computing es un modelo de tecnología basado en una combinación de recursos de hardware y software que, disponibles bajo la modalidad de servicio, pueden ser utilizados por individuos y organizaciones. Esta tecnología posibilita que los recursos puedan ser utilizados en todo momento, desde cualquier lugar en el que se encuentre el usuario, por medio de diferentes tipos de dispositivos (PC, notebook, netbook, tablets, smartphones), gracias a su capacidad de procesamiento y conexión a través de Internet.
Los primeros en adoptar esta tecnología fueron los individuos, y lentamente se han ido incorporando las organizaciones, que si bien identifican las ventajas de este modelo, se plantean dudas e inquietudes respecto de aspectos vinculados a la seguridad física y lógica de sus datos, y de las normativas legales que regulan la ubicación física de los mismos.
Las entidades financieras, no escapan a este análisis, dado que como toda organización busca optimizar el uso de la tecnología informática y los niveles de inversión y gastos aplicados, pero deben afrontar los retos que en materia de seguridad y marco regulatorio les presenta esta tecnología.

Palabras clave: Cloud computing, entidades financieras, seguridad, aspectos regulatorios, modelos de implementación, modelos de servicio, data centers, virtualización.

1 Introducción.

El concepto de *Cloud Computing* adquiere difusión pública a mediados de la primera década del 2000, a partir de que millones de personas comenzaron a hacer uso de las aplicaciones instaladas sobre infraestructura de hardware y software, disponible a través de Internet. El camino se inició con servicios de mail electrónico, como Hotmail, Yahoo y Gmail, por citar algunos, se potenció con la aparición de las redes sociales, y otros servicios como Google Drive, Open Drive, Dropbox, etc..
Todo esto y la proliferación de dispositivos móviles como notebooks, netbooks, tablets y smartphones, promueve que millones de usuarios puedan tener acceso a aplicaciones, transferir archivos o integrarse a redes sociales y/o laborales, desde cualquier lugar y en cualquier momento, e inclusive cambiar los hábitos y las formas de trabajar de las personas y las empresas [6].
Cloud Computing, juntamente con Big Data, Mobile Technology y Social Network constituyen lo que se ha dado en llamar la tercera plataforma tecnológica.
A diferencia de lo que ha sucedido con anterioridad, donde las nuevas tecnologías eran adoptadas primero por las organizaciones, en el caso de *Cloud Computing,*

fueron los individuos los primeros en incursionar en ella, y luego lentamente, las organizaciones.
Esto no es casual, pues si bien se reconocen en *Cloud Computing* muchas ventajas, hay varios retos vinculados a los aspectos de seguridad física y lógica de los datos, que provoca en las organizaciones dudas respecto de su adopción.
Varias entidades financieras argentinas han analizado las ventajas de esta tecnología, pero se plantean inquietudes acerca de la seguridad de los datos y respecto de los aspectos regulatorios.
Este artículo, pretende describir las principales características de la tecnología Cloud Computing sus ventajas, desventajas, modelos de servicio y de implementación, evaluar las diferentes alternativas de uso que los bancos pueden hacer de esta tecnología, e identificar los motivos que impulsan y condicionan a los bancos en adoptar esta tecnología así como la innovación organizativa que producen en las áreas de IT de las organizaciones.

2 Que es Cloud Computing.

Según el National Institute of Standard and Technologies (NIST) "*Cloud Computing es un modelo que permite en forma ubicua, conveniente y compartida, el acceso bajo demanda, a través de la red, a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar rápidamente y liberarlos con un esfuerzo mínimo de gestión e interacción con el proveedor de servicios…"* [10].
El término "ubicuo", da idea de la disponibilidad en forma permanente en el tiempo, desde cualquier lugar y a través de cualquier dispositivo, para hacer uso de los servicios de IT ofrecidos en el modelo "cloud".
El concepto de "*Cloud Computing*", también se asocia a:

- Abstracción: de toda implementación física. Los usuarios finales y desarrolladores de aplicaciones en la nube, no necesitan conocer la ubicación física de los servidores y sistemas de almacenamiento de datos, como tampoco de la administración y operación de esos entornos.
- Virtualización: tecnología que posibilita que sobre un mismo servidor físico puedan estar ejecutándose más de un servidor lógico o virtual, con diferentes sistemas operativos y compartiendo los recursos de procesamiento disponibles.

3 Cloud Computing. Características.

El NIST identifica cinco características esenciales que reúne la tecnología *Cloud Computing*:

a) Servicio "On Demand": es la posibilidad del cloud consumer de auto-gestionar, sin necesidad de intervención del cloud provider, la capacidad de procesamiento, el espacio de almacenamiento en disco y los recursos de la red, de acuerdo a las necesidades del negocio [10].
Esta característica lo distingue de los servicios "on premise" de data centers corporativos propietarios, en los cuales las áreas de IT dependen de la disponibilidad de los recursos de hardware y software existente, o de realizar inversiones para contratar ampliaciones de equipos y/o licencias de software adicionales, y la afectación de los recursos humanos con perfil técnico adecuado para cumplimentar el requerimiento dentro del plan de trabajo.

El modelo "*Cloud*", se basa en la abstracción que el proveedor del servicio cuenta con los recursos de hardware, software y humanos para atender las necesidades del cliente, de acuerdo al nivel de servicio previamente pactado [6] y este puede adecuarse dinámicamente según las necesidades de la organización.

b) Acceso amplio a la red IP: capacidad y disponibilidad de la red de datos, para que pueda ser accedida a través de protocolos estándar, de manera de promover el uso de múltiples dispositivos tales como notebooks, netbooks, mobile phones, tablets, y desktops [10].
c) Recursos compartidos: los recursos informáticos del cloud provider, conforman un pool destinado a servir a múltiples cloud consumers, a través de un modelo "multi-tenant" o de múltiples usuarios, con diferentes recursos físicos y virtuales que son asignados y reasignados en forma dinámica de acuerdo a la demanda de los cloud consumers. Esta característica contribuye a mejorar los costos de oportunidad de acceder y utilizar recursos de IT.
d) Elasticidad: los recursos de IT se asignan/desasignan según la necesidad del cloud consumer, siendo en apariencia para éste ilimitados, y disponibles en todo momento [10].
   El proceso de asignación/des-asignación inclusive puede ser automático.
e) Servicio medido: está ligada a los conceptos de Servicio On Demand y Elasticidad, y tiene que ver con la posibilidad del cloud consumer de saber qué cantidad de recursos dispone y efectivamente usa, y poder determinar los costos asociados.

Adicionalmente se pueden agregar:

f) Capacidad de monitoreo: el cloud consumer debe poder contar con herramientas provistas por el cloud provider que le permitan monitorear el rendimiento y calidad de los servicios contratados y utilizados [6].
g) Interfaces para integración de aplicaciones: consiste en la provisión de APIs (Application Program Interfaces) estandarizadas, de manera que el cloud consumer pueda integrar sus aplicaciones legacy con las aplicaciones en la "nube". Esta es una condición necesaria para posibilitar la interoperabilidad de los sistemas en la "nube" con otras aplicaciones propias del cliente [6].

4 Modelos de implementación.

Básicamente se identifican tres modelos de implementación de *Cloud Computing*:

a) Public Cloud o Nube Pública
b) Private Cloud o Nube Privada
c) Hybrid Cloud o Nube Híbrida

Además de los modelos mencionados, el NIST incorpora el modelo de Community Cloud o Nube Comunitaria [10].

Public Cloud: se trata de infraestructura tecnológica (hardware, software de base, aplicaciones y servicios) que está disponible para el uso público en general. Este tipo de "nube" puede estar gestionado por una empresa, entidad académica o gubernamental o combinaciones de ellas [10].

Por lo general una public cloud, está alojada en más de un data center del cloud provider, ubicado en diferentes sitios geográficos, y los servicios son ofrecidos a múltiples cloud consumers, quienes comparten los mismos recursos.
La gestión de seguridad, la provisión de los recursos, y el mantenimiento en funcionamiento de la infraestructura ofrecida, es responsabilidad directa del cloud provider [6].

Private Cloud: la infraestructura de una private cloud es gestionada y utilizada por una única organización. La gestión puede estar delegada en un tercero, pero bajo supervisión directa de la organización. Asimismo la nube puede estar dentro de los límites físicos de la organización o fuera de la misma.
El rasgo distintivo de este tipo de implementación, es que la seguridad física y lógica, así como la operación y administración, es realizada por la misma organización propietaria de la nube privada, quien adopta las características del modelo de la tecnología de *Cloud Computing*, para concentrar el acceso de todos usuarios, locaciones y departamentos de una organización a un conjunto de recursos que se brindan a través de la nube [5].
Desde el punto de vista de los roles, dentro de la misma organización se hallan el de cloud provider y el cloud consumer. El primero lo cumple el departamento de IT, y el de consumer el resto de las áreas que requieren recursos de la nube privada.

Hybrid Cloud: según la definición que proporciona el NIST, "*es la composición de dos o más nubes (ej. privada y pública), que siguen siendo entidades únicas, pero que se integran entre ellas por tener tecnologías compatibles que les permiten compartir datos y aplicaciones, y ser portables entre ellas"* [10].
Este modelo de despliegue de la tecnología Cloud, es aplicable por aquellas organizaciones que, por motivos de seguridad deciden implementar una nube privada sobre la cual instalan sus aplicaciones críticas y datos de producción sensibles, pero que las integran con nubes públicas con la finalidad de que éstas provean recursos en casos de picos de demanda, o bien para la instalación de ambientes no productivos (ej.: desarrollo y *testing* de aplicaciones) o para de uso de aplicaciones no críticas, o ambientes de recupero previstos en los DRPs (Disaster Recovery Plan).

Community Cloud: esta implementación propuesta por el NIST, la define como "*la infraestructura que está preparada para ser utilizada en forma exclusiva por una comunidad de cloud consumers que comparten en común una misión, políticas de seguridad, regulaciones y compliance. Esta nube puede ser administrada y operada por uno o más cloud consumers integrantes de la comunidad, o por un tercero"* [10].
Este tipo de implementación de nube, es aplicable por lo general en organismos estatales o integrantes de holdings, que si bien son organizaciones independientes entre sí, comparten una misma misión, políticas de gestión, de seguridad etc.

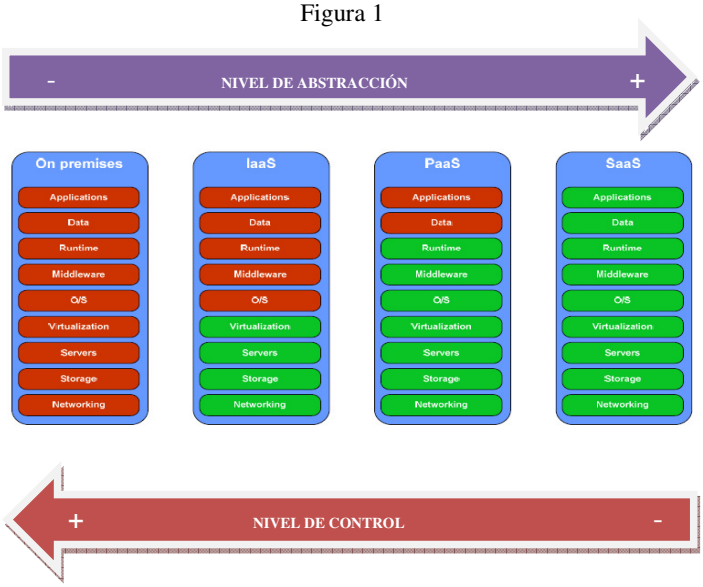
5 Modelos de Servicio.

Existen básicamente tres modelos de servicio, en la nube:
a) Infraestructure as a Service o Infraestructura como Servicio (IaaS)
b) Platform as a Service o Plataforma como Servicio (PaaS)

c) Software as a Service o Software como Servicio (SaaS)

Independientemente de los modelos citados, hay una variada cantidad de combinaciones dependiendo de los recursos de IT ofrecidos. Como ejemplo de estos modelos de servicio se pueden citar: Storage as a Service, Desktop as a Service y Process as a Service.
La figura 1, ayuda a describir cada una de las modalidades básica de servicio, y los niveles de control y de responsabilidad del cloud consumer y del cloud provider.

Figura 1



Fuente: [12].

A medida que aumenta en nivel de abstracción según el modelo de servicio cloud que se adopte, disminuye el nivel de control y de gestión sobre la infraestructura de IT, aplicaciones y seguridad.

a) Infraestructura como servicio: Es el modelo de servicio cloud, que más se aproxima al concepto de infraestructura "on premise" o propietario. De acuerdo al NIST, este tipo de servicio se define como la capacidad de procesamiento, infraestructura de red y almacenamiento puesta a disposición del cloud consumer, para que pueda instalar libremente, sistemas operativos, motores de bases de datos, aplicaciones propias y/o de terceras partes [10].
El cloud consumer asume el control a partir de la capa de sistema operativo en adelante, es decir, hasta la aplicación inclusive. Por el contrario, no tiene capacidad de gestión sobre la infraestructura subyacente: software de virtualización de servidores y los niveles más bajos del stack de servicios. Esta modalidad es apropiada para aquellos cloud consumers que quieren tener control

sobre el entorno lógico en el cual corren sus aplicaciones de negocio, sin que ello implique inversiones en infraestructura de data center, hardware, y redes de conectividad.

El cloud provider, ofrece estos servicios en entornos virtualizados, es decir, que sobre un mismo hardware, puede configurar múltiples entornos virtuales, sobre los cuales cada cloud consumer puede instalar una versión de sistema operativo diferente. Por esta razón, el cloud provider asume el control del software de virtualización.

b) Plataforma como servicio: Se lo define como la capacidad ofrecida al cloud consumer para que pueda desarrollar aplicaciones utilizando lenguajes de programación, bibliotecas, servicios y herramientas de apoyo provistos por el cloud provider [10]. El cloud provider pone a disposición un ambiente "ready to use", conformado por un set de productos y herramientas de desarrollo pre-configurados, que le facilitan al cloud consumer cubrir el ciclo de vida de una aplicación [5].

   Esta opción puede ser de utilidad para quienes desarrollan aplicaciones para terceros, sean estos usuarios de la nube o no, y también para las organizaciones que ven en esta modalidad la posibilidad de escalar en plataformas de desarrollo sin necesidad de realizar inversiones.

   Desde el punto de vista del control, bajo esta modalidad, el cloud consumer no tiene gestión sobre la infraestructura en la cual se desarrollan las aplicaciones (red de datos, servidores, sistema operativo, motor de base de datos, almacenamiento), pero sí sobre las aplicaciones que despliega, su configuración, así como de los datos que utiliza.

   Ejemplos de soluciones en la nube de plataforma como servicio, son Windows Azure, Google App Engine, Force.com, entre otras.

c) Software como servicio: El NIST define esta modalidad de servicio como: "*La capacidad ofrecida al cloud consumer de utilizar las aplicaciones del cloud provider que se ejecutan en una infraestructura cloud. Las aplicaciones son accesibles desde diferentes dispositivos cliente a través de una interfaz de cliente delgado, como un navegador web (por ejemplo, el correo electrónico basado en la web) o una interface. El cloud consumer no administra ni controla la infraestructura sobre la cual se ejecuta la aplicación: red de datos, servidores, sistemas operativos, almacenamiento y capacidades de aplicación, incluso individuales, con la posible excepción de los ajustes de configuración de la aplicación que son específicas del usuario*" [10].

   Este es el modelo de servicio de *Cloud Computing* más evolucionado y de mayor nivel de abstracción al que puede acceder un cloud consumer. Su responsabilidad de gestión y de control sobre la aplicación está limitada a determinadas funciones de parametrización, y en algunos casos, hasta la configuración y/o asignación de los permisos a los usuarios que accederán al sistema. El cloud consumer no tiene posibilidad de gestionar los recursos subyacentes a la aplicación. Como contrapartida el cloud provider asume la mayor responsabilidad de gestión sobre la infraestructura de red, servidores, almacenamiento, sistema operativo, mantenimiento e implementación de nuevas versiones del sistema aplicativo.

Otra característica significativa de esta modalidad de servicio en la nube, es que el cloud consumer no necesita instalar aplicaciones en forma local, ya que puede accederlas por medio de un navegador a través de Internet, y mediante cualquier dispositivo de acceso (notebook, netbook, tablet, o smatphone). Como contraprestación abona un cargo que puede estar en función de la cantidad de licencias de usuario final, o conexiones concurrentes, espacio de almacenamiento ocupado, entre otras modalidades.

Ejemplos de software como servicio, se pueden mencionar a Google Apps, el CRM (Customer Relationship Management) de SalesForce.Com, Office 365, Microsoft Exchange Online, y similares.

6 Oportunidades y retos de Cloud Computing.

Los CIO's enfrentan habitualmente diferentes desafíos para dar respuesta a los requerimientos de la organización. *Cloud Computing* pretende dar respuesta a algunos de estos desafíos, tales como:

a) Optimizar la utilización de los recursos de IT: una de las tareas más complejas del responsable de IT de una organización, es la adecuada planificación estratégica y táctica de los recursos informáticos con los que debe contar para dar efectivo soporte a las actividades del negocio, y con la presión de las áreas financieras de reducir los niveles de inversión y de gastos de la organización. Alcanzar el punto de equilibrio entre la falta y la subutilización de recursos no es simple de obtener. *Cloud Computing* da una respuesta a este problema, pues pone a disposición de los cloud consumers todos los recursos técnicos disponibles para que se auto-aprovisionen de acuerdo a sus necesidades. Desde esta manera es posible reducir los niveles de inversión necesarios para incorporar y/o actualizar la plataforma de IT instalada, hasta el extremo de poder llevar un modelo basado en CAPEX a uno totalmente basado en OPEX, donde la organización solo paga por aquello que efectivamente utiliza.

b) Estar actualizado tecnológicamente: la aparición de nuevas tecnologías, obliga a las organizaciones a mantenerse actualizadas en materia de equipamiento y software. Este proceso requiere de nuevas inversiones, entrenamiento y una planificación acorde para la puesta en marcha de los cambios, sin disrupciones en el servicio. *Cloud Computing,* hace posible que los cloud consumers puedan acceder a nuevas tecnologías de IT sin necesidad de realizar inversiones y contar con personal técnico entrenado.

c) Contar con recursos humanos entrenados: por igual razón que la indicada en el punto precedente, los responsables de IT deben afrontar el desafío de mantener permanentemente capacitado a su personal técnico. Este proceso se puede complejizar debido a que no siempre hay profesionales disponibles en cantidad suficiente.

d) Asegurar alta disponibilidad de los servicios: asegurar la disponibilidad de los servicios informáticos en forma "on site", y "off site" para los casos de situaciones de contingencia que afecten al sitio de producción requiere recursos económicos adicionales y de personal entrenado. En contraposición, el modelo tradicional u "*on premise*" exige mayor nivel de inversión e implica costos de mantenimiento adicionales.

Pero así como a *Cloud Computing* se le reconocen ventajas, también existen aspectos que son retos que deben afrontar quienes pretenden adoptar esta tecnología:

a) Incremento de las vulnerabilidades de seguridad: desde el momento en que una organización decide trasladar a la "nube" sus datos, la responsabilidad sobre su seguridad y confidencialidad pasa a estar compartida con el proveedor del servicio. El límite de la confianza del cliente hacia el proveedor, se extiende a medida que se pasa de una nube privada a una nube pública.
   Otro punto importante de vulnerabilidad, deriva de una cualidad básica del modelo Cloud, que es el de compartir recursos entre múltiple usuarios (multienancy). Esto trae como consecuencia, una superposición de los límites de confianza entre múltiples clientes del servicio, que implica un incremento en la exposición de los datos, de forma que personas u organizaciones faltas de ética puedan vulnerar normas o principios de confidencialidad [5].
b) Reducción del IT Governance: a medida que la tecnología informática ha ido adquiriendo importancia estratégica dentro de las organizaciones, quienes tienen la responsabilidad de dirigirlas consideran como parte integral de ese gobierno un adecuado liderazgo de las estructuras y procesos de IT para asegurar que contribuya a sostener y extender las estrategias de la organización y sus objetivos [13].
   La migración de un entorno "on premise" a un ambiente *Cloud*, impacta en el gobierno de IT debido a que se introducen los riesgos derivados de la calidad de operación del proveedor del servicio. Estos riesgos aumentan dependiendo del modelo de implementación del servicio *cloud* que se elija. Si el service provider es poco fiable o no cumple adecuadamente con el nivel de servicio acordado, puede poner en riesgo la normal operación del negocio [5].
   Una forma de mitigar este riesgo, es la existencia de un contrato con el proveedor cuyas cláusulas hayan sido analizadas por las áreas técnicas y legales de la empresa, y que contemple un acuerdo de nivel de servicio (SLA) aceptable para ambas partes, además de la realización de inspecciones técnicas, monitoreos y auditorías permanentes.
c) Portabilidad limitada: tiene que ver con la facilidad que tiene un cloud consumer, de trasladar sus datos y servicios de IT, de un proveedor a otro, o de pasar al modelo "on premise" [3].
   Este es un punto crítico que impacta directamente en la gobernabilidad de IT de una organización en razón de la dependencia que el cloud consumer asume respecto del proveedor del servicio. Una forma de reducir esta dependencia, es contar con estándares de procesos, datos y sistemas, de manera que se puedan integrar aplicaciones de diferentes proveedores, o diferentes plataformas o nubes.
   De acuerdo al documento publicado por el NIST sobre la arquitectura de los componentes de una solución de servicios *Cloud*, el cloud provider debe proveer los mecanismos necesarios para dar a soporte a la portabilidad de datos, a la interoperabilidad de los servicios y la portabilidad de los sistemas [9].
   La falta de mecanismos de portabilidad y/o estándares de interoperabilidad puede ser una traba a la hora de decidir migrar servicios a la nube [13].
d) Compliance y regulaciones legales: Desde el punto de vista legal o regulatorio, existen normas que limitan a las organizaciones la posibilidad sus datos fuera del

país o a países con los cuales no hay convenios bilaterales. Este es un punto importante, pues los clouds providers cuentan con data centers en ubicados en diferentes países, siendo complejo determinar la ubicación exacta de los datos [13].

7 Cloud Computing. Su uso en las entidades bancarias argentinas.

Para analizar las posibilidades de que la tecnología cloud computing pueda ser adoptada por las entidades financieras situadas en la República Argentina, es conveniente hacer un repaso de las principales normas que regulan la actividad.
En primer lugar la actividad financiera está regulada por la ley 21.526 y sus modificatorias. Uno de los puntos importantes a tener en cuenta es el establecido en el artículo 39 que obliga a las entidades a mantener el "secreto bancario", que les impide "revelar las operaciones pasivas que realicen" con sus clientes, a excepción de requerimientos judiciales, del BCRA u organismos recaudadores [7]. En otros términos, las entidades están obligadas a mantener la confidencialidad de los datos de sus clientes.
El BCRA, como entidad de contralor, ha emitido una serie de comunicaciones de cumplimiento obligatorio por las entidades financieras, en materia de tecnología y seguridad informática. Entre estas se destacan las comunicaciones A 4609/06, 5374/12 [1], [2].
Es importante señalar que la Com. A 4609, en su sección 7 prevé la posibilidad de que las entidades financieras deleguen *"…en terceros actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas"*. Si bien la norma no es específica para la actividad de *Cloud Computing,* contiene ciertos puntos que le son aplicable como la responsabilidad del directorio de la entidad financiera en el análisis de los riesgos de delegar actividades en terceros, requisitos formales que debe reunir la contratación del proveedor, así como el control y auditorías que la entidad debe realizar al proveedor, entre otras [1].
En cuanto a la Com. A 5374, establece los requisitos de seguridad relacionados con los canales electrónicos utilizados por las entidades financieras para dar servicios a sus clientes (control de acceso, integridad y registro, monitoreo y control, gestión de incidentes) [2].

Por otra parte, las entidades están alcanzadas por la ley 25.326 de protección de datos personales. En particular en los siguientes artículos:

a) Artículo 2: define conceptos tales como datos personales y sensibles, los medios de archivo sean electrónicos o no, el tratamiento de los datos a través del procesamiento electrónico o automatizado y el responsable del archivo, base o banco de datos [8].
b) Artículo 9: referido a la seguridad de los datos, reafirma que el "*responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas"* para garantizar "*la seguridad y confidencialidad de los datos personales",* a la vez que prohíbe el registro de datos personales en archivos o registros *"que no reúnan las condiciones técnicas de integridad y seguridad"* [8].

c) Artículo 10: establece el concepto de "*deber de confidencialidad"* según el cual el responsable del archivo o banco de datos o terceros intervinientes en el proceso, están obligados a mantener en secreto de los mismos. Solo releva de este secreto cuando hay a un requerimiento judicial o por razones "*seguridad pública, la defensa nacional o la salud pública"* [8].

d) Artículo 11: fijas las condiciones para realizar la cesión de datos. La cesión se conforma cuando todo o una parte de una base de datos es entregada por el *cedente*, que es el titular de la base de datos personales, a un *cesionario,* con la limitación de que los datos cedidos sean utilizados dentro de los fines relacionados con los intereses legítimos del cedente y cesionario [11].
Dos consideraciones importantes a tener en cuenta, son que el cedente debe contar "*con el previo consentimiento del titular de los datos",* pudiendo ser este consentimiento revocado en cualquier momento, y además, que es responsable solidario con el cesionario del cumplimiento de la LEY 25.326 [8].

e) Artículo 12: prohíbe la transferencia de datos personales de cualquier tipo "*con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados".* Se excluye explícitamente de esta obligación a las transferencias bancarias o bursátiles en lo referido a la transacción propiamente dicha. Sobre este punto en particular, el decreto del Poder Ejecutivo Nacional 1558/2001 reglamentario de esta ley, faculta a la Dirección Nacional de Datos Personales a evaluar de oficio o a pedido de un interesado, el nivel de protección que proporciona un país u organismo internacional a los datos a fin de autorizar la transferencia de los mismos [4].
Es importante tener en cuenta que para la Argentina, Estados Unidos, es considerado un país donde la normativa vigente no ofrece un nivel adecuado de protección, por lo que la transferencia de datos desde Argentina hacia Estados Unidos requiere, en cada caso, de un pedido de autorización a la Dirección Nacional de Protección de Datos Personales (DNPDP). Este no es un tema menor, pues cada organización que quiera transferir datos hacia Estados Unidos debe solicitar una evaluación de parte de la DNPDP.

8 Posibilidades concretas de aplicar cloud computing en las entidades bancarias.

Es una tendencia clara en las organizaciones a ser más eficientes, es decir brindar más y mejores servicios a sus clientes optimizando sus costos.
Las entidades bancarias del mercado argentino, aún con las ventajas que ofrece el modelo *Cloud Computing*, no lo han adoptado masivamente, y las que han comenzado a incursionar, lo han hecho en aplicaciones no vinculadas al core business, como el mail corporativo, soluciones de productividad y colaboración, aplicaciones de oficina.
Migrar a la "nube" las aplicaciones core, es evidentemente un paso crítico, y las nuevas tecnologías requieren de un proceso de maduración del mercado y de los proveedores antes de que sean adoptadas en forma masiva, y más aún si son disruptivas, como es el caso de *Cloud Computing*.

También generan innovación desde el punto de vista organizativo, al tener que reconvertir al personal técnico de las áreas de IT, dedicado a gestionar operativamente los recursos informáticos de la entidad, para cumplir tareas más orientadas a auditoría y control, que a tareas operativas.
Otro aspecto importante es que los principales oferentes de los servicios en la nube tienen sus centros de datos fuera del territorio nacional, por lo que condiciona a las entidades a asumir el riesgo de llevar sus aplicaciones y datos de negocio a la nube, debido a que estos podrían estar en jurisdicciones que no son consideradas adecuadas desde el punto de vista de protección de los datos para las autoridades argentinas.

La adopción de la *Cloud Computing*, será un proceso que los bancos no podrán ignorar, y para el cual se presentan diferentes estrategias:

a) Software as a Service para aplicaciones no críticas del negocio: llevar a la nube bajo la modalidad de Software as a Service (SaaS), las aplicaciones "no core" y no diferenciadoras de una entidad a otra en cuanto al proceso de negocio. Entre estas aplicaciones se encuentran las herramientas de productividad, colaboración y comunicación unificada (mail, software de oficina, calendario, almacenamiento compartido, etc.).
   Asimismo, se considera dentro de este alcance, otras aplicaciones para la gestión de compras y stock, gestión de recursos humanos, service desk, gestión de proyectos, entre los más comunes.
   En un nivel más avanzado, también puede incluirse dentro de esta estrategia, la utilización bajo la forma de SaaS de herramientas de CRM.
   Se considera a éste como un primer paso hacia Cloud Computing, y que permite a las entidades ganar confianza en esta tecnología.
b) Infraestructura como servicio (IaaS): Esta modalidad de servicio, se considera viable para los bancos, y aplicable para los siguientes casos de uso:
   I. Configuración de ambientes para desarrollo y prueba de aplicaciones. En este caso las ventajas no solo están desde el punto de vista económico, dado que la entidad no debe mantener inversiones en este tipo de plataformas, sino que adicionalmente estos ambientes pueden ajustarse dinámicamente dependiendo de los requerimientos del momento.
   II. Configuración de un ambiente de recovery. Este es quizás el más avanzado, dado que implica tener la infraestructura de IT que respalda los ambientes productivos, en un proveedor. Esta opción la visualizamos como el paso previo a la migración a una public cloud de todo el entorno productivo bojo la forma IaaS.
c) Community Cloud: considerando las ventajas que brinda una economía de escala, otra opción es el desarrollo de una community cloud conformada por aquellas entidades nacionales medianas o chicas en función de su volumen de cuentas y transacciones, y que además aplican políticas comunes de seguridad de la información.
   Esta community cloud, podría ser gestionada por un tercero, pero bajo las directivas de seguridad y control de los bancos propietarios de la community cloud.

Esta estrategia también es aplicable a las entidades financieras públicas, en razón de que comparten políticas financieras, y por las características que en tienen en común por ser propiedad de entidades gubernamentales.
Los aspectos de seguridad física y lógica, y de alta disponibilidad de los servicios informáticos "on site" y "off site", adquieren en este escenario una importancia significativa, pues cualquier incidente de seguridad o que afecte la disponibilidad de los servicios informáticos pone en riesgo la operación de varias entidades en el mercado.

d) Private Cloud: este modelo también es posible de ser implementado por grandes entidades que operan en el mercado argentino, y en particular las que tienen filiales en otros países de la región, manteniendo de esta forma el control directo de los aspectos sensibles de seguridad, y a la vez obtener las ventajas del modelo Cloud.

9 Conclusión.

El modelo de Cloud Computing tiene aportes importantes desde el punto de vista de optimización de costos y de actualización tecnológica, beneficiando no solo a las entidades, sino también a la sociedad en general, debido a la oferta de productos y servicios tecnológicamente más avanzados y a menor costo por transacción para el usuario/cliente final. Medidas de este tipo contribuyen también, a una mayor bancarización de la sociedad.
En materia de entidades financieras públicas, la implementación de una community cloud, más allá de las ventajas económicas y técnicas mencionadas anteriormente, podrían constituirse en un caso testigo, para el desarrollo de una estrategia en materia de Cloud Computing que incluya a todos los organismos del Estado Nacional.
Sin embargo aún persisten ciertas observaciones respecto de la seguridad y confidencialidad de los datos, y cómo el gobierno de IT de una entidad financiera se ve afectado por la delegación de su infraestructura IT y aplicaciones, a la gestión de un tercero.
Por otra parte, el hecho de que grandes cloud providers (Google, Microsoft, Amazon, etc.) no cuenten con infraestructura de data center dentro de los límites del país, implican de alguna manera una barrera para su adopción.
Otro elemento a tener en cuenta, es la arquitectura de sus aplicaciones core, las cuales muchas de ellas corren en entornos propietarios y tienen un alto grado de personalización, lo cual hace más complejo el proceso de migrar a soluciones de software existentes en la nube.
Asimismo, y en materia regulación pública aplicable a las entidades financieras, será necesaria una revisión y actualización del marco regulatorio vigente para fijar los criterios y estándares que deberán tener en cuenta las entidades al momento de optar por Cloud Computing.
No obstante, en opinión del autor, mientras esta adecuación normativa se produce, los bancos migrarán hacia Cloud Computing todos aquellos servicios en los cuales no vean riesgos de pérdida de confidencialidad de los datos sensibles de su operación o no sean diferenciadores de los servicios que ofrecen, integrándolos con su plataforma on premise. Difícilmente opten por migrar a una public cloud sus aplicaciones críticas.

10 Referencias.

[1] BANCO CENTRAL DE LA REPUBLICA ARGENTINA. Com. A 4609. Circular RUNOR 1-805. 2006. http://www.bcra.gov.ar/

[2] BANCO CENTRAL DE LA REPUBLICA ARGENTINA. Com. A 5374. Circular RUNOR 1-1005. 2012. http://www.bcra.gov.ar/

[3] CLOUD SECURITY ALLIANCE. *Security Guidance for Critical Areas of Focus in Cloud ComputingV2.1*.2009. HTTP://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[4] DECRETO 1558/2001. *Protección de los Datos Personales.* 2001. http://www.jus.gob.ar/datos-personales.aspx

[5] ERL, Thomas. MAHMOOD, Zaigham y PUTTINI, Ricardo. *Cloud Computing. Concepts, Technology & Architecture*. 1ª- ed. Westford, Massachusetts, USA: Prentice Hall, Mayo 2013. 487 p. (Service Technology Series). ISBN-13: 978-0-13-338752-0. ISBN-10: 0-13-338752-6.

[6] JOYANES AGUILAR, Luis. *Computación en la nube. Estrategias de cloud computing en las empresas.* 1ª – ed. México: Alfaomega Grupo Editor. Julio 2012. 520 p. (NTICS). ISBN: 978-607-707-468-7.

[7] LEY 21.526. *Ley de Entidades Financieras.* 1977 y Modificatorias. http://www.bcra.gov.ar/

[8] LEY 25.326. *Protección de Datos Personales.* 2000. http://www.jus.gob.ar/datos-personales.aspx

[9] LIU, Fang. TONG, Jin. MAO, Jian, y otros. *NIST Cloud Computing Reference Architecture.* National Institute of Standards and Technology. Especial publication. 500-292. 2011. http://www.nist.gov/itl/cloud/index.cfm

[10] MELL, Peter y GRANCE, Timothy. *The NIST Definition of Cloud Computing.* National Institute of Standards and Technology. Especial publication 800-145. 2011. http://www.nist.gov/itl/cloud/index.cfm

[11] PALAZZI, Pablo. *La Protección de los Datos Personales en la Argentina.* . 1ª – ed. Argentina: Editorial Errepar. Setiembre 2004. 325 p. ISBN: 987-01-0313-8.

[12]RISTOV, Sasko. GUSEV, Marjan. y KOSTOSKA, Magdalena. *Cloud Computing Security in Business Information System.*

[13]CLOUD SECURITY ALLIANCE. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf