MAESTRÍA EN TECNOLOGÍA INFORMÁTICA Y COMUNICACIONES

CLOUD COMPUTING. SU APLICACIÓN EN LA BANCA PRIVADA ARGENTINA.

HECTOR NOCETI – LU 1041682

COHORTE: TIC *2012/2013*

Director del Trabajo Final

MBA Ing. Aníbal Freijo, Universidad Argentina de la Empresa

30 de Junio de 2014

UNIVERSIDAD ARGENTINA DE LA EMPRESA

FACULTAD DE INGENIERÍA Y CIENCIAS EXACTAS

ÍNDICE.

AGRADECIMIENTOS

Deseo expresar mi agradecimiento a quien dirigió este trabajo, Mag. Ing. Aníbal Freijo y a la Mag. Ing. Bibiana Rossi, coordinadora de la maestría TIC, quienes me apoyaron durante el proceso de elaboración.

A los Sres.: Norberto Aneise, Carlos Azcona, Edgardo González, Carlos A. Megide, Fabián Romero, Pablo Recepter y Enrique Rubinstein, a quienes entrevisté; por brindarme su tiempo y claridad en sus opiniones, que fueron material imprescindible para la realización de este trabajo.

Al Lic. Pedro Maidana, que me ayudó en la gestión de varias entrevistas.

Al Lic. Pablo Coronato, por sus opiniones, comentarios y lecturas de este trabajo.

También a mi esposa, Beatriz, que supo entender el tiempo libre que le quité para dedicarlo a este proyecto personal.

ABSTRACT.

Cloud Computing is a technology model based on a combination of hardware and software resources that are available in the form of service to be used by individuals and organizations.

This technology enables users to make use of available resources at any time, from wherever they are, and connecting through any device, thanks to its processing power and connection via Internet.

Those who have adopted this technology first are the people in the domestic environment, and the organizations have joined slowly. The organizations identified the advantages of this model, but they have questions and doubts relating to the physical and logical aspects of their data security, and legal regulations governing the physical location of data.

This analysis very much applies to financial institutions, which also seek to optimize the use of computer technology and minimize expenses and investment, but which face particularly significant security and regulation issues due to the highly sensitive nature of the information that they managed.

RESUMEN.

Cloud Computing es un modelo de tecnología basado en una combinación de recursos de hardware y software que están disponibles bajo la modalidad de servicio para ser utilizados por individuos y organizaciones. Esta tecnología posibilita a sus usuarios que hagan uso de los recursos disponibles en todo momento, desde el lugar en que se encuentren, y conectándose a través de cualquier dispositivo, gracias a su capacidad de procesamiento y conexión a través de Internet.

Los primeros en adoptar esta tecnología han sido las personas en el entorno doméstico, 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 regulación les presenta esta tecnología.

1. INTRODUCCIÓN.

El concepto de *Cloud Computing* o "Computación en la Nube" (en adelante se utilizará la expresión en inglés), surge como respuesta a la necesidad de usuarios: personas y organizaciones, de poder disponer de recursos de IT (Information Technology: hardware, software, aplicaciones, y redes) bajo la modalidad de servicio, con independencia del lugar en el que se encuentren físicamente, y de acuerdo a sus necesidades de uso.

La consultora International Data Corporation (IDC), en un informe presentado en mayo del 2013 sobre Tendencias de TI y Telecomunicaciones, concluye que *Cloud Computing,* junto con *Big Data, Movilidad y Social Business* constituyen las principales tendencias de IT que representan una innovación constante. En Argentina, y en particular sobre *Cloud Computing*, según el estudio citado, un 44% de las empresas considera implementar o ya es usuario de servicios en la "nube". [SEMINARA, Juan P. y otro. 2013].

El concepto de *Cloud Computing* adquiere difusión pública a mediados de la primera década del 2000, pero en realidad, viene siendo utilizada desde varios años antes por millones de usuarios que abrieron sus cuentas de *e-mails* en algunos de los servidores de correo público como Hotmail o Gmail. Más recientemente, ese uso se extendió a la guarda de archivos personales en sitios como Dropbox, Google Drive, Open Drive, Amazon o iCloud, o en la participación de redes sociales.

La tecnología de *Cloud Computing*, se basa en el desarrollo y crecimiento de las siguientes tecnologías:

1. Redes IP (*Internet Protocol*);
2. Web 2.0;
3. Virtualización;
4. *Data Center* o Centro de Datos; y
5. Redes de banda ancha;

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. [JOYANES AGUILAR, Luis. 2012].

En resumen, y siguiendo el razonamiento de Joyanes Aguilar, la tecnología de "*Cloud Computing se está configurando actualmente como un nuevo modelo de computación, que está produciendo un gran cambio en el modo de trabajo de las organizaciones y empresas".* [JOYANES AGUILAR, Luis. 2012].

1.1. PLANTEAMIENTO DE LA CUESTIÓN.

La tecnología de *Cloud Computing* es considerada por consultoras internacionales de primer nivel tales como Gartner e International Data Corporation (IDC), como una de las tecnologías disruptivas, que es adoptada cada vez más, no solo por los individuos, sino también por las organizaciones.

Según Joyanes Aguilar, existen una serie de factores clave que motivan a las organizaciones a migrar de sus modelos "*On-Premise*", o propietarios, de infraestructura de IT, a la tecnología "Cloud" [JOYANES AGUILAR, Luis. 2012]. Se entiende por "*On-Premise*" al conjunto de los recursos de IT: hardware, software de base y aplicaciones de negocio, que están "*hosteados*" dentro del perímetro de seguridad físico y lógico controlado por una organización. [ERL, Thomas y otros. 2013].

Entre los factores clave que impulsan el cambio se destacan:

a) Organizativos y operacionales: en la economía moderna y como parte de la globalización, las empresas han comenzado a adoptar el modelo de especialización en su "*core business*", delegando en terceros todas aquellas actividades, que si bien son importantes, no se consideran como parte del núcleo de negocios de la organización. Entre estas actividades "delegables", muchas organizaciones incluyen todas las vinculadas a las áreas de IT, lo que las impulsa a dejar en manos de empresas especializadas todo lo relacionado con ellas.
b) Económicos y financieros: muchas organizaciones ven en la adopción de la tecnología de *Cloud Computing*, la posibilidad de reducir sus inversiones en IT y los costos fijos que requiere su operación, convirtiéndolos en gastos variables,

en función de los recursos utilizados. Simplificando, se podría afirmar que el usuario de los servicios "*Cloud*", sólo paga por aquellos recursos que utiliza.

c) Fácil adecuación a las necesidades del negocio: esto tiene que ver con la capacidad del proveedor de servicios "*Cloud*", de poner disponibles para el usuario, en corto tiempo, nuevas aplicaciones o actualizaciones, así como también recursos de infraestructura de IT, acompañando el crecimiento de su volumen de negocios, y otorgando la capacidad de ajustar los recursos a las necesidades reales del cliente.
d) Actualización tecnológica: la posibilidad del usuario o cliente del servicio "*Cloud*", de acceder a nuevas tecnologías y mantenerse actualizado en las mismas, sin necesidad de realizar inversiones o contar con recursos entrenados.
e) Ubicuidad: definida como la capacidad de poder acceder y utilizar los recursos de IT, desde cualquier lugar geográfico, en cualquier momento y con cualquier dispositivo de acceso.

Siguiendo al mismo autor, en contraposición a los factores claves que motivan la adopción de *Cloud Computing*, aparecen una serie de obstáculos que son objeto de preocupación a la hora de decidir. Estos son los principales:

a) Seguridad de los datos: tiene que ver con aspectos vinculados a la protección de los datos, su confidencialidad, integridad y confiabilidad, así como su respaldo por medio de copias de back-up, como medida de protección ante la pérdida, robo o destrucción de los datos originales. Existe, podría decirse el mito, de que los datos de una organización solo están seguros, si se encuentran dentro de su perímetro de seguridad físico y lógico. Adicionalmente, por los fundamentos mismos de la tecnología *Cloud Computing*, el usuario puede llegar a desconocer el lugar en el que se encuentran físicamente alojados sus datos.
b) Gobierno de IT: el hecho de dejar en manos del proveedor de servicios "*Cloud*", la gestión de los recursos de IT utilizados para la operación del negocio, debilita la función de gobierno de IT (IT *Governance*) desde el momento en que la gestión pasa a estar compartida entre proveedor y usuario, perdiendo éste último autonomía. El nivel de gestión compartida varía en función del modelo de implementación y de servicio cloud adoptado.

c) Fiabilidad del proveedor: la fijación de criterios de selección del proveedor de los servicios "*Cloud*", el establecimiento de acuerdos de nivel de servicio o SLA (*Service Level Agreement*) entre proveedor y cliente, así como el monitoreo y control de las actividades del proveedor de servicios "*Cloud*", es un proceso complejo y de difícil implementación.

d) Limitaciones del marco legal y regulatorio: los proveedores de servicios "*Cloud*", frecuentemente instalan sus data centers en lugares geográficamente convenientes, no solo por razones de aprovisionamiento de energía o climáticas, sino también por cuestiones legales o impositivas de los países en los cuales se instalan.

   Esto puede ser una fuerte limitación para muchas organizaciones a la hora de optar por esta tecnología, debido a la existencia de limitaciones legales o regulatorias que impiden que los datos vinculados a sus operaciones puedan estar físicamente ubicados fuera de su país de origen.

e) Portabilidad: una de las principales inquietudes de los usuarios de servicios "*Cloud*" está vinculada con el grado de facilidad de poder migrar los servicios de un proveedor a otro, o bien de minimizar el riesgo de depender de un único proveedor, integrando la solución con más de uno. Esto impone la existencia de estándares, que deben ser respetados por todos los proveedores. Aun así, la portabilidad de los servicios en la "nube", no es de fácil implementación.

Todos estos factores clave, adquieren especial importancia, cuando el potencial usuario de la tecnología "*Cloud*" es una entidad financiera. Las objeciones presentadas tienen un peso particularmente significativo, pues, lo que se pone en riesgo es uno de sus principales activos: la información de las operaciones financieras de sus clientes.

1.2. OBJETIVOS.

El objetivo del presente trabajo es realizar un análisis cualitativo respecto de las posibilidades de utilización de la tecnología de *Cloud Computing*, por las entidades financieras del mercado argentino. Las entidades financieras, están regidas por un estricto marco legal y regulatorio, no solo desde el punto de vista administrativo,

contable y operacional, sino también en los aspectos vinculados a los sistemas de información y seguridad de la información.

1.2.1. OBJETIVOS GENERALES.

De acuerdo a lo expresado precedentemente, nos fijamos como objetivos generales del presente trabajo:

a) Analizar si *Cloud Computing* es una tecnología adoptable por las entidades financieras.
b) Determinar si la adopción de *Cloud Computing* es aplicable a la totalidad de los servicios de IT de una entidad o solo parcialmente.
c) Evaluar si hay limitaciones dentro del marco legal y regulatorio para que las entidades adopten esta tecnología.

1.2.2. OBJETIVOS ESPECIFICOS.

a) Conocer las principales características de la tecnología de *Cloud Computing*, sus principales ventajas, desventajas, y modalidades de servicio.
b) Evaluar las diferentes alternativas de implementación de *Cloud Computing* que podrían adoptar las entidades financieras.
c) Identificar los principales motivos impulsores y condicionantes en la adopción de esta tecnología por las entidades financieras.

1.2.3. ALCANCE DEL TRABAJO.

Este trabajo limita su análisis a las principales entidades financieras del segmento privado que operan en el mercado argentino, habiéndose elegido para la muestra cuatro de entre los diez bancos privados más importantes del sistema financiero, de acuerdo al ranking elaborado por el Banco Central de la República Argentina (BCRA), y otras tres entidades privadas de diferente tamaño de manera de complementar la muestra.

El marco temporal del presente trabajo, está comprendido entre los meses de Julio/2013 a Abril/2014.

Según información del BCRA al mes de abril de 2014, el ranking de los diez primeros bancos privados, se integra de la siguiente forma:

Figura 1.1 – Ranking de Bancos Privados. [BCRA. Información de Entidades. Grupo de Entidades. 10 Primeros bancos privados. Nómina de Entidades. Abril 2014].

10 PRIMEROS BANCOS PRIVADOS Información actualizada a Abril de 2014

Nomina del grupo

CODIGO	DENOMINACION
00191	BANCO CREDICOOP COOPERATIVO LIMITADO
00007	BANCO DE GALICIA Y BUENOS AIRES S.A.
00044	BANCO HIPOTECARIO S.A.
00285	BANCO MACRO S.A.
00034	BANCO PATAGONIA S.A.
00072	BANCO SANTANDER RIO S.A.
00017	BBVA BANCO FRANCES S.A.
00016	CITIBANK N.A.
00150	HSBC BANK ARGENTINA S.A.
00015	INDUSTRIAL AND COMMERCIAL BANK OF CHINA

Desde el punto de vista normativo, se define como bancos y entidades financieras, a aquellas organizaciones que están alcanzados por la Ley de Entidades Financieras (Ley 21.526), las normas dictadas por el BCR como ente regulador, y la ley de Protección de Datos Personales (Ley 25.326).

Las entidades financieras, están alcanzadas por estrictas regulaciones respecto del secreto bancario, aplicado a las operaciones realizadas por sus clientes, y por normas del BCRA que fijan “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con la tecnología informática y los sistemas de información” [BCRA. 2006]. Por esta razón, la adopción de *Cloud Computing* en el ámbito de este tipo de organizaciones, es una decisión compleja, que requiere de análisis no solo de los aspectos técnicos y económicos, sino también de aspectos vinculados a la seguridad de la información, legal y regulatorio.

2. ENFOQUE METODOLÓGICO.

El presente trabajo consiste en un estudio descriptivo de tipo cualitativo, que pretende especificar las características técnicas, ventajas y desventajas de la tecnología de *Cloud Computing* y las posibilidades de ser adoptada por las entidades financieras del mercado argentino. La clasificación está basada en la definición de que "*los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis (Danhke, 1989). Es decir, miden, evalúan o recolectan datos sobre diversos conceptos (variables), aspectos, dimensiones o componentes del fenómeno a investigar* "[HERNÁNDEZ SAMPIERI, Roberto y otros. 2006].

Este trabajo se desarrolló en base a siete (7) entrevistas a funcionarios que ocupan posiciones de *Chief Information Officer* (CIO), *Chief Technology Officer* (CTO) y *Chief Information Security Officer* (CISO) de importantes entidades financieras privadas que operan en el mercado argentino, para establecer en qué medida y alcance esta tecnología puede ser adoptada por sus instituciones. Entre los entrevistados se encuentran:

a) Sr. Norberto Aneise – Sub. Gerente de Comunicaciones e Infraestructura – BBVA Banco Francés S.A.
b) Sr. Carlos Azcona – CIO Compensadora Electrónica S.A. (COELSA).
c) Sr. Edgardo González – CIO Banco de Servicios y Transacciones S.A. (BST).
d) Sr. Carlos A. Megide – Gte. De Arquitectura Tecnológica y Metodología – ISBAN – Banco Santander Río.
e) Sr. Fabián Romero – CTO Banco Supervielle S.A.
f) Sr. Pablo Recepter – CIO Banco Credicoop Cooperativo Limitado.
g) Sr. Enrique Rubinstein - CISO Industrial and Commercial Bank of China (ICBC).

Para la realización de entrevistas se preparó una serie de preguntas guías, que se adjuntan como Anexo.

Es importante dejar en claro que las opiniones profesionales vertidas por los ejecutivos, son a título personal.

También se ha recurrido para esta investigación, a bibliografía específica, así como a documentos publicados en Internet por diferentes organizaciones internacionales tales como Cloud Security Alliance (CSA), National Institute of Standard and Technology (NIST), Institute of Electrical and Electronics Engineers (IEEE), entre otras.

Por otro lado, se han utilizado informes de consultoras de primer nivel como Gartner e International Data Corporation (IDC), y también de empresas proveedoras de tecnología: CISCO, Microsoft y VMware entre otras.

Para la revisión de los aspectos legales y regulatorios, se ha recurrido a la Ley de Entidades Financieras (Ley 21.526), a la Ley de Protección de Datos Personales (LPDP, Ley 25.326) y su reglamentación, así como a las Comunicaciones A del BCRA 2699, 4609 y 5374), y dictámenes emitidos por la Dirección Nacional de Protección de Datos Personales (DNPDP), dependiente del Ministerio de Justicia de la Nación, como órgano de aplicación de la LPDP.

Toda la bibliografía mencionada, está detallada en el capítulo 9 - Referencias Bibliográficas, de este trabajo.

3. ESTADO DEL ARTE.

Como una primera aproximación al concepto de *Cloud Computing*, se lo puede definir como el conjunto de hardware y software que se brinda fundamentalmente como servicio, y que facilita a los usuarios el acceso a las aplicaciones. [JOYANES AGUILAR, Luis. 2012].

Hay quienes se refieren a *Cloud Computing* como una tecnología [SRIRAM, Sudhir 2011], y hay quienes lo identifican como un modelo que aún es un paradigma en evolución [MELL, Peter y otros.2011].

Cloud Computing, posibilita a las organizaciones poder acceder a los recursos de IT a través de Internet, mediante un proceso de aprovisionamiento rápido, con bajo o nulo nivel de inversión de capital, y basado en un esquema de costos variables y relativamente bajos en función de los recursos utilizados [ACCENTURE. 2012].

El informe "Hype Cycle for Emerging Technologies, 2012" [GARTNER, Inc. 2012], publicado en julio 2012 por la consultora internacional Gartner, que reúne las tecnologías informáticas más importantes de todas las áreas de investigación, permite visualizar aquellas que tienen una especial relevancia por ser signo de transformación y por su potencial alto impacto. El informe menciona entre las diez principales tendencias en Information Technology (IT), a las siguientes:

- Mobile
- Web Apps con HTML5
- The personal cloud
- The internet of things
- *Cloud Computing*
- Strategic Big Data
- Actionable analytics
- In memory computing
- Virtual appliances integrated ecosystems
- Enterprise App Stores

El Gartner Hype Cycle es una metodología diseñada por la consultora Gartner, que permite visualizar en forma gráfica como una tecnología o aplicación evolucionará en

el tiempo, y que es de ayuda a quienes deciden en las organizaciones en materia de IT.

Esta metodología prevé cinco niveles de maduración:

a) *Technology Trigger*: se trata de tecnologías que se hallan en la fase inicial de desarrollo, en ocasiones solo en ambientes académicos, y sobre las cuales se han realizado pruebas de concepto. En esta etapa, a menudo, se trata de tecnologías sin viabilidad comercial comprobable. [GARTNER].

a) *Peak of Inflated Expectation:* se ubican en este nivel aquellas tecnologías que adquieren publicidad a partir de casos de éxito, no exentas de fallas, y que son adoptadas por aquellas organizaciones que tienen por política ser pioneras en adoptar tecnologías emergentes. [GARTNER].

b) *Trough of Disillusionment:* es una etapa en la que se ubican aquellas tecnologías respecto de las cuales declina el interés en realizar nuevas experiencias, o no han sido exitosas ciertas implementaciones. Solo permanecen ofertando estas tecnologías, aquellos proveedores que invierten en mejorar sus soluciones a fin satisfacer los requerimientos hechos por quienes las adoptaron tempranamente. [GARTNER].

c) *Slope of Enlightenment:* en este nivel de madurez, se ubican las tecnologías sobre las cuales hay casos concretos de cómo benefician a las organizaciones, y son ampliamente comprendidas en los ámbitos tecnológicos y de negocios. Los proveedores que ofrecen estas tecnologías, liberan al mercado segundas o terceras generaciones de estas tecnologías que recogen recomendaciones de usuarios o de organizaciones de usuarios. En esta etapa, las organizaciones más conservadoras se mantienen cautelosas respecto de su adopción. [GARTNER].

d) *Plateau of Productivity:* las tecnologías que se ubican en este nivel, son aquellas sobre las cuales hay criterios claros sobre la viabilidad de su adopción, tienen amplia aplicación y relevancia en el mercado. [GARTNER].

En particular, sobre *Cloud Computing*, el citado estudio ubica en dos etapas de maduración, los diferentes modelos de implementación de esta tecnología.

En posición ascendente de la curva (ver Figura 3.1) en la etapa *Peak of Inflated Expectation,* ubica a los servicios de Hybrid Cloud (combinación de Private Cloud y Public Cloud). Según el estudio de Gartner, las organizaciones tienen la necesidad y el deseo de crecer en la integración de los servicios internos con los ofrecidos en la nube por diversas razones, entre ellas para obtener capacidad adicional de recursos de IT, optimizando costos y mejorando la calidad de servicio.

El modelo Hybrid Cloud Computing, según Gartner, abre el camino hacia un modelo de cloud computing unificada en la que hay una sola nube que se compone de varios conjuntos de recursos (internos o externos) que se pueden utilizar, según sea necesario, sobre la base de los cambiantes requisitos empresariales. Este enfoque ideal sería ofrecer el mejor modelo económico y la máxima agilidad en la disponibilidad de recursos. Estima que este modelo de Cloud Computing alcanzará la etapa de madurez entre los siguiente cinco a diez años. [GARTNER. 2012].

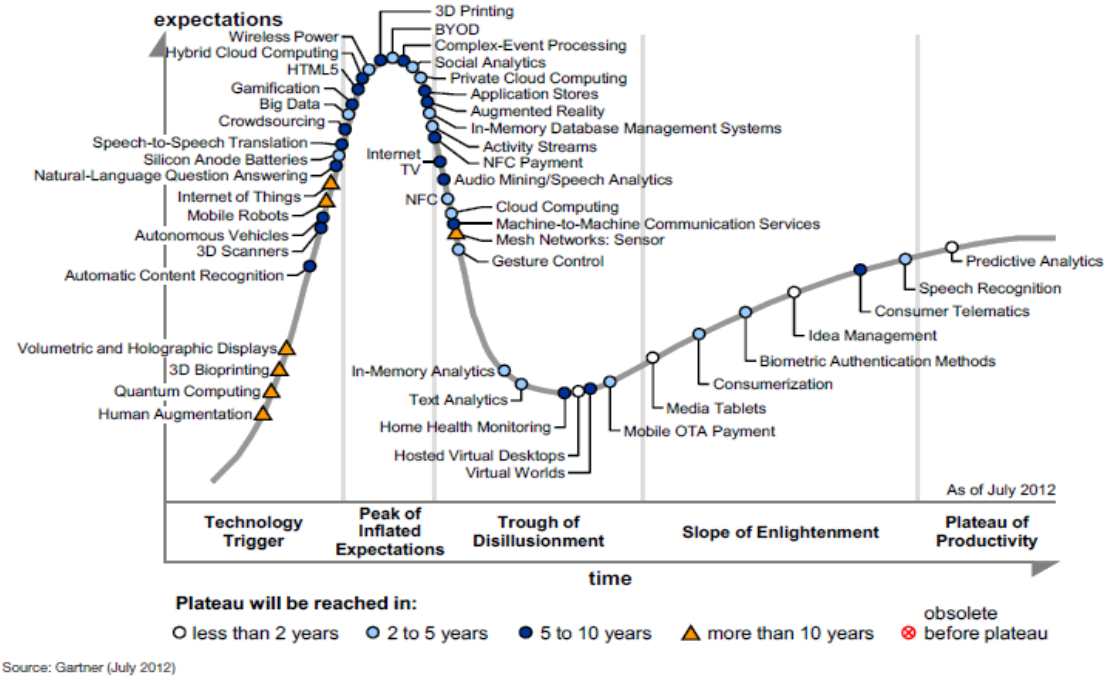
También dentro de la etapa *Peak of Inflated Expectation* (ver Figura 3.1), pero en la parte descendente de la curva, Gartner ubica al modelo de implementación Private Cluod Computing. Según la consultora, las organizaciones que construyen un servicio en la nube privada, de alguna forma intentan emular a los proveedores de servicios en la nube para adquirir beneficios similares, pero dentro de su control y, a menudo en sus propias instalaciones. Esto incluye procesos de estandarización y automatización, así como herramientas de autogestión de servicios, y de medición de los recursos utilizados. Según Gartner, varias de estas tecnologías están en evolución, y en muchos casos requieren herramientas personalizadas a las necesidades de la organización. [GARTNER. 2012].

Para Gartner, la mayoría de las implementaciones de nubes privadas, serán parte de la evolución de la implementación de las técnicas de virtualización, lo que permitirá alcanzar una reducción de costos y niveles de inversión mediante la optimización en el uso de los recursos disponibles, y mayor celeridad en el proceso de puesta disposición de los usuarios de los recursos que necesitan. Asimismo estima que el modelo de Private Cloud alcanzará su etapa de madurez entre los siguientes dos a cinco años, es decir. . [GARTNER. 2012].

La tecnología de Cloud Computing, en sus diferentes modelos de implementación, tiene múltiples ventajas en cuanto escalabilidad, elasticidad, y economía, pero existen una serie de factores y elementos condicionantes, que hacen que las organizaciones analicen sobre la conveniencia de llevar a esta tecnología la totalidad de los servicios de IT. . [GARTNER. 2012].

Si bien Gartner considera que aún es poco probable que los usuarios abandonen por completo o cambien sus modelos "*on premise*" o propietarios y migren sus sistemas de misión crítica a la "nube" en un futuro cercano, existe una tendencia cada vez más marcada al consumo de determinados servicios cloud de una manera rentable.

Figura 3.1 – Hype Cycle for Emerging Technologies. [GARTNER, Inc. 2012].



Source: Gartner (July 2012)

El desarrollo de esta tecnología, inclusive, está impulsando un cambio en la forma de comercialización de las grandes empresas de software. Empresas como Microsoft que han basado su estrategia en la comercialización de licencias de software, hoy es uno de los principales "*players*" en la comercialización de servicios en la "nube". Otras empresas como Google, Amazon y Salesforce.com son otros de los fuertes proveedores de servicios de *Cloud Computing*.

Cisco e Intel publicaron en el año 2013 el informe "The Impact of Cloud on IT Consumption Models", basado en una encuesta realizada a 4.226 CIOs. Este informe señala que la tecnología de *Cloud Computing* ya es un hecho, y que está creciendo rápidamente. Un promedio del 23% de la inversión en IT se destina a esta tecnología. Asimismo destaca una diferencia clave países desarrollados y emergentes, respecto de los motivos por los cuales es adoptada esta tecnología:

a) En Estados Unidos, Reino Unido, Alemania y Canadá los disparadores de la elección son la reducción de costos, capacidad "on demand" y costos más predecibles.
b) En Brasil, India, China, y otros emergentes, el disparador es la agilidad para adecuarse al crecimiento del negocio y la productividad.

También el estudio rescata que hay básicamente tres factores que actúan como inhibidores a la hora decidir por la "nube". Se citan por orden de importancia: los "*issues*" en materia de seguridad informática, la complejidad de gestión de la operación, y la falta o dificultades de integración e interoperabilidad entre sistemas propios y los de proveedores externos. [BRADLEY, Joseph y otros. 2013].

Sobre el impacto de *Cloud Computing* en los bancos, la consultora internacional Accenture afirma en su informe "A new era in banking. Cloud Computing changes the game" [ACCENTURE. 2012] que los bancos comerciales tradicionales en el mundo, tendrán que hacer frente a dos desafíos:

a) Adaptar los productos y canales a través de los cuales los ofrecen, para adecuarse a las nuevas y cambiantes exigencias de sus clientes, que demandan mejor calidad de atención, y productos y servicios más acordes a sus necesidades.
b) Readecuar sus procesos operativos para hacerlos más competitivos y centrados en el cliente. En este sentido, han surgido nuevos competidores de los bancos tradicionales, algunos de los cuales no son instituciones formalmente bancarias, que realizan la gestión financiera así como la prestación de servicios de pago a sus clientes en forma on-line, ágil y a bajo costo, basado en la utilización de servicios en la nube. Como ejemplo se pueden citar a Google Wallet y PayPal.

El cambio de comportamiento de los clientes orientándose al uso de la web, la tecnología mobile y la participación en las redes sociales, está impulsando a los bancos a rediseñar sus modelos de negocio. Accenture identifica tres modelos:

a) El "analytical multichannel bank", modelo de integración avanzado de todos los canales digitales disponibles para que el cliente opere con el banco. Esto se complementa con la recolección de datos del cliente, que permite a la entidad diseñar productos con costos a la medida del perfil de sus clientes. [ACCENTURE. 2012].
b) El "social engaging bank", es un modelo a través del cual los bancos interactúan con sus clientes utilizando las redes sociales, de manera de conocer sus preferencias, y también mitigar el riesgo de quejas o reclamos. Se complementa con la utilización de soluciones de CRM (Customer Relationship Management) para la oferta de productos y servicios acordes a las necesidades del cliente. [ACCENTURE. 2012].
c) El "digital ecosystem bank", modelo a través del cual los bancos ofrecen una variedad de servicios propios o de terceras partes basados en la tecnología mobile (ej.: mobile commerce, mobile payments). [ACCENTURE. 2012].

Accenture considera que, *Cloud Computing* tendrá un roll importante en los bancos, dado que les permitirá adecuarse a los cambios del mercado con rapidez, a bajo costo y con la calidad de servicio necesaria. Visualiza tres escenarios o tendencias:

a) Servicios basados totalmente en *Cloud Computing.* Se trata de entidades nuevas, cuyo modelo de negocio esta basado en brindar acceso mobile a su plataforma de servicios disponibles en tecnología web. A diferencia de las entidades tradicionales, no cuentan con sucursales físicas para la atención de sus clientes. Como ejemplo se puede citar a BankSimple, que ofrece a sus clientes servicios financieros accesibles a través de Internet desde cualquier dispositivo mobile, a partir de la relación con una tarjeta de débito. [ACCENTURE. 2012].

BankSimple, no es un banco en sí mismo, sino que ofrece a sus clientes servicios financieros a partir de acuerdos a asociaciones que establece con entidades bancarias tradicionales.

Estas nuevas entidades, a diferencia de los bancos tradicionales, no tienen compromisos con aplicaciones "legacy", las cuales deben seguir manteniendo, y además pretenden evitar realizar inversiones de capital para desarrollar su infraestructura de IT, razón por la cual los servicios basados en *Cloud Computing* representan una buena opción.

b) El desarrollo de "Private Cloud" o nubes privadas como un paso previo a la adopción de "Hybrid Clouds" y "Public Clouds".

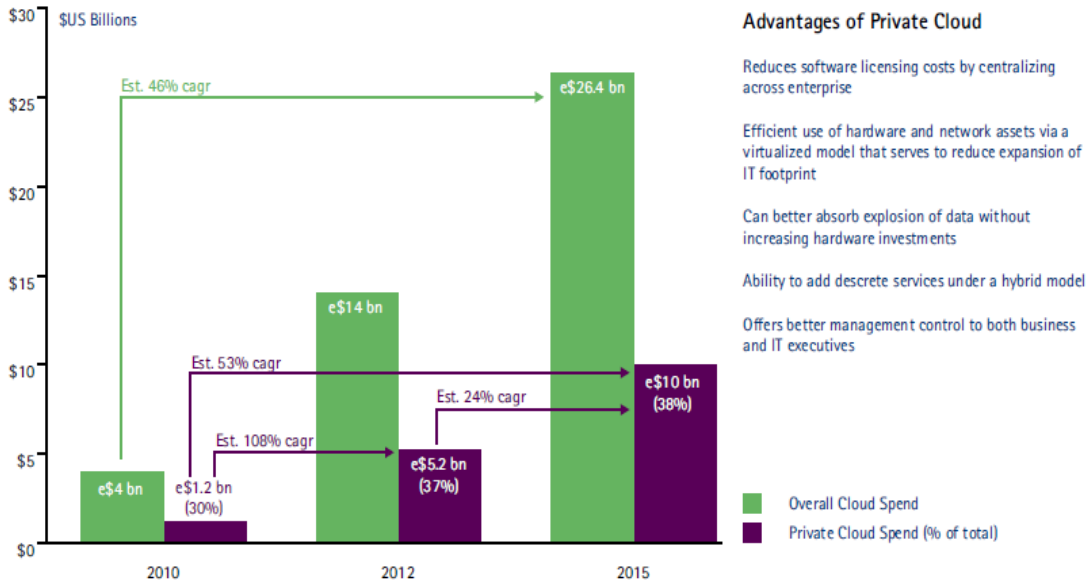
   Las ventajas derivadas de la utilización de los servicios en la nube, son apreciadas por las organizaciones, pero en el caso de los bancos tradicionales, deben vencer la resistencia a confiar los datos de sus clientes a proveedores que ofrecen servicios en Public Clouds, generadas no solo por razones de seguridad, sino también debido a limitaciones que surgen de las regulaciones existentes en cada país. Para superar esta resistencia, y a la vez poder obtener las ventajas del modelo Cloud, Accenture prevé que las entidades adoptarán el concepto de Private Cloud. En la figura 3.2, se puede observar como estima evolucionará el gasto en private clouds respecto del gasto global en servicios cloud, realizado por las entidades financieras a nivel mundial. [ACCENTURE. 2012].

c) La adopción de "Public Clouds" para la migración de aquellos servicios y procesos considerados no "core" por los bancos.

   Hay bancos que han iniciado un proceso de evolución hacia los servicios Cloud, y comenzaron a migrar aquellas aplicaciones que consideran no diferenciadoras de otros competidores, y fundamentalmente, no forman parte de los sistemas transaccionales que mantienen información sensible de sus clientes.

Dentro de esta categoría se incluyen el mail corporativo, las aplicaciones de oficina, herramientas internas de colaboración (audio y video sobre redes IP) y soluciones para compartir conocimiento, sistemas de gestión de compras y recursos humanos, así como herramientas de CRM (Customer Relationship Management).

Figura 3.2 – Gasto estimado en Private Cloud por las entidades financieras a nivel mundial. [ACCENTURE. 2012].



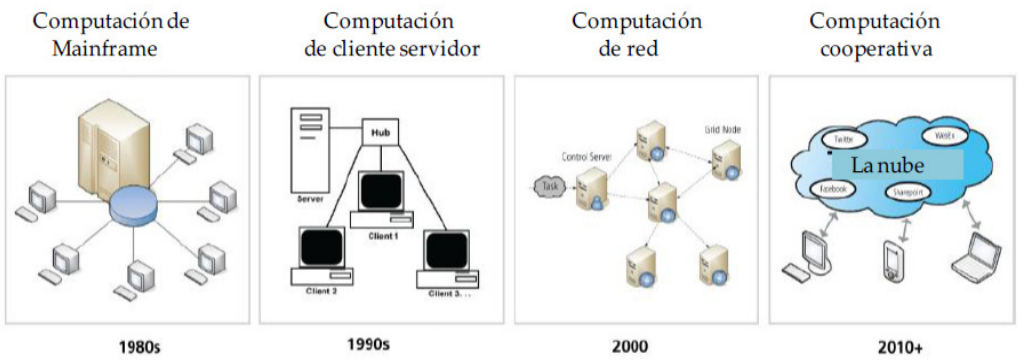
Source: The Tower Group: "Destination 2015 – Spending on Cloud Computing in FS." By FS Senior Research Director Rodney Nelsestuen, June 2011.
Note: Spending estimates based on assumption of no clear global cloud standards

4. MARCO TEÓRICO.

4.1. ANTECEDENTES DEL CONCEPTO DE CLOUD COMPUTING.

"*Cada 15 años, más o menos, un conjunto de avances tecnológicos permite que surja un nuevo modelo al mismo tiempo que las empresas se dan cuenta de que el actual enfoque se está agotando. La PC no fue una pequeña mainframe. Cambió la forma en que las personas interactuaban con las computadoras. La web no fue solo un tipo diferente de PC. Cambió radicalmente el modo en que la gente interactúa con los negocios. Lo mismo ocurre con la nube. La nube no es solo una nueva forma de manejar centros de datos. Es un enfoque totalmente nuevo de IT. – Donald Ferguson, vicepresidente ejecutivo. CA Technologies"* [IANSITI, Marco y otro. 2011]. Esta frase resume de modo conciso, las tres grandes plataformas de la evolución de la Tecnología Informática. Las figuras 4.1 y 4.2 representan esta evolución de la informática, las que se describen a continuación.

Figura 4.1 – Etapas de evolución de la informática. [IANSITI, Marco y otro. 2011]



a) 1er. Plataforma: surge con la aparición del mainframe en la década de 1960, basado en un nuevo estándar diseñado por IBM con la aparición del System/360 y que se extiende hasta comienzos de la década de 1980. Los mainframes eran utilizados por aplicaciones de software que ayudaban a gestionar y automatizar múltiples procesos de negocio. [IANSITI, Marco y otro. 2011]. Sus principales características son:
   a. Procesamiento totalmente centralizado.

b. Terminales sin capacidad de procesamiento.
c. Redes con protocolos propietarios.
d. Miles de aplicaciones disponibles. [SEMINARA, Juan P. y otro. 2013].
e. Millones de usuarios. [SEMINARA, Juan P. y otro. 2013].

b) 2da. Plataforma: se extiende desde comienzo de la década de 1980, aproximadamente, hasta mediados de la década del 2000. Se inicia con la aparición de los primeros procesadores de texto y el surgimiento de las computadoras personales (PC). Precisamente en 1981, IBM introduce al mercado su PC IBM-5150.

Impulsado por la aparición de las hojas de cálculo, las capacidades de edición y de presentación, las PC's se introdujeron en la mayoría de las empresas proporcionándoles a los empleados autonomía en el manejo de software.

El crecimiento en el uso de las PC's en las empresas, impulsó un nuevo desafío: lograr compartir en el ámbito de las oficinas, archivos con información que era generada en cada puesto de trabajo. Esto dio lugar a la aparición de las redes LAN (*Local Area Network*) y junto con ellas, las aplicaciones Cliente/Servidor. A partir de este nuevo hito, surge el concepto de aplicaciones departamentales, las cuales dejan de procesarse en los mainframes. [IANSITI, Marco y otro. 2011].

La necesidad de conectar redes LAN ubicadas en diferentes ubicaciones geográficas de una misma compañía, abre el camino para el desarrollo de las redes WAN *(Wide Area Network*) y posteriormente la aparición de Internet con la adopción como estándar del protocolo IP (*Internet Protocol*).

Las características salientes de esta plataforma son:

a. Puestos de trabajo con capacidad de procesamiento local.
b. Redes con protocolos estándares.
c. La cantidad de usuarios se cuenta por cientos de millones. . [SEMINARA, Juan P. y otro. 2013].
d. Decenas de miles de aplicaciones en uso. . [SEMINARA, Juan P. y otro. 2013].

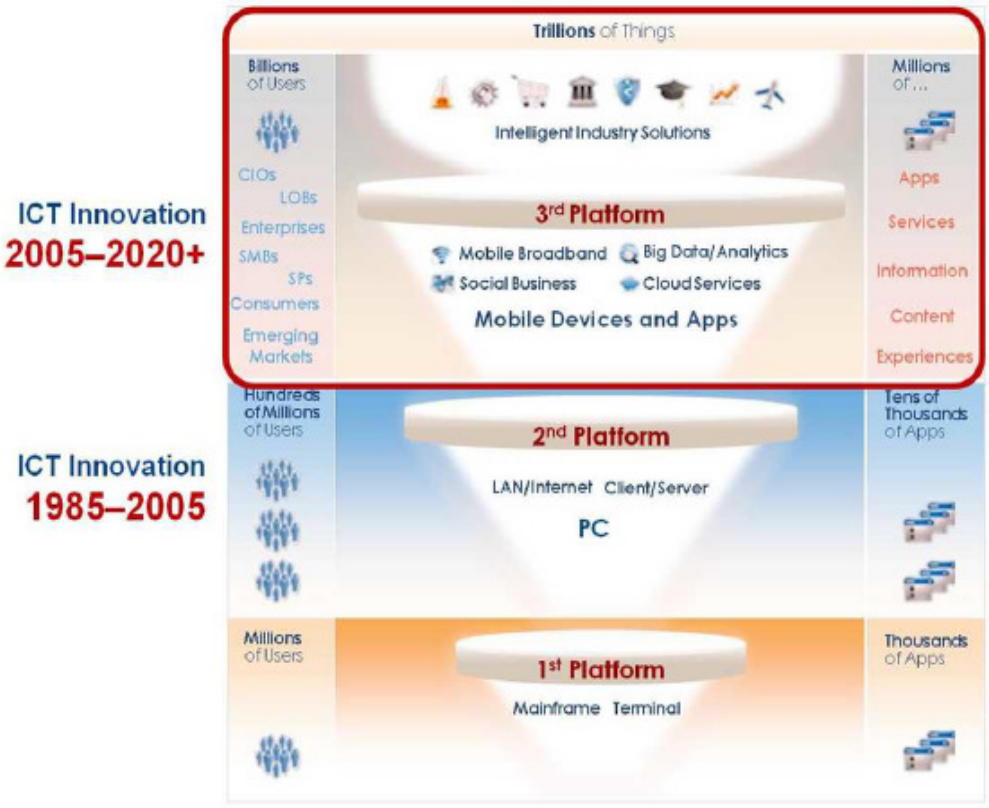
c) 3er. Plataforma: Se inicia aproximadamente a mediados de la década del 2000. Se basa en cuatro pilares:

a. Tecnología Mobile: el crecimiento en la venta de dispositivos móviles: *notebooks, netbooks, tablets y smartphones*, está impulsando a los usuarios a demandar mayor conectividad y nuevas funcionalidades en las aplicaciones existentes, y además, estar disponibles en todo momento y lugar.
b. Big Data: involucra a las tecnologías de almacenamiento y manipulación de grandes volúmenes de datos, en muchos casos no estructurados y provenientes de redes sociales, que son gestionados a través de bases de datos relacionales u otras tecnologías de almacenamiento y búsqueda, en donde el espacio ocupado con datos se mide en Zettabytes (ZB), que es el equivalente a 1000 millones de terabytes (TB).
c. Social Networks: surgen a partir del concepto de Web 2.0, donde se produce un cambio de paradigma sobre el uso de Internet y sus funcionalidades. Los usuarios dejan de tener un comportamiento pasivo, de ser solo consumidores de datos que les proporcionan las aplicaciones disponibles en la web, para pasar a tener una actitud colaborativa, es decir tienen la posibilidad de participar activamente en la red, subiendo sus comentarios, fotos, y compartir contenidos. [JOYANES AGUILAR, Luis. 2012]
d. Cloud Computing: surge como la necesidad de ofrecer bajo la modalidad de servicio, los recursos informáticos de hardware, software y servicios asociados. Se apoya en dos grandes pilares: la tecnología de data center y la virtualización. [JOYANES AGUILAR, Luis. 2012]

Las características salientes de la tercera plataforma tecnológica, son:

a. Ubicuidad: concepto asociado a la idea de la disponibilidad de las aplicaciones desde cualquier punto de la red, accesible a través de mecanismos estándares independientemente del dispositivo, y en todo momento.
b. Utilización masiva de Internet.
c. La cantidad de usuarios se cuenta en miles de millones. [SEMINARA, Juan P. y otro. 2013].
d. Millones de aplicaciones en uso. [SEMINARA, Juan P. y otro. 2013].

Figura 4.2 – Evolución de las plataformas tecnológicas. [SEMINARA, Juan P., y otro. 2013]



4.2. QUÉ ES CLOUD COMPUTING.

La definición más completa sobre *Cloud Computing* la proporciona 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.*

Este modelo de nube se compone de cinco características esenciales, tres modelos de servicio y cuatro de implementación". [MELL, Peter y otros.2011].

La palabra "ubicuo", de acuerdo al diccionario de la lengua española significa "estar presente a un mismo tiempo en todas partes". Este término aplicado a la definición de *Cloud Computing*, quiere dar idea de la disponibilidad en forma permanente en el

tiempo, desde cualquier lugar y a través de cualquier dispositivo, de los servicios de IT que se ofrecen.

También la palabra "*Cloud*" desde el punto de vista de IT, está asociado a los siguientes conceptos:

- 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 (*storage*), 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. [JOYANES AGUILAR, Luis. 2012].

4.3. CARACTERÍSTICAS DEL CLOUD COMPUTING.

El National Institute of Standard and Technology, en el documento "*The NIST Definition of Cloud Computing",* identifica cinco características esenciales que reúne la tecnología cloud:

a) Auto servicio "*on demand*": implica que un cloud consumer, tiene la posibilidad 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 sus necesidades. [MELL, Peter y otro. 2011].

   Esta característica supone una diferencia bien notable respecto de los servicios "*on premise*" o *data centers* corporativos propietarios, en donde la incorporación de recursos de hardware y software requiere de un análisis sobre la disponibilidad existente, o necesidades de inversión para contratar ampliaciones de equipos y/o licencias de software adicionales, y la afectación de los recursos humanos con perfil técnico para cumplimentar el requerimiento dentro del plan de trabajo.

   El modelo "*Cloud*", se basa en 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. [JOYANES AGUILAR, Luis. 2012].

b) Acceso amplio a la red IP: tiene que ver con la 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 dispositivos heterogéneos (ej.: *notebooks, netbooks, mobile phones, tablets, y desktops*). [MELL, Peter y otro. 2011].

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, los diferentes recursos físicos y virtuales son compartidos entre varios cloud consumers. El cloud consumer no tiene control alguno de los recursos físicos utilizados, pudiendo llegar a conocer, a lo sumo, el lugar geográfico en el cual está situado el data center en el que están sus datos y aplicaciones. [MELL, Peter y otro. 2011].

d) Elasticidad: los recursos de IT (procesamiento, memoria, almacenamiento o storage, y velocidad de acceso a la red), se deben poder asignar y desasignar elásticamente, inclusive en forma automática, según la necesidad del cliente del servicio (on demand). Para el cliente, los recursos informáticos son, en apariencia, ilimitados en capacidad, y pueden ser utilizados en cualquier momento. [MELL, Peter y otro. 2011].

e) Servicio medido: Los sistemas en *Cloud* se controlan automáticamente y el uso de los recursos es optimizado mediante herramientas de medición adecuadas al tipo de servicio (espacio de almacenamiento en disco, capacidad de procesamiento, *bandwidth* o ancho de banda del enlace de datos, cantidad de cuentas de usuarios activos, etc.). [MELL, Peter y otro. 2011].

Adicionalmente a las características enunciadas por el NIST, se pueden agregar estas otras:

f) Capacidad de monitoreo: el cliente de los servicios de *Cloud*, debe poder contar con herramientas que le permitan monitorear el rendimiento de los servicios contratados. Las herramientas de monitoreo deben ser provistas por el cloud provider, y acordadas con el cloud consumer, debido a que son el elemento de medición de la calidad del servicio que debe estar pactado en el contrato entre ambas partes. [JOYANES AGUILAR, Luis. 2012]. A través de las herramientas de monitoreo, el cloud consumer debe poder controlar los recursos informáticos utilizados, medida en que los usa, performance de rendimiento y otros

indicadores, de manera que a través de información transparente, ambas partes, puedan controlar la gestión del servicio "*Cloud*". [MELL, Peter y otro. 2011].

g) Interfaces para integración de aplicaciones: otras de las características que debe reunir el servicio *Cloud*, es la posibilidad de contar con *Application Program Interfaces* (APIs) 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. [JOYANES AGUILAR, Luis. 2012].

4.4. PRINCIPALES OPORTUNIDADES.

Las principales ventajas y oportunidades de la tecnología de *Cloud Computing* por la cual las organizaciones se inclinan a su adopción, derivan de la necesidad de dar respuesta a los desafíos que afrontan sus departamentos de IT.

A continuación mencionamos los desafíos más importantes, y porqué *Cloud Computing* es la respuesta:

a) Utilización adecuada de la capacidad instalada: 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 (*capacity planning)*.

   Muchas veces, por optimismo, se realizan inversiones excesivas en recursos que luego son sub-utilizados, obligando a las compañías a amortizarlos en pocos años dificultándoles la maximización del retorno sobre la inversión realizada (ROI: *Return On Investment*). En otros casos, por pesimismo, se invierte menos de lo necesario provocando un stress de la capacidad instalada para absorber un pico en el volumen de actividad, o a veces, la rapidez de respuesta que requieren los negocios, se contrapone con los tiempos necesarios para seleccionar la tecnología, cumplir con los procesos internos de autorización de nuevas inversiones y aprovisionamiento de los recursos, instalación y puesta en marcha.

Este es un proceso complejo que requiere mantener un balance adecuado para dar respuesta a los picos de demanda exigidos por el negocio, sin comprometer a la compañía en inversiones innecesarias.

Una de sus principales ventajas de *Cloud Computing*, consiste en poder contar con los recursos de IT necesarios, para dar respuesta a las necesidades de la organización sin correr los riesgos de una planificación pesimista que se traduzca en una incapacidad para asistir al negocio o, por el contrario, incurrir en inversiones en recursos que son subutilizados. [ERL, Thomas y otros. 2013].

A partir de este modelo "on demand", la sensación que percibe el *cloud consumer* es que los recursos informáticos disponibles en la "nube" son infinitos, y que puede hacer uso de ellos rápidamente y liberarlos con la misma facilidad una vez que la necesidad dejo de existir.

b) Actualización tecnológica: 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 planificación para la puesta en marcha de los cambios, sin disrupciones en el servicio.

   En el modelo *Cloud Computing,* es el cloud provider quien asume la tarea de mantenerse actualizado tecnológicamente, dado que es parte de su "core business". De esta manera los responsables de IT no deben afrontar el desafío de mantener permanentemente capacitado a su personal técnico, y la dificultad en reclutar recursos humanos profesionales en informática con buen nivel de formación, que no siempre hay disponibles en el mercado en cantidad suficiente.

c) Reducción de costos y de los niveles de inversión: en el modelo propietario u "*on premise"*, existen básicamente dos tipos de costos que impactan en los presupuestos de las áreas de IT: el de adquirir nueva infraestructura y los costos de mantenerla en operación, y amortización.

   La adopción de *Cloud Computing,* contribuye a la reducción de los costos e inversiones de las organizaciones, en razón de que:

i. Se pasa de un modelo de capitalización o “capex”, donde los recursos forman parte de los activos, a un modelo de costo por servicios u “opex”, donde la organización paga por los recursos de IT que efectivamente utiliza. Adicionalmente, por razones de escala, el precio de compra de hardware y software que realizan los cloud providers, es más ventajoso que el que puede obtener un cloud consumer en forma individual.
ii. No requiere que el cloud consumer mantenga recursos técnicos entrenados en las diferentes tecnologías utilizadas (especialistas en sistemas operativos, administradores de base de datos, técnicos en redes, desarrolladores, etc.).
iii. El mantenimiento técnico del hardware instalado y de las licencias de software de base (sistemas operativos, motores de base de datos, herramientas de desarrollo, etc.) dejan de estar a cargo del cloud consumer.
iv. La actualización técnica motivada por la aparición de nuevas versiones de software y la gestión de parches de software (*patch management*), dejan de ser responsabilidad del cloud consumer, ya que es el cloud provider quien se ocupa de estas tareas. Además de los riesgos propios de este tipo de actualizaciones, también los costos suelen ser importantes, dado que obligan a contar con entornos de prueba o testing para las nuevas versiones, además de las tareas propias que implican la implementación de los cambios.
v. Se evitan o reducen los costos administrativos que implican el seguimiento del stock de licencias, renovación y mantenimiento de los contratos con los múltiples proveedores de infraestructura y servicios. [ERL, Thomas y otros. 2013].

d) Agilidad: para desenvolverse en el mundo actual de los negocios, las organizaciones deben contar con la habilidad de poder adaptarse rápidamente a las necesidades de sus clientes y al ecosistema en el que desarrollan su actividad. Las áreas de IT no son ajenas a este proceso, sino que tienen el desafío de ajustarse a esos cambios, adaptando sus recursos de hardware, software y servicios, no solo en etapas de crecimiento sino también en las de

reducción del volumen de negocio. [ERL, Thomas y otros. 2013]. En el modelo "*on premise*" estos ajustes suelen ser lentos y costosos.

En cambio, en el modelo de *Cloud Computing*, se pueden disponer de los recursos de hardware y software en forma ágil, dinámica y por el tiempo que sea necesario. [ERL, Thomas y otros. 2013]. Para ello, hace uso de la tecnología de virtualización, que puede definirse como un mecanismo de abstracción que posibilita que sobre un mismo hardware o software de base, se puedan proveer múltiples instancias virtuales que comparten la misma capacidad de procesamiento, inclusive con diferentes sistemas operativos. [ERL, Thomas y otros. 2013].

Antes de la aparición del concepto de virtualización, los recursos de hardware y software conformaban un entorno estático e inseparable. Las primeras aplicaciones de virtualización, posibilitaron que sobre un mismo servidor físico, se pudieran instalar múltiples máquinas virtuales con diferentes sistemas operativos, que compartían los mismos recursos de hardware. Desde la perspectiva del usuario, cada máquina virtual se comporta como si fuera un mismo servidor físico.

Sin la tecnología de virtualización, sería sumamente complejo gestionar un servicio de *Cloud Computing*, dado que lentificaría y encarecería el proceso de asignación de recursos, su escalabilidad, así como también la mejora de performance, la disponibilidad, y administración, entre otras.

En el punto 4.9 se abordará en detalle esta tecnología.

e) Alta disponibilidad: otra de las responsabilidades más importantes de los CIO's y CTO's, es asegurar la alta 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. El modelo "*on premise*" exige mayor nivel de inversión e implica mayores costos de mantenimiento.

   En este punto *Cloud Computing* se apoya en tecnologías como las de Clustering, que consiste en conjuntos independientes de recursos de IT que están

interconectados y que trabajan como un único sistema. Su finalidad es reducir la posibilidad de disrupción de los servicios y aumentar la resiliencia ante fallas. En otros términos, el concepto de cluster implica equipamiento redundante y sistemas preparados para funcionar ante fallas. [ERL, Thomas y otros. 2013].

A su vez esto se complementa con la utilización de la tecnología Grid Computing, en la cual los recursos tecnológicos están organizados en uno o más agrupamientos lógicos, que están coordinados para proveer alta performance de procesamiento. [ERL, Thomas y otros. 2013].

Los fundamentos de "*grid computing*" han influido en la tecnología *cloud*, específicamente en lo vinculado con el acceso a redes de datos, balanceo de carga de procesamiento, sistemas autónomos para administrar configuraciones de equipos, distribución de pool de recursos, escalabilidad y resiliencia. [ERL, Thomas y otros. 2013].

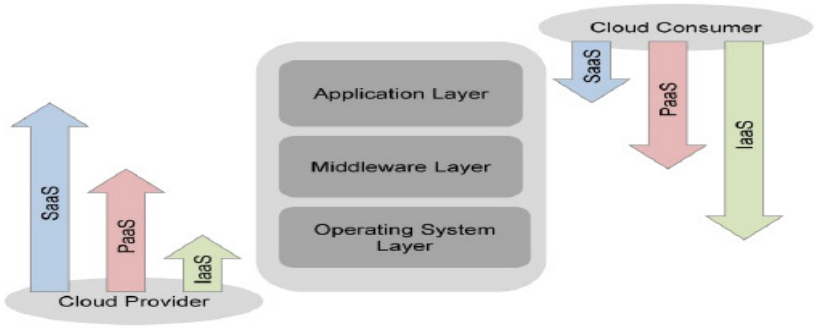
4.5. RETOS DEL MODELO DE CLOUD COMPUTING.

Si bien son importantes las ventajas que ofrece esta tecnología, también existen reparos de la organizaciones para adoptarla totalmente. Entre esos reparos se hallan:

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. En la figura 4.3 se representa como es la superposición de los límites de confianza y controles entre cloud consumer y cloud provider.

   Otro punto importante de vulnerabilidad, deriva de una cualidad básica de la tecnología Cloud, que es la de compartir recursos entre múltiples usuarios. 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. [ERL, Thomas y otros. 2013].

Figura 4.3 – Ámbito de aplicación de control del Cloud Provider y el Cloud Consumer. [LIU, Fang y otro. 2011].



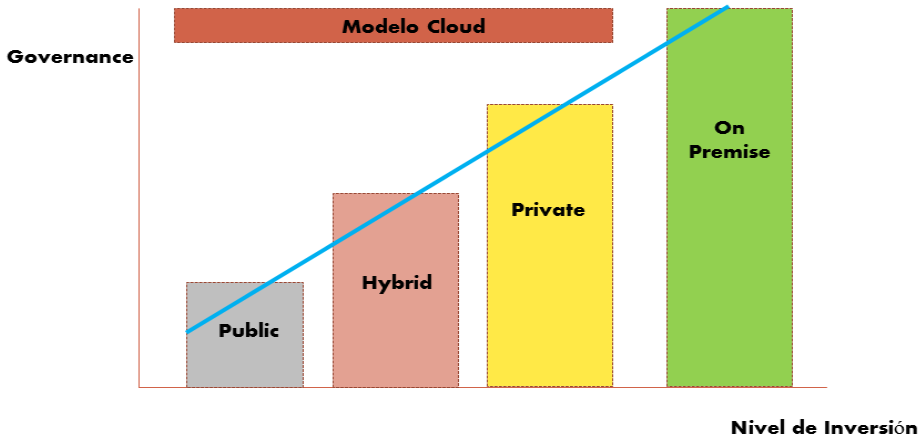
b) Reducción del IT Governance: a medida que la tecnología informática ha ido adquiriendo importancia estratégica dentro de las organizaciones, quienes tienen la responsabilidad de dirigir las organizaciones, consideran como parte integral de ese gobierno un adecuado liderazgo de las estructuras y procesos de IT, para asegurar que contribuya a sostener y extender las estrategias de la organización y sus objetivos.

   La migración de un entorno propietario u "*on premise*" a un ambiente *Cloud*, impacta en el gobierno de IT debido que se introducen los riesgos asociados a la forma en que opere el 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. [ERL, Thomas y otros. 2013].

   Una forma de mitigar este riesgo, es la realización de una buena evaluación de las cualidades de los potenciales proveedores del servicio, y la formalización de la relación cliente/proveedor a través de un contrato, cuyas cláusulas hayan sido analizadas por las áreas técnicas y legales de la empresa, y en el que se contemple un acuerdo de nivel de servicio (*Service Level Agreement* – SLA) aceptable para ambas partes, además de la realización de inspecciones técnicas, monitoreos y auditorías periódicas.

En la figura 4.4 se muestra la relación que hay entre el nivel de inversión requerido de acuerdo al tipo de implementación del modelo de *Cloud Computing*, y del modelo "*on premise*". A medida que se aleja del modelo propietario y se acerca al de public cloud, disminuyen el nivel de inversión requerido y también la capacidad de gobierno de IT en la organización.

Figura 4.4 – Comparación de nivel de inversión en el modelo "on premise" y Cloud Computing



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*". [CLOUD SECURITY ALLIANCE. 2009].

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. Por portabilidad de datos se entiende como la posibilidad que tiene el cloud

consumer de copiar objetos de datos dentro y hacia fuera de la "nube" así como la posibilidad de hacer vuelcos masivos de los mismos. Por interoperabilidad de servicios, se considera la facilidad con la que debe contar el cloud consumer para integrar datos y servicios de la nube con otras aplicaciones propietarias o "*legacy"* que están en ambientes *"on premise*" o, con otros cloud providers. Por portabilidad de los sistemas, se entiende como la capacidad que tiene el cloud consumer de migrar servicios de un cloud provider a otro, se trate de instancias de máquinas virtuales, aplicaciones, datos o servicios. [LIU, Fang y otros. 2011].

La falta de estándares de interoperabilidad puede ser una traba a la hora de decidir migrar servicios a la nube.

d) Compliance y regulaciones legales: uno de los retos de la tecnología *cloud*, está vinculado con los aspectos legales y contractuales que vinculan al cloud consumer con el cloud provider.
En el punto 6.2 se tratarán estos temas enfocados desde la óptica del negocio financiero/bancario.

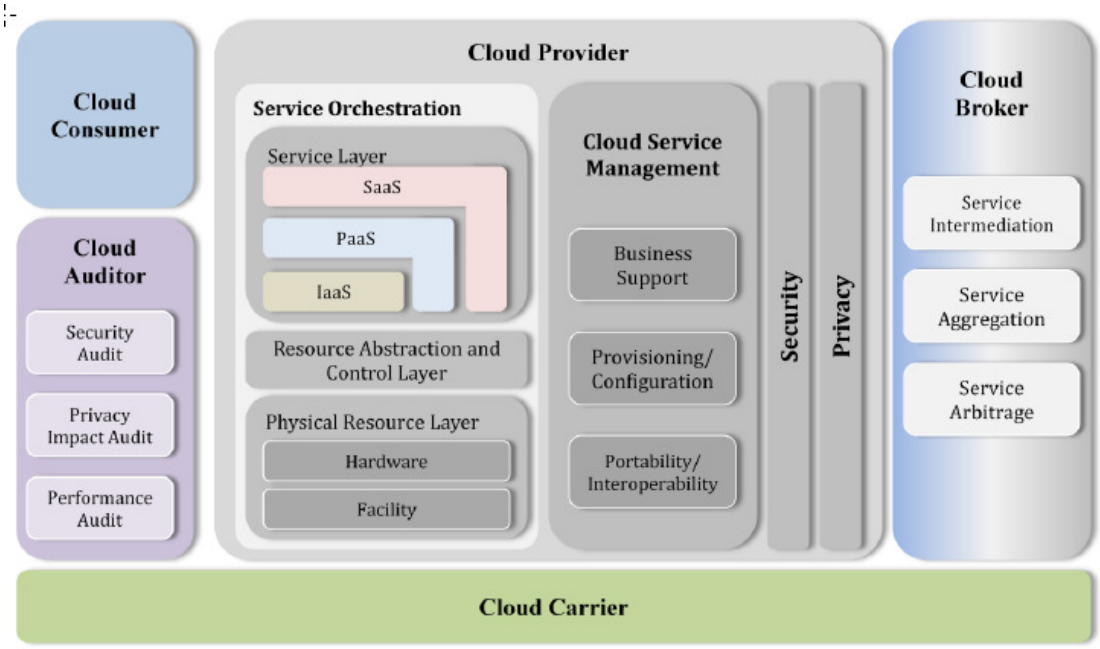
4.6. PRINCIPALES PARTICIPANTES DE LOS SERVICIOS EN LA "NUBE".

En la figura 4.5 se representa la arquitectura del modelo conceptual del servicio de *Cloud Computing*, con la referencia de las principales partes intervinientes.

a) Cloud Consumer: es la persona u organización que establece una relación con un cloud provider, para utilizar los servicios de computación en la nube. El cloud consumer es quien evalúa los distintos tipos de servicios ofrecidos por los cloud providers, que se adapten a sus requerimientos, condiciones de uso y niveles de prestación. [LIU, Fang y otros. 2011].

El cloud consumer es además quien debe especificar los niveles de servicios en cuanto a calidad, performance, seguridad, disponibilidad, y resiliencia, así como las condiciones que le faciliten la portabilidad de sus datos y aplicaciones a otro proveedor. [LIU, Fang y otros. 2011].

Figura 4.5 – Modelo conceptual de Cloud Computing. [LIU, Fang y otros. 2011].



Dependiendo del tipo de servicio Cloud, varían las posibilidades disponibles para el cloud consumer. A modo enunciativo se indican algunos de ellos:

i. *Cloud consumer* de infraestructura de IT: hace uso de los recursos de infraestructura de data center de producción y/o de recovery, servidores virtuales, sistemas de almacenamiento de datos (*Storage)*, recursos de networking, etc. y conserva la administración desde los sistemas operativos instalados sobre los servidores virtuales, los motores de base de datos así como la gestión de las aplicaciones de negocio.
ii. *Cloud consumer* de plataformas tecnológicas de IT: utiliza los ambientes de sistemas operativos y de base de datos definidos y administrados por el cloud provider. El cloud consumer esta limitado a gestionar exclusivamente su aplicación de negocio y sus datos.
iii. *Cloud consumer de application software*: servicios de correo electrónico, herramientas de automatización de oficina, aplicaciones de CRM (*Customer Relationship Management*), aplicaciones de ERP (*Enterprise Resource Planning*), aplicaciones de administración de recursos humanos,

administración de documentos, redes sociales, herramientas de colaboración, entre otras.

b) Cloud Provider: es la entidad que proporciona las aplicaciones y facilita la infraestructura de IT para la prestación del servicio. [JOYANES AGUILAR, Luis. 2012].

Las actividades y responsabilidades asociadas del *Cloud Provider*, varían según el tipo de servicio cloud que brinde:

i. Como proveedor de infraestructura de IT, se encarga de adquirir el equipamiento sobre el cual se estructura el servicio, es decir servidores, soluciones de *storage*, redes, y todo lo vinculado con el espacio requerido para el alojamiento de los equipos, incluyendo sistemas de control de acceso, detección y extinción de incendios, servicio de energía ininterrumpida, y aire acondicionado. Como un nivel de abstracción, el cloud provider de infraestructura de IT, utiliza software de virtualización para el despliegue de servidores, *storage* y redes que es utilizado por diferentes cloud consumers. Bajo la modalidad de proveedor de servicios de infraestructura de IT, el cloud provider tiene bajo su responsabilidad la administración del equipamiento físico y del software de virtualización que le permite el armado y gestión de las múltiples instancias virtuales que ofrece a sus cloud consumers. [LIU, Fang y otros. 2011].

ii. Como proveedor de plataformas tecnológicas de IT, se ocupa de brindar y gestionar plataformas para desarrollo y testing de aplicaciones, motores de bases de datos, componentes de *middleware*, kits de herramientas de desarrollo, herramientas de monitoreo y gestión de aplicaciones, etc. [LIU, Fang y otros. 2011].

iii. Como proveedor de software en la “nube”, tiene la tarea y responsabilidad de configurar, mantener actualizado el funcionamiento de las aplicaciones de software montadas sobre una infraestructura cloud para que estén disponibles para los cloud consumers. En este caso el cloud provider asume la mayor parte de la responsabilidad de la gestión y control de las

aplicaciones e infraestructura, mientras que la responsabilidad del cloud consumer se limita a gestionar los usuarios que pueden utilizar la o las aplicaciones y administrar sus parámetros específicos. [LIU, Fang y otros. 2011].

c) Cloud Auditor: es un tercero independiente del cloud provider y del cloud consumer, que puede examinar los servicios brindados en la nube con la finalidad de emitir opinión técnica al respecto. Estas auditorías se llevan a cabo para verificar y evaluar, mediante la revisión de evidencias objetivas, el cumplimiento de normas y calidad de los servicios proporcionados por el cloud provider en materia de controles de seguridad física y lógica, confidencialidad, performance, disponibilidad, políticas y normas acordadas con el cloud consumer. [LIU, Fang y otros. 2011].
d) Cloud Broker: tiene el rol de intermediar en la relación entre el cloud consumer y el o los cloud providers, brindándole al primero los servicios que el broker contrata directamente con los cloud providers. En otras palabras no hay una relación contractual directa entre el proveedor real del servicio y el cloud consumer. Esta figura toma sentido cuando se trata de organizaciones medianas o pequeñas y la integración de servicios cloud se torna compleja de gestionar. [LIU, Fang y otros. 2011].

Según el NIST, los servicios brindados por un cloud broker, pueden ser de tres tipos:

i. Servicios de Intermediación: en este caso el broker brinda un servicio complementario que suma valor agregado a un servicio ya existente. Como ejemplo se pueden citar software de control de acceso de usuarios, herramientas de medición de performance, etc. [LIU, Fang y otros. 2011].
ii. Agregación de Servicios: el broker combina e integra varios servicios en uno, inclusive de diferentes cloud providers.
iii. Arbitraje de Servicio: significa que un bróker tiene la flexibilidad de elegir servicios de múltiples providers. Es un modelo similar al de agregación de

servicios, con la diferencia que los servicios agregados no son fijos. [LIU, Fang y otros. 2011].

e) Cloud Carrier: es el que proporciona conectividad y transporte a nivel de redes de comunicaciones, entre los cloud consumers y cloud providers. [LIU, Fang y otros. 2011]. Los cloud carriers, a través de las redes de telecomunicaciones que gestionan, proporcionan a los cloud consumers el acceso a los servicios provistos por los cloud providers, y deben acordar niveles de calidad de servicio que garanticen la conectividad entre ambas partes (cloud consumer y cloud provider).

4.7. 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 uno más que es el *Community Cloud* o Nube Comunitaria. [MELL, Peter y otros. 2011]. A continuación se describe cada uno de estos modelos.

Public Cloud: se trata de infraestructura tecnológica (hardware, software de base, aplicaciones y servicios) que están disponibles para el uso público en general. Este tipo de "nube" puede estar gestionado por una empresa, entidad académica o gubernamental o combinaciones de ellas. [MELL, Peter y otros. 2011].

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.

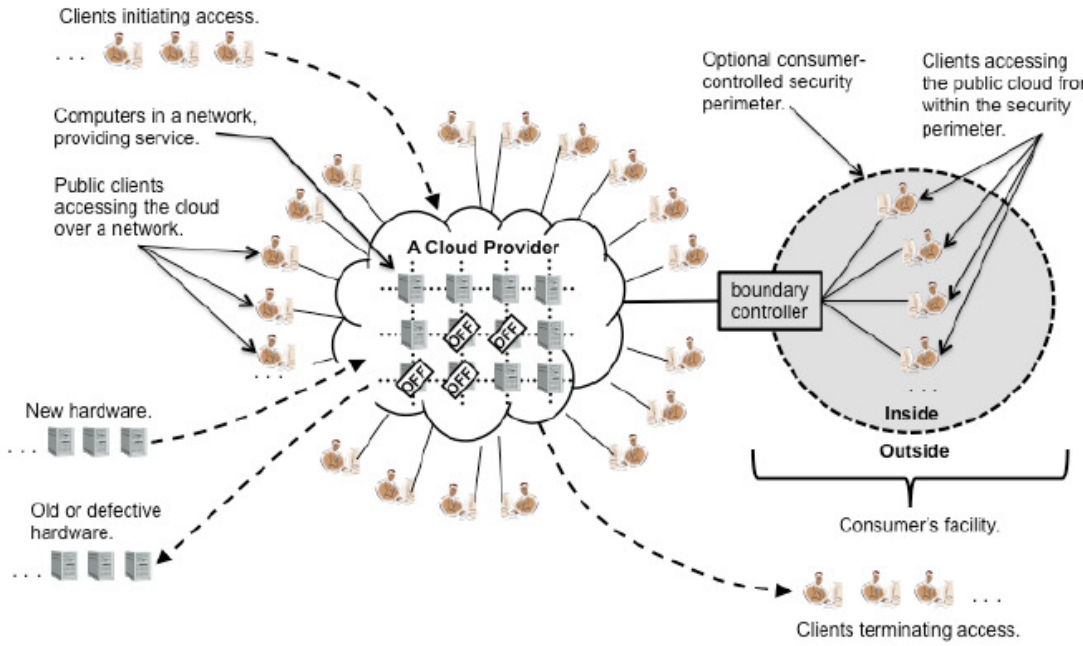
La gestión de seguridad, la provisión de los recursos, y el mantenimiento en funcionamiento de la infraestructura ofrecida, es responsabilidad directa del cloud provider. [JOYANES AGUILAR, Luis. 2012]

Entre otros proveedores de servicios Cloud sobre nube pública, se encuentran:

i. Salesforce
ii. Microsoft
iii. Google
iv. Amazon
v. Yahoo

En la figura 4.6 se muestra la arquitectura de una public cloud. En la imagen se puede observar que existen dos tipos de cloud consumers: los que tiene un perímetro de seguridad propio desde el cual se conectan a la nube, y otros que acceden directamente a través de un acceso Internet.

Figura 4.6 – Public Cloud. [BADGER, Lee y otros. 2012].



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.

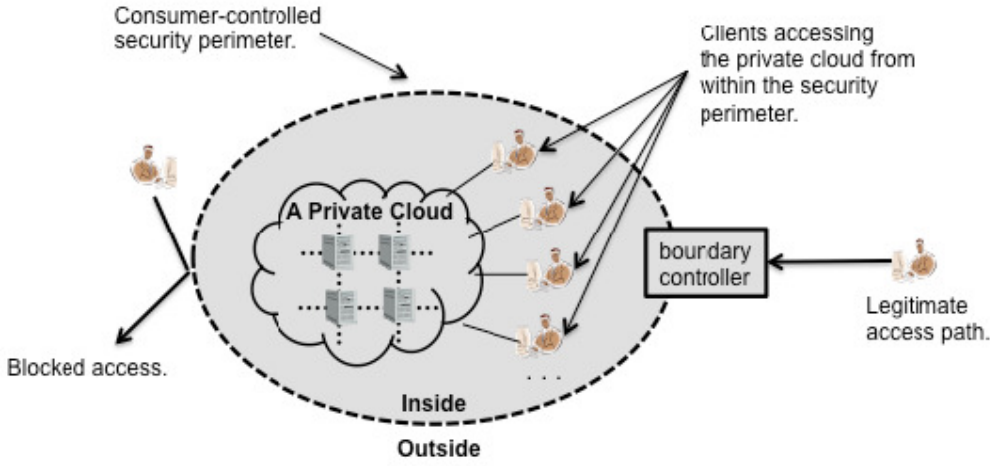
El rasgo distintivo de este tipo de implementación, es que la seguridad física y lógica, así como la operación y administración, es realizada por la misma organización propietaria de la nube privada, quien adopta las características del modelo *Cloud Computing*, para concentrar el acceso de todos usuarios, locaciones y departamentos de una organización a un conjunto de recursos que se brindan a través de la nube. [ERL, Thomas. 2012].

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.

En una misma organización pueden coexistir el modelo de private cloud, y recursos de IT que están en la modalidad "*on-premise*". La diferencia entre ambos modelos esta en el hecho de que bajo el modelo de private cloud los recursos de IT son compartidos entre diferentes cloud consumer internos, y mantienen las ventajas propias del modelo cloud (elasticidad, accesibilidad, agilidad de despliegue, uso compartido entre múltiples cloud consumers internos, etc.), mientras que los recursos bajo la modalidad "*on-premise*", no son multitenant, y en la medida que interactúen con los recursos dispuestos en una nube privada, se los considera como parte integrante del cloud consumer. [ERL, Thomas. 2012]. A modo de ejemplo se puede citar el caso de nubes privadas que coexisten con entornos que, por razones de confidencialidad se mantienen como "on-premise" tales como aplicaciones de auditoría, de gestión de recursos humanos, que no comparten sus recursos físicos y de software con otros usuarios.

La figura 4.7 muestra la estructura de una *private cloud*, en donde se puede apreciar que dentro del mismo perímetro de seguridad se hallan los cloud consumers y los recursos utilizados.

Figura 4.7 –Private Cloud. [BADGER, Lee y otros. 2012].

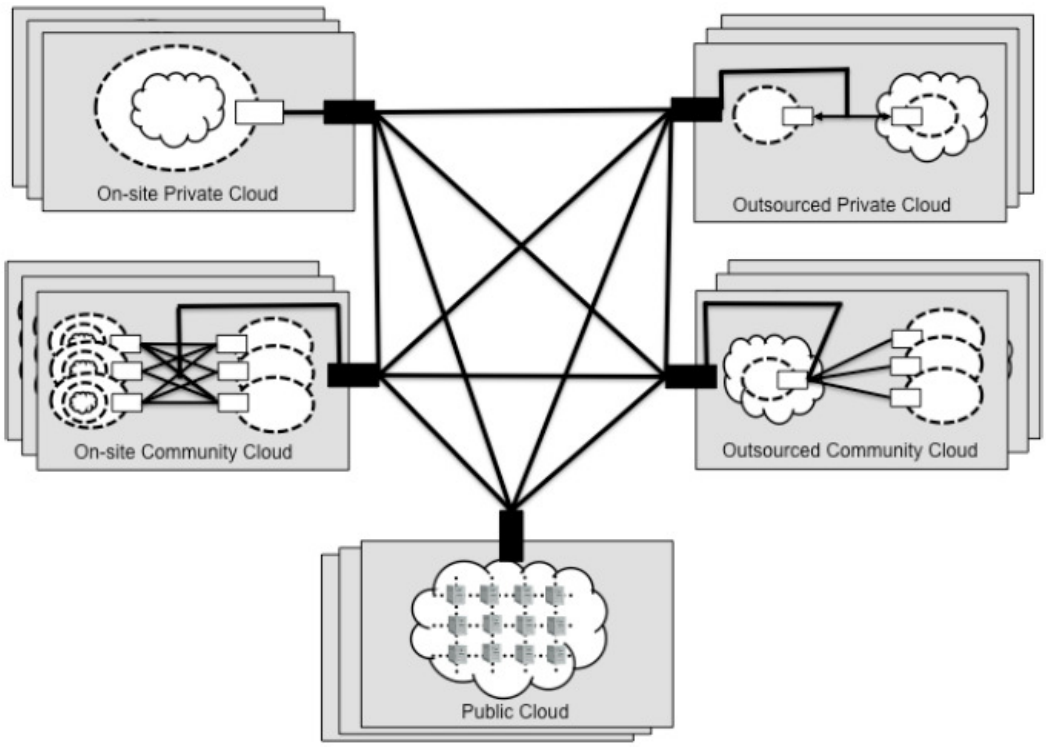


Hybrid Cloud: según la definición que proporciona el NIST, "*es la composición de dos o más nubes (private y public), que siguen siendo entidades únicas, pero que se integran entre ellas por tener tecnologías compatibles que les permiten compartir datos y aplicaciones, y ser portables entre ellas".*[MELL, Peter y otros. 2011].

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 el uso de aplicaciones no críticas, o ambientes de recupero ante de desastres.

En la figura 4.8 se describe una nube híbrida. Este tipo de implementaciones, puede ser utilizado en casos en que el cloud consumer requiere recursos adicionales para atender picos de demanda, o en situaciones de contingencia.

Figura 4.8 – Hybrid Cloud. [BADGER, Lee y otros. 2012].

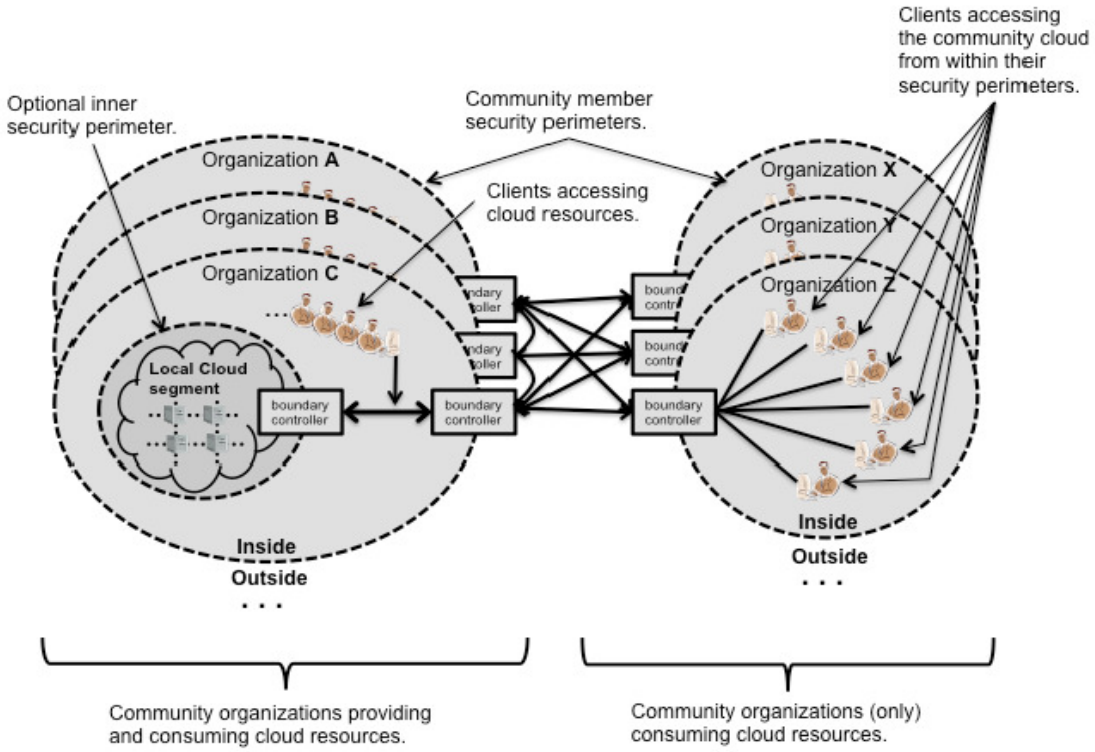


Community Cloud: esta implementación propuesta por el NIST, la define como "*la infraestructura que está preparada para ser utilizada en forma exclusiva por una comunidad de cloud consumers que comparten en común una misión, políticas de seguridad, regulaciones y compliance. Esta nube puede ser administrada y operada por uno o más cloud consumers integrantes de la comunidad, o por un tercero".* [MELL, Peter y otros. 2011].

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.

En la figura 4.9 se describe una *community cloud*. Cada organización puede implementar su propio perímetro de seguridad.

Figura 4.9 – Community Cloud. [BADGER, Lee y otros. 2012].



4.8. MODELOS DE SERVICIO.

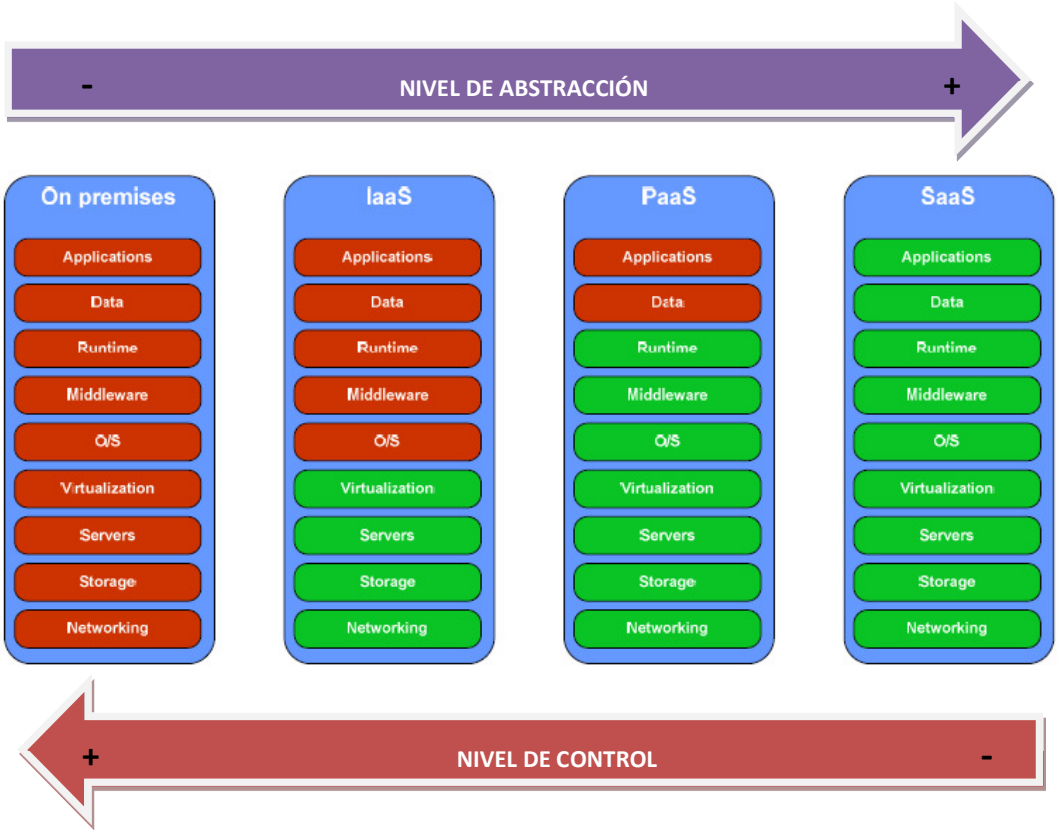
Existen básicamente tres modelos de servicio en la nube:

a) *Infraestructure as a Service* (IaaS) o Infraestructura como Servicio.
b) *Platform as a Service* (PaaS) o Plataforma como Servicio.
c) *Software as a Service* (SaaS) o Software como Servicio.

Independientemente de los modelos mencionados, 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 (STaaS), Desktop as a Service (DaaS) y Business Process as a Service (BPaaS)*.

La figura 4.10, ayuda a describir cada una de las modalidades básicas de servicio, y los niveles de control y de responsabilidad del cloud consumer y del cloud provider.

Figura 4.10 – Comparativo entre “on premise” y IaaS – PaaS – SaaS. [RISTOV, Sasko y Otros. 2013].



El gráfico permite visualizar como varía el nivel de control del cloud consumer sobre las distintas capas de servicio, según se trate del modelo “*on premise*”, o de los distintos modelos de *Cloud*, a medida que aumenta el nivel de abstracción. Así, por ejemplo, en el modelo “on premise” la organización tiene la administración total desde la capa de aplicación hasta la de networking, mientras que en el otro extremo, la modalidad de “Software as a Service” el cloud consumer no tiene administración sobre ningún componente del stack.

De la misma manera, a medida que se avanzar en el modelo *Cloud*, crece el nivel de abstracción del cloud consumer respecto de los servicios. Ese crecimiento en el nivel de abstracción, es directamente proporcional al nivel de control que asume el cloud provider e inversamente proporcional al que delega el cloud consumer.

Seguidamente se describen cada uno de los modelos de servicio.

a) Infraestructura como servicio: Es el modelo de servicio cloud, que más se aproxima al concepto de infraestructura "*on premise*". 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. [MELL, Peter y otros. 2011].

   El cloud consumer asume el control desde la capa de sistema operativo hacia arriba de la pila, es decir hasta la aplicación inclusive. Por el contrario, no tiene capacidad de gestión sobre la infraestructura subyacente, es decir a partir del software de virtualización hacia los niveles más bajos del *stack* de servicios (ver figura 4.10). 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. El cloud provider, asume el control del software de virtualización y los recursos subyacentes.

b) Plataforma como servicio: Se lo define como l*a 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 [MELL, Peter y otros. 2011]. 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. [ERL, Thomas y otros. 2013].

   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 de servicio, el cloud consumer, no tiene responsabilidad sobre la infraestructura en la cual se desarrollan las aplicaciones (red de datos, servidores, sistema operativo, 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 las más conocidas.

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*" [MELL, Peter y otros. 2011].
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 contratadas, de la cantidad conexiones concurrentes, y/o del espacio de almacenamiento ocupado, entre otras modalidades.

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

4.9. VIRTUALIZACIÓN.

4.9.1. DEFINICIÓN.

El NIST define el concepto de virtualización como "*la simulación del software y/o hardware sobre el cual se ejecuta otro software. Este entorno simulado se denomina Máquina Virtual (Virtual Machine) (VM)".* [SCARFONE, Karen y otros. 2011].

Diferentes tipos de recursos físicos pueden ser virtualizados:

- Servidores: un server físico puede ser migrado a un entorno virtual.
- Almacenamiento en disco: se representan a través de soluciones implementadas sobre diferentes tecnologías: NAS (Network Access Storage), SAN (Storage Area Network) sobre Internet SCSI (iSCASI), Fiber Channel (FC), o Fiber Channel over Ethernet (FCoE).
- Equipamiento de red de comunicaciones: equipamiento activo de redes de comunicaciones tales como *routers* y *switches* pueden ser objeto de virtualización. Esto ha dado lugar al desarrollo de una nueva tecnología denominada SDN (Software Defined Networks).

En este punto se describirán las técnicas de "*full virtualization"* o virtualización completa de servidores, empleada en los centros de datos.

4.9.2. ANTECEDENTES.

La virtualización es una tecnología desarrollada desde finales de la década de 1970, por los fabricantes de *mainframes*, con el objetivo de optimizar el uso de los recursos de hardware disponibles, permitiendo a los usuarios contar con más de un entorno con sistemas operativos diferentes ejecutándose en un mismo equipo físico.

Con el advenimiento de la PC en la década de 1980, la aparición de aplicaciones cliente-servidor y la reducción de los costos del hardware, la virtualización fue relegada. A su vez dadas las particularidades y las dependencias de las aplicaciones

de negocio respecto del entorno de hardware y software de base sobre el cual corren, promovió la descentralización de aplicaciones de tal forma, que provocaron el crecimiento de la infraestructura de servidores instalados en las organizaciones. Esta arquitectura organizada en forma de “silos” implica en los hechos, que cada aplicación tiene para su propio uso, todos los recursos físicos de procesamiento y de almacenamiento disponibles en el servidor físico en el que está instalada. Esta situación conlleva el crecimiento del espacio ocupado en los data centers, y el consiguiente aumento de consumo de energía y exigencias de refrigeración, así como el incremento en la cantidad de recursos humanos dedicados a administrarla.

Este modelo no es eficiente en el uso de recursos de hardware, dado que en la práctica, se da que un determinado equipamiento es sub-utilizado mientras que otras aplicaciones requieren al máximo de recursos sin la posibilidad de obtenerlos de los que están ociosos en otro server. Toda esta situación motivó que el concepto de virtualización comenzara a imponerse nuevamente en las organizaciones. [JOYANES AGUILAR, Luis**.** 2012].

En la figura 4.11 se representa una típica arquitectura de tipo “silo”, en la que cada aplicación cuenta con recursos de hardware y software de base asignados para su uso exclusivo. Es posible apreciar cómo esta separación hace que sea prácticamente inviable la reasignación de recursos de hardware de un servidor a otro en caso de saturación.

A través de la virtualización, es posible compartir recursos físicos sin que ello impacte en cambios en las aplicaciones de negocio. A través de este modelo de abstracción, las aplicaciones corren en ambientes virtuales que simulan el entorno físico que ésta necesita. Lo concreto es que en un entorno virtualizado las aplicaciones no interactúan con los dispositivos físicos en forma directa, sino a través de una capa de software que simula los recursos de hardware. [PANIAGUA MACIA, Claudio. 2006].

La figura 4.12 representa un modelo de virtualización en donde se puede observar como los recursos de hardware y software son compartidos.

Figura 4.11 – Recursos de IT organizado por silos. [PANIAGUA MACIA, Claudio. 2006].

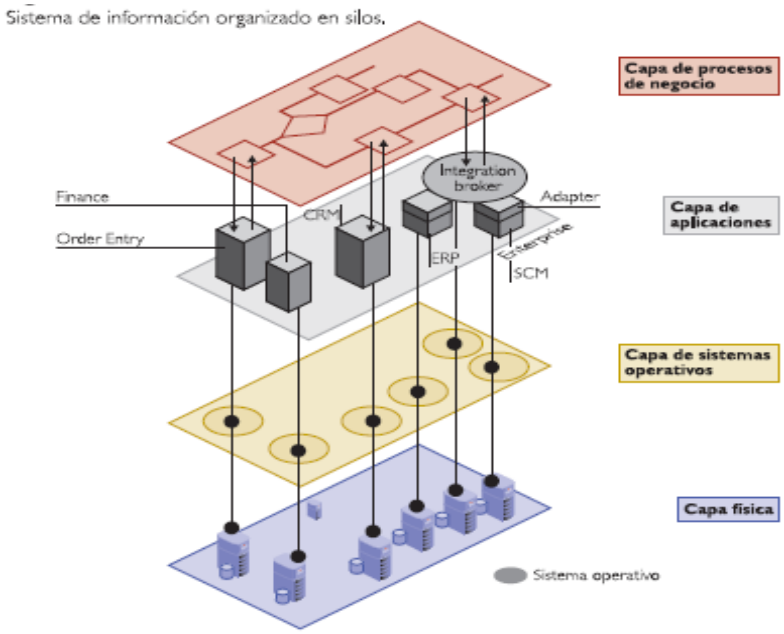
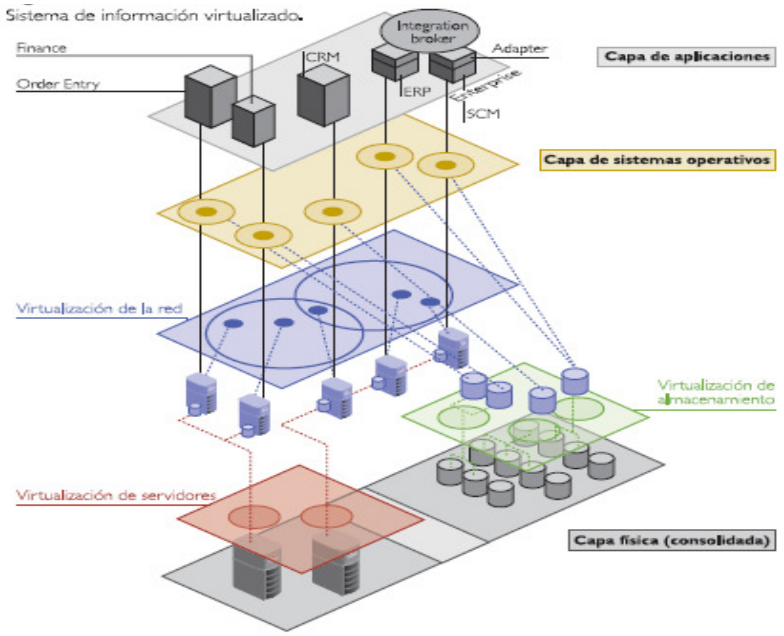


Figura 4.12 – Recursos de IT virtualizados. [PANIAGUA MACIA, Claudio. 2006].



4.9.3. PRINCIPALES OBJETIVOS DE LA VIRTUALIZACIÓN.

a) Optimización de recursos: es ésta una de las razones más invocadas para la adopción de la virtualización, y tiene que ver con hacer eficiente el uso de los recursos de hardware existente, y evitar adquisiciones innecesarias. También contribuye a la reducción del consumo de energía eléctrica y de refrigeración.

b) Escalabilidad: Posibilita el despliegue rápido de nuevos servidores a partir de imágenes pre-configuradas de acuerdo a las políticas de la organización, así como la asignación/des-asignación de recursos en forma dinámica de acuerdo a las necesidades del negocio. De esta manera se puede hacer frente a requerimientos puntuales sin necesidad de contar con demasiados recursos ociosos.

   Esta característica contribuye a la optimización de los recursos de hardware disponibles.

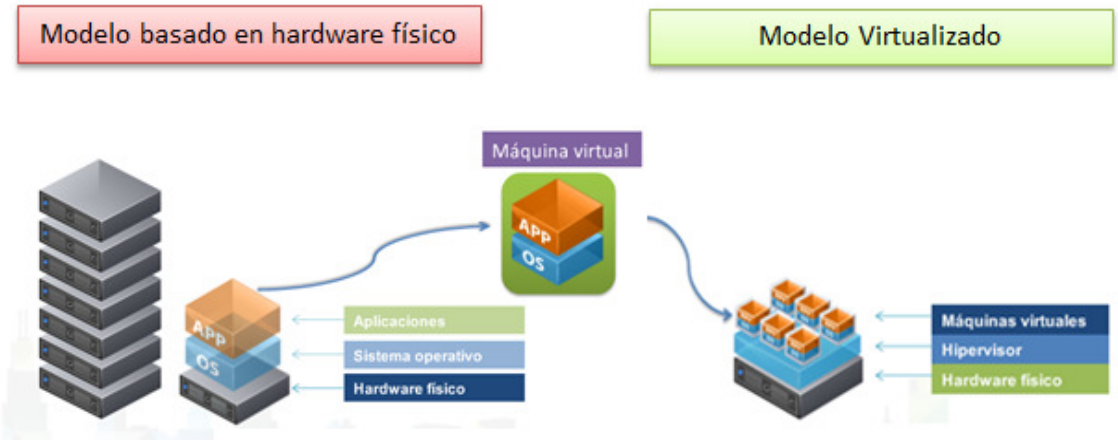
c) Administración: el software de virtualización provee herramientas que facilitan las tareas de supervisión del entorno sobre el cual se hallan instaladas las máquinas virtuales, a la vez que automatizan tareas rutinarias.

d) Disponibilidad: contribuye a minimizar el tiempo de downtime de los servidores debido a fallas de hardware o a tareas de mantenimiento programadas, y a facilitar la implementación de planes de recuperación ante desastres mediante la replicación de las máquinas virtuales en un site alternativo al de producción.

4.9.4. VIRTUALIZACIÓN DE SERVIDORES. ARQUITECTURA.

En el modelo de "*full virtualization*" de servidores, sobre un mismo hardware físico se configura una o más máquinas virtuales (Virtual Machines - VM) independientes, y sobre cada una de ellas se instala un sistema operativo y la o las aplicaciones que se ejecutan sobre esta instancia. Cada una de las instancias de sistema operativo y sus aplicaciones se ejecuta en la capa superior de un hardware virtual. En la figura 4.13 se representa gráficamente la arquitectura de la virtualización completa de servidores.

Figura 4.13 – Arquitectura de servidores virtualizados. [VMWARE. 2013].



Como se aprecia en la figura precedente, en el "Modelo basado en hardware físico", cada servidor físico tiene instalado un sistema operativo y en la capa superior las aplicaciones. En el "Modelo Virtualizado", entre el hardware y las máquinas virtuales se adiciona una capa de software denominada "*Hypervisor*" (o Hipervisor) que gestiona los recursos para las máquinas virtuales, convirtiendo los recursos físicos de hardware en recursos de software. El *Hypervisor* es un nivel de abstracción, que simula para cada máquina virtual los recursos de hardware físico que ésta última necesita.

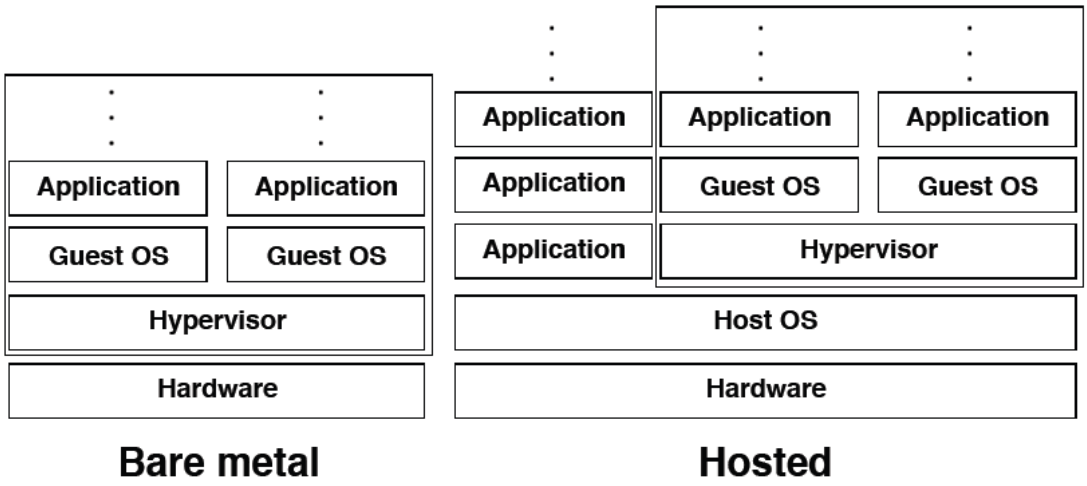
La virtualización completa se puede encarar de dos formas: como virtualización nativa o también denominada "*bare metal*", o como virtualización hosteada o alojada. En la virtualización nativa, el *Hypervisor* se ejecuta directamente sobre el hardware físico, mientras que en la virtualización hosteada, el *Hypervisor* se ejecuta sobre un sistema operativo anfitrión (Ver figura 4.14)

La virtualización nativa respecto de la hosteada, tiene las siguientes ventajas operativas y de seguridad:

a) Añade menos complejidad y vulnerabilidades, al no tener que interactuar el hypervisor con un sistema operativo anfitrión.
b) Mejora el rendimiento de hardware, al eliminarse una capa adicional del software.
c) Mejora la seguridad del entorno, en la medida que esté bien asegurado el hypervisor.

d) Disminuye los riesgos, al eliminar posibles puntos de falla adicionales.

Figura 4.14 – Virtualización Nativa vs. Alojada. [SCARFONE, Karen y otros. 2011].



4.9.5. VIRTUALIZACIÓN DEL ALMACENAMIENTO EN DISCO.

La creciente necesidad de las organizaciones de mantener cada vez más datos "en línea" para ser consultados, la digitalización de procesos y documentos, la virtualización de servidores, y de desktops de usuarios finales, traen aparejada la necesidad de crecer y optimizar los recursos de espacio en disco utilizados por las aplicaciones y los usuarios.

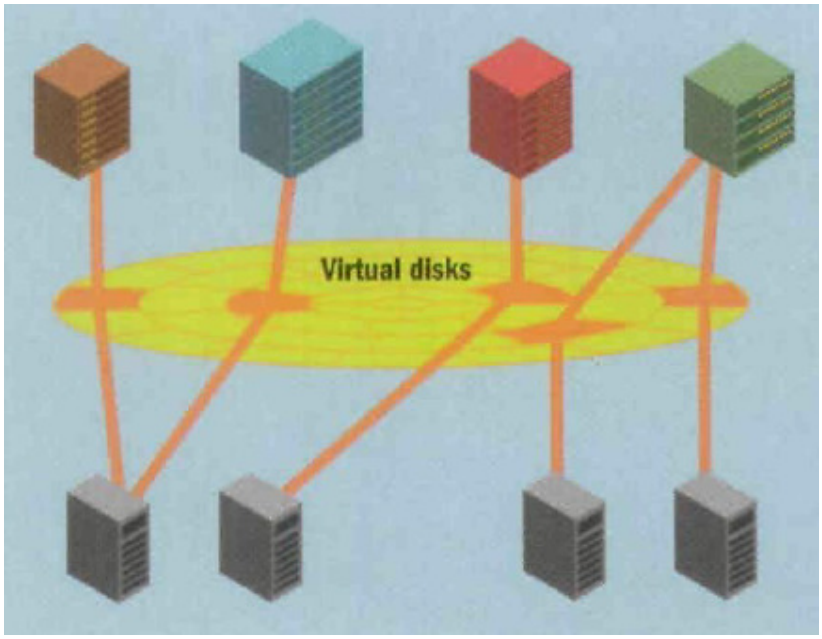
De la misma manera que en el caso de los servidores, en una arquitectura en silos, el espacio en disco esta directamente asociado a la aplicación que se ejecuta en ese hardware, y en caso de contar con espacio en disco disponible, este no puede ser reasignado a otra aplicación más demandante, que esté corriendo en otro server. Esto causa incremento de costos de mantenimiento de hardware, de gestión, de captura de back-ups para resguardo de datos, y además de un desaprovechamiento de recursos disponibles.

El concepto de virtualización del almacenamiento (*storage virtualization*), tiene similitudes al de virtualización de servidores, pudiéndose resumir como el agrupamiento de almacenamiento en disco de diferentes tecnologías en pooles, para que pueda ser compartido por múltiples aplicaciones en forma concurrente (ver figura 4.15). La virtualización enmascara frente a las aplicaciones, la complejidad y la gestión de múltiples dispositivos físicos de diferentes tecnologías y redes de

almacenamiento. Cada pool de espacio en disco (*storage pool*), puede estar conformado por discos físicos que forman parte de diferentes arreglos (*arrays*).

La virtualización del almacenamiento, facilita la implementación de técnicas de protección de datos que incrementan la disponibilidad de los servicios ante fallas de hardware (ej.: *mirroring, y snapshot*), así como de planes de contingencia frente a siniestros en los centros de datos. También proveen herramientas de gestión que permiten incrementar los niveles de calidad de servicio. [NORALL, Steve. 2007].

Figura 4.15 – Virtualización de almacenamiento en disco. [NORALL, Steve. 2007].



Existen básicamente dos tipos de tecnologías para implementar la virtualización de almacenamiento:

a) NAS (*Network Attached Storage*): se trata de almacenamiento de archivos en dispositivos que están conectados a la misma red en la que se encuentran los servidores y desktops. Las soluciones de tipo NAS, trabajan a nivel de archivo entre el cliente (server o desktop) y el dispositivo de almacenamiento.
b) SAN (*Storage Area Network*): es una red dedicada a brindar acceso a dispositivos de almacenamiento a nivel de bloques de datos, mediante el uso de diferentes protocolos de conexión: *Fiber Channel* (FC), *Fiber Channel over*

Ethernet (FCoE), iSCSI *(Internet Small Computer System Interface*). A través de esta tecnología, se pone a disposición de los servidores el almacenamiento de matrices de discos que simulan ser locales.

4.10. TECNOLOGÍA DE DATA CENTERS.

De acuerdo a la definición de la Telecommunications Industry Association (TIA) dada en su estándar TIA-942, se define como data center al "*edificio o parte de un edificio cuya función principal es la de albergar equipamiento informático"* crítico de una organización.

El *data center* de una organización, y en particular el de los bancos, es un recurso crítico en razón de que es el lugar en el que residen servidores, soluciones de storage, y equipamiento de red, sobre el cual están instaladas las aplicaciones y datos que dan soporte a las operaciones del negocio. Sin temor a exagerar, puede afirmarse que es tan importante en un banco su tesoro de valores, como su data center. Por ende, uno de los atributos claves que debe reunir el data center de una entidad financiera, es su confiabilidad.

El estándar TIA-942, establece las pautas que deben reunir los data centers en los siguientes puntos:

a) Disponibilidad: tiene que ver con el nivel de uptime que debe reunir. La norma establece cuatro niveles (*Tiers*):
   I. Tier I: data centers que pueden verse afectados por disrupciones ocasionadas por hechos imprevistos o planificados. No cuentan con el nivel de redundancia adecuada en materia de equipamiento mecánico eléctrico y de refrigeración, y pueden no contar con piso técnico, UPS y/o grupo electrógeno. El nivel de disponibilidad comprometido es de 99,641%.
   II. Tier II: si bien tienen cierto equipamiento redundante, no cuentan con sistemas de distribución eléctrico redundante, lo que puede originar que en determinados casos se deba sacar de servicio equipamiento informático debido a la realización de tareas de mantenimiento. Sí deben contar con piso técnico, UPS y grupo electrógeno. El nivel de disponibilidad comprometido es de 99,741%.

III. Tier III: cuenta con múltiples paths de distribución de energía y sistemas de refrigeración. Permite que se puedan realizar tareas de mantenimiento programadas sin que se afecte el servicio. De todas maneras no está protegido ante disrupciones motivadas por actividades no previstas o errores de operación. El nivel de disponibilidad comprometido es de 99,982%.

IV. Tier IV: los data centers certificados en esta categoría, pueden realizar cualquier tarea de mantenimiento programado sin disrupción del servicio, y soportar fallas imprevistas sin que impacte en la carga crítica. Todos sus componentes son tolerantes a fallas (*fault-tolerant*). El nivel de disponibilidad comprometido es de 99,995%.

b) Espacio y topología: entre las pautas a tener en cuenta a la hora definir el lugar y espacio físico que será destinado a un data center, deben considerarse:

I. Espacio actual ocupado, y espacio de expansión para futuras ampliaciones.

II. Un diseño topológico adecuado que contemple, sala de carriers de comunicaciones (primaria y secundaria), y área de distribución principal para los equipos de comunicaciones que conforman el *backbone*, áreas de distribución horizontal y gabinetes (*racks*) con equipos *rackeables* y *no rackeables*, y un área de operaciones y soporte. En la figura 4.16 se presenta un diagrama con la topología de un data center Tier IV previsto por la norma TIA-942.

c) Distribución de cableado: el estándar prevé un cableado de *backbone* redundante, que interconecta las equipos terminales de los carriers con los routers y switches de core ubicados en el área de distribución principal.

También prevé un cableado denominado “horizontal” redundante, y en diferentes tecnologías (fibra óptica y cobre) que interconecta los equipos de comunicación central con los switches de red local (LAN) a los cuales se conectan los equipos informáticos.

Las mejores prácticas recomiendan la utilización de racks o gabinetes de cableado para asegurar una administración de los cables y prever un crecimiento ordenado.

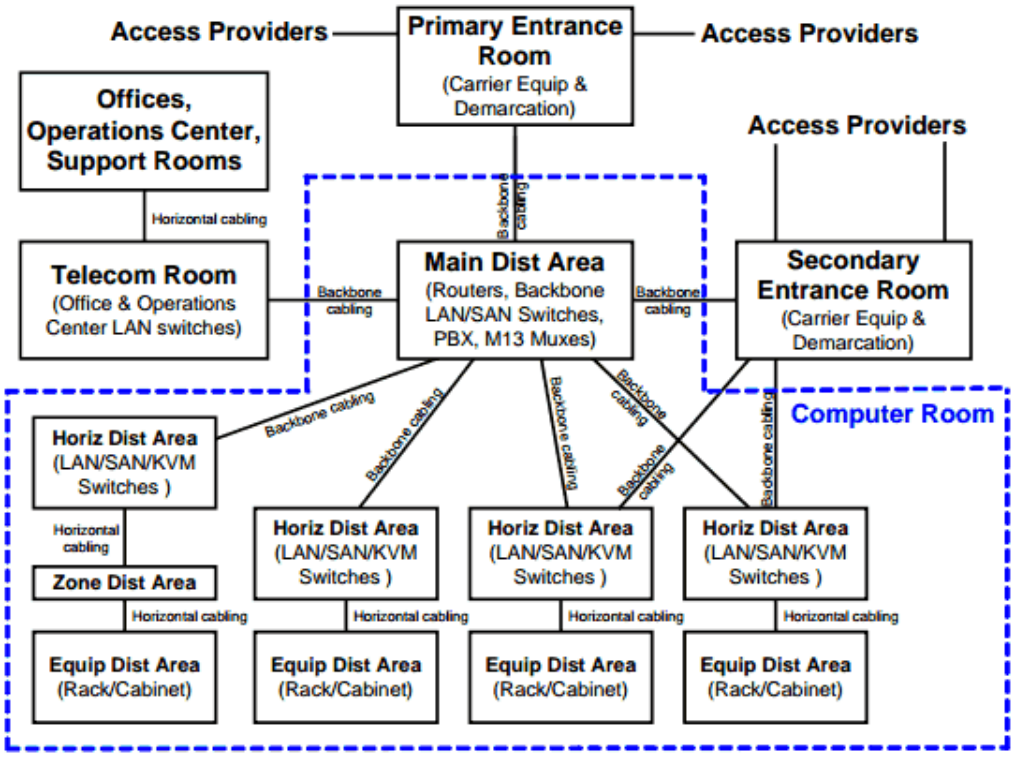
En cuanto al tendido del cableado de datos, puede ser realizado por debajo de piso técnico o elevado, mediante la utilización de bandejas portantes. Respecto

de la fibra óptica, la recomendación es, debido a la fragilidad del material, que se transporte por bandeja separada de los de cobre.

Es mandatorio, que el cableado de suministro de energía este soportado en bandejas separadas por debajo de piso técnico, para evitar los efectos de electromagnetismo.

Respecto de la conexión de los equipos al cableado horizontal, se reconocen tres métodos: directo, interconexión o cruzada. El método recomendado por las buenas prácticas, es el de conexión cruzada, en razón de su confiabilidad y agilidad al momento de introducir cambios y o nuevo equipamiento en el data center.

Figura 4.16 – Topología de data center con acceso a múltiples salas. : [TELECOMUNICATIONS INFRASTRUCTURE STANDARD FOR DATA CENTERS. 2004].



d) Energía: el suministro eléctrico de un data center es una de sus partes vitales. Para alcanzar niveles de confiabilidad similares a los de Tier III o IV, se requiere:

I. Acometida de más de un proveedor de energía de red, y de diferentes fuentes.
II. Contar con servicio ininterrumpido de energía. Ello se consigue a través de equipamiento denominado UPS (*Uninterrupted power supplies*), que evita ante un corte en el suministro de red, que el data center quede sin energía hasta que se completen las maniobras de activación de los sistemas de generación alternativos (grupo electrógeno).
III. Circuitos eléctricos redundantes para soportar todos los equipos críticos del data center. Para ello es importante que todos los equipos informáticos cuenten con doble fuente de poder.
IV. Contar con generadores eléctricos en el sitio.

e) Refrigeración: el mantenimiento de niveles de temperatura adecuados dentro del data center, es un factor importante para el normal funcionamiento de los equipos informáticos. Los estándares sobre diseño de data center, establecen un procedimiento conocido "pasillo caliente/pasillo frío" ("*hot aisle/cold aisle*"), según el cual los *racks* se disponen en hileras de tal manera que el frente de los equipos dé al pasillo frio y el contra-frente al pasillo caliente. En otros términos en el pasillo frío están los rack frente a frente, y en el caliente dorso contra dorso.

   Este diseño posibilita que el aire frío llegue a los equipos por el frente y se expulse el aire caliente por la parte trasera del rack, evitando mezclar el aire frío con el caliente. Así no solo se mejora la ventilación de los equipos, si no que se optimiza el uso de los equipos de aire acondicionado, reduciendo el consumo de energía eléctrica y la emisión de gases.

g) Seguridad física: hay dos aspectos críticos a tener en cuenta en materia de seguridad física:
   I. La protección del equipamiento ante posibles siniestros como incendios o inundaciones, mediante la instalación de sistemas de detección y extinción de incendios provocados por material eléctrico, y la instalación de detectores de humedad debajo del piso técnico.

II. El control de acceso a las salas donde se encuentra el equipamiento. Estos lugares deben estar adecuadamente protegidos contra el acceso de personas no autorizadas.

5. SEGURIDAD EN CLOUD COMPUTING.

Una de las principales preocupaciones de quienes evalúan migrar sus aplicaciones y/o su infraestructura a *Cloud Computing*, están vinculadas con los aspectos de seguridad de la información.

Alrededor del tema de la seguridad existen diferentes tipos de posturas, a veces contradictorias, o ciertas confusiones. Entre las más comunes se pueden citar:

a) Considerar en las organizaciones que se tiene un control más estricto de los datos, si estos están almacenados dentro de su propia infraestructura, en lugar de una cloud. [JOYANES AGUILAR, Luis, 2012].
b) Asociar private o public cloud con "cloud internas o externas". No necesariamente una private cloud es "interna", dado que ciertos servicios como podrían ser los de infraestructura, bien pueden ser prestados por un tercero y estar alojados en un sitio ajeno a la organización.
c) Confiar que el cloud provider, por tratarse de empresas especializadas en tecnología de la información, tienen condiciones de seguridad superiores a las implementadas en una organización. Si bien esto puede ser cierto, hay dos aspectos de seguridad que no deben soslayarse:
    a. los ataques dentro de la red interna efectuados por usuarios infieles no dejarán de producirse; y
    b. que la adopción de la tecnología cloud potencia la probabilidad de ataques en razón de que los recursos informáticos se comparten.
d) Adoptar la tecnología cloud considerando solo los aspectos económicos. Si bien es cierto que los ahorros pueden ser considerables, una buena práctica sugerida por la Cloud Security Alliance, es la de invertir parte de ese ahorro en implementar mayores controles y auditorias sobre el servicio cloud contratado.
e) No analizar en profundidad las normativas legales vigentes, regulatorias de la actividad de la organización, que pueden estar limitando el alcance de la prestación del servicio por parte del cloud provider.

Dependiendo del modelo de implementación cloud elegido, varía la responsabilidad por la gestión del servicio, la propiedad de la infraestructura y la posibilidad de que los recursos sean compartidos o no.

En la figura 5.1, se presentan todas estas combinaciones en un cuadro de doble entrada. En las filas del cuadro esta cada uno de los modelos de implementación (public, private, community e hybrid cloud), y en las columnas se representa cada uno de los siguientes aspectos: quién gerencia los recursos de IT (esto incluye la operación, la seguridad, compliance, etc.); quién es el propietario de la infraestructura de IT; dónde están ubicados físicamente los recursos de IT; y por último las características de los cloud consumers. Así por ejemplo, es posible determinar que en el modelo de implementación private cloud, la infraestructura puede ser gestionada por la organización o por un tercero, la propiedad de los recursos puede ser propia de la organización o de un tercero, los recursos pueden estar dentro del perímetro de los edificios de la organización o fuera de él, pero los cloud consumers son organizaciones que consideran los temas legales, contractuales y fijan políticas para asegurarse de la confiabilidad de los servicios.

Figura 5.1 – Modelos de implementación. [CLOUD SECURITY ALLIANCE. 2009].

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Organization Or Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] *Management includes: governance, operations, security, compliance, etc...*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

5.1. PRINCIPALES ISSUES.

A continuación se describen las cuestiones de seguridad más relevantes, que deben ser objeto de especial evaluación en tiempo de decidir sobre la adopción de *Cloud Computing*. Algunas de ellas son comunes al modelo *on premise*.

a) Confidencialidad: esta característica implica, que el acceso a los datos debe estar controlado, de manera que solo puedan acceder a ellos los usuarios autorizados, independientemente de la instancia en la que se encuentren los datos: almacenados en dispositivo, o mientras son transportados por la red de comunicaciones. En la tecnología cloud el aspecto de confidencialidad es crítico, dado que los datos suelen estar almacenados en soluciones de storage que son compartidas por múltiples cloud consumers, además que estos son transportados a través de redes públicas, como Internet.
b) Integridad: es la cualidad por la cual los datos no deben ser alterados por personas y/o procesos no autorizados. Mantener la integridad de los datos se extiende también a los procesos que los modifican, a la forma como se almacenan, como se trasmiten y de la manera como se recuperan.
c) Autenticidad: tiene que ver básicamente con dos cuestiones:
    I. Asegurar que los datos fueron originados por quien dice haberlo hecho, y que los mismos no han sido alterados en ningún momento. Esto se logra a través de la implementación de la firma digital. De esta manera se resuelve el problema de la autenticación de un usuario y el no repudio de las transacciones que haya realizado.
    II. Verificar la autenticidad de un sitio web o la autenticidad e integridad del software de una aplicación. Esto se logra a partir de la implementación de certificados digitales emitidos por entidades denominadas autoridades certificantes. Esta medida de seguridad es a los efectos de evitar que alguien pueda simular un sitio web. El uso de certificados digitales, es una práctica necesaria para las organizaciones que operan en comercio electrónico a través de Internet.
d) Disponibilidad: es la capacidad de garantizar que los datos y aplicaciones estén accesibles dentro de la ventana de tiempo acordada entre el cloud provider y el cloud consumer. Asegurar disponibilidad "*on site*" implica que las aplicaciones y

datos están disponibles más allá de fallas de hardware, software, y del uptime del data center.

Asegurar la disponibilidad "*off site*" es garantizar el acceso a las aplicaciones y datos aún en casos de contingencias que pongan fuera de servicio el data center de producción o principal.

5.2. PUNTOS ESTRATÉGICOS Y TÁCTICOS DE SEGURIDAD.

En el momento de evaluar la decisión de migrar a *Cloud Computing*, deben considerarse tres aspectos:

a) El modelo de implementación cloud que se pretende adoptar.
b) Decisiones estratégicas que tienen impacto en el gobierno de IT y de la organización.
c) Decisiones tácticas vinculadas con la implementación, operación y control del servicio cloud.

La organización Cloud Security Alliance (CSA) en su *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, presenta agrupados en dos grandes categorías, uno estratégico o de gobierno y otro táctico u operacional, los dominios que considera críticos en la toma de decisión sobre la tecnología Cloud. [CLOUD SECURITY ALLIANCE. 2009].

Los puntos considerados por la CSA como estratégicos para el gobierno de IT de una organización, son:

a) Gobierno y gestión de riesgo de IT. La organización que evalúa la posibilidad de migrar sus servicios de IT a la tecnología Cloud, debe poder medir cual es el riesgo que asume por incapacidad operacional del cloud provider o por incumplimiento de los acuerdos contractuales, incapacidad para asegurar y proteger la confidencialidad de los datos de la organización, y la incapacidad propia de la organización para saber seleccionar al cloud provider adecuado, así como saber identificar las limitaciones legales y regulatorias aplicables.

   Cualquiera de estos aspectos inadecuadamente evaluado, puede poner en riesgo la continuidad de la organización.

b) Aspectos legales y regulatorios. Este un aspecto no menor a avaluar en la toma de la decisión de migrar a C*loud Computing*. No solo desde el punto de vista de las normas que regulan la actividad de la organización, en el caso de este trabajo el de las entidades financieras, sino también las de protección de datos personales, convenios internacionales, etc. Es importante saber en qué lugar geográfico se almacenarán los datos y las aplicaciones de la organización, dado que no siempre existen convenios bilaterales entre países que garanticen la confidencialidad de los datos así como la posibilidad de ser puestos a disposición en caso de procesos judiciales.

c) Auditoría y compliance. Otro de los temas críticos en el proceso de evaluación de migrar a la tecnología cloud, es considerar la posibilidad que el cloud provider pueda cumplir con las políticas de seguridad existentes en la organización, o si las mismas deben adecuarse y medir, en este caso, el impacto del cambio. Por otra parte existen también los riesgos propios de no poder contar con las evidencias necesarias ante auditorías internas y/o externas.

d) Gestión del ciclo de vida de la información. Un aspecto sensible de utilizar los servicios de *Cloud Computing*, tiene que ver con la protección de los datos almacenados en la infraestructura del cloud provider, no solo vinculado al acceso por parte de los usuarios autorizados, sino con las medidas necesarias para asegurar la no pérdida de los mismos, por fallas de hardware o software, y las medidas de protección para asegurar que en caso de pérdida de medios de soporte que contienen datos sensibles, estos no puedan ser utilizados.

e) Portabilidad e Interoperabilidad: la selección de un cloud provider puede significar una mala decisión, si debido a los incumplimientos en el servicio prestado, excesivo costo o desaparición del mismo, la organización no puede o le resulta complejo migrar a otro cloud provider.

   Por ello es importante conocer si el cloud provider seleccionado utiliza herramientas y productos estándares de mercado y si cuenta con interfaces de integración estándar (APIs).

Entre los puntos considerados por la CSA dentro de la categoría de tácticos u operacionales, se hallan:

a) Seguridad Informática, plan de continuidad de negocios y plan de recupero ante desastres. Las organizaciones que adopten la tecnología de *Cloud Computing*, requieren dedicar recursos profesionales capacitados en el permanente monitoreo de las condiciones de seguridad del cloud provider y su ajuste a las políticas de la organización y a las mejores prácticas.

   También deben validarse que los planes de recupero ante desastres del cloud provider estén actualizados, así como la realización y participación en las pruebas del plan de recuperación.

b) Operación del data center. Implica entender cómo están compartimentados los servicios brindados por el cloud provider (procesamiento, gestión de redes, soporte, seguridad) para poder identificar el grado de separación de funciones y controles.

   Desde el punto de vista de los recursos de hardware y software, es importante conocer si el cloud provider utiliza soluciones estándar de mercado, su grado de actualización tecnológica, si cuenta con soporte técnico de sus proveedores, y la calidad del mismo.

   Dado que una de las características de *Cloud Computing* es la utilización compartida de los recursos entre diferentes cloud consumers, es imprescindible conocer cuáles son los criterios de asignación y reasignación de los recursos, y los criterios aplicados al momento de compartir los recursos entre los cloud consumers.

c) Incidentes. Tratamiento, reporte y mitigación. El hecho que en *Cloud Computing* los recursos e infraestructura utilizados estén, por lo general, fuera de los límites físicos del cloud consumer, hacen que éste último deba prever los mecanismos para enterarse de los incidentes sufridos por el cloud provider y que puedan directa o indirectamente afectarle.

   Es importante que en el contrato que vincula al cloud consumer con el cloud provider, estén acordados los mecanismos de notificación de los incidentes, la posibilidad que el cloud provider pueda realizar un análisis forense de las circunstancias que lo originaron y las medidas de remediación que se tomaron para evitar que se vuelvan a producir.

d) Seguridad de las aplicaciones. Particularmente en el caso de la modalidad de servicio *Software as a Service* (SaaS), es importante que el cloud consumer analice la arquitectura de seguridad prevista en la aplicación, sobre todo considerando que estas aplicaciones son utilizadas en entornos web y accedidas desde Internet.

   Debe verificarse especialmente la administración de los perfiles de usuario, y del registro de logging que mantiene la aplicación a fin de poder realizar un adecuado seguimiento de la actividad de los usuarios.

   Si la modalidad de servicio es *Infraestructure as a Service* (IaaS) o *Platform as a Service* (PaaS), este análisis involucra las políticas de virtualización y la administración de las imágenes de los máquinas virtuales configuradas para cada cloud consumer.

e) Encriptación de datos y administración de claves. Esta es una medida de seguridad necesaria para proteger los datos sensibles ante cualquier pérdida casual o intencional, y que en el caso de la tecnología de *Cloud Computing*, adquiere mayor relevancia, ante la circunstancia de que los datos estén almacenados en una infraestructura que puede ser ajena a la organización propietaria de esos datos.

   Desde la óptica de los datos que se encriptan, es recomendable mantener claves distintas, según se trate de datos en uso o datos almacenados como resguardo.

   Desde la óptica de las claves de encriptación, es recomendable que las claves sean administradas por el cloud consumer, manteniendo de esta manera independencia de la operación que realiza el cloud provider con los datos. Es importante además un adecuado esquema de resguardo y recupero de las claves de encriptación.

f) Identificación de usuarios y control de acceso. Uno de los aspectos críticos y que implican mayores cambios en las organizaciones que adoptan *Cloud Computing*, tiene que ver con la gestión segura y oportuna de las claves de usuario, así como la fortaleza del sistema de gestión de claves de usuario, de manera que se ajuste a las políticas de seguridad del cloud consumer.

   Dependiendo del tipo de servicio adoptado por el cloud consumer, la gestión de cuentas de usuario y sus claves, varía desde la tarea de asignar los usuarios y

perfiles de acceso a una aplicación como es el caso en el *Software as a Service* (SaaS), hasta la definición y gestión de los esquemas de seguridad como es en el caso de la modalidad *Infraestructure as a Service* (IaaS).

En el caso de usuarios externos al cloud consumer, como podrían ser clientes o proveedores, es importante evaluar las fortalezas del esquema de autenticación y de gestión de sus identidades y contraseñas como usuarios, así como la seguridad en la conexión entre éstos y la aplicación, a fin de evitar el repudio de las transacciones que realicen usando la aplicación. Este tema está íntimamente ligado con el punto de seguridad en las aplicaciones y las políticas referidas a la gestión de contraseñas de usuario definidas por la organización (ej. Complejidad de la contraseña, cantidad mínima de caracteres exigible, historial de contraseñas, cantidad de intentos fallidos)

También es necesario, contar con un *log* o registro de auditoría que permita determinar la cantidad de veces un usuario accede, detalle de los intentos fallidos, bloqueos de la cuenta de usuario, cambios de contraseña, etc..

g) Virtualización: como se describió en el punto 4.9, la virtualización es una de las tecnologías puntales de *Cloud Computing*.

Desde el punto de vista de seguridad, al incorporar la virtualización el componente del *hypervisor*, agrega otro posible frente de ataque, sea para acceder desde una máquina virtual a otra, y de esa forma recuperar información sensible, o bien a un posible ataque de denegación de servicio.

Es por ello que el cloud consumer, debe evaluar los criterios aplicados por el cloud provider en la asignación de los entornos virtuales, de manera de determinar si se comparten en un mismo entorno físico máquinas virtuales productivas con otras de desarrollo o testing, la aplicación de análisis de tráfico de red entre máquinas virtuales, así como el establecimiento de políticas de seguridad mínima para todas las máquinas virtuales que se configuren.

5.3. PRINCIPALES AMANEZAS A LA SEGURIDAD.

Un reciente estudio publicado por la organización Cloud Security Alliance en febrero de 2013 [CLOUD SECURITY ALLIANCE. 2013], identifica cuales son las principales amenazas de seguridad que afectan a la tecnología de *Cloud Computing*. Este

trabajo recoge las conclusiones de este estudio, y presenta tales amenazas en orden decreciente del nivel de su gravedad:

a) Pérdida de confidencialidad de los datos. Para hacer frente a esta vulnerabilidad, se ha comenzado a utilizar con mayor frecuencia los mecanismos de cifrado de los datos. Esta solución trae aparejado un nuevo desafío para los cloud consumers, y es el de implementar políticas de administración de las claves, pues su pérdida inhabilita el acceso a los datos de una organización.

b) Pérdida de datos. La pérdida de datos se puede originar en debilidades del esquema de seguridad implementado por el cloud provider y/o el cloud consumer, por errores operativos, o siniestros que puedan destruir los dispositivos de almacenamiento.

   Los métodos de prevención más comunes para la pérdida de datos es mantener copias de seguridad en sitios alternativos. No obstante esta solución implica duplicar los esquemas de seguridad para proteger los datos productivos como las copias de respaldo.

c) Apropiación de usuarios y contraseñas. Una de las formas de realizar fraudes por medio de la utilización indebida de claves de usuario, es mediante el robo de contraseñas, o el uso de técnicas de phishing o la explotación de vulnerabilidades del software utilizado. En *Cloud Computing* estas posibilidades se ven incrementadas, por diferentes factores: recursos compartidos entre diferentes cloud consumers, vulnerabilidades de seguridad en la infraestructura y en las aplicaciones, debilidad en los controles efectuados por el cloud consumer, etc.

   Para hacer frente a este tipo de ataques, los cloud consumers deben implementar soluciones de autenticación doble (ej. Usuario y contraseña más el uso de un dispositivo físico (*token*) o tarjeta de coordenadas), o también mediante la utilización de sistemas on time password.

d) Application Program Interface (APIs) no segura. Los cloud consumers emplean interfaces provistas por los cloud providers para integrar las aplicaciones en la nube con otras desarrolladas internamente, y en algunos casos para autenticar sus usuarios internos y externos.

La vulnerabilidad en este caso, se origina en debilidades propias de la arquitectura de seguridad de los módulos de interfaces desarrollados por el cloud provider.

e) Ataques de denegación de servicio. Son ataques destinados a evitar que los usuarios puedan acceder a los servicios y/o aplicaciones disponibles en la nube. Las técnicas de denegación de servicio, consisten en generar un tráfico tal que sature la capacidad de procesamiento de los servidores, el "*bandwidth*" de una red o el espacio en disco disponible.

   Este tipo de ataques afectan la imagen de las organizaciones que brindan servicios a sus clientes mediante aplicaciones en la nube, debido al malestar que generan a los clientes la indisponibilidad y/o lentitud de los servicios utilizados.

f) Ataques internos. Una de las principales fuentes de ataques proviene de empleados, contratados y/o proveedores de una organización que tiene acceso a su red interna. Si bien este problema de seguridad es anterior al surgimiento de la tecnología de *Cloud Computing*, con esta última se potencia, debido a la infidelidad en la que pueden incurrir quienes prestan servicios para el cloud provider.

g) Abuso de los servicios cloud. Una de las características de la tecnología de *Cloud Computing* es la de poner a disposición de un cloud consumer una importante cantidad de recursos de tecnología, a la que quizás no tendría posibilidades por los niveles de inversión que se requieren.

   Si bien esto en sí mismo no es objetable y es esencia de un servicio cloud, se plantea una cuestión de mal el uso de los recursos que se ponen a disposición de un cloud consumer. Este último bien podría emplear tales recursos para realizar ataques de denegación de servicio que afecten a otros cloud consumers, o explotar debilidades en los esquemas de seguridad implementados por el cloud provider, para acceder a datos sensibles de otros cloud consumers.

h) Evaluación insuficiente de un cloud provider. Las bondades de la tecnología *Cloud Computing* (reducción de costos operativos y de inversión, disponibilidad de recursos *on demand*, actualización tecnológica, etc.) son un atractivo importante para que muchas organizaciones se inclinen por la adopción de esta tecnología.

Decidir en forma apresurada la adopción de esta tecnología, pone en situación de riesgo al cloud consumer, al no evaluar en profundidad todos los aspectos de seguridad involucrados, así como las condiciones contractuales en materia de responsabilidad asumidas por el cloud provider ante incumplimientos con el servicio comprometido, la forma de medición, y los aspectos legales y regulatorios involucrados.

i) Vulnerabilidad en compartir recursos. Una de las características salientes de la tecnología de *Cloud Computing*, consiste en que los recursos tecnológicos dispuestos por el cloud provider, puedan ser compartidos entre múltiples cloud consumers. Es aquí donde se presentan posibles vulnerabilidades, cuando la arquitectura de los componentes de infraestructura (IaaS), plataforma de despliegue de aplicaciones (PaaS) o aplicaciones (SaaS) no fueron adecuadamente diseñados para soportar a múltiples cloud consumers. Esta vulnerabilidad es de alto riesgo pues afecta a todos los cloud consumers que hacen uso de los recursos de ese cloud provider.

6. EL NEGOCIO BANCARIO Y LA TECNOLOGÍA INFORMÁTICA.

6.1. CARACTERÍSTICAS PRINCIPALES DE LA ACTIVIDAD.

La ley 21.526 de Entidades Financieras, define como "bancos" a las *"personas o entidades privadas o públicas –oficiales o mixtas- de la Nación, de las provincias o municipalidades que realicen intermediación habitual entre la oferta y la demanda de recursos financieros".* [LEL 21.526 LEY DE ENTIDADES FINANCIERAS. 1977].

El artículo 2do. de esta ley, cita las diferentes clases de entidades que están incluidas en la norma, entre las que se encuentran los *"bancos comerciales",* que están dentro del alcance del presente trabajo en lo referente a la utilización de la tecnología de *Cloud Computing*.

Las entidades financieras, debido al crecimiento del volumen y complejidad de las transacciones realizadas, su dispersión geográfica, el ofrecimiento de nuevos servicios y los múltiples canales de atención, han adoptado la tecnología informática como una forma de agilizar su operatoria, reducir costos operativos y competir por más y mejores servicios.

La tecnología informática les posibilita a las entidades y a sus clientes, disponer de información "*on line – real time*" sobre el movimiento de sus cuentas, y brindar una serie de servicios en forma electrónica que permite a los clientes operar en cualquier momento y desde cualquier ubicación. Así se desarrollaron servicios a través de nuevos canales como la banca telefónica, las redes de cajeros automáticos, los sistemas de banca electrónica por Internet para ser accedidos desde una PC de escritorio, notebook, tablet o smartphones. Los clientes, a través de estos medios pueden, además de consultar el saldo de sus cuentas, realizar transacciones como depósitos a plazo, transferencias entre cuentas, pagos, compras electrónicas con debito en cuenta o tarjeta, cambio de moneda, etc. A todo esto, debe agregarse el apoyo que brinda la informática a las tareas de back office de los bancos, la implementación de controles más sofisticados, y la detección de posibles fraudes.

Debido a la fuerte adopción de tecnología informática por los bancos, ésta pasó a ser un recurso clave y crítico en el funcionamiento de una entidad. Se puede afirmar, sin duda, que los datos y aplicaciones son un activo valioso para los bancos, y como

tal requieren de un especial resguardo y protección ante posibles pérdidas o accesos no autorizados.

Tal es la importancia que adquiere la tecnología informática en el ámbito bancario, que una falla grave en sus sistemas informáticos puede tener impacto negativo desde el punto de vista de reputación y hasta patrimonial en una entidad. De allí que el Banco Central de la República Argentina, como organismo de control, haya dictado normas específicas en materia de tecnología y seguridad informática.

6.2. MARCO LEGAL Y REGULATORIO.

6.2.1. NORMATIVA ACERCA DE CLOUD COMPUTING.

En Argentina, en materia de *Cloud Computing,* no existe normativa legal específica que regule la relación entre cloud provider y cloud consumer. No obstante, los especialistas en derecho informático reconocen que existen normas que se pueden aplicar en la contratación de los servicios de *Cloud Computing*, tales como las que surgen del Código Civil y de Comercio en materia contratos así como los principios generales de responsabilidad civil. [FAZZALARI, Raúl M. 2011].

Por otra parte, en el sector informático a nivel nacional e internacional se están desarrollando una serie de estándares y de buenas prácticas que adoptan los cloud providers. [FAZZALARI, Raúl M. 2011]. Algunas de esas instituciones que participan definiendo estándares sobre *Cloud Computing*, fueron citadas en este trabajo: National Institute of Standards and Technology (NIST), Cloud Security Alliance (CSA), entre otros.

Es importante involucrar, desde el inicio del proceso de análisis de contratación de servicios informáticos a la nube, además de las áreas de IT y seguridad Informática, a los especialistas en derecho para que participen en la redacción de las cláusulas contractuales que establecen las responsabilidades civiles y penales entre las partes.

El Dr. Raúl Martínez Fazzalari, abogado especialista en derecho de las telecomunicaciones y audiovisual [FAZZALARI, Raúl M. 2011], enumera los aspectos relevantes que deben estar consignados en un contrato de servicio de *Cloud Computing*:

a) La utilización de estándares abiertos de tecnología.

b) El uso de tecnologías que permitan la portabilidad de aplicaciones y datos de un cloud provider a otro.
c) La fijación de políticas de seguridad física (detección y extinción de incendios, servicio de energía ininterrumpida, refrigeración de las instalaciones, control de acceso de personas autorizadas, etc.) y lógica acordadas con el cliente, para proteger la confidencialidad, y evitar la adulteración y pérdida de datos.
d) La propiedad intelectual de los desarrollos que el cloud consumer realice utilizando los recursos de hardware y software del cloud provider.
e) La realización de auditorías periódicas por parte del cloud consumer, o las requeridas por sus entidades regulatorias de contralor.
f) La definición de los criterios de medición de la calidad del servicio brindado por el cloud provider, así como las penalidades en caso de cumplimiento.
g) El acceso a las herramientas de medición de utilización del servicio, a fin de control del costo en función del uso.
h) Establecer los mecanismos de notificación de cambios de gerenciamiento de parte del cloud provider.
i) Establecer los mecanismos de notificación por parte del cloud provider, de los incidentes que pongan en riesgo los datos y aplicaciones del cloud consumer.
j) Establecer los mecanismos de control de cambios en las condiciones establecidas en el contrato.
k) Establecer los términos y condiciones de finalización del contrato, que deberá incluir los procedimientos de destrucción de los datos almacenados en las instalaciones del cloud provider.
l) Establecer las causales y mecanismos de resolución del contrato en forma anticipada por falta de cumplimiento de alguna de las partes, incluyendo los plazos para el traslado de los servicios.

6.2.2. NORMATIVA APLICABLE A ENTIDADES FINANCIERAS.

LEY 21.526 DE ENTIDADES FINANCIERAS.

Las entidades financieras están específicamente reguladas por la ley 21.526 y sus modificatorias. Conforme al alcance de este trabajo, es importante hacer foco en los siguientes artículos:

a) Artículo 1. Define el ámbito de aplicación de la ley: *"Quedan comprendidas en esta Ley y en sus normas reglamentarias las personas o entidades privadas o públicas —oficiales o mixtas — de la Nación, de las provincias o municipalidades que realicen intermediación habitual entre la oferta y la demanda de recursos financieros.".* [LEY 21.526. 1977].

b) Artículo 2. Detalla las clases de entidades financieras que están dentro del alcance de la ley: "*Quedan expresamente comprendidas en las disposiciones de esta Ley las siguientes clases de entidades:*

a) Bancos comerciales;

b) Bancos de inversión;

c) Bancos hipotecarios;

d) Compañías financieras;

e) Sociedades de ahorro y préstamo para la vivienda u otros inmuebles;

f) Cajas de crédito.

La enumeración que precede no es excluyente de otras clases de entidades que, por realizar las actividades previstas en el artículo 1°, se encuentren comprendidas en esta ley.". [LEY 21.526. 1977].

c) Artículo 4. Define al BCRA como autoridad de aplicación de la ley, y la autoriza a emitir las normas reglamentarias para cumplir con su rol de entidad de contralor: *"El Banco Central de la República Argentina tendrá a su cargo la aplicación de la presente ley, con todas las facultades que ella y su Carta Orgánica le acuerdan. Dictará las normas reglamentarias que fueren menester para su cumplimiento, a cuyo efecto deberá establecer regulaciones y exigencias diferenciadas que ponderen la clase y naturaleza jurídica de las entidades, la cantidad y ubicación de sus casas, el volumen operativo y las características económicas y sociales de los sectores atendidos, dictando normas específicas para las cajas de crédito. Ejercerá también la fiscalización de las entidades en ella comprendidas.".* [LEY 21.526. 1977].

d) Artículo 39. Establece el principio legal básico, que obliga a las entidades a mantener la confidencialidad de los datos de sus clientes: "*Las entidades comprendidas en esta ley no podrán revelar las operaciones pasivas que realicen.*

Sólo se exceptúan de tal deber los informes que requieran:

a) Los jueces en causas judiciales, con los recaudos establecidos por las leyes respectivas;

b) El Banco Central de la República Argentina en ejercicio de sus funciones;

c) Los organismos recaudadores de impuestos nacionales, provinciales o municipales sobre la base de las siguientes condiciones:

— Debe referirse a un responsable determinado;

— Debe encontrarse en curso una verificación impositiva con respecto a ese responsable, y

— Debe haber sido requerido formal y previamente.

Respecto de los requerimientos de información que formule la Dirección General Impositiva, no serán de aplicación las dos primeras condiciones de este inciso.

d) Las propias entidades para casos especiales, previa autorización expresa del Banco Central de la República Argentina.

El personal de las entidades deberá guardar absoluta reserva de las informaciones que lleguen a su conocimiento." [LEY 21.526. 1977].

LEY 25.326 DE PROTECCIÓN DE DATOS PERSONALES (LPDP).

Las entidades financieras también están alcanzadas por la ley 25.326 de Protección de Datos Personales (LPDP). En particular hacemos hincapié en este trabajo en los siguientes artículos:

a) Artículo 2. Define los siguientes conceptos:

"— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

— Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o

procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

— Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

— Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

— Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

— Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

— Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable." [LEY 25.326. 2000].

Es importante señalar, que judicialmente no se consideran datos sensibles los referidos a la situación crediticia de las personas [PALAZZI, Pablo. 2004]. No obstante el artículo de 26 de la LPDP se ocupa de dar precisiones sobre este aspecto (ver ítem g).

b) Artículo 9. Referido a la seguridad de los datos, afirma que: "*El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o*

no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.", a la vez que prohíbe el registro de datos personales en archivos o registros *"que no reúnan las condiciones técnicas de integridad y seguridad".* [LEY 25.326. 2000].

Los aspectos de seguridad, se extienden más allá de los dispositivos técnicos y normativos implementados, debiendo llegar también a la formación e información adecuada del personal que trabaja con los datos [PALAZZI, Pablo. 2004]. Esta consideración debe tenerse en cuenta a la hora de evaluar los servicios provistos por un cloud provider.

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 los mismos, *"aún después de de finalizada su relación con el titular de los datos"* [LEY 25.326. 2000]. Solo releva de este secreto cuando hay a un requerimiento judicial o por razones "*seguridad pública, la defensa nacional o la salud pública".* [LEY 25.326. 2000].

d) Artículo 11. Establece las condiciones para la cesión de datos:

"*1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.*

2. El consentimiento para la cesión es revocable.

3. El consentimiento no es exigido cuando:

a) Así lo disponga una ley;

b) En los supuestos previstos en el artículo 5° inciso 2;

c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate." [LEY 25.326. 2000].

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. [PALAZZI, Pablo. 2004].

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, y que es responsable solidario con el cesionario del cumplimiento de la LPDP. [LEY 25.326. 2000].

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.
Sin embargo, el artículo 12 del decreto reglamentario de la LPDP, fija que la prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales no rige, cuando el titular de los datos hubiera consentido expresamente la cesión. [DECRETO 1558/2001. 2001].
El mismo artículo 12 del decreto 1550/2001, faculta a la Dirección Nacional de Protección de Datos Personales (DNPDP) a evaluar de oficio o a pedido de la parte interesada el nivel de protección de proporcionado por las normas de un Estado u Organismo Internacional. [DECRETO 1558/2001. 2001].
En este sentido hay que destacar que por decisión de la Comunidad Europea del 30 de Junio de 2003, y de acuerdo al a Directiva 95/46/CE del Parlamento

Europeo, la Argentina es considerada como país que garantiza un nivel adecuado de protección de datos personales, habilitando a los países de la Comunidad a transferir datos hacia Argentina. [C(2003)1731 final. 2003].

En sentido contrario, 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 evaluación por parte de la DNPDP. Existen múltiples dictámenes emitidos por la DNPDP respecto de este punto. [DNPDP N° 12/03. 2003]. [DNPDP N° 248/05. 2005]. [DNPDP N° 270/06. 2006]. [DNPDP N° 17/08. 2008]. [DNPDP N° 48/09. 2009]. [DNPDP N° 07/11. 2011]. [DNPDP N° 22/13. 2013]. [DNPDP N° 06/14. 2014]. [DNPDP N° 11/14. 2014].

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.

f) Artículo 25. Regula la prestación de servicios informatizados.

"1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.". [LEY 25.326. 2000].

Este artículo es claramente aplicable a las publics clouds en donde los clouds consumer hacen uso de la modalidad de software como servicio (software as a service). En estos casos hay un tercero que presta el servicio, el cloud provider, que tendrá acceso a los datos almacenados en archivos y/o base de datos. [PALAZZI, Pablo. 2004].

g) Artículo 26. Refiere a la prestación de servicios de información crediticia, y regula el tratamiento de los datos personales de carácter patrimonial. Impone tres tipos de limitaciones:
   I. Limitación al contenido de la información: "*datos personales de carácter patrimonial relativos a la solvencia económica y al crédito"*. [PALAZZI, Pablo. 2004].
   II. Limitación de las fuentes de las cuales provienen: pueden ser obtenidos de fuentes accesibles al público, o procedentes de información que fue expresamente autorizada por el titular con su consentimiento. [PALAZZI, Pablo. 2004].
   III. Limitación temporal según la antigüedad del dato: *"Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho".* [LEY 25.326. 2000].

COMUNICACIÓN A 4609 del BCRA.

El BCRA, también 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 Comunicación A 4609 [BCRA. Com. A 4609. 2006].

Es importante señalar que la Comunicación 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 aplicables, tales como:

a) Pone en cabeza del directorio de la entidad financiera, la responsabilidad de "*establecer y aprobar formalmente políticas basadas en un previo análisis de riesgos"*, para llevar el proceso de delegación de actividades *"vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas"*. Además, para que no quede duda alguna, aclara que la

delegación en un tercero de estas actividades "*nunca debe entenderse como transferencia de las responsabilidades primarias".*

b) La delegación de los servicios debe formalizase a través de contratos que "*definan claramente el alcance de los servicios, las responsabilidades y acuerdos sobre confidencialidad y no divulgación".*

c) El control de la gestión que sobre la protección de los activos de información realice el tercero proveedor del servicio, debe ser realizado por recursos propios de la entidad financiera.

d) Cláusulas mínimas que deben estar previstas en la redacción del contrato de delegación de actividades al tercero: "*alcance de las actividades; los niveles mínimos de prestación de servicios y su tipo; la participación de subcontratistas; los derechos a realizar auditorías por parte de la entidad; compromisos de confidencialidad; los mecanismos de resolución de disputas; la duración del contrato; cláusulas de terminación del contrato; los mecanismos de notificación de cambios en el control accionario y en los cambios de niveles gerenciales; el procedimiento por el cual la entidad pueda obtener los datos, los programas fuentes, los manuales y la documentación técnica de los sistemas, ante cualquier situación que pudiera sufrir el proveedor externo por la cual dejara de prestar sus servicios o de operar en el mercado*".

e) El contrato debe dejar claramente expresado la posibilidad que el BCRA pueda realizar auditorías en las instalaciones del proveedor y acceder a los datos y documentación técnica relacionada vinculada a la entidad financiera.

f) La responsabilidad del proveedor de aplicar las pautas mínimas establecida por la Com. A 4609 en lo referente a las actividades de IT delegadas por la entidad financiera.

g) La exigencia de que el proveedor que *"brinde servicios a múltiples organizaciones, ya sean entidades o de otro tipo de negocio",* evidencie una clara separación de actividades de manera que los datos y aplicaciones utilizados por una entidad financiera en particular, cuenten con un "*entorno de seguridad individual"* que pueda ser controlado y monitoreado por la propia entidad, exclusivamente.

h) La entidad que delegue actividades de IT a un tercero proveedor, debe contar con un plan de continuidad de negocios *"a los fines de no cesar con las actividades normales de la entidad financiera y asegurar la continuidad de los servicios ante cualquier situación que pudiera sufrir el proveedor externo por la cual dejara de prestar sus servicios".*

COMUNICACIÓN A 5374 del BCRA.

La Comunicación A 5374, fija una serie de requisitos de seguridad relacionados con los canales electrónicos utilizados por las entidades financieras para dar servicios a sus clientes. La norma establece "*procesos de referencia"* entre los que se destacan:

a) Control de Acceso: relacionado con el desarrollo e implementación de medidas de seguridad para proteger la identidad de los usuarios, mecanismos de autenticación, segregación de roles.
b) Integridad y Registro: destinado a controlar la integridad y registro de las transacciones realizadas sobre el canal electrónico, manejo de información sensible de los datos y tracking de toda la actividad realizada por el cliente en el canal electrónico.
c) Monitoreo y Control: proceso relacionado con la recolección y análisis de datos para detección de fallas, intentos de intrusión, indisponibilidad del servicio.
d) Gestión de Incidentes: proceso vinculado a la "*detección, evaluación, contención y respuesta"* ante un incidente de seguridad que se produzca sobre un canal electrónico.

6.3. CASOS RELEVADOS DEL MERCADO FINANCIERO.

En este punto se presenta el material obtenido de las entrevistas mantenidas con los ejecutivos de entidades financieras mencionados en el capítulo 2 – Enfoque Metodológico.

6.3.1. CASO BANCO CREDICOOP COOPERATIVO LIMITADO.

Banco Credicoop Cooperativo Limitado, es una entidad bancaria nacional, con 253 sucursales habilitadas y 1066 cajeros automáticos (ATM's) instalados. [BCRA. Información de Entidades. Junio 2013].

Al momento de realización de la entrevista (noviembre 2013), la entidad incluyó dentro de su plan estratégico de sistemas y tecnología, el análisis sobre el grado de madurez de la tecnología *Cloud Computing* con la finalidad de evaluar alternativas de migración de determinados servicios.

Evaluaron la posibilidad de llevar su correo electrónico corporativo a la tecnología Cloud bajo la modalidad de software as a service, ofrecida por uno de los providers conocidos del mercado. Si bien la opción Cloud resultaba muy conveniente desde el punto de vista económico, consideraron que aún no era el momento oportuno desde el punto de vista de madurez técnica para dar el salto hacia esta opción, por lo que implementaron la plataforma de email sobre infraestructura propia.

Dentro de los planes del área de IT, está en estudio la implementación de una private cloud, sobre la cual se instalarán ambientes de desarrollo y testing de aplicaciones. Se lo considera un paso en la evolución hacia el mundo Cloud.

No evalúan en el corto plazo, la migración a una Cloud pública de las aplicaciones core que dan soporte al negocio. Diferentes razones motivan esta decisión, entre ellas: aspectos de seguridad lógica y confidencialidad de los datos, el hecho de que los datos estén alojados en data centers cuya ubicación no se conoce con precisión, aspectos legales y normativos.
Otros de los aspectos que se tienen en cuenta en la decisión es el nivel de customización y de integración que tienen las aplicaciones utilizadas por la entidad, lo que dificultaría el proceso de migración a la nube. Por las mismas razones de complejidad y de integración, no consideran la migración a la nube, del ambiente de recovery.

6.3.2. CASO ICBC – INDUSTRIAL AND COMMERCIAL BANK OF CHINA.

El Industrial and Commercial Bank of China (ICBC), es una entidad internacional, que cuenta con 104 sucursales habilitadas y 812 cajeros automáticos (ATM's) instalados. [BCRA. Información de Entidades. Junio 2013].

El Banco ICBC, ha evaluado soluciones en la nube dentro de la cual se analiza la posibilidad de migrar su correo electrónico corporativo bajo la modalidad de software as a service. Uno de los puntos de implementación sobre el cual han puesto especial

foco, es la seguridad de los datos y especialmente aquellos que serán afectados ante la eventual integración de sus servicios de Active Directory (servicio de directorio para administrar las cuentas de usuario) con la solución de correo implementada en la nube.

También ha llevado adelante un proyecto de virtualización de escritorio (Desktop as a Service) que está en proceso de implementación sobre una private cloud. Esta implementación no solo tiene el objetivo de reducir el TCO (Total Cost of Ownership), sino que además es una solución que posibilita en casos de contingencia de alguno de los edificios principales de la entidad, que los empleados puedan seguir trabajando desde otra locación.

También utilizan en la modalidad de software as a service, una solución para el filtrado de mail spam proveniente desde Internet.

Respecto de las aplicaciones core del negocio, no está previsto llevarlo a un entorno Cloud. Actualmente esos servicios están bajo la modalidad de outsourcing, dónde el Banco fija las políticas, administra la seguridad lógica, y la gestión de las cuentas de usuarios. Por otra parte, el equipamiento informático utilizado por el Banco y sobre el cual están instaladas las aplicaciones de negocio, es de su uso exclusivo, es decir no está compartido. También gestiona sus propios respaldos de datos (back-ups) y la guarda de los mismos.

Tampoco consideran viable llevar a la nube el centro de recupero de datos, dado que le caben las mismas consideraciones que para el entorno de producción.
Sí han implementado en la modalidad de software as a service, algunos sitios web no transaccionales y que ofrecen solo información estática de bajo riesgo. Si bien no son aplicaciones que administren datos sensibles del negocio, desde el área de Seguridad Informática de la entidad, se hacen periódicamente chequeos de seguridad para evitar posibles vulnerabilidades y la eventual afectación de la marca. Cabe mencionar que, todo servicio que se terceriza o se lleva al esquema de servicio en la nube, exigió de controles específicos para asegurar su correcta funcionalidad y el cumplimiento de las regulaciones vigentes, incurriéndose por esta razón en costos adicionales.

6.3.3. CASO COELSA – CÁMARA COMPENSADORA ELECTRÓNICA S.A.

La Cámara Compensadora Electrónica - COELSA, es una entidad conformada por los bancos y que está regulada por el BCRA a través las comunicaciones A 2557 y A 2575 que establecen sus formas de operar y requisitos mínimos que deben cumplir desde el punto de vista de tecnología informática.

A diferencia de los bancos, el principal riesgo que debe mitigar es el informático o sistémico, dado que, de la Cámara Compensadora depende el sistema electrónico nacional de pagos entre las entidades, el que debe realizarse dentro de la ventana horaria dispuesta por el Banco Central. Por ende, cualquier falla en sus sistemas informáticos pone en riesgo la compensación de valores de todo el sistema financiero. Es por esta particularidad que se puede afirmar que core del negocio de COELSA pasa por sus sistemas informáticos, y su principal objetivo desde el punto de vista de IT, es asegurar la continuidad de los servicios.

Respecto de la tecnología de *Cloud Computing*, la han analizado pero no la adoptaron, en particular en el modelo de cloud pública. Entre los motivos que influyeron en la decisión, se encuentran razones de índole regulatorias y por considerar que aún no se ha alcanzado la madurez tecnológica adecuada requerida por la actividad. Sí han considerado la implementación de una cloud privada.

A la fecha de este estudio, COELSA tiene sus aplicaciones transaccionales bajo el esquema de outsourcing, y en cuanto al equipamiento informático central (servidores y almacenamiento) está bajo la modalidad de “collocation” o “housing”, es decir alquilan espacio en un data center de los existentes en el mercado local. Este mismo modelo aplica tanto para el ambiente de producción como para el de recovery.

La fijación de las políticas de seguridad y su control está dentro del ámbito de la entidad COELSA.

Otro de los servicios que COELSA tiene tercerizado, es el reservorio de imágenes digitales de los documentos que compensa.

No han considerado llevar a la nube pública, en la modalidad de software como servicio, las aplicaciones de oficina, el correo electrónico, y las aplicaciones core. Si bien se reconocen las ventajas de optimización de costos de dicho modelo, el hecho

de que existan regulaciones y controles específicos del BCRA, así como la obligación de tener que garantizar la continuidad de servicio hacen que la decisión de migrar a esta plataforma no sea viable.

6.3.4. CASO BST – BANCO DE SERVICIOS Y TRANSACCIONES S.A.

Banco de Servicios y Transacciones S.A. (BST), es una entidad bancaria nacional, con 30 sucursales habilitadas y 8 cajeros automáticos (ATM's) instalados. [BCRA. Información de Entidades. Junio 2013].

El Banco BST, ha evaluado soluciones en la nube, en particular bajo el modelo de "software as a service", para aquellas aplicaciones que considera no críticas para el negocio, y que no representan un riesgo para la confidencialidad de los datos de sus clientes, y en la medida que los costos lo justifiquen. Un ejemplo de este tipo de servicios, es la utilización de software para normalización de domicilios y teléfonos.

Uno de los principales factores que influyeron en la decisión de no adoptar la tecnología de *Cloud Computing*, y sobre todo en la modalidad de implementación de "public cloud", está vinculado al marco regulatorio que rige la actividad. También influye en la decisión, la necesidad de garantizar la disponibilidad de los servicios de sistemas. Este es punto considerado crítico por el tipo de negocios que desarrolla la entidad, que requiere que los sistemas esté disponibles para los usuarios los siete días de la semana en la ventana horaria de 08:00 a 22:00.

Respecto de las aplicaciones core del negocio, no está previsto llevarlo a un entorno Cloud. Actualmente esos servicios están bajo la modalidad de outsourcing, pero con la particularidad de que utilizan particiones virtuales de servidores con distintas arquitecturas de hardware, que pueden a su vez, estar alojando otras particiones virtuales que no necesariamente son del Banco. Es decir que el equipamiento no es de uso exclusivo de la entidad. Esto les permite optimizar costos dado que solo pagan por los recursos que utilizan, y además les posibilita ajustar la capacidad de procesamiento de acuerdo a las necesidades del negocio, mediante la modalidad "on demand". Las políticas de seguridad sobre los entornos virtuales utilizados por el banco, son fijadas y controladas por la propia entidad

El ambiente de recovery es propio de la entidad.

No consideran por el momento migrar a la nube aplicaciones de mail y aplicaciones de oficina.

El desarrollo de las aplicaciones críticas se hace fuera de la entidad. No obstante, el testing de las mismas se realiza dentro del ámbito cuya seguridad es administrada por el banco, en razón de la confidencialidad de los datos que se utilizan.

6.3.5. CASO BANCO SUPERVIELLE S.A.

Banco Supervielle S.A., es una entidad bancaria nacional, con 184 entre sucursales y centros de pago habilitados, y 570 cajeros automáticos (ATM's) instalados. [BCRA. Información de Entidades. Junio 2013].

El Banco Supervielle, ha considerado la adopción de la tecnología *Cloud Computing*, para algunas aplicaciones que no forman parte del core business del negocio. Una de las aplicaciones que están analizando migrar a un esquema de nube pública en la modalidad de software as a service, es el correo electrónico corporativo. Entre los aspectos más sensibles se halla el de la seguridad de los datos, la posible necesidad de tener que integrar de los servicios de Active Directory (servicio de directorio para administrar las cuentas de usuario) con la solución de correo implementada en la nube, así como el tiempo de respuesta al usuario, sobre todo a los que están ubicados en las sucursales, debido a que el acceso a Internet es a través del sitio central, lo que agrega más saltos hasta llegar al servidor de destino.

También analizaron utilizar, bajo la modalidad de software as a service en una cloud pública, la red social privada Yammer destinada a que los empleados puedan compartir información personal o grupal.

Los sistemas transaccionales y los que soportan la actividad del negocio, están bajo la modalidad "on premise". El entorno productivo es propio y el ambiente de recovery está bajo la modalidad de outsourcing, pero con políticas de seguridad y de gestión definidas por la entidad. No está en los planes migrar a la tecnología de *Cloud Computing* esta infraestructura por razones de confidencialidad de los datos y transacciones de los clientes, así como por cuestiones de índole normativo y regulatorio.

Entre los principales desafíos considerados al momento de decidir adoptar la tecnología cloud, y sobre todo en la modalidad de cloud pública, se encuentran los aspectos de seguridad en el acceso a los datos, calidad del servicio en el transporte de datos a través de Internet, y la portabilidad del servicio cuando se decide discontinuar la relación con el proveedor.

Por razones similares a las señaladas en los párrafos previos, tampoco consideran viable llevar a la nube los ambientes de desarrollo y testing.

Tampoco consideran viable llevar a la nube el centro de recupero de datos, dado que le aplican las mismas consideraciones que para el entorno de producción. Han implementado en la modalidad de software as a service, ciertos sitios web no transaccionales y que ofrecen solo información estática de bajo riesgo. Si bien no son aplicaciones que administren datos sensibles del negocio, desde el área de Seguridad Informática de la entidad, se hacen periódicamente chequeos para evitar posibles vulnerabilidades. Cabe mencionar que, todo servicio que se terceriza o se lleva al esquema de servicio en la nube, exigió de controles específicos para asegurar su correcta funcionalidad y el cumplimiento de las regulaciones vigentes, incurriéndose por esta razón en costos adicionales.

Por último, han realizado pruebas de virtualización de los desktops pero dentro de un esquema “on premise”, al igual que la virtualización de los módulos core de la solución de telefonía IP que tiene implementada la entidad.

6.3.6. CASO BANCO SANTANDER S.A.

Banco Santander Rio S.A., es una entidad bancaria internacional, con 312 sucursales habilitadas, y 2070 cajeros automáticos (ATM’s) instalados. [BCRA. Información de Entidades. Junio 2013].

La entidad ha analizado y está en consideración el uso de *Cloud Computing* pero de manera restringida. Uno de los factores más importantes que influyen en la decisión es la elasticidad en la planificación de los recursos informáticos, como también la oportunidad y bajo riesgo que se asume en algunos temas.

Entre las modalidades de implementación considerada como más adecuada para el ámbito bancario, es el esquema de private cloud. No obstante el entrevistado

considera que el modelo “on premise” no es factible remplazarlo totalmente en la actual coyuntura, “principalmente por temas de negocio, de legislación y confidencialidad” de los datos.

Entre las razones que motivan a adoptar *Cloud Computing*, destaca la posibilidad que brinda esta tecnología, “para el armado rápido de ambientes previos en general y para proyectos con metodología ágil en particular”, para una rápida adecuación a las necesidades del negocio.

Respecto de los desafíos y/o limitaciones que demoran la decisión de migrar las aplicaciones a la nube, y sobre todo en un esquema de nube pública, el entrevistado considera que hay que poner énfasis en los aspectos vinculados a la seguridad física, y lógica (acceso y confidencialidad de los datos), a los aspectos legales y regulatorios, a las auditorias y externas, y la calidad del servicio de transporte de datos sobre Internet.

En cuanto a las aplicaciones que llevaría a la nube en la modalidad de software as a service, no considera a aquellas que son críticas para el negocio. Sí “algunos aplicativos como Gestión de Proveedores, siempre y cuando no manejen datos sensibles de la empresa o el tercero. De ninguna manera aplicaciones que tengan información de RRHH.”

Bajo la forma de Platform as Service, considera posible la utilización de ambientes de desarrollo, testing y quality assurance (QA), pero haciendo “especial hincapié en que los datos deben pasar previamente por un proceso de enmascaramiento lo suficientemente robusto para asegurar la confidencialidad de los mismos”.

6.3.7. CASO BBVA – BANCO FRANCÉS S.A.

BBVA Banco Francés S.A., es una entidad bancaria internacional, con 244 sucursales habilitadas, y 1395 cajeros automáticos (ATM’s) instalados. [BCRA. Información de Entidades. Junio 2013].

La entidad tiene como estrategia corporativa la adopción de la tecnología de *Cloud Computing* para toda la organización, con diferentes alcances. Como un primer paso dentro esa estrategia, se realizó la migración a las herramientas de comunicación y colaboración de Google Apps, bajo a la modalidad de Software as a Service. Este

proceso alcanzó a la filial de Argentina y otras de Latinoamérica. El objetivo de esta migración es potenciar la gestión colaborativa a nivel corporativo. Dentro del alcance de esta migración se encuentran:

a) mail corporativo;
b) gestión interactiva de documentos, planillas de cálculo y presentaciones, sin necesidad de contar con software de oficina instalado en el puesto de trabajo. Esto facilita el compartir los archivos y tener colaboración a distancia en la creación y edición de documentos que se tengan que hacer en conjunto.
c) High Performance Desktop (HPD), la intranet corporativa basada en *Cloud Computing*, con Google como partner. Desde la intranet, los usuarios acceden a las aplicaciones disponibles en la nube o a las que están instaladas en la filial de cada país.
d) La gestión de los usuarios que acceden a las aplicaciones que están en la nube pública, está centralizado a nivel corporativo, en la casa matriz de la entidad.

Asimismo, dentro de la estrategia de adopción de la tecnología de *Cloud Computing*, la entidad ha construido en España, país de su casa matriz, un data center certificado como Tier IV, uno de los pilares para el armado de una private cloud en donde estarían instaladas las principales aplicaciones que dan soporte al core business de las filiales. Actualmente, la entidad a nivel corporativo, tiene implementada una private cloud en donde se encuentran las aplicaciones críticas de negocio, siendo sus cloud consumers filiales ubicadas en Latinoamérica, entre las que no se encuentra la de Argentina, por temas regulatorios.

Entre los factores más importantes que influyeron en la decisión de la organización de adoptar la tecnología de *Cloud Computing*, además de las ya conocidas como: economía de escala y simplificación de la estructura entre otras, se encuentra la de integración a nivel corporativo como el objetivo de alcanzar una plataforma colaborativa a nivel de todas las filiales que conforman el grupo BBVA.

Entre las modalidades de implementación consideradas, se trataría de una hybrid cloud, dado que se integrarían servicios y aplicaciones de public cloud, con otras

aplicaciones, que por razones de confidencialidad de los datos o motivos regulatorios, están sobre la private cloud o en ambientes on premise de la entidad.

En el caso particular de la filial Argentina, el ambiente productivo de las aplicaciones que dan soporte al core business, están instaladas en un ambiente on premise, y su site de recovery está en modalidad outsourcing, principalmente por motivos regulatorios.

En cuanto a otras aplicaciones no críticas para el negocio, está en análisis migrar a la nube, en la modalidad de software as a service, el sistema de gestión de Recursos Humanos. En cuanto al sistema de gestión de compras utilizado por la filial Argentina, es corporativo y está instalado en la casa matriz. Desde el punto de vista corporativo, existe como estrategia el desarrollo de una private cloud para dar servicios a todas las filiales de la entidad.

Los servicios de comunicación de voz, está entre las posibles migraciones a la modalidad cloud.

Otro paso importante en dirección hacia la adopción de esta tecnología, son los avances hechos en materia de virtualización de puestos y servers encarados por la organización. A la fecha de este trabajo, la filial argentina ha virtualizado los puestos de trabajo de sus usuarios.

Bajo la modalidad de Platform as Service, actualmente no tienen implementaciones. Asimismo no está en consideración migrar bajo esta modalidad, los ambientes de desarrollo, testing y quality assurance (QA) vinculados a las aplicaciones críticas de negocio.

6.3.8. CUADRO COMPARATIVO DE LAS ENTIDADES RELEVADAS.

A continuación se presenta un cuadro comparativo, con los resultados de la encuesta realizada.

Por una cuestión de espacio y de visualización, el cuadro se divide en dos partes.

Cuadro resumen del relevamiento de entidades – Parte 1

	Credicoop	**ICBC**	**COELSA**
Evaluaron o evalúan adoptar Cloud Computing	Si. Para aplicaciones no core como el mail.	Si. Para el servicio de mail y escritorio de usuarios.	Si.
Consideran totalmente remplazable el modelo on-premise	No. Mantendrían las aplicaciones core.	No. Mantendrían las aplicaciones core.	No.
Motivos de adopción de Cloud Computing	Económicos.	Económicos y tecnológicos.	Económicos.
Motivos que consideran limitantes para adoptar Cloud Computing	Seguridad y normativos.	Seguridad y normativos.	Normativos.
Modalidad de implementación que adoptaría	Private.	Private.	Private.
Que servicio adoptaría o adoptó como SaaS.	No tiene. Evaluaron migrar el servicio de mail corporativo.	Evaluaron migrar el servicio de mail. Migraron el servicio de filtrado de mails externos y páginas web institucionales publicadas en Internet.	No tiene.
Cloud Computing como PaaS	No tiene.	No tiene.	No tiene.

Cuadro resumen del relevamiento de entidades – Parte 2

	BST	Supervielle	Santander	BBVA
Evaluaron o evalúan adoptar Cloud Computing	Si, en modalidad SaaS para aplicaciones no críticas.	Si, para algunas aplicaciones no core como el mail.	Si, pero de manera restringida.	Sí, a nivel corporativo y con diferentes alcances.
Consideran totalmente remplazable el modelo on-premise	No, para las aplicaciones core.	No, para las aplicaciones core del negocio.	No, por razones de negocio, confidencialidad de los datos, y marco regulatorio.	A nivel corporativo tienen proyectado la construcción de una private cloud para dar servicio a todas las filiales de Latinoamérica.
Motivos de adopción de Cloud Computing	Económicos.	Económicos y tecnológicos.	Elasticidad en la planificación y uso de recursos de IT, costos, oportunidad y bajo riesgo en algunos aspectos.	Economía de escala, simplificación de estructura e integración a nivel de corporación.
Motivos que consideran limitantes para adoptar Cloud Computing	Regulatorios.	Seguridad de los datos, velocidad de acceso, portabilidad y regulatorios.	Seguridad física y lógica de los datos, aspectos regulatorios, y de auditoria interna y externa, y calidad de servicio en Internet.	Regulatorios y seguridad.
Modalidad de implementación que adoptaría	SaaS para aplicaciones no críticas.	SaaS para aplicaciones no críticas.	Private.	Híbrida, dado que las aplicaciones core estarían en una private cloud y otras no críticas en una public cloud.
Que servicio adoptaría o adoptó como SaaS.	Normalización de datos de clientes.	Mail corporativo y aplicaciones de redes sociales privadas.	CRM, gestión de Recursos Humanos y Compras.	Tienen implementado, herramientas de productividad, oficina y colaboración.
Cloud Computing como PaaS	No tiene.	No tiene.	Lo utilizaría para ambientes de desarrollo, y testing.	No tiene.

7. CLOUD COMPUTING Y LOS BANCOS PRIVADOS DEL MERCADO ARGENTINO.

7.1. ESTADO ACTUAL Y POSIBILIDADES DE ADOPTAR CLOUD COMPUTING.

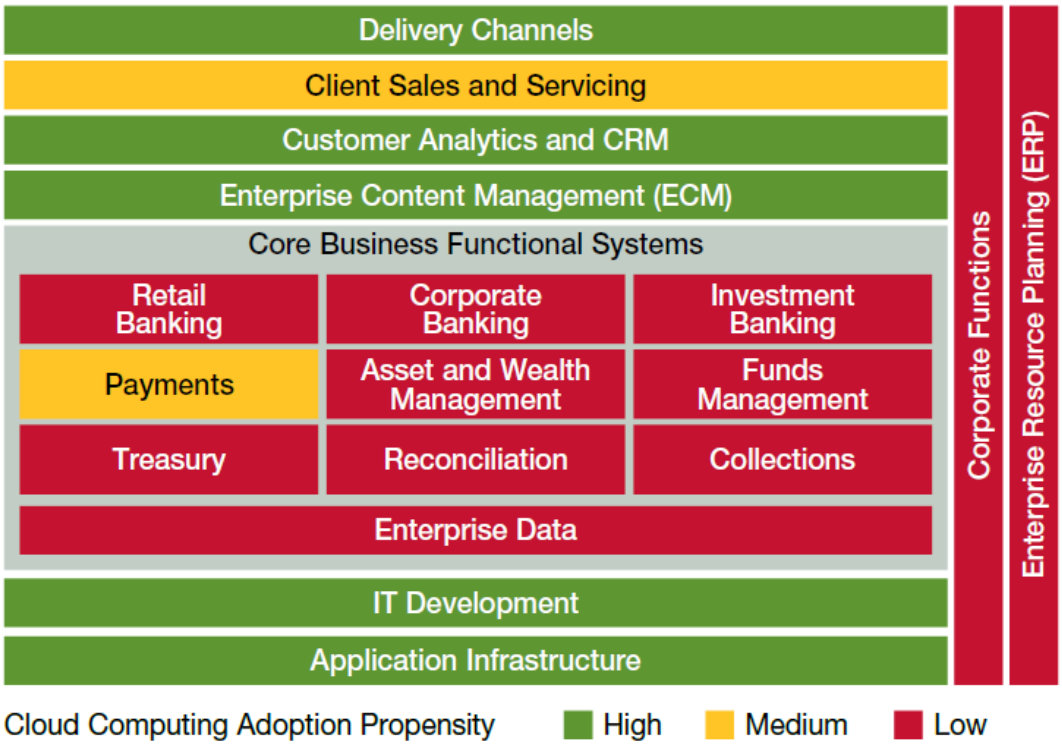
A partir de los datos obtenidos en el relevamiento de campo realizado en las entidades citadas en el punto 6.3. se comprueba principalmente que:

a) La tecnología de Cloud Computing no es ajena a las entidades financieras, pues todas, en mayor o menor medida, han iniciado el proceso de evaluación para su adopción, y en ciertos casos hasta han migrado algunas de sus aplicaciones.
b) La mayoría reconoce en Cloud Computing una forma de reducir los niveles de inversión y los gastos operativos de la infraestructura de IT.
c) Las entidades no han dado pasos concretos en migrar a ambientes cloud sus aplicaciones críticas de negocio, tanto de producción como recovery.
d) Hay avances en aprovechar la tecnología cloud para migrar aplicaciones de oficina, en particular el servicio de correo corporativo, donde hay casos concretos de migraciones exitosas (ej. caso BBVA).
e) Algunas entidades están dando pasos en migrar a ambiente cloud el desktop de trabajo de los usuarios (caso BBVA) y otras están en proceso de evaluación. En algunos casos, como paso previo, prevén virtualizar los puestos de trabajo de los usuarios en ambientes “on premise”.
e) Comparten la visión de que *Cloud Computing,* es una tecnología aún no madura para el mercado.
f) Los aspectos de seguridad de la información y regulatorios, siguen siendo uno de los principales issues que tiene la tecnología *Cloud Computing,* para las entidades financieras.

Asimismo, los resultados obtenidos en el relevamiento, se encuadran con lo manifestado por la consultora CapGemini en su informe [SRIRAM, Sudhir. 2011], cuando se refiere a la propensión de los bancos a adoptar Cloud Computing, dependiendo de la criticidad de las aplicaciones. En el gráfico siguiente se puede visualizar cuales de las áreas son las más adecuadas para migrar a *Cloud Computing.* Así por ejemplo de observa que las aplicaciones vinculadas al core business de los bancos son las menos candidatas a ser migradas a la nube. En

contraposición, las herramientas colaborativas y de CRM, entre otras, son las primeras en ser migradas en la modalidad de Software as a Service

Figura 7.1 – Aplicaciones que según la criticidad son mas viables de migrar a Cloud Computing por los bancos. [SRIRAM, Sudhir. 2011]



7.2. CLOUD COMPUTING Y SU FUTURO EN EL MERCADO FINANCIERO ARGENTINO.

Las nuevas tecnologías requieren de un proceso de maduración antes de que sean adoptadas en forma masiva, y más aún si son disruptivas, como es el caso de *Cloud Computing*.

Es cierto que existen issues en materia de seguridad, citados en el capítulo 5, que hacen más compleja la decisión de las entidades financieras de ir hacia esta tecnología, pero también lo es el hecho que aporta soluciones a una serie de necesidades que tienen las entidades como renovarse tecnológicamente, mantener un nivel capacidad acorde al movimiento del mercado, y todo esto, siendo cada vez más eficientes en las inversiones y costos de operar su infraestructura de IT.

En opinión del autor de este trabajo, la adopción de la tecnología *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: casi todas las entidades relevadas, han evaluado, y en algunos casos adoptado, 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 para relacionamiento con los clientes, como podría ser el caso de SalesForce.

   Consideramos que este es 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, la consideramos 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: Otra opción que consideramos viable, es el desarrollo de una community cloud por aquellas entidades nacionales, que pueden conseguir ventajas de una economía de escala en razón de su tamaño y volumen de operación, y en razón de que deben aplicar 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 escenarios 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: de las entidades relevadas, surge también que son reacias a confiar los datos sensibles de sus clientes en una public cloud. Esto se debe, entre otros motivos, a la limitación impuesta por la ley de Protección de Datos Personales respecto de la ubicación física de los datos, es particular fuera de los límites del país, y al impacto que desde el punto de vista de reputación puede provocar en un banco, cualquier violación de los aspectos de la seguridad sobre los datos de sus clientes (confidencialidad, integridad, disponibilidad, etc.).

   En base a esto es que es posible que los entidades privadas mas grandes que operan en el mercado argentino, y en particular las que tienen filiales en otros países de la región, vean como una solución viable la implementación de una private cloud, para soportar la operación de todas las filiales, manteniendo de esta forma el control directo de los aspectos sensibles de seguridad, y a la vez obtener las ventajas del modelo Cloud.

Otro aspecto importante esta vinculado con las normas que regulan la actividad financiera. Si bien no hemos hallado regulación específica sobre la prestación de servicios de *Cloud Computing,* sí las hay en materia de protección de datos

personales y de secreto bancario respecto de las operaciones pasivas que realicen los clientes con los bancos.

En este punto en particular, nos encontramos con dos grandes limitaciones para la adopción de los servicios de una public cloud bajo la modalidad de software as a service: por un lado los principales cloud providers son empresas de origen estadounidense (Amazon, Google, Microsoft, entre otras) cuyos data centers están, ubicados en Estados Unidos, país que para la legislación argentina no ofrece un nivel adecuado de protección de los datos personales. A esto se agrega que los bancos están obligados por la Ley de Entidades Financieras, a mantener absoluta reserva de las transacciones realizadas por sus clientes (Art. 39. Ley 21526).

Una alternativa de solución para esta limitación, es que los clouds providers desarrollen publics clouds dentro del ámbito geográfico de la Argentina para que las entidades no incumplan con la citada ley.

8. CONCLUSIÓN.

En el desarrollo de este trabajo se han descripto las principales características de la tecnología *Cloud Computing,* sus modalidades de implementación y de servicio. Asimismo se identificaron los motivos que impulsan a su adopción, así como los principales issues en materia de seguridad, legales y regulatorias.

En lo que a entidades financieras se refiere, se han presentado las principales normas que regulan la actividad y un relevamiento de entidades financieras de diferente magnitud, y la actitud de las mismas frente a esta tecnología.

Es indudable que la tecnología de Cloud Computing tiene aportes importantes desde el punto de vista de optimización de costos y de actualización tecnológica. 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 los 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.

En opinión del autor de este trabajo, las entidades en mayor o menor medida optarán por migrar ciertos servicios a la nube, siguiendo alguna de las estrategias señaladas en el punto 7.2, pero difícilmente opten por migrar a una public cloud sus aplicaciones críticas, considerando que los principales cloud providers ofrecen sus servicios en data center ubicados en Estados Unidos, país que según la regulación argentina no ofrece condiciones adecuadas de protección de los datos personales tal como surge de varios dictámenes emitidos por la DNPDP.

Optar por este último camino expondría a las entidades a tener que recurrir al consentimiento del titular de los datos para que lo autorice a llevarlos a un país que no ofrece adecuada protección según la legislación argentina, lo cual es prácticamente imposible de implementar, o incumplir con el marco regulatorio, constituyéndose solidariamente responsables ante la pérdida de confidencialidad de los datos de sus clientes, además del riesgo operacional.

Por otra parte difícilmente el BCRA, vea con agrado la decisión de concentrar en procos cloud providers, la gestión de los sistemas informáticos de los bancos, no

solo por el riesgo sistémico que conlleva, sino también por el impacto que tendría en la reducción del personal de IT del mercado local que hoy se desempeña en las entidades.

9. REFERENCIAS BIBLIOGRAFICAS.

- **ACCENTURE.** *A new era in banking. Cloud Computing changes the game.* Publication [en línea]. 2012. [consulta 4 oct. 2013]. <http://www.accenture.com/us-en/Pages/insight-new-era-banking-cloud-computing.aspx>
- **BADGER, Lee. GRANCE, Tim. PATT-CORNER, Robert. VOAS, Jeff.** *NIST Cloud Computing Synopsis and Recommendations.* National Institute of Standards and Technology. Especial publication. 800-146 [en línea]. 2012. [consulta 09 sep. 2013].< http://www.nist.gov/itl/cloud/index.cfm >
- **BCRA**. Com. A 2699. Banco Central de la República Argentina. Circular CAMCO 1-104 [en línea]. 1998. [consulta 15 Sep. 2013]. < http://www.bcra.gov.ar/ >.
- **BCRA**. Com. A 4609. Banco Central de la República Argentina. Circular RUNOR 1-805 [en línea]. 2006. [consulta 15 Sep. 2013]. < http://www.bcra.gov.ar/ >.
- **BCRA**. Información de Entidades. Tipo de Entidades. Bancarias y Financieras. [en línea]. Junio 2013. [consulta nov. 2013]. < http://www.bcra.gov.ar/
- **BCRA**. Información de Entidades. Grupo de Entidades. 10 Primeros bancos privados. Nómina de Entidades. [en línea]. Abril 2014. [consulta 29 Sep. 2014]. < http://www.bcra.gov.ar/
- **BRADLEY, Joseph. MACAULAY, James. NORONHA, Andy y SETHI, Hiten**. *The Impact of Cloud on IT Consumption Models. Study Report. CISCO-Intel* [en línea]. 2013. [consulta 15 ago. 2013]. < http://www.cisco.com/ >
- **C(2003)1731 final**. *DECISION DE LA COMISION de 30/06/2003.* [en línea]. 2003. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/media/33379/DecisionUE.pdf>
- **CLOUD SECURITY ALLIANCE**. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1* [en línea]. 2009. [consulta 07 sep. 2013]. < HTTP://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf >
- **CLOUD SECURITY ALLIANCE**. *The Notorious Nine. Cloud Computing Top Threats in 2013.* [en línea]. Febrero 2013. [consulta 07 sep. 2013] < http://www.cloudsecurityalliance.org/topthreats >
- **DECRETO 1558/2001.** *Protección de los Datos Personales.* [en línea]. 2001. [consulta 05 oct. 2013]. < http://www.jus.gob.ar/datos-personales.aspx >

- **DNPDP N° 12/03.** *DICTAMEN DNPDP N° 12/03.* [en línea]. 2003. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/datos-personales.aspx >
- **DNPDP N° 248/05.** *DICTAMEN DNPDP N° 248/05.* [en línea]. 2005. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/datos-personales.aspx >
- **DNPDP N° 270/06.** *DICTAMEN DNPDP N° 270/06.* [en línea]. 2006. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/datos-personales.aspx >
- **DNPDP N° 17/08.** *DICTAMEN DNPDP N° 17/08.* [en línea]. 2008. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/datos-personales.aspx >
- **DNPDP N° 48/09.** *DICTAMEN DNPDP N° 48/09.* [en línea]. 2009. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/datos-personales.aspx >
- **DNPDP N° 07/11.** *DICTAMEN DNPDP N° 07/11.* [en línea]. 2011. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/datos-personales.aspx >
- **DNPDP N° 22/13.** *DICTAMEN DNPDP N° 22/13.* [en línea]. 2013. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/datos-personales.aspx >
- **DNPDP N° 06/14.** *DICTAMEN DNPDP N° 06/14.* [en línea]. 2014. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/datos-personales.aspx >
- **DNPDP N° 11/14.** *DICTAMEN DNPDP N° 11/14.* [en línea]. 2014. [consulta 09 oct. 2014]. < http://www.jus.gob.ar/datos-personales.aspx >
- **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.
- **GARTNER**, Inc. *Hype Cycle for Emerging Technologies, 2012.* Industry Research. G00233931.
- **GARTNER,** Inc. *Research Methodologies.* [en línea]. [consulta 2 oct. 2014]. <http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp >
- **HERNÁNDEZ SAMPIERI, Roberto. FERNANDEZ COLLADO, Carlos. BAPTISTA LUCIO, Pilar.** *Metodología de la Investigación.* 4ta. ed. México: Mc Graw Hill/Interamericana Editores. Abril 2006. 850 p. ISBN 970-10-5753-8.
- **IANSITI, Marco y HERMAN, Kerry**. *CA Technologies: Bajar la nube a la tierra.* Harvard Business School [en línea]. Junio 2011. [consulta 17 sep. 2013]. <

https://cb.hbsp.harvard.edu/cb/pl/22109663/22110463/b0833e58a26994c49be38bb4a4345a22 >

- **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.
- **LEY 21.526.** *Ley de Entidades Financieras.* [en línea]. 1977 y Modificatorias. [consulta nov. 2013]. < http://www.bcra.gov.ar/
- **LEY 25.326.** *Protección de Datos Personales.* [en línea]. 2000. [consulta 05 oct. 2013]. < http://www.jus.gob.ar/datos-personales.aspx >
- **LIU, Fang. TONG, Jin. MAO, Jian, y otros**. *NIST Cloud Computing Reference Architecture*. National Institute of Standards and Technology. Especial publication. 500-292 [en línea]. 2011. [consulta 31 ago. 2013].< http://www.nist.gov/itl/cloud/index.cfm >
- **FAZZALARI, Raúl M.** *Aspectos Regulatorios. Los retos del Cloud Computing.* Logicalis Now. Julio 2011, año 5, n. 14, p. 52-55.
- **MELL, Peter y GRANCE, Timothy**. *The NIST Definition of Cloud Computing.* National Institute of Standards and Technology. Especial publication 800-145 [en línea]. 2011. [consulta 31 ago. 2013]. < http://www.nist.gov/itl/cloud/index.cfm >
- **NORALL, Steve**. *Storage Virtualization.* InfoWorld. Volume 29. [en línea]. 2007. [consulta 05 feb. 2014]. Biblioteca EBSCO
- **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.
- **PANIAGUA MACIA, Claudio**. *La virtualización de los recursos tecnológicos, impulsor del cambio en la empresa.* Universia Business Review. [en línea]. 2006. ISSN 1698-5117. [consulta 05 feb. 2014]. Biblioteca EBSCO.
- **RISTOV, Sasko. GUSEV, Marjan. y KOSTOSKA, Magdalena.** *Cloud Computing Security in Business Information Systems.* International Journal of Network Security & Its. Applications. Vol. 4. N°2. [en línea]. 2012. [consulta 10 abr. 2013]. Biblioteca EBSCO.
- **SCARFONE, Karen. SOUPPAYA, Murugiah. y HOFFMAN, Paul.** *Guide to Security for Full Virtualization.* National Institute of Standards and Technology.

Especial publication 800-125 [en línea]. 2011. [consulta 22 nov. 2013]. < http://www.nist.gov/itl/cloud/index.cfm >

- **SEMINARA, Juan P. y AGION, Leandro**. *Tendencias de TI y Telecomunicaciones.* IDC. Argentina. Mayo 2013.
- **SRIRAM, Sudhir.** *Cloud Computing in Banking.* Capgemini. Consulting, Technology, Outsourcing. Publication [en línea]. 2011. [consulta 4 oct. 2013]. <http://www.capgemini.com/resource-file-access/resource/pdf/ >
- **TELECOMUNICATIONS INFRASTRUCTURE STANDARD FOR DATA CENTERS**. TIA/EIA 942. Draft 5.0. Junio 2004.
- **VMWARE**. *Aspectos fundamentales de la virtualización del centro de datos VMware.* [en línea]. 2013. [consulta 10 ene. 2014]. < http://www.vmware.com/ >

10. ANEXOS.

GUIA DE ENTREVISTA

Tema de entrevista: Tecnología de Cloud Computing y su aplicación en las entidades financieras.

Conformidad del entrevistado: La información obtenida en esta entrevista, solo será utilizada con fines académicos. ¿Acepta que sea mencionada la fuente?

Fecha: __/__/____.

Entrevistado:

1) ¿Ha considerado o analizado adoptar la tecnología de Cloud Computing para su Institución?

2) ¿Considera que la elasticidad en la planificación del uso de los recursos es un factor clave a la hora de decidir por Cloud Computing?

3) ¿Qué esquema de implementación adoptaría: Pública, Privada o Híbrida?

4) ¿Considera que el modelo “on premise” es totalmente remplazable en una entidad financiera?

5) A su criterio: ¿Qué razones lo motivarían a adoptarla?:
   a. Costo (CAPEX vs OPEX).
   b. Actualización de tecnológica.
   c. Reducción de estructura.
   d. Rápida adecuación a las necesidades del negocio.
   e. Mejora en la disponibilidad del servicio.

6) ¿Cuáles son los principales motivos o desafíos que considera son una limitante a la hora de decidir mover aplicaciones a la “nube”?:
   a. Aspectos de seguridad física.
   b. Aspectos de seguridad lógica (accesos y confidencialidad de los datos).

c. Cuestiones legales y regulatorias.
d. Objeciones de auditoría interna y/o externa.
e. Confiabilidad de los proveedores.
f. Dificultad para controlar los niveles de SLA.
g. Dificultad en la portabilidad del servicio.
h. Calidad de Servicio en el transporte de datos por Internet.

7) ¿Si adoptara por un modelo de servicio Software as a Service", qué tipo de aplicaciones llevaría a la nube?
   a. Críticas del core business
   b. Secundarias (ej.: CRM, gestión de RRHH, gestión de proveedores,)
   c. Aplicaciones de oficina (mail, otras)
   d. Virtual Desktop
   e. PBX Virtual
   f. Pagina Institucional y/o Intranet

8) ¿Utilizaría los servicios de Cloud Computing como Platform as Service? ¿En qué casos?:
   a. Ambientes de desarrollo.
   b. Ambiente de testing y QA.
   c. Entornos de recovery.
   d. Virtual Desktop
   e. PBX Virtual
   f. Pagina Institucional y/o Intranet