GESTIÓN DE LA INFORMACIÓN EN LA NUBE

Un enfoque preservador

TRABAJO DE FIN DE MÁSTER

Realizado por Liu Can

Dirigido por María Manuela Moro Cabero

y Elvira Julieta Miguélez González

Universidad de Salamanca, 2016

MÁSTER EN SISTEMAS DE INFORMACIÓN DIGITAL

UNIVERSIDAD DE SALAMANCA

FACULTAD DE TRADUCCIÓN Y DOCUMENTACIÓN

MÁSTER EN SISTEMAS DE INFORMACIÓN DIGITAL

Trabajo de Fin de Máster

Gestión de la información en la nube

Un enfoque preservador

Autor: Liu Can

Tutoras: Profª. Drª. María Manuela Moro Cabero

y Profª. Drª. Elvira Julieta Miguélez González

Salamanca, 2016

ASIENTO CATALOGRÁFICO

Título:
Gestión de la información en la nube: un enfoque preservador

Autor:
Can, Liu

Directoras:
Moro Cabero, María Manuela
Miguélez González, Elvira Julieta

Palabras clave:
[ES] computación en la nube, tecnología de la nube, gestión de la información, seguridad de la información, servicios en la nube

[EN] cloud computing, cloud technology, information management, information security, cloud services

Clasificación UNESCO:
Materias: 63: Sociología 6307: Cambio y desarrollo social 630707: Tecnología y cambio social

Fecha:
2016-9-5

Resumen:
[ES] En el presente trabajo se describe la tecnología de la nube en la gestión de la información desde el punto de vista preservador para detectar sus puntos fuertes y débiles, así como las propuestas de mejora. Se introducen los conocimientos básicos de la tecnología de la nube, se centran específicamente en los aspectos legales sobre la gestión de contenidos almacenados en la nube y se analizan las últimas tendencias de desarrollo de esta materia. Este trabajo tiene como fin ofrecer una base de referencia fundamental a partir de la cual se podrán desarrollar futuros trabajos más específicos sobre la gestión de la información en la nube.

Abstract:
[EN] In this paper we describe the cloud technology in information management from the point of preserver's view to identify their strengths and weaknesses, and improvement proposals. Basic knowledges of cloud technology are introduced, specifically focus on the legal aspects of the management of content stored in the cloud and the latest trends of development of this area are

analyzed. This work aims to provide fundamental reference base from which we can develop more specific works on information management in the cloud in the future.

Descripción:
Trabajo de Fin de Máster en Sistemas de Información Digital, curso 2015-2016

Sumario

Índice de figuras

Índice de gráficos

Índice de tablas

“不積跬步，無以至千里。”

- 荀子

“Un viaje de mil millas comienza con un pequeño paso.”

- Xún Zǐ

CAPíTULO 0
OBJETIVOS Y METODOLOGíA

En el Capítulo 0 se presentarán brevemente los objetivos y la metodología de la realización del trabajo.

0. Capítulo 0: Objetivos y metodología

El nacimiento de la tecnología de la nube ha creado una nueva era en la que se ofrecen diversas oportunidades y diversos servicios innovadores en el campo de la gestión de la información. Sin embargo, también ha traído nuevos retos, tales como las cuestiones de la seguridad de información, la protección de datos personales, la garantía del acceso continuo de los contenidos digitales almacenados en la nube, etc.; aspectos que son fundamentales e imprescindibles tener en consideración a la hora de la adecuada planificación e implementación de la metodología de la gestión de la información desde el punto de vista preservador. Con la realización de presente Trabajo fin de Máter intentamos ofrecer un panorama sobre los aspectos comentados anteriormente para poder abordar una visión general sobre esta materia en la actualidad.

Los objetivos generales de nuestro trabajo son:

- Ofrecer un panorama y una visión general, desde el punto de vista preservador, de la aplicación de la tecnología de la nube (*cloud computing*) en la gestión de la información.
- Analizar la tendencia de desarrollo de la tecnología de la nube y extraer a partir de ello los aspectos asociados a la gestión de la información.
- Detectar las ventajas e inconvenientes de la tecnología de la nube en la gestión de la información y abordar recomendaciones correspondientes.

Pare ello, hemos redactado el cuerpo del trabajo aplicándole la siguiente metodología:

- **Capítulo 1**
  Este capítulo se dedica a la introducción del *cloud computing* en el que se incluyen los conocimientos básicos sobre ello. Para poder realizarlo se lleva a cabo la revisión bibliográfica, la extracción y la recopilación de información a partir de ella, ya que se trata de un trabajo teórico-descriptivo, y una buena selección de las fuentes de consulta podrá mejorar la contextualización del trabajo.

- **Capítulo 2**
  Este capítulo trata de una parte nuclear de nuestro trabajo, ya que se incluyen los aspectos asociados a la seguridad, la privacidad y la protección de información almacenada en la nube, así como otros enfoques legislativos sobre la contratación, los roles que desempeñan los clientes y los proveedores de servicios en la nube y sus derechos y deberes correspondientes. Todo ello son materiales que un preservador tendría que estudiar. Para ello se centra en tres puntos básicos: el ámbito internacional -analizamos una serie Normas ISO que se tratan de la seguridad, la privacidad de la información almacenada en la nube y los asuntos legales asociados a la contratación de servicios-, el ámbito en

España, -destacamos fundamentalmente los aspectos sobre la protección de datos personales y los relacionamos con la gestión de la información en la nube basándonos en la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) y su Reglamento de Desarrollo (RDLOPD), aprobado por R.D. 1720/2007- y otras normativas y certificaciones -mediante las tablas destacamos sus contenidos principales para servir como material complementario de este capítulo-.

- **Capítulo 3**
  El capítulo 3 se divide entre dos partes. En la primera parte, hemos realizado una recopilación de información para presentar tanto la situación actual del uso de la tecnología de la nube como los nuevos productos basados en la misma para mejorar la gestión de la información, con el fin de detectar sus puntos fuertes. En la segunda parte, detectamos la actitud sobre la tecnología de la nube de las empresas a través del análisis del informe de investigación, realizado por RightScale en 2016 sobre el estado de la nube.

- **Capítulo 4**
  En el capítulo 4 destacamos los puntos débiles de la tecnología de la nube en la gestión de la información, así como las propuestas y recomendaciones de futuras líneas de investigación.

- **Bibliografía**
  Hemos realizado una selección de la bibliografía para que sean mayoritariamente fuentes publicadas dentro de los últimos 5 años para mantener su valor especialmente en el análisis de tendencias del desarrollo de la tecnología de la nube. para la relación bibliográfica del trabajo hemos seguido el modelo APA 6ª ed.

Para finalizar esta parte y antes de pasar a presentar el cuerpo del trabajo, me gustaría expresar mi más sincero agradecimiento a una serie de personas, sin ellas no habría sido posible la realización de este trabajo: en primer lugar, a José Luis Alonso Berrocal, por sus aclaraciones de los términos informáticos. En segundo lugar, a las directoras de este trabajo, María Manuela Moro Cabero y Elvira Julieta Miguélez González, por la ayuda de la selección de la bibliografía, la corrección de la redacción, su confianza absoluta en mí y apoyo incondicional en la realización del trabajo. Muchas gracias por orientarme.

"Is it time we should change our mindset to accept new things?"

- Sharon Q. Yang

CAPÍTULO 1
INTRODUCCIÓN AL CLOUD COMPUTING

En este capítulo se incluirán los aspectos introductorios del *cloud computing* para aportar un concepto básico sobre ello.

1. Capítulo 1: Introducción al *cloud computing*

Gracias al rápido avance en las tecnologías de la información y las telecomunicaciones (TIC), cada vez hay más recursos de información que se han convertido en recursos digitales, tales como las bases de datos de gran dimensión, las galerías de imágenes, los archivos audiovisuales y otros formatos de multimedia. Estos soportes de gran capacidad de almacenamiento y de alta velocidad de transmisión de la información han lanzado un gran desafío a los soportes tradicionales, ya que han satisfecho las necesidades y deseos del público tanto en la adquisición de la información como en la transformación de los modos de vida. Por lo tanto, ha surgido una estrecha vinculación entre el público y los recursos de información.

Sin embargo, aunque el desarrollo de las TIC nos pueda beneficiar en muchos aspectos, podría resultar peligroso si no lo tratamos de manera oportuna. Por un lado, debido a que una vez se deterioran e incluso se pierden, el valor de los datos digitales puede desaparecer sin manera de recuperación alguna. Por otro lado, todavía no hay una suficiente conciencia para abordar los cambios traídos por la evolución de las TIC, por lo que la infraestructura técnica de apoyo de la gestión puede quedarse obsoleta e imposibilitar su accesibilidad.

En el campo de la gestión y preservación de la información digital, los principales retos a los que se está enfrentando son el deterioro del soporte de almacenamiento, la obsolescencia del hardware y la dependencia de software. Entonces el aseguramiento de la legibilidad e inteligibilidad, así como la conservación de la autenticidad e integridad de los recursos digitales se han convertido en el trabajo nuclear de la gestión y preservación de la información digital.

1.1 El *cloud computing*

Los servicios de la computación en la nube (*cloud computing*), surgidos como consecuencia de la situación comentada, de acuerdo al Centro Criptográfico Nacional (CCN, 2014), se podrán considerar como una propuesta tecnológica eficiente y capaz de proporcionar servicios en red de forma ágil y flexible.

Con respecto a la definición del *cloud computing*, todavía no existe una definición oficial, ya que tras la realización de la revisión bibliográfica sobre los artículos que se tratan los temas de computación y tecnologías, los autores muestran distintas definiciones (Yang, 2012).

A continuación, se incluyen algunas definiciones en inglés realizadas por distintos autores destacando su idea principal por palabras clave:

- Wolf (2010, p. 30) destaca el "acceso externo", al señalar que el *cloud computing* es *"any server usage or software application you can access outside of your local server."*[1]

- Horrigan (2008, p. 1) subraya los conceptos de acceso ubicuo y usuario final, al considerarlo como "*an emerging architecture by which data and applications reside in cyberspace, allowing users to access them through any web-connected device.*"[2]

- Goldner (2011, p. 3) resalta el nuevo modelo de servicios TI, al aportar la escueta definición del *cloud computing*, como sigue: "*is a new technology model for IT services.*"[3]

- Los conceptos de software y hardware, son resaltados por Ojala y Tyrväinen (2011, p. 41), al especificar que el *cloud computing* es "*software applications delivered through the internet, and also the hardware and system software that is used within data centers to provide those services*."[4]

A pesar de la variedad de definiciones existentes del concepto *cloud computing*, resulta muy evidente que la definición puede adaptarse a contextos diferentes. No obstante, existe una definición citada con mayor frecuencia realizada por el *National Institute of Standards and Technology* (NIST) en el documento NIST SP-800-145, y éste ha sido traducido al español por el Centro Criptográfico Nacional (CCN, 2014, p. 5), tal y como se muestra a continuación:

- "La provisión de servicios en la nube es un modelo para permitir el acceso por red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio".

[1] Traducción al español: (El *cloud computing* es) cualquier servidor o software/aplicación al que podemos acceder fuera del servidor local.

[2] Traducción al español: (El *cloud computing* es) Una arquitectura emergente mediante la cual los datos y aplicaciones residen en el ciberespacio, lo que permite que los usuarios puedan acceder a ellos a través de cualquier dispositivo conectado a Internet.

[3] Traducción al español: El *cloud computing* es un nuevo modelo tecnológico para los servicios de la Tecnología de la Información (TI).

[4] Traducción al español: (El *cloud computing* son) aplicaciones del software distribuidas por el internet, y también son el hardware y los softwares del sistema que se utilizan dentro de los centros de datos para proporcionar esos servicios.

Atendiendo al *National Archives and Records Administration* (NARA, 2010), el *cloud computing* es una tecnología reciente que nos permite acceder y utilizar servicios de computación y datos compartidos a través de internet o una red virtual privada. Este servicio permite que los usuarios puedan acceder a los recursos sin preocuparse de la infraestructura en la que se basan u otras cuestiones técnicas.

Tres aspectos definitorios a destacar del conjunto de definiciones: *tecnología reciente* que conforma una *infraestructura de servicios* que permiten el *acceso* por red, a los que, desde la óptica de la finalidad de servicio inherente a un documentalista añadimos, para/por el *cliente (y/o) usuario final*.

1.2 Características esenciales del *Cloud Computing*

Tras la introducción del concepto básico de *cloud computing*, pasaremos a explicar en el presente subapartado cuáles son las características fundamentales para poder comprender su funcionamiento.

Para ello, cabe destacar las caracterizaciones del NIST, siendo la institución designada para el desarrollo de estándares y guías para los trabajos que se están llevando a cabo el *Federal Cloud Computing*, quién ha identificado 5 características esenciales del *cloud computing* (Mell & Grance, 2011) que enumeramos:

- **Auto-servicio a demanda**
  El usuario puede adquirir y ajustar unilateralmente la capacidad de computación según necesidades concretas, tales como el tiempo de servidor o el almacenamiento en red, sin interacciones humanas con el proveedor (CSP, *Cloud Service Provider*).

- **Acceso amplio a través de redes**
  Acceso estándar a los servicios ofrecidos por el CSP mediante cualquier plataforma de cliente liviano[5] o pesado[6] siempre que tengan conexión a la red (e. g., portátiles, teléfonos, etc.).

- **Espacio de compartición de recursos**
  Los recursos del CSP están agrupados para servir a varios consumidores aplicando el modelo multi-tenencia. La agrupación de recursos incluye recursos

5 Cliente liviano: es una computadora cliente o un software de cliente en una arquitectura de red cliente-servidor que depende primariamente del servidor central para las tareas de procesamiento, y se enfoca principalmente en transportar la entrada y la salida entre el usuario y el servidor remoto.

6 Cliente pesado: se denomina cliente pesado al programa "cliente" de una arquitectura cliente-servidor cuando la mayor carga de cómputo está desplazada hacia la computadora que ejecuta dicho programa.

físicos o virtuales que se asignan o se reasignan dinámicamente bajo demanda concreta del consumidor. Aunque normalmente los consumidores no son capaces de saber ni controlar la ubicación exacta de los recursos, todavía podrán delimitar ubicaciones a un alto nivel de abstracción (país, comunidad, centro de datos, etc.). Entre los tipos de recursos se incluyen: almacenamiento, procesamiento, ancho de banda, memoria y máquinas virtuales.

- **Rápido y elástico**
  La capacidad puede proveerse de forma rápida y elástica para satisfacer las distintas demandas. Para el consumidor, las capacidades son ilimitadas y están disponibles de cualquier cantidad en cualquier momento.

- **Servicio consumido**
  Los sistemas de la nube controlan y optimizan automáticamente el uso de los recursos a través de la capacidad de medición en un nivel de abstracción adecuado dependiendo del tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda, cuentas de usuario, etc.). La situación del uso de los recursos está supervisada, controlada y reportada para posteriormente poder mejorar la transparencia tanto para el CSP como para el consumidor del servicio.

Por último, de acuerdo con la Guía de seguridad de las TIC (CCN, 2014, p. 7), es imprescindible destacar “la posible dependencia de terceros en los servicios en la nube”. A partir de lo señalado en la Guía, “la tendencia mayoritaria apunta hacia externalizar los servicios en la nube a terceros delegando en ellos todas las tareas de mantenimiento, adquisición de sistemas, gestión de la capacidad, etc.”.

Como consecuencia, el organismo contratante se ha convertido en el responsable de la garantía de seguridad de la información. Por lo tanto, atendiendo al CCN, se deben “estudiar adecuadamente las condiciones del servicio y las medidas de seguridad aplicadas para confirmar que son adecuadas para los requisitos exigidos a la organización cliente”.

Para finalizar este subapartado, podríamos concluir que, además de las anteriores 5 características citadas por el NIST, habría que considerar desde el enfoque preservador, también, una sexta, atendiendo a su predominio, centrada en la “externalización de los servicios”, así como una séptima, inherente a la responsabilidad en materia de seguridad de la información, que recae en el organismo contratante.

1.3 Modelos de despliegue de servicios en la nube

Tras las explicaciones de las características principales del *cloud computing*, a

continuación, pasaremos a presentar los modelos de despliegue de servicios en la nube. De acuerdo con Aleem y Ryan Sprott (2012), aunque los modelos de despliegue dependen de la capacidad del CSP, por lo general, existen 4 combinaciones para desplegar la plataforma de la nube:

- Nubes privadas: son un modelo de despliegue cuya infraestructura es operada por una única entidad. Normalmente las nubes privadas son más atractivas para las entidades que requieren un mayor grado de control de los datos, ya que pueden almacenar todos los datos en su propia infraestructura informática.

- Nubes públicas: tal y como indica su nombre, se trata de un modelo al que pueden acceder múltiples usuarios simultáneamente. Sin embargo, el CSP sigue teniendo el control de la infraestructura de esta nube.

- Nubes comunitarias: la infraestructura de la nube está compartida por varias organizaciones con principios o intereses similares. Este modelo suele ser controlado u organizado por la comunidad o por un tercero.

- Nubes híbridas: son una composición de dos o más modelos anteriores. Dicho de otra forma, en este modelo hay ciertos servicios que se ofrecen de forma pública y otros de forma privada. Por ejemplo, las organizaciones pueden desplegar aplicaciones no críticas en la nube pública mientras mantienen los servicios importantes en su nube privada para tener cierto grado de control.

Tal y como es posible observar, estos modelos disponen de distintas formas del tratamiento de datos, lo que podrá resultar interesante, desde la perspectiva del preservador, estudiar cómo éstas afectan a la seguridad de la información y la protección de datos de carácter personal. Estos aspectos se ampliarán posteriormente en el desarrollo del trabajo.

1.4 Niveles de servicio

A medida que el CSP de la nube ofrece acceso a los recursos a su cliente vía internet, podrán proporcionar otros servicios de valor añadido bajo demanda. En general, cuentan con tres niveles principales: Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e *Infraestructura* como Servicio (IaaS). Sin embargo, hay proveedores que ofrecen servicios mixtos en los que se combinan características de todos ellos (Peña-López, 2013). A través de la siguiente figura es posible identificar claramente la jerarquía de servicios de *cloud computing* (Figura 1):

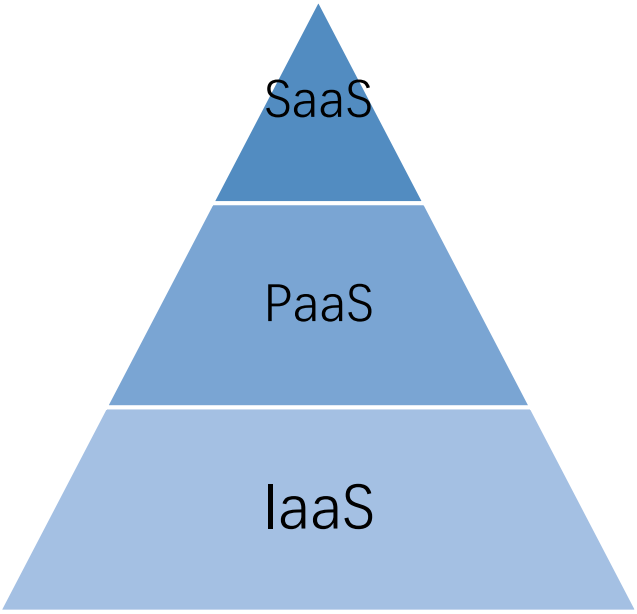

Figura 1. Jerarquía de servicios de *cloud computing*.
Fuente: Elaboración propia

A continuación, detallamos cada uno de los niveles:

- **Software como Servicio (Software *as a Service* o *Saas*)**
  En este nivel de servicio el CSP proporciona al cliente softwares que procesan en la infraestructura de la nube. Los softwares son accesibles a través de una interfaz de cliente liviano (por ejemplo: correos electrónicos basados en Web) desde distintos dispositivos cliente. El consumidor no se encarga de la administración de la infraestructura de la nube, salvo alguna configuración limitada del software para clientes específicos.

- **Plataforma como Servicio (*Platform as a Service* o *Paas*)**
  En este nivel, se despliegan las aplicaciones adquiridas o creadas por el consumidor en la infraestructura de la nube a través de herramientas o lenguajes de programación proporcionadas por el CSP. Es decir, el CSP ofrece una plataforma en la que el usuario podrá realizar desarrollo de softwares. El consumidor no gestiona ni controla directamente la infraestructura de la nube (entorno de la red, servidor, sistemas operativos, almacenamiento, etc.), sino que tiene permiso de controlar las aplicaciones desplegadas, así como la configuración del entorno de *hosting*.

- **Infraestructura como Servicio (*Infrastructure as a Service* o *IaaS*)**
  En este nivel, el consumidor alquila las capacidades básicas de *computing,* tales como: procesamiento, almacenamiento y red, para poder desplegar o procesar softwares, sistemas operativos o aplicaciones sobre ellas. Aunque el consumidor

no se encarga de la administración de la infraestructura, todavía es capaz de controlar los sistemas operativos, almacenamiento, softwares o aplicaciones desplegados e incluso algunos componentes de la red (por ejemplo: *firewall* de *host*).

Tomando como base los modelos de servicio antedichos, aportamos las siguientes explicaciones para una mejor comprensión de estos conceptos:

- El SaaS es el nivel más alto de servicio. La aparición del SaaS ha sustituido el antiguo modelo en que la organización cliente compraba y mantenía el hardware, los sistemas operativos y las aplicaciones en premisa privada (Ojala y Tyrväinen, 2011). Se trata de que el usuario es el beneficiario directo de los software*s* o aplicaciones facilitados por el CSP. Hoy en día casi todos nosotros estamos beneficiándonos de este servicio, aunque muchas veces no tenemos esa conciencia. Por ejemplo, el servicio de correo electrónico puede ser uno de los servicios más típico que estamos utilizando. Además, hay muchos otros softwares/aplicaciones que ofrecen servicios en el servidor que se podrían considerar también como una parte del SaaS (por ejemplo: álbumes web, blogs, etc.). Conforme indica Han (2011), bajo el entorno del SaaS, lo que está realizando el consumidor es consumir las aplicaciones proporcionadas por el CSP del servicio a través de una interfaz de cliente liviano, por ejemplo, un navegador de web, sin preocuparse por las tareas de mantenimiento, tareas que el CSP llevaría a cabo.

- El PaaS es el nivel intermediario entre el SaaS y el IaaS. En esta *capa de abstracción*[7], atendiendo a lo que indica Dhar (2012), las tareas que se podrán realizar ya no solo consisten en la abstracción técnica, sino también en los servicios esenciales de la infraestructura de aplicaciones, tales como: computación, mensajería, conectividad, control de acceso, etc. Este tipo de servicio se enfatiza en la entrega de un entorno de apoyo -podría ser un servidor de bases de datos o un sistema operativo- en que el usuario pueda desarrollar sus propias aplicaciones. Esto es, en cierto sentido, en vez de tener la infraestructura como premisa para poder empezar a desarrollar aplicaciones para que el usuario las consuma, ahora podremos centrarnos exclusivamente en la funcionalidad de las aplicaciones. De esta manera, lo que permite supondrá un gran ahorro, tanto en el proceso de desarrollo como de procesamiento y mantenimiento.

- En cuanto al IaaS -siendo el nivel inferior de servicio en *cloud computing*- en

7 Término empleado para expresar una forma de ocultar los detalles de implementación de ciertas funcionalidades. Su ventaja principal es permitir que se centre solamente en las tareas que se realizan en una capa concreta sin preocuparse por el funcionamiento interno de la capa de abajo. Su término en inglés es "abstraction layer".

general, se trata de un tipo de servicio que está dirigido a proporcionar *máquinas virtuales* y espacios de almacenamiento al usuario final (Kwame Adjei, 2015). Para evitar posibles malentendidos del término "infraestructura" -que normalmente se entiende como instalaciones físicas- merecería la pena aclararse que, según Dhar (2012), en el ámbito de contratación de servicios en la nube, el término "infraestructura" podría hacer referencia a dos aspectos simultáneamente: el CSP se encarga de administrar la infraestructura física (servidores, componentes de la red, etc.) mientras externaliza al cliente final la infraestructura virtual de procesamiento completa bajo demanda (máquinas virtuales, espacios de almacenamiento, etc.), incluyendo la entrega y apoyo técnico (vía World Wide Web) de una completa infraestructura informática. De acuerdo con Pérez San-José et al. (2011, p. 9), este nivel de servicio "puede ser visto como una evolución de los Servidores Privados Virtuales que ofrecen actualmente las empresas de *hosting*".

Tras las aclaraciones de los niveles de servicios del *cloud computing*, se han realizado las siguientes tablas tomando como base la taxonomía de *OpenCrowd Cloud Solutions* elaborada por el *Cloud Security Alliance* (CSA, 2011, p.17) para demostrar la diversidad de ofertas disponibles del *cloud computing* hoy en día (Tabla 1, 2 y 3).

SaaS	
Taxonomía	Ejemplos
Gestión de contenidos	Clickability
	SpringCM
	CrownPoint
Gestión de documentos	NetDocuments
	DocLanding
	Knowledge TreeLive
	SpringCM
Gestión de relaciones con los clientes (*Customer relationship management*, CRM)	NetSuite
	Parature
	Responsys
	Rightnow
	LiveOps
	MSDynamics
	Salesforce.com
	Oracle On Demand
Redes sociales	Ning
	Zembly
	Amitive
	Jive SBS
Facturación	Aria Systems
	eVapt

	Redi2
	Zuora
Ventas	Xactly
	StreetSmarts
	Success Metrics
Productividad de escritorio	Zoho
	Google Apps
	HyperOffice
	Ms Office Web Apps
Finanzas	Concur
	Xero
	Workday
	Expensify
	Intuit Quickbooks Online

Tabla 1. Ejemplos de ofertas de SaaS.

Tal y como se puede observar en la Tabla 1, en el nivel superior se registran los servicios de gestión de contenidos, gestión de documentos, gestión de relaciones con los clientes, redes sociales, facturación, ventas, productividad de escritorio y finanzas. Adjunto a esta relación de servicios se incluyen ejemplos variados sobre cada uno de ellos.

PaaS	
Taxonomía	Ejemplos
Propósito general	Force.com
	Etelos
	LongJump
	Rollbase
	Bungee Connect
	Google App Engine
	Engine Yard
	Caspio
	Qrimp
	MS Azure
	Mosso Cloud Sites
	VMforce
	Intuit Partner Platform
	Joyent Smart Platform
Inteligencia de negocio	Aster DB
	Quantivo
	Cloud9 Analytics

	K2 Analytics
	LogiXML
	Oco
	PivotLink
	Clario Analytics
	ColdLight Neuron
	Vertica
Integración	Amazon SQS
	Amazon SNS
	Boomi
	SnapLogic
	IBM Cast Iron
	Gnip
	Appian Anywhere
	HubSpan
	Informatica On-Demand
Desarrollo y pruebas	Keynot Systems
	SOASTA
	SkyTap
	Aptana
	LoadStorm
	Collabnet
	Rational Software Delivery Servicies
Bases de datos	Amazon SimpleDB
	Mosso Drizzle
	Amazon RDS

Tabla 2. Ejemplos de ofertas de PaaS.

En la Tabla 2, vinculada al nivel intermedio, se incluyen las ofertas de los posibles tipos de plataformas agrupados en la columna izquierda, tales como: propósito general, inteligencia de negocio, integración, desarrollo y pruebas, bases de datos. En la columna derecha se muestran los ejemplos correspondientes. A continuación, se muestra en la Tabla 3, taxonomía para el nivel de infraestructura.

IaaS	
Taxonomía	Ejemplos
Almacenamiento	Amazon S3 & EBS
	Rackspace Cloud Files
	Nirvanix
	AT&T Synaptic
	Zetta

Cloud Broker[8]	RightScale
	enStratus
	Kaavo
	CloudKick
	CloudSwitch
Computación	Amazon EC2
	Serve Path GoGrid
	Rackspace Cloud Servers
	Joyent Cloud
	Flexiant Flexiscale
	Elastichosts
	Terremark
	iTRiCity
	LayeredTech
	Savvis Cloud Compute
	Verizon CaaS
	AT&T Synaptic
	Sungard Enterprise Cloud
	Navisite
Gestión de servicios	Scalr
	CohesiveFT
	Ylastic
	CloudFoundry
	NewRelic
	Cloud42
	Amazon CloudWatch
	Amazon VPC

Tabla 3. Ejemplos de ofertas de IaaS.

En la Tabla 3 se pueden visualizar, por un lado, los tipos de infraestructuras que se ofrecen por el CSP al usuario final (almacenamiento, *Cloud Broker*, computación y gestión de servicios); por otro lado, los ejemplos de IaaS que se pueden encontrar en el mercado.

Además de todas las ofertas vistas en las tablas, también existen otros ejemplos de la aplicación de las tecnologías de *cloud computing* en el ámbito bibliotecario, especialmente centrados en los Sistemas Integrados de Gestión de Bibliotecas (ILS, por sus siglas en inglés). Por ejemplo, Breeding (2011) ha listado en su estudio una serie de productos de la nube para las bibliotecas, tales como se muestra a continuación en la tabla (Tabla 4):

[8] Un tercero que actúa como intermediario entre el cliente de un producto de cloud computing y el proveedor de ese producto.

Producto	Organización
Koha	Koha
DuraCloud	DuraSpace
Ex Libris	Alma
Web-scale Management Services	Online Computer Library Center (OCLC)
Kuaili Open Library Environment	Kuali Foundation
Web-scale Management Solution	Serials Solutions
Sierra	Innovative Interfaces, Inc.

Tabla 4. Productos de la nube para las bibliotecas.

Entre las organizaciones mostradas en la tabla, hay algunas que han comenzado a ofrecer los ILSs como soluciones en la nube. Según Yang (2012), existen muchos vendedores que están ofreciendo opciones para los servicios de *hosting* de los ILSs clásicos como soluciones en la nube, mientras que otros están desarrollando una nueva generación de ILSs, especialmente para la nube. Por ejemplo, en 2011, OCLC entregó su producto Web-scale Management Services como un ILS en la nube. Ex Libris lanzó el producto Alma en 2012 como un ILS basado en la nube integrado por una capa de descubrimiento (el OPAC). El producto Koha también es un ILS basado en la nube desde que nació.

1.5 Conclusiones del capítulo 1

A través del capítulo 1, de carácter introductorio al *cloud computing*, se ha trazado un bosquejo sobre sus características principales, los modelos de despliegue de sus servicios, los niveles de servicios y las posibles ofertas que se pueden adquirir hoy en día en el mercado. Tras todo ello, somos conscientes del atractivo y la competitividad de la nube. Sin embargo, es fundamental tener en cuenta que las ganancias en costes, eficiencia, accesibilidad y flexibilidad deben ser sopesadas contra los riesgos asociados a la seguridad y privacidad de la información.

En el capítulo 2 abordaremos las fuentes normativas, legislativas y reglamentarias, así como cualquier otro tipo de código, relacionadas con el *cloud computing*, con el fin de elaborar un marco jurídico y normativo sobre ello.

"It is important to note however that security issues that are associated with cloud computing are intensified by cloud computing but not explicitly caused by it."

- Siani Pearson y Azzedine Benameur

CAPÍTULO 2
MARCO JURÍDICO-NORMATIVO

En este capítulo se explicarán los marcos de referencia aplicables al *cloud computing* centrándose específicamente en los aspectos sobre la seguridad y privacidad de datos personales.

2. Capítulo 2: Marco jurídico-normativo

Actualmente, la utilización de la nube está transformando la forma en que adquirimos y consumimos la información, ya que afecta no solo el modo del acceso a la información sino también a las funciones informáticas. Esto es, podemos acceder a la información almacenada en la nube desde cualquier lugar siempre que disponga de conexión a internet y de permiso(s) de acceso.

Sin embargo, esta gran ventaja que han ofrecido los servicios en la nube se muestra, a su vez, como un aspecto que conlleva muchas implicaciones jurídicas. Atendiendo a lo anteriormente expuesto, hoy en día, la tendencia mayoritaria apunta hacia externalizar los servicios en la nube a terceros, y debido a que, en numerosos casos, los servidores también se pueden externalizar a través del modelo IaaS, la información que se transfiere en ellos podría ocasionar situaciones muy delicadas sobre la seguridad y privacidad de la misma.

A partir de esta perspectiva, en este capítulo pasaremos a detallar las normativas que regulan el tratamiento de datos en servicios de *cloud computing* centrándonos en los aspectos sobre la seguridad y privacidad de la información, con el fin de aportar un marco de referencia para la gestión de la información en la nube.

Al respecto se abordarán códigos, tanto en el ámbito internacional, nacional como desde la perspectiva de diversos códigos y otros referentes de uso.

2.1 Ámbito internacional

Con un alcance internacional, de carácter facultativo destacamos 3 normas ISO de gran relevancia que pasamos a detallar.

2.1.1 ISO/IEC 27018:2014

La Norma ISO/IEC 27018:2014 *Tecnología de la información. Técnicas de seguridad. Código de práctica para la protección de información personal identificable (IPI) en nubes públicas que actúan como encargados del tratamiento*, editada en 2014 por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), es una norma fundamental que se suma a otras sobre seguridad, como por ejemplo, el estándar de requisitos sobre sistemas normalizados de SI, UNE-ISO/IEC 27001:2014 *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.* Además, el antecitado estándar, es el primero, de alcance internacional sobre privacidad en la nube que se

ha creado basado fundamentalmente en leyes y regulaciones emitidas en la Unión Europea.[9]

En concreto, se centran en la regulación de los roles que se deberían desempeñar y los deberes que tienen que cumplir los participantes en el proceso del tratamiento de los datos. Atendiendo a Sánchez y Recio (2015, pp. 20-23), el estándar contiene indicaciones sobre los siguientes tres enfoques:

- **Enfoque del CSP**
  1. Tiene que ser transparente, tanto en los términos y condiciones de sus servicios como en las prácticas de negocio que se llevan a cabo.

  2. Tiene que ayudar al cliente al cumplimiento de las leyes y regulaciones de protección de datos personales o de privacidad, y de seguridad demostrándole compromiso.

  3. El CSP es el responsable en la adopción de sus funciones como encargado del tratamiento. Además, tiene obligación de facilitar al cliente la prueba necesaria de que ha sido auditado de modo independiente y periódicamente.

- **Enfoque del cliente**
  1. Tiene el derecho de controlar el tratamiento de los datos personales que ha facilitado al proveedor.

  2. Puede incorporar los compromisos del CSP en el contrato, siempre que estén en virtud de la ISO/IEC 27018, y saber qué tipo de información tiene que solicitarle.

  3. Tiene garantías complementarias de limitación del uso de datos personales por parte del CSP. Dicho de otra forma, el CSP no podrá utilizarlos con fines comerciales o promocionales sin autorización por parte del contratante.

- **Enfoque de las autoridades de protección de datos y otras autoridades reguladoras**
  1. Pueden obtener fácilmente garantías de cumplimiento basándose en la Norma ISO/IEC 27018.

[9] ISO/IEC 27018:2014 Tecnología de la información. Técnicas de seguridad. Código de práctica para la protección de información personal identificable (IPI) en nubes públicas que actúan como encargados del tratamiento.
Fuente: http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

2. Son capaces de impulsar buenas prácticas u otros temas relacionados con la protección de datos personales tomando como marco de referencia dicha norma.

3. La Norma ISO/IEC 27018 y otros estándares pueden considerarse como una medida proactiva por el responsable (el cliente del servicio) y el encargado del tratamiento (el CSP) que están sujetos al cumplimiento.

Tal y como es posible observar, la ISO/IEC 27018 ha creado un nuevo esquema cliente-proveedor en el que el cliente de los servicios en la nube se ha convertido en el responsable del tratamiento de datos. Es decir, el cliente tiene la responsabilidad de decidir sobre el tratamiento de los datos para que el CSP -en calidad de encargado del tratamiento- siga sus instrucciones. Por lo tanto, antes de contratarse con un servicio ofrecido por el CSP, el cliente tendrá que fijarse en los términos y condiciones del servicio, ya que, según dicha norma, elegir un CSP es una decisión responsable que podrá influir en todas tareas que se van a llevar a cabo posteriormente.

En cuanto al CSP, también se le ha exigido que, no solo dé transparencia a los términos y condiciones de sus servicios y a las actividades de negocio que llevan a cabo, sino que también implique la adopción de medidas en materia de protección de datos personales para que el cliente contratante sea consciente y tenga conocimiento de que sus derechos de privacidad están garantizados.

Por último, merece la pena mencionar que, de acuerdo con Sánchez y Recio (2015, pp. 22), con la publicación de la ISO/IEC 27018, el modelo ISO en la TIC referido a la nube pública estaría más completo y enriquecido (Figura 2).

Figura 2. Modelo ISO en la TIC referido a la nube pública.
Fuente: Elaboración propia.

De acuerdo con la Figura 2, podríamos decir que la ISO/IEC 27018 es una norma que se suma tanto a la calidad (UNE-ISO/IEC 20000) como a la seguridad (UNE-ISO/IEC 27001 y UNE-ISO/IEC 27002) y que "permite a los proveedores de la nube pública evaluar riesgos e implementar controles para la protección de los datos personales almacenados" (Sánchez y Recio, 2015, p. 20).

Además, con respecto a la ISO/IEC 27017:2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services,* publicada a finales del año 2015, que también ha sido una norma especializada en temas sobre los controles de seguridad de la información de los servicios en la nube, pasaremos a detallar su alcance y contenido en la siguiente sección.

2.1.2 ISO/IEC 27017:2015

Actualmente, la nube es una de las innovaciones más utilizadas en los negocios. A medida que los servicios en la nube ganan éxitos en casi todos los campos, la garantía de la seguridad de los datos almacenados en ella se está convirtiendo en una demanda común por parte del usuario. Debido a la naturaleza de estos servicios, su mercado es global, con CSPs distribuidos por amplias áreas geográficas y los datos transferidos rutinariamente cruzando las fronteras nacionales. Por consiguiente, cada vez es más urgente la existencia de una norma regulatoria con directrices internacionales sobre ese asunto.[10]

Por ello, la Norma ISO/IEC 27017:2015 es un estándar que proporciona una serie de directrices para los controles de seguridad de la información que se aplican a los servicios en la nube a través de los siguientes puntos:[11]

- Orientación adicional para los controles pertinentes especificados en la ISO/IEC 27002;

- Controles adicionales determinados con directrices que se relacionan específicamente a los servicios en la nube.

Además, esta norma también ofrece controles y orientaciones tanto para los clientes

[10] Security toolbox protects organizations from cyber-attacks.
Fuente: http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref2032

[11] ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
Fuente: http://www.iso.org/iso/catalogue_detail?csnumber=43757

de los servicios como para el CSP. Por ejemplo, la sección 6.1.1, en la que se explican los roles y responsabilidades en la seguridad de la información, se han añadido, además de las indicaciones existentes en la sección 6.1.1 en la ISO/IEC 27002:2013, los siguientes aspectos (IsecT, 2016):

- **Para el cliente de los servicios en la nube**
  "The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities, and confirm that it can fulfil its allocated roles and responsibilities. The information security roles and responsibilities of both parties should be stated in an agreement. The cloud service customer should identify and manage its relationship with the customer support and care function of the cloud service provider."[12]

- **Para el CSP**
  En esta línea, remarcando los roles y responsabilidades en seguridad de la información se recoge lo siguiente:
  "The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers."[13]

Además, Satoru Yamasaki, en calidad de miembro participante en la creación de este estándar, ha indicado lo siguiente:[10]

> *"ISO/IEC 27017 will help service providers come to a common understanding with their customers regarding adequate security controls and their implementation guidance. This international standard for cloud security controls will facilitate the development and expansion of secure cloud computing systems."*[14]

Tal y como se puede observar, es evidente que, por un lado, la ISO/IEC 27017 ha

[12] Traducción al español: El cliente de los servicios en la nube debe estar de acuerdo con el CSP de la asignación adecuada de los roles y responsabilidades en la seguridad de la información, y confirmar que pueda cumplir esa asignación. Los roles y responsabilidades en la seguridad de la información de ambas partes deben ser establecidos bajo un acuerdo común. El cliente de los servicios en la nube debe identificar y gestionar su relación con la parte del apoyo del cliente y prestar atención a la función a la función que desempeña el CSP.

[13] Traducción al español: El CSP debe redactar y concertar una adecuada asignación sobre los roles y responsabilidades en la seguridad de la información con su cliente, los otros CSPs y sus proveedores.

[14] Traducción al español: La norma ISO/IEC 27017 ayudará a los CSPs en llegar a un entendimiento común con sus clientes con respecto a los controles adecuados de seguridad de la información y sus directrices de implementación. Dicha norma internacional para los controles de seguridad en la nube facilitará el desarrollo y expansión de los sistemas seguros de computación en nube.

completado la ISO/IEC 27002 con aspectos especializados en los asuntos sobre la seguridad de la información almacenada en la nube; por otro lado, aunque las responsabilidades están determinadas entre ambas partes (el cliente y el CSP), en realidad, el cliente es el responsable de la decisión sobre la utilización de los servicios en la nube. Esa decisión se debe tomar atendiendo a los roles y responsabilidades determinados por el CSP. Mientras que, el CSP es el encargado de la seguridad de la información según se establece previamente con su cliente contratante en el acuerdo de los servicios en la nube. Es decir, la ISO/IEC 27017, no solo ha heredado las ideas principales de la ISO/IEC 27018, al respecto de que en las actividades que se llevan a cabo en el ámbito de la nube, el cliente es el responsable del tratamiento de datos, y el CSP, el encargado ese tratamiento, sino que, también, ha creado una estructura en que se interrelacionan estrechamente ambas partes para conseguir una mejor garantía de la seguridad de la información y una forma más oportuna de la gestión de datos, especialmente en la era de la nube.

2.1.3 ISO 14641-1:2012

Además de las dos normas ISO comentadas anteriormente -cuyos contenidos se enfocan específicamente en los asuntos de la privacidad y seguridad en la nube- existen otras normas ISO, como por ejemplo, la Norma ISO 14641-1:2012 *Archivo electrónico – Parte 1: Especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de información digital*, aunque no precisamente tratan de la nube, sus contenidos pueden ser adaptados, en muchas ocasiones, tanto para regular las actividades que se llevan a cabo en los procesos de contratación de servicios en la nube, como pueden considerarse como marco jurídico-normativo complementario en la resolución de cuestiones sobre la misma.

En la Norma ISO 14641-1:2012, merecería la pena destacar, desde la perspectiva de los contratos y prestaciones de servicios a terceros, algunos aspectos relaciones con los servicios prestados en la nube en los apartados 13 y 14, tales como se muestran a continuación:

Apartado 13: Tercera parte de confianza prestadora de servicios de archivo

13.1: Actividades de la tercera parte de confianza prestadora de servicios de archivo

- Puntos destacados:
  - Por parte de la organización cliente, debería verificar que la tercera parte de confianza prestadora de servicios de archivo disponga de todos los certificados correspondientes a los servicios indicados en el contrato antes de firmarlo.

- Por parte de la tercera parte, en resumen, debería presentar todos los certificados de las actividades que se van a llevar a cabo, y, en todo caso, garantizar la seguridad, la privacidad y la confidencialidad de la información de la organización cliente.

13.2: Modelo de contrato del servicio

13.2.5: Seguridad y protección de datos

- Puntos destacados:
  - La tercera parte debería asumir una serie de deberes, tales como: la conservación, la garantía de la seguridad e integridad y la legibilidad de los documentos electrónicos, y, la seguridad del acceso a los servicios.

13.2.7: Transferencia y continuidad

- Puntos destacados:
  - La otra tercera parte debería garantizar la integridad y la recuperación de la información transferida.

13.2.9: Restitución

- Puntos destacados:
  - Al finalizar todas las actividades contractuales, la tercera parte debería realizar la devolución completa al cliente. En caso de que la organización contratante lo solicitara previamente, la tercera parte podrá seguir conservando sus datos durante un período determinado.

13.2.10: Confidencialidad y datos personales

- Puntos destacados:
  - La tercera parte debería adoptar todas las medidas necesarias para garantizar la confidencialidad de la información del cliente contratante y sus datos personales.

13.2.12: Subcontratación

- Puntos destacados:
  - La tercera parte podrá subcontratar servicios siempre que informe al cliente, y seguirá siendo el responsable de los servicios prestados.

Apartado 14: Prestadores de servicio

- Puntos destacados:
  - En general, en este apartado se enfoca en las soluciones de los servicios de archivo prestados por los subcontratados aparte de las terceras partes de confianza, tales como: la confirmación de los requisitos que se deberían cumplir antes de firmar el contrato, la información que se debería incluir obligatoriamente en el contrato y la garantía de la autenticación, la integridad

y la confidencialidad de los datos cuando éstos se transfieren.

Tras el breve análisis de los apartados 13 y 14 en la ISO 14641, podríamos observar que existen muchos aspectos que han sido mencionados en la ISO/IEC 27017 y la ISO/IEC 2018, como por ejemplo, los apartados sobre la seguridad, la privacidad de información y la protección de datos personales. Por lo tanto, es evidente que esta norma podrá ser de gran apoyo para la resolución de los asuntos asociados en la nube.

En cuanto a las regulaciones de las actividades de subcontratación, se explicarán más detalladamente en el siguiente apartado bajo el marco nacional de España.

2.2 Ámbito en España

Con respecto al ámbito español, destacamos la LOPD [Ley 15/1999] y el Reglamento que la desarrolla [RD 1720/2007], que disponen de gran relevancia en las cuestiones de protección de datos de carácter personal.

2.2.1 Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) y su Reglamento de Desarrollo (RDLOPD), aprobado por R.D. 1720/2007

Uno de los fenómenos derivado de los servicios en la nube podría ser el desconocimiento del lugar exacto en que se almacenan los datos por parte del cliente. Atendiendo a las características esenciales de *cloud computing*, el cliente se mantiene independiente de la ubicación exacta de los recursos, aunque éste podrá delimitar la ubicación a un alto nivel de abstracción. No obstante, si los recursos pertenecientes al cliente contienen datos de carácter personal, la situación cambiará completamente.

La LOPD, es una Ley Orgánica española que afecta directamente los aspectos sobre los modos de implementación del tratamiento de datos de carácter personal. En el campo de *cloud computing*, es indispensable apoyarse en dicha normativa para una gran parte de tareas que se realizan a través de las tecnologías de la nube, ya que existen numerosos servicios en la nube que se basan en el tratamiento de datos, siendo muchos de ellos de carácter personal. Asimismo, la Agencia Española de Protección de Datos (AEPD), es el órgano encargado de la garantía del cumplimiento de dicha ley en de España; a su vez, tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos.

Al realizar un análisis detallado del contenido de la LOPD[15], cabría destacar los

[15] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Fuente: https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

siguientes puntos que están relacionados con la gestión de la información en la nube:

- **Artículo 3. Definiciones.**

En esta sección, podremos localizar las definiciones relacionadas con las cuestiones que se deben tener en cuenta de seguridad de la información y protección de datos; sobre todo, aquellas aplicables al cliente y al CSP en el proceso de la contratación de servicios de *cloud computing*.

- **Datos de carácter personal**
  Cualquier información concerniente a personas físicas identificadas o identificables.

- **Tratamiento de datos**
  Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- **Responsable del fichero o tratamiento**
  Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

- **Encargado del tratamiento**
  La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Desde la perspectiva del preservador de la información almacenada en la nube, estas definiciones han aportado un marco coherente en el que se incluyen casi todas las aclaraciones de las dudas que podrán surgir en los procesos del tratamiento de datos o la contratación de los servicios en la nube, especialmente, cuando se trata de asuntos sobre seguridad y privacidad de datos personales.

A continuación, presentamos un gráfico considerando las jerarquías para mostrar las relaciones entre las definiciones citadas (Figura 3).

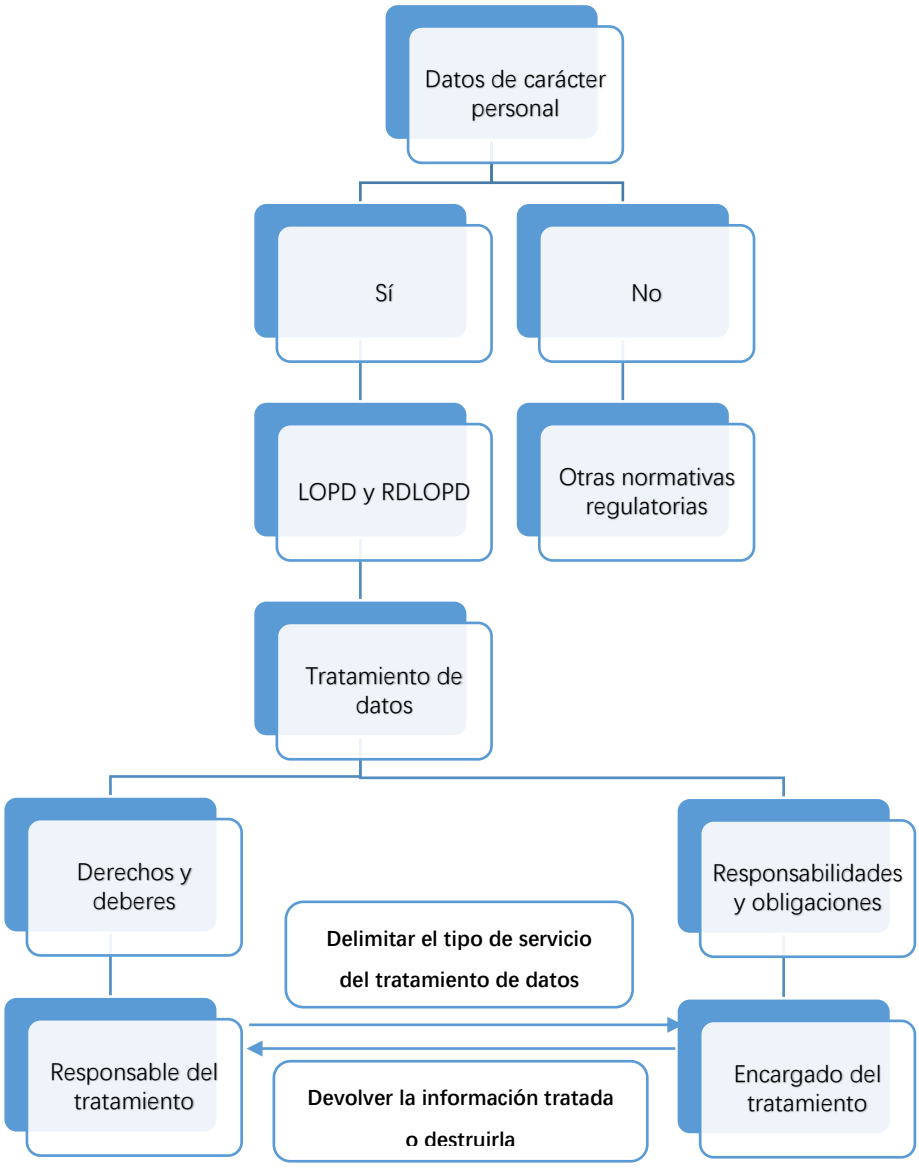

Figura 3. Relaciones entre las definiciones de Datos de carácter personal, Tratamiento de datos, Responsable del tratamiento y Encargado del tratamiento.
Fuente: Elaboración propia.

Mediante la Figura 3 podemos identificar claramente tanto los roles que desempeñan los participantes en los procesos del tratamiento de datos como las relaciones entre los mismos. Además, resulta muy interesante que, en el artículo 5 del RDLOPD[16], al diferenciarse de la definición presentada en el artículo 3 de la LOPD sobre el "encargado del tratamiento", la misma haya sido modificada por la siguiente:

> "*La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del*

[16] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
Fuente: https://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio."

Indudablemente, comparando con la definición correspondiente en la LOPD, el RDLOPD ha enfatizado especialmente la "relación jurídica" entre el encargado del tratamiento y el responsable del tratamiento, cuando este aspecto no se encuentra especificado en la LOPD.

Con respecto a la seguridad de los datos y el acceso a los datos por cuenta de terceros -que están regulados en los Artículos 9 y 12 en la LOPD, Artículos 20, 21 y 22 y el Título VIII en el RDLOPD- nos hemos basado tanto en las propias cláusulas como en la guía sobre la seguridad y privacidad del *cloud computing* para empresas elaborada por el equipo del Observatorio de la Seguridad de la información (Pérez San-José et al., 2011) del Instituto Nacional de Tecnologías de la Comunicación (INTECO), para extraer las ideas principales sobre esta materia, sobre todo para dar una orientación de los deberes u obligaciones que deberán cumplir el responsable y el encargado del tratamiento de datos cuando firman contratos de servicios en la nube. Estas ideas se muestran a continuación:

- **Artículos 9 y 12 en la LOPD, Artículos 20, 21 y 22 y el Título VIII en el RDLOPD**
  - **Seguridad de los datos**
    1. Implantar las medidas técnicas y organizativas para garantizar la seguridad de los datos de carácter personal.

    2. Evitar cualquier tipo de tratamiento de datos no autorizado.

    3. Asegurar que los ficheros que contienen datos de carácter personal y las personas que intervengan en el tratamiento de estos datos reúnan los requisitos y condiciones establecidos por las regulaciones correspondientes.

  - **Acceso a los datos por cuenta de terceros**
  - **Por parte del responsable**
    1. Antes de contratar un servicio, supervisar que si el encargado del tratamiento reúne las garantías para el cumplimiento de lo dispuesto en el RDLOPD.

    2. Firmar un contrato en el que se regulan expresamente las instrucciones del responsable del tratamiento.

  - **Por parte del encargado**

1. Seguir las instrucciones del responsable del tratamiento de datos.

2. No utilizar los datos con fin distinto al que figure en el contrato suscrito por ambas partes.

3. Los datos de carácter personal deben de ser destruidos o devueltos al responsable cuando finalice el contrato.

4. Con respecto a la subcontratación, el encargado del tratamiento puede realizarla siempre que esté autorizado por el responsable del tratamiento y que cumpla los requisitos correspondientes de la LOPD y el RDLOPD.

Además de las ideas principales extraídas de la LOPD y el RDLOPD, cabe destacar a su vez la exclusión de la aplicación de la regulación para las comunicaciones de datos personales, cuyo contenido se encuentra en el artículo 12 de la LOPD:

> "*No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.*"

De acuerdo con la guía citada anteriormente, esta exclusión podrá facilitar, en cierto sentido, la oferta de servicios prestados a través de la nube, ya que muchos de ellos se basan en el acceso a los datos del responsable por parte del encargado para poder ejecutar las tareas del tratamiento de datos.

Como complemento, el concepto de la subcontratación se encuentra detallado en el artículo 21 del RDLOPD. En el ámbito respecto a los servicios en la nube, es muy frecuente que el CSP subcontrate con un tercero para externalizar la infraestructura y gestionar los servicios basados en su nube. En la Guía de seguridad de las TIC (CCN - Centro Criptográfico Nacional, 2014) se enumeran los siguientes ejemplos de la subcontratación:

- Contratación de personal
- Contratación de instalaciones
- Contratación de servicios de comunicaciones
- Contratación de servicios de copias de respaldo

Conforme a las cláusulas correspondientes, aunque se admite la subcontratación por parte del encargado del tratamiento de datos para mejorar el rendimiento y la calidad de sus servicios, o bien para otros motivos con los que se beneficien tanto el CSP como el cliente, es su obligación cumplir los requisitos establecidos en el RDLOPD. Esto es, el encargado siempre debe ser autorizado por el responsable para

subcontratar con un tercero, o, dicha acción está comunicada al responsable o especificada previamente en el contrato.

Al revisar detalladamente el contenido de la LOPD y el RDLOPD, es evidente que existen muchas cláusulas que se podrán aplicar perfectamente al ámbito de los servicios en la nube. En general, estas normativas han exigido un alto nivel de transparencia en los entornos en la nube, ya que los materiales en que se basan los servicios son datos de carácter personal, o mejor dicho, son información sensible. Para poder tratarlos de forma adecuada, es indispensable que el cliente y el CSP cumplan las obligaciones determinadas en la LOPD y el RDLOPD, especialmente los requisitos relacionados con la seguridad de los datos, así como el acceso a los datos por cuenta de terceros.

2.3 Otras normativas y certificaciones

Además de todas las regulaciones destacadas en los apartados anteriores, todavía existe un número relevante de normativas que se pueden aplicar al campo de los servicios en la nube, así como al de las certificaciones.

De acuerdo con el estudio realizado por *Cloud Security Alliance España* e *ISMS Forum Spain* (2015, pp. 11-41), nos hemos basado en ello para la realización del siguiente listado en el que se expresan el conjunto de normativas y certificaciones aplicables a esta materia.

LEGISLACIONES	
Esquema Nacional de Interoperabilidad	
Organización responsable	Ministerio de la Presidencia, Gobierno de España
Finalidad	Garantizar el nivel adecuado de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas.
Recursos	Normas técnicas de interoperabilidad y guías de implementación.
Accesible en: http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Esquema_Nacional_de_Interoperabilidad.html	
Esquema Nacional de Seguridad	

Organización responsable	Centro Nacional de Inteligencia (CNI)
Finalidad	Garantizar el cumplimiento con respecto a la gestión de la seguridad de la información para toda administración pública.
Recursos	En cuanto a los aspectos sobre el *cloud computing*, se encuentran detallados en el documento CNN-STIC-823, elaborado por la CNI.
Accesible en: http://administracionelectronica.gob.es/ctt/ens#.V4oWDOiLQ2x	

Tabla 5. Legislaciones aplicables al entorno de los servicios en la nube.

Tal y como se puede observar en la Tabla 5, se destacan el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad, como legislaciones fundamentales y aplicables. A continuación, se presentarán unos productos de certificaciones profesionales en la Tabla 6.

CERTIFICACIONES PROFESIONALES	
Cloud Security Alliance Security, Certificate of Cloud Security Knowledge	
Organización responsable	Cloud Security Alliance
Finalidad	Evaluar el conocimiento del profesional sobre los escenarios y requisitos de seguridad en la nube.
Aspectos destacables	Cuenta con una serie de acreditaciones que cubren los siguientes campos: arquitecturas en la nube, cumplimiento legal y auditoría, portabilidad, interoperabilidad, respuesta a incidentes, cifrado y gestión de claves, etc.
Accesible en: https://cloudsecurityalliance.org/education/ccsk/#_info-video1	
Cloud Security Alliance Security, Certificate of Cloud Security Professional	
Organización responsable	Cloud Security Alliance e (ISC)$^{2®}$
Finalidad	Respaldar los conocimientos y experiencia de los profesionales que trabajan en entornos en la nube desde la perspectiva tanto técnica como de negocio para mejorar el rendimiento y la calidad de los servicios en la nube ofrecidos por los CSPs.

Aspectos destacables	Dispone de 6 áreas principales, tales como: architectural concepts & design requierements, cloud data security, cloud Platform & Infrastructure security, cloud application security, operations, legal & compliance.
Accesible en: https://www.isc2.org/ccsp/default.aspx?utm_campaign=ccsp&utm_source=csa&utm_medium=certtopnav	

Tabla 6. Certificaciones profesionales para el entorno de servicios en la nube.

En la Tabla 6, se pueden visualizar 2 productos de certificaciones profesionales: *Certificate of Cloud Security Knowledge* y *Certificate of Cloud Security Professional*, ambas han sido elaboradas por la *Cloud Security Alliance*. A continuación, se presentarán una serie de guías de uso sobre los servicios en la nube en la Tabla 7.

GUÍAS DE USO	
CCN-STIC-823 Guía de seguridad de las TIC, utilización de servicios en la nube	
Organización responsable	Gobierno de España, Ministerio de la Presidencia, Centro Nacional de Inteligencia, Centro Criptológico Nacional
Finalidad	Hacer contemplar los aspectos de seguridad para la adopción de la nube e identificar las medidas de seguridad que deben cumplir los CSPs.
Enfoque(s) principal(es)	La introducción de los conocimientos básicos de la nube, así como los aspectos jurídicos-normativos sobre la misma.
Accesible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html	
Opinion 05/2012 on Cloud Computing del Article 29 data protection working party	
Organización responsable	Article 29 data protection working party (conjunto de las Agencias de Protección de Datos europeas)
Finalidad	Analizar todos los aspectos relevantes para los CSPs que operan en el Área Económica Europea y a sus clientes, especificando todos los principios

	aplicables de la Directiva Europea de Protección de Datos (95/46/EC) y la Directiva de e-privacidad 2002/58/EC (revisada en 2009/136/EC) donde sean relevantes
Enfoque(s) principal(es)	Análisis de riesgos de la nube a partir de la perspectiva de la protección de datos.
Accesible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf	
Guía para clientes que contraten servicios de Cloud Computing	
Organización responsable	Gobierno de España, Ministerio de Justicia, Agencia Española de Protección de Datos
Finalidad	Ofrecer a los clientes un conocimiento introductorio para la explicación continua de las garantías contractuales, riesgos, conocimientos de protección de datos, etc.
Enfoque(s) principal(es)	Guía de carácter divulgativo para los clientes para facilitar su comprensión de los aspectos que deben tenerse en cuenta sobre la protección de datos en la nube. (Desde la perspectiva del cliente contratante.)
Accesible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf	
Orientaciones para prestadores de servicios de Cloud Computing	
Organización responsable	Gobierno de España, Ministerio de Justicia, Agencia Española de Protección de Datos
Finalidad	Proporcionar a los CSPs una guía orientativa.
Enfoque(s) principal(es)	Guía de carácter complementario de la Guía para clientes que contraten servicios de Cloud Computing. (Desde la perspectiva de los CSPs.)
Accesible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf	

Tabla 7. Guías de uso para el entorno de servicios en la nube.

Tal y como es posible observar en la Tabla 7, es evidente que, las guías presentadas se incluyen las siguientes especificaciones, tales como: conocimiento básico sobre los servicios en la nube, protección de datos, guía desde la perspectiva del cliente contratante y la misma, pero desde el punto de vista de los CSPs. En la siguiente Tabla 8, se presentarán una serie de códigos de buenas prácticas.

CÓDIGOS DE BUENAS PRÁCTICAS	
CSA Cloud Control Matrix	
Organización responsable	Cloud Security Alliance
Finalidad	Ofrecer una serie de principios de seguridad para los CSPs y ayudar a los clientes en la valoración del riesgo de seguridad antes de contratarse con un servicio en la nube.
Contenidos	Normalización de las expectativas de seguridad, la taxonomía de la nube, la terminología y las medidas de seguridad a implementar.
Accesible en: https://cloudsecurityalliance.org/group/cloud-controls-matrix/	
Cloud Industry Forum Code of Practice (CIF COP)	
Organización responsable	Cloud Industry Forum
Finalidad	Obtener un alto nivel de transparencia y confianza para la negociación en la nube.
Contenidos	Un esquema de certificación que contiene varios documentos: resumen ejecutivo, guía para realizar la certificación de primera parte, guía para CSPs, un documento de código de buenas prácticas y otro de términos y condiciones.
Accesible en: https://resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes/code-of-practice	

Tabla 8. Códigos de buenas prácticas para el entorno de servicios en la nube.

En la Tabla 8 podemos observar 2 códigos de buenas prácticas: *Cloud Control Matrix*, elaborado por CSA; y *Cloud Industry Forum Code of Practice*, elaborado por *Cloud Industry Forum*. En la última tabla se presentarán una serie de productos de certificaciones de sistema.

CERTIFICACIONES DE SISTEMA	
ISO 20000-1:2011 Service Management System, Requirements	
Organización responsable	International Organization for Standardization
Finalidad	Exigir el cumplimiento de una serie de requisitos en el diseño, transición, provisión y la mejora de los servicios TIC.
Accesible en: http://www.iso.org/iso/catalogue_detail?csnumber=51986	
Cloud Security Alliance Open Certification Framework	
Organización responsable	Cloud Security Alliance
Finalidad	Certificación basada fundamentalmente en la confianza para los CSPs.
Accesible en: https://downloads.cloudsecurityalliance.org/initiatives/ocf/OCF_Vision_Statement_Final.pdf	
Cloud Security Alliance Security, Trust & Assurance Registry	
Organización responsable	Cloud Security Alliance
Finalidad	Un modelo de certificación de CSP.
Accesible en: https://cloudsecurityalliance.org/star/	
EuroCloud Star Audit	
Organización responsable	EuroCloud
Finalidad	Un modelo de certificación de CSP enfocado en el cumplimiento de los requisitos contractuales, técnicos y organizativos.
Accesible en: https://staraudit.org/	
Payment Card Industry Data Security Standard	
Organización responsable	Payment Card Industry (PCI) Security Standard Council
Finalidad	Una normativa de cumplimiento obligatorio para la gestión, el trámite y/o almacenamiento de datos de tarjeta de crédito

Accesible en: https://es.pcisecuritystandards.org/pci_security/	
Statement on Standards for Attestation Engagements No. 16	
Organización responsable	American Institute of Certified Public Accountants (AICPA)
Finalidad	Una normativa de análisis y evaluación para realizar las verificaciones del cumplimiento de los requisitos y su eficacia para evaluar el grado de adecuación de los controles internos de la prestación de servicios por la organización.
Accesible en: http://ssae16.com/SSAE16_overview.html	

Tabla 9. Certificaciones de sistema para el entorno de servicios en la nube.

Mediante la información presentada en la Tabla 9, podemos observar que, los productos de certificaciones de sistema se han centrado en los siguientes aspectos: la optimización de los servicios TIC; la confianza, los requisitos contractuales, técnicos y organizativos para los CSPs; la gestión, el trámite y/o almacenamiento de datos de tarjeta de crédito; las verificaciones del cumplimiento de los requisitos y su eficacia para la evaluación del grado de adecuación de los controles internos de la prestación de servicios por la organización.

La observación de la información presentada en las tablas (Tabla 5 – Tabla 9), favorece una visión general de esta clase de normativas y productos certificadores, a la cual deben añadirse los contenidos explicados detalladamente en los apartados anteriores referentes a la ISO/IEC 27018, la ISO/IEC 27017, la LOPD y el RDLOPD, sobre los marcos de referencia aplicables al entorno de servicios en la nube.

Como se ha expresado en el conjunto de tablas, en cuanto a las normativas relativas al mismo, dispone de varias categorías de documentos regulatorios: destacan el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad, como legislaciones aplicables; CSA *Cloud Control Matrix* y *Cloud Industry Forum Code Of Practice* (CIF COP), como códigos de buenas prácticas; CCN STIC 823 Guía de seguridad de las TIC, utilización de servicios en la nube, Article 29 WP 196, Guía APD para clientes que contraten servicios de *Cloud Computing*, Guía APD para prestadores de servicios de *Cloud Computing*, como guías de uso; ISO 20000-1:2011 *Service Management System, Requirements, Cloud Security Alliance Open Certification Framework* (CSA OCF), *Cloud Security Alliance Security, Trust and Assurance Registry* (CSA STAR), *Eurocloud Star Audit*, *Payment Card Industry Data Security*

Standard (PCI DSS), *Statement on Standards for Attestation Engagements 16* SOC1, SOC2, SOC3 (SSAE 16 1-2-3), *Cloud Security Alliance Security*, *Certificate of Cloud Security Knowledge* (CSA CCSK) y *Cloud Security Alliance Security*, *Certificate of Cloud Security Professional* (CSA CCSP), como productos de certificaciones asociadas. Así, las seis últimas (Tabla 9) se reconocen como certificaciones de sistema mientras que las dos primeras (Tabla 6) se tratan de certificaciones profesionales.

2.4 Conclusiones del capítulo 2

Mediante el capítulo 2, se presentan los marcos de referencia aplicables al entorno de servicios en la nube, tanto desde la perspectiva internacional, como centrándonos en la situación nacional de España.

En cuanto a las conclusiones del presente capítulo, destacamos, por un lado, la existencia de una diversidad de normativas o/y productos de certificaciones en las que incluyen los aspectos fundamentales que se deben tener en cuenta tanto por el responsable del tratamiento de datos (el cliente) como por el encargado (el CSP) en las actividades comerciales y en los procesos de contratación en el entorno de servicios en la nube.

A su vez, se han determinado los requisitos que se deben cumplir obligatoriamente por ambas partes para que ese entorno sea más normalizado y se aseguren o garanticen los derechos del cliente y el CSP. Por otro lado, estos marcos de referencia, a pesar de disponer de un número amplio de estándares a esta materia, en su mayoría no son específicas de la nube. Según *Cloud Security Alliance España* (2015, p. 9), existe un número relevante de los marcos de referencia que se tratan de “ámbitos TIC de forma general, y las organizaciones lo adoptan para un entorno en la nube”.

A pesar de que el *cloud computing* aporta numerosas ventajas, se observa una serie de riesgos especialmente relacionados con el almacenamiento externo de datos de clientes. Los CSPs requieren cierto nivel de acceso a la información del cliente contratado para poder prestarle los servicios en la nube. Por lo tanto, es muy importante que el cliente sea capaz de confiar en su CSP para tratar sus datos de forma confidencial y respetar su privacidad. Para ello, se requiere que el cliente sea informado sobre los niveles de seguridad y que el CSP disponga de una certificación de seguridad adecuada. Esto es, que ambas partes cumplan sus obligaciones exigidas en tanto las normativas comentadas en este capítulo como las futuras regulaciones, para que los servicios en la nube cumplan su función.

Visto los capítulos 1 y 2, hemos conocido tanto el concepto básico de *cloud computing* como su marco jurídico-normativo en el que se ubica. A continuación, en el capítulo 3 pasaremos a comentar la situación actual del uso de los servicios en la nube y a

centrarnos específicamente en algunas aplicaciones prácticas basadas en la misma sobre la gestión de la información, para poder detectar sus puntos fuertes, así como los aspectos que podrán servir de ejemplo para esa materia.

"Forget about IT as you know it today."

- R. J. Moore

CAPíTULO 3
LA NUBE DEL PRESENTE

En este capítulo se explicarán, tanto la situación actual del uso de la tecnología de la nube como los nuevos productos basados en la misma para mejorar la gestión de la información, con el fin de detectar sus puntos fuertes, así como la actitud sobre la tecnología de la nube que mantienen las empresas.

3. Capítulo 3: La nube del presente

Una de las características del *cloud computing* del presente, por la que se distingue de la TI tradicional, es el modelo innovador de servicios prestados en la nube. Es decir, en vez de destacar los productos informáticos (las aplicaciones), se enfatiza más la calidad de los servicios.

Actualmente, es posible afirmar que el *cloud computing* no solo ha reducido la necesidad de la red, sino que también ha cambiado la función del ordenador. Dado que ya no hace falta que los terminales informáticos prioricen el funcionamiento concreto de las aplicaciones, por lo tanto, resultará más fácil reajustarlas. La alta capacidad de escalabilidad se puede considerar como una de las características más llamativas del *cloud computing*. El despliegue y la realización de las aplicaciones en el servidor podrá facilitar, por un lado, el compartimiento de datos entre distintos tipos de terminales; mientras que, por otro lado, favorecerá la interacción entre los usuarios y los terminales de una forma uniforme (como por ejemplo, a través del navegador web).

3.1 Panorama internacional de las tecnologías del *cloud computing* y el estado de la industria

En el presente subapartado pasamos a comentar las estrategias principales de la nube (por ejemplo, sobre el sector público, el mercado, etc.) que han desarrollado en distintos países y el estado de desarrollo de una serie de empresas, con el fin de ofrecer un panorama internacional sobre esta materia.

3.1.1 Los últimos avances de Estados Unidos, la Unión Europea y Australia

- **Estados Unidos**:
  1. Posicionar la tecnología del *cloud computing* y su industria como uno de los medios más importantes para mantener la competitividad nuclear nacional.

  2. Atendiendo a una serie de políticas asociados al *cloud computing* establecida por EEUU, se indican expresamente la necesidad del incremento de compras del sector público y el desarrollo activo del mercado.

  3. El Ejército de EEUU (Fuerza Aérea y la Armada), el Ministerio de Justicia, Ministerio de Agricultura, Ministerio de Educación y otros departamentos se han incorporado los servicios en la nube.

4. El contenido del documento *Federal Cloud Computing Strategy*[17], publicado en el año 2011, consiste en:
   - Fomentar la innovación,
   - Desarrollar activamente el mercado
   - Construir un ecosistema de *cloud computing* y promover un desarrollo coordinado de la industria de la nube.

- **Destacamos:**
  Tal y como es posible observar, EEUU ha concedido una gran importancia a la tecnología del *cloud computing* en las estrategias nacionales de desarrollo, así como el papel nuclear que puede desempeñar el mercado.

➢ **La Unión Europea**

1. En 2012, la Comisión Europea lanzó la estrategia *Unleashing the potential of cloud computing in Europe*[18], en el que se destacan los siguientes aspectos:
   - Reducir y simplificar numerosas normas y/o estándares técnicos.
   - Establecer una serie de normas y/o estándares sobre la seguridad y justicia.
   - Aclarar las políticas de mercado.
   - Construir un mercado europeo del *cloud computing.*
   - Promover a que los CSPs amplíen al alcance de sus servicios en la nube y que proporcionen servicios de gestión de la información *online* de buena relación calidad-precio.

2. El documento *A Digital Single Market Strategy for Europe*[19], adoptado en 2015, tiene como objetivo crear oportunidades digitales para las personas y empresas, y mejorar la posición de Europa como líder mundial en la economía digital. Esta estrategia dispone de 16 iniciativas que se entregarán a finales de 2016, incluyendo el lanzamiento del *European Cloud Initiative* con el fin de fomentar la confianza y la confidencialidad del *cloud computing* en Europa.

   El *European Cloud Initiative* incluye las siguientes iniciativas:
   - Proporcionar soluciones para las certificaciones dentro del territorio europeo, incluyendo elementos de web y la seguridad de información.
   - Protección de datos personales.

[17] Documento accesible en:
https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf
[18] Documento accesible en:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[19] Documento accesible en:
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192

- Acuerdos sobre niveles de servicio.
- Interoperabilidad y portabilidad de datos.
- Condiciones y cláusulas contractuales.
- Previsión de la capacidad de los servicios en la nube en Europa.
- El establecimiento de un *European Research Open Science Cloud.*

- **Destacamos:**
  Al diferenciarse de las estrategias adoptadas por EEUU, además de la construcción activa de un mercado de servicios en la nube, la UE se enfoca especialmente en las cuestiones sobre la seguridad de la información, así como la normalización de dichos servicios.

➢ **Australia**

1. En 2011, el *Australian Government Information Management Office* (AGIMO) publicó el documento *Australian Government Cloud Computing Policy: Maximising the Value of Cloud*[20]. Posteriormente, en el mayo de 2013 y en el octubre de 2014, se actualizó y se publicó la versión 2.0 y 3.0. Dicho documento es de carácter orientativo sobre el uso de los servicios en la nube por parte de los departamentos gubernamentales, incluyendo las legislaciones asociadas, los apoyos financieros, las especificaciones de seguridad, etc.

2. En 2013, el AGIMO publicó el documento *The Australian Public Service Big Data Strategy: Improved understanding through enhanced data-analytics capability*[21], cuyo contenido se basa en 6 principios del *big data*, y tiene como objetivo promover que el sector público realice la reforma de servicios mediante el análisis del *big data*, así como la mejora de las políticas públicas.

3. Igualmente, en 2013, el gobierno de Nueva Gales del Sur publicó el documento *NSW Government Cloud Services Policy and Guidelines*[22], con el fin de mejorar las operaciones y servicios gubernamentales y reducir los costos operativos a través de una tecnología más flexible y fiable.

[20] Documento disponible en:
http://www.finance.gov.au/files/2012/04/Australian-Government-Cloud-Computing-Policy-Version-2.0.pdf

[21] Documento disponible en:
https://www.finance.gov.au/files/2013/06/Draft-Big-Data-Strategy.pdf

[22] Documento disponible en:
https://11217-presscdn-0-50-pagely.netdna-ssl.com/wp-content/uploads/2013/09/NSW-Government-Cloud-Services-Policy-and-Guidelines.pdf

- **Destacamos:**
  En Australia, el sector público ha desempeñado un rol importante en el desarrollo de la nube, ya que, de acuerdo con las políticas introducidas sobre los servicios en la nube en los últimos años, en su mayoría están orientadas a ello.

Tras la revisión de los 3 casos internacionales, es evidente que muchos países y/u organizaciones internacionales han reconocido la importancia de las tecnologías de la nube y su papel en la competencia tecnológica internacional. No obstante, las estrategias sobre la misma que ha adoptado cada país se diferencian, dependiendo de las políticas nacionales de desarrollo.

3.1.2 La situación de desarrollo de las empresas

- **Amazon**
  Amazon Web Service (*AWS*) lanzó su "escritorio como servicio" (DaaS) *WorkSpaces*[23], con el fin de seguir ampliando su ecosistema de la nube. Cada escritorio necesita la CPU, memoria, almacenamiento, red y la GPU, y AWS los puede ofrecer todos.

- **Destacamos:**
  Amazon sigue construyendo su propio ecosistema de la nube, integrándole todos los elementos imprescindibles o complementarios proporcionados por sí mismo.

- **Microsoft**
  En 2013, Microsoft lanzó el sistema operativo basado en la nube *Cloud OS*, en el que se incluía una serie de productos y servicios en la nube de clase empresarial, tales como: *Windows Server 2012 R2*, *System Center 2012 R2* y *Windows Azure Pack*.[24]

  Windows Azure[25] es un sistema operativo de servicios en la nube y puede servir para el desarrollo, alojamiento de servicios y el entorno de gestión de servicios. Dicho sistema operativo puede ofrecer un entorno de almacenamiento y de

[23] Más información en: https://aws.amazon.com/es/workspaces/?nc1=h_ls

[24] Las últimas versiones son *Windows Server 2016* y *System Center 2016*.

[25] Más informacion en: http://www.microsoft.com/es-es/server-cloud/products/windows-azure-pack/overview.aspx

cálculo bajo demanda para los desarrolladores para que puedan alojar, ampliar y gestionar aplicaciones Web en Internet a través del centro de datos de Microsoft.

- **Destacamos:**
  Es evidente que en los últimos años Microsoft ha lanzado varios productos y/o servicios en la nube. Siendo una compañía dedicada al desarrollo del software, Microsoft ha sido muy consciente de la tendencia mundial del desarrollo de la nube en los últimos años, y a su vez ha realizado un ajuste oportuno de su estructura industrial.

➢ **IBM**

En 2013, IBM lanzó una serie de servicios en la nube privada basada en *OpenStack*[26] y otros estándares de la nube, y desarrolló una aplicación del almacenamiento en la nube *InterCloud*, en la cual los usuarios pueden realizar la migración de datos entre varias nubes. Esta aplicación tiene como fin ofrecer una mejor protección de información y hacer el *cloud computing* más flexible.

En diciembre de 2013, IBM adquirió la empresa Aspera[27]. Además de aportar la seguridad y la previsibilidad, Aspera aporta una forma de transferencia de datos de gran volumen basada en *cloud computing* más rápida, más previsible y de mejor relación calidad-precio, con prestaciones tales como: copia de seguridad del almacenamiento de la empresa, intercambio de imagen virtual o un acceso rápido a la nube para aumentar la capacidad de procesamiento.

- **Destacamos:**
  IBM ha prestado mucha atención a garantizar la seguridad de los productos y/o servicios en la nube, así como un mejor rendimiento de ellos.

➢ **Oracle Corporation**

A finales de 2013, la compañía Oracle Corporation anunció convertirse en patrocinador de la Fundación *OpenStack*, con el fin de integrar los componentes de gestión de la nube ofrecidos por *OpenStack* a sus propios productos[28], y promover la compatibilidad entre *OpenStack* y los servicios en la nube

[26] Más información en: https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W21ed5ba0f4a9_46f4_9626_24cbbb86fbb9

[27] Más información en: http://www-03.ibm.com/press/us/en/pressrelease/42782.wss

[28] Oracle Solaris, Oracle Linux, Oracle VM, Oracle (IaaS), Oracle ZS3, Axiom, StorageTek, etc.

proporcionado por Oracle Corporation[29].

En 2016, Oracle Corporation ha realizado varias adquisiciones que podrían llamar la atención, tales como se muestran a continuación:

- En el 29 de abril de 2016, Oracle Corporation adquirió la compañía Textura, empresa dedicada a la gestión de contratos y pagos en la nube para el área de la construcción, por un valor de 663 millones de dólares.[30]

- En el 4 de mayo de 2016, Oracle Corporation adquirió la compañía Opower, reconocido como el proveedor líder de los servicios en la nube en el sector público, por un valor de 532 millones de dólares.[31]

- En el 28 de julio de 2016, Oracle Corporation adquirió la compañía NetSuite, empresa de software en la nube, por un valor de 9.300 millones de dólares.[32]

- **Destacamos:**
  A partir de las adquisiciones de empresas realizadas por Oracle Corporation en 2016, se pueden observar que, dicha compañía también ha reconocido el cambio de las necesidades del mercado en el ámbito de los servicios y/o productos informáticos, así como el papel que han desempeñado los servicios en la nube en los últimos años. Conocido como una de las compañías más famosas en el desarrollo de software y de bases de datos, Oracle Corporation ha seguido la tendencia de la nube y sigue manteniendo su competitividad nuclear.

➢ **Otras compañías importantes**

- **HP** presenta una nueva serie de servicios en la nube basados en la plataforma *HAVEn*, de análisis del *big data*[33]. HP ofrece servicios de distintos campos, incluyendo soluciones de análisis del *big data* de forma extremo a extremo, inteligencia de clientes, cadena de suministro, operaciones, análisis de datos de sensores, etc.

- **DELL** lanza su aplicación cliente *Dell Wyse*[34], para poder proporcionar a las

[29] Exalogic, servicios del *cloud computing* de Oracle, servicios del almacenamiento en la nube de Oracle, etc.

[30] Fuente: https://www.oracle.com/corporate/pressrelease/oracle-buys-textura-042816.html
[31] Fuente: https://www.oracle.com/corporate/pressrelease/oracle-buys-opower-050216.html

[32] Fuente: https://www.oracle.com/corporate/acquisitions/netsuite/index.html

[33] Más información en: http://www8.hp.com/es/es/software-solutions/big-data-platform-haven/

[34] Más información en: http://www.dell.com/us/business/p/cloud-client

compañías como Citrix, Microsoft, VMware todo tipo de soluciones de virtualización de escritorio de forma extremo a extremo y de característica segura, eficaz y gestionable.

- **AT&T** ofrece servicios en la nube bajo demanda para las empresas[35]. Se pueden configurar y desplegar servicios de plataforma, capacidad de cálculo o virtualización dependiendo de las necesidades de los clientes sobre la seguridad, gestión y rendimiento.

- **CA Techologies** lanza servicios del almacenamiento en la nube exclusivamente enfocándose en el *System z*. Mediante la realización de la copia de seguridad almacenada en la nube, CA Techologies consigue ayudar a su cliente a reducir el coste del tratamiento de datos (como por ejemplo, en el IBM *System z*).[36]

- **Rackspace**, siendo el creador de la plataforma del *cloud computing* de código abierto *OpenStack*, adquirió a finales de 2013 la empresa israelita de las tecnologías de la nube ZeroVM[37]. Dicha empresa tiene productos como *hypervisor*, que son especializados en la nube y que están diseñando teniendo en cuenta las fortalezas y limitaciones del *cloud computing*.

- **Destacamos:**
  Al revisar los últimos movimientos estratégicos de las compañías más prestigiosas en el mercado de la TI, se pueden observar que, en los últimos años, los servicios asociados a las tecnologías de la nube han ocupado una posición imprescindible en sus objetivos estratégicos, bien por la variedad de nuevos servicios basados en la nube lanzados recientemente, o bien por las actividades de adquisición de otras compañías para fortalecer su competitividad en el mercado. El cloud computing y sus productos/servicios se están convirtiendo en la corriente principal del mercado de la TI.

A través de la realización de este subapartado, tal y como índica su título, hemos tenido una visión general sobre las políticas nacionales de la nube de algunos países, así como el estado de desarrollo y de aplicación de la misma. Además, a partir de los casos, hemos realizado breves análisis sobre en qué realmente consiste y cuáles son las razones por las que se adquieren otras compañías para fortalecer sus propias

[35] Más información en: https://www.business.att.com/enterprise/Portfolio/cloud/
[36] Más información en: http://www.ca.com/us/~/media/Files/SolutionBriefs/1368-mfsuite-ibm-rational-dev-sys-zunit-test-sb-final.pdf

[37] Más información en: http://www.zerovm.org/

estructuras industriales, cambios de políticas de la nube para promover la competitividad nuclear nacional, o bien desarrollar nuevos productos y/o servicios para mantener la cuota del mercado. Todo ello apunta hacia una realidad: el *cloud computing* y sus productos auxiliares se han convertido en esenciales en la era digital.

3.2 Tendencia del desarrollo del *cloud computing* basada en la estadística

Visto el subapartado anterior, en el presente subapartado analizaremos el informe de investigación realizado por RightScale[38] para detectar las distintas perspectivas de la tendencia del desarrollo y de la aplicación del *cloud computing* de hoy en día.

3.2.1 El informe de investigación de RightScale

A principios del año 2016, RightScale publicó el informe de investigación anual *State of the Cloud*, demostrando la tendencia de la adopción y la aplicación del *cloud computing*.

RightScale es una compañía de servicios de gestión de multi-nube, y empezó dicha investigación en enero del año 2016, con un total de 1.060 encuestados. Entre ellos, el 61% es de América del Norte. En la mayoría de los 1.060 encuestados, el 41% es de empresas grandes (más de 1.000 empleados) y el 59%, de pequeñas y medianas (menos de 1.000 empleados). Además, más de la mitad de los encuestados se dedican a las TIs o a trabajos de operación/mantenimiento, mientras que el resto, de departamentos de desarrollo o de negocio.

El informe de investigación ha mostrado una serie de conclusiones interesantes sobre la última tendencia desde las distintas perspectivas del *cloud computing,* tales y como se muestran a continuación:

[38] Más información en: https://www.rightscale.com/lp/state-of-the-cloud?campaign=701700000015euh; ver informe completo en: http://assets.rightscale.com/uploads/pdfs/RightScale-2016-State-of-the-Cloud-Report.pdf

- **La adopción de la nube híbrida se ha incrementado**

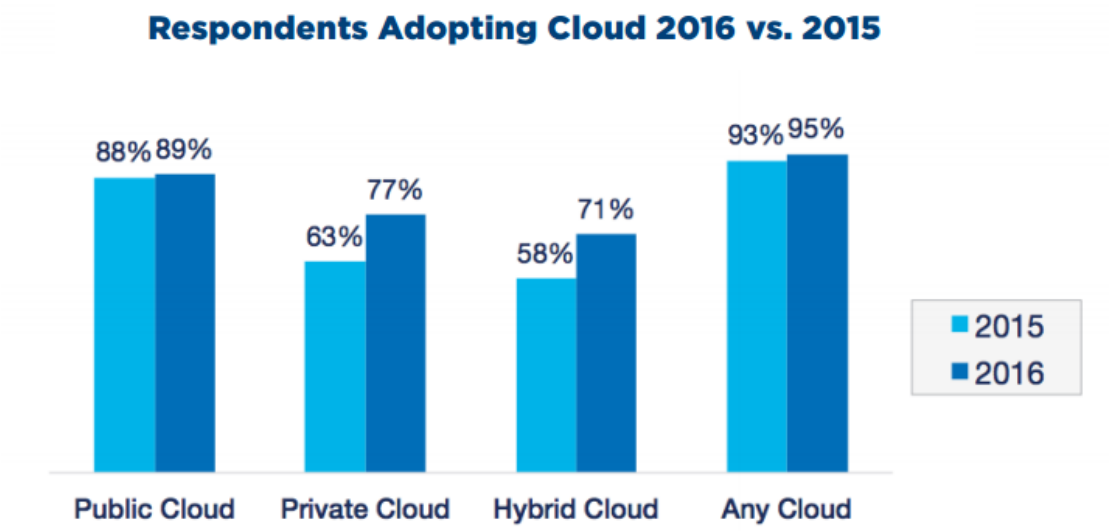

Gráfico 1. Adopción de la nube por los encuestados.
Fuente: *RightScale 2016 of the Cloud Report.*

En el Gráfico 1 podemos observar que, la adopción de la nube híbrida ha experimentado un gran incremento entre el año 2015 y 2016. El 95% de los encuestados está utilizando servicios del *cloud computing*; este porcentaje se ha aumentado ligeramente en comparación con el 93% observado en el año 2015.

El porcentaje de la utilización de la nube pública solo ha aumentado un 1%, mientras que el de la nube privada se ha incrementado un 14%. Como consecuencia, gracias al porcentaje del incremento de la utilización de la nube privada, el de la nube híbrida también ha aumentado desde un 58% hasta un 71%, ya que se define la misma como la que utiliza simultáneamente el espacio de compartición de recursos de los otros dos modelos de la nube.

- **El uso de plataformas de la nube**

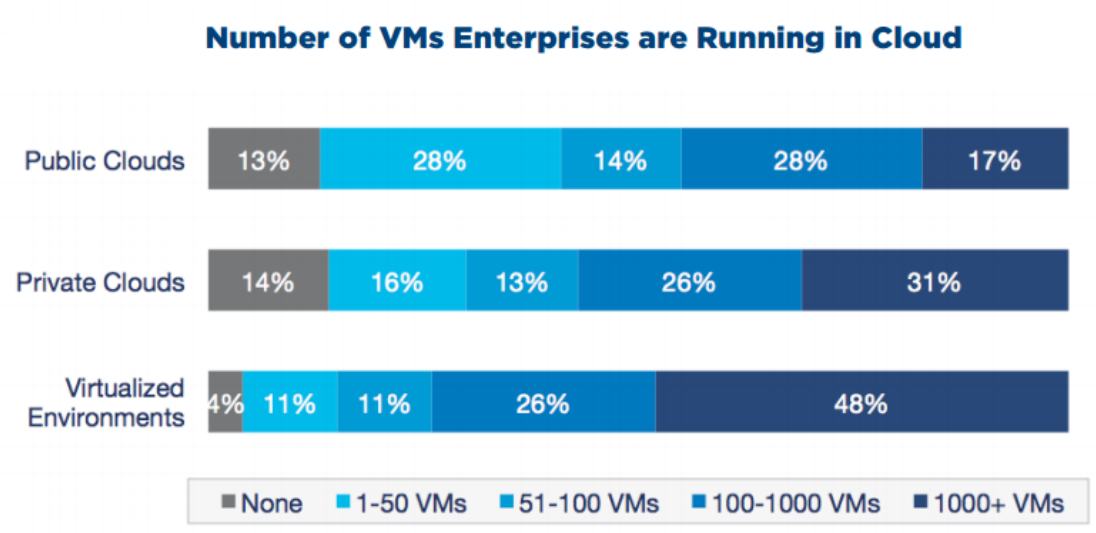

Gráfico 2. Número de máquinas virtuales que procesan en la nube.
Fuente: *RightScale 2016 of the Cloud Report.*

Atendiendo al informe, el promedio del número de las plataformas de la nube que utiliza cada empresa encuestada es un 6, cuando las 3 son plataformas de la nube pública y otras 3, son las de la nube privada.

De acuerdo con el Gráfico 2, en el año 2016, existen más del 17% de las empresas encuestadas que han desplegado más de 1.000 máquinas virtuales en la plataforma de la nube pública, cuando ese porcentaje en 2015 era de un 13%[39]. Asimismo, el porcentaje de la nube privada también ha aumentado de un 22% hasta un 31%, lo que podrá significar que las cargas de trabajos empresariales se están transfiriendo gradualmente a las plataformas de la nube.

Igualmente, el porcentaje del despliegue de las máquinas virtuales en entornos virtuales por parte de las empresas encuestadas se ha incrementado de un 42% hasta un 48%, lo que podrá causar también el aumento de la utilización de las plataformas de la nube privada, ya que, de acuerdo con lo que se indica en el informe, éstas podrían ser mejoradas o promovidas a partir de los entornos virtuales.

[39] Ver el informe completo del año 2015 en: http://assets.rightscale.com/uploads/pdfs/RightScale-2015-State-of-the-Cloud-Report.pdf

- **Falta de recursos y conocimientos**

Top 5 Challenges Change with Cloud Maturity

Place	Cloud Beginners	Cloud Explorers	Cloud Focused
#1	**Lack of resources/ expertise** (38%)	**Lack of resources/ expertise** (34%) ↑ 3	**Lack of resources/ expertise** (26%) ↑ 5
#2	**Security** (35%)	Compliance (32%)	Building a private cloud (19%)
#3	Compliance (34%)	Managing costs (30%)	Managing costs (18%)
#4	Managing multiple cloud services (30%)	**Security** (28%) ↓ 2	Managing multiple cloud services (18%)
#5	Governance/Control (29%)	Managing multiple cloud services (26%)	**Security** (17%) ↓ 4

Gráfico 3. Los primeros desafíos cambian a medida que se madura la nube.
Fuente: *RightScale 2016 of the Cloud Report.*

El problema de la seguridad ha sido una de las principales causas por la que los equipos de la TI desconfían de la nube pública desde hace mucho tiempo. Sin embargo, ese fenómeno ha sido sustituido por la falta de recursos y conocimientos de la nube.

Tal y como se muestra en el Gráfico 3, "*Lack of resources/expertise*[40]*"* se ha convertido en el primer desafío al utilizar el *cloud computing*. A pesar de que las empresas grandes tienen más preocupaciones sobre las cuestiones asociadas a la seguridad que las empresas pequeñas y medianas, también habría que tener en cuenta que, entre las primeras, el porcentaje de las que consideran la seguridad como un reto principal se ha reducido de un 47% hasta un 37% en los últimos dos años.[39]

Los encuestados en diferentes etapas de madurez (*Cloud Beginners, Cloud Explorers, Cloud Focused*) del *cloud computing* han ordenado los principales retos cuando lo utilizan. Aunque sus *feedbacks* varían, la falta de recursos/conocimientos del *cloud computing* ha ocupado la primera posición.

[40] Traducción al español: Falta de recursos/conocimientos

- **El incremento del número de empresas que adoptan *DevOps***

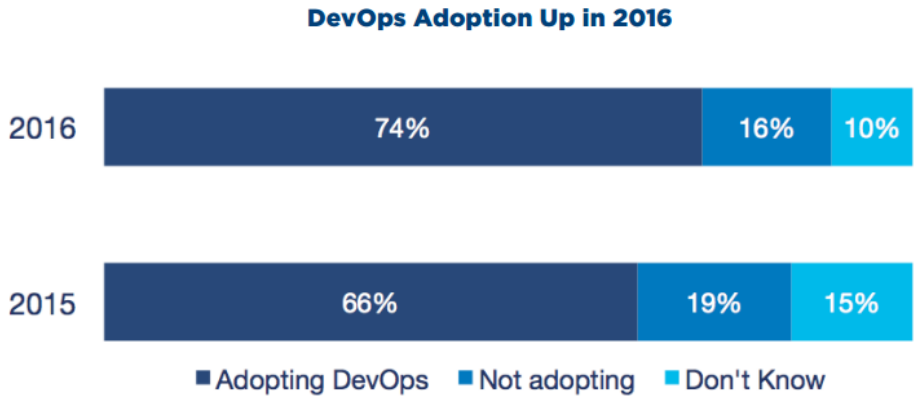

Gráfico 4. Adopción de *DevOps* en 2016 y 2015.
Fuente: RightScale 2016 of the Cloud Report.

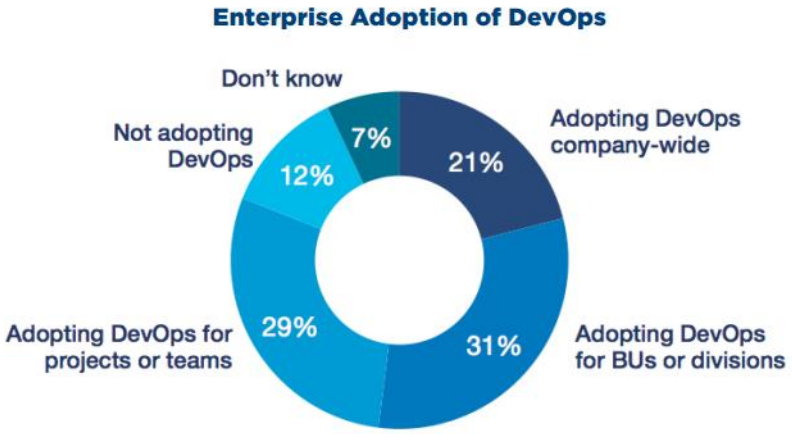

Gráfico 5. Empresas que adoptan *DevOps*.
Fuente: *RightScale 2016 of the Cloud Report*.

De acuerdo con Debois (2011), *DevOps* es un acrónimo inglés de *Development* y *Operations*, cuyo contenido hace referencia a una cultura de comunicación y colaboración entre los desarrolladores de aplicaciones (*Dev*) y los trabajadores de operaciones/mantenimiento (*Ops*) en las TIs cuando automatizan los procesos de la entrega de software y el cambio de infraestructura. Esa cultura tiene como objetivo establecer un entorno en el que los trabajos de construcción, prueba y publicación del software puedan ser más rápidos, frecuentes y de forma más fiable.

En el Gráfico 4 podemos observar que, el porcentaje de la adopción de *DevOps* se ha incrementado desde un 66% en 2015 hasta un 74% en 2016, por lo que significa que, muchas empresas han prestado atención a esa cultura de trabajar con el fin de mejorar el rendimiento empresarial.

No obstante, no debería olvidarse de que, el grado de adopción de *DevOps* entre las empresas varía mucho. Solamente el 21% de las empresas ha adoptado *DevOps* a nivel empresarial, mientras que el resto solo lo adopta en las unidades de negocio o en los equipos de trabajo.

- **La adopción de la nube pública entre las empresas grandes, pequeñas y medianas**

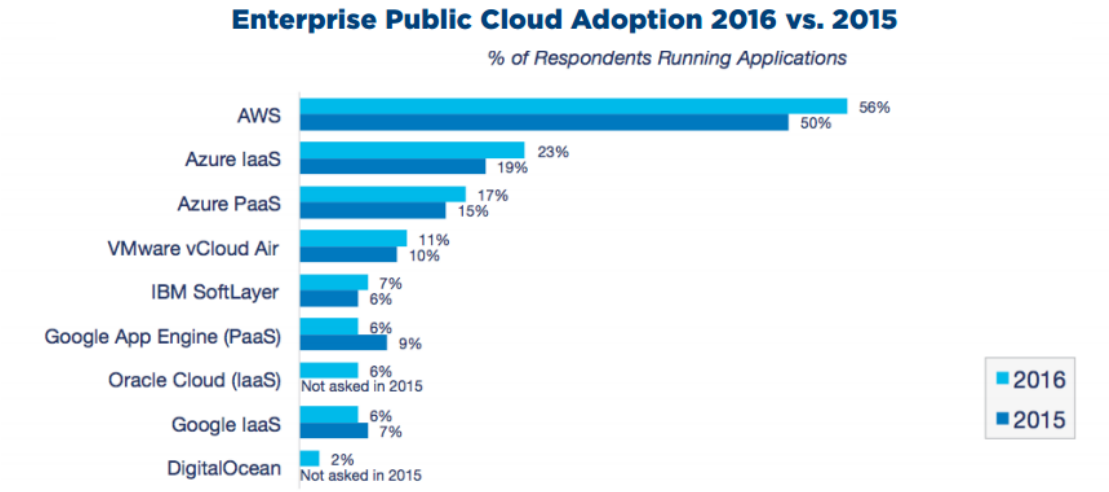

Gráfico 6. Comparación de la adopción de la nube pública en las empresas grandes entre los años 2015 y 2016.
Fuente: *RightScale 2016 of the Cloud Report.*

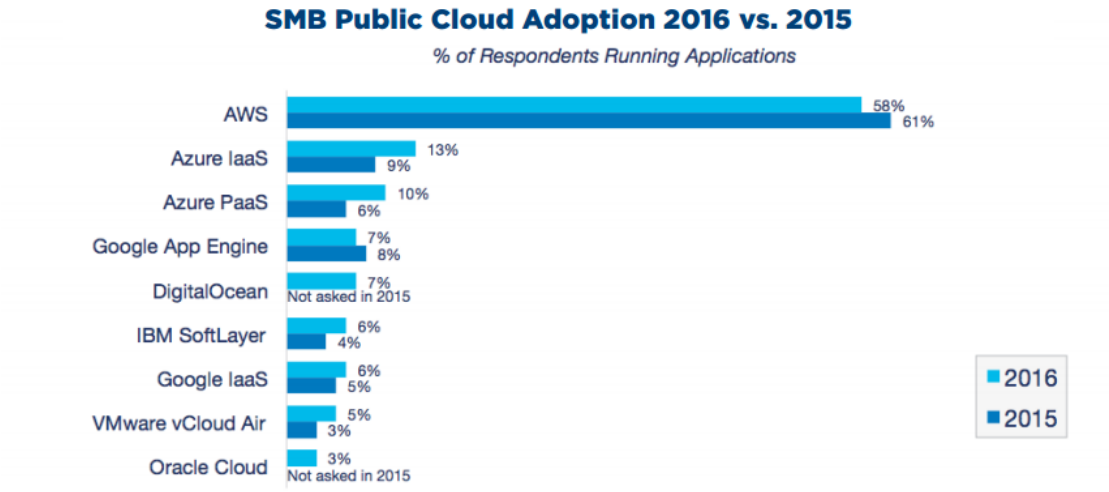

Gráfico 7. Comparación de la adopción de la nube pública en las empresas pequeñas y medianas entre los años 2015 y 2016.
Fuente: *RightScale 2016 of the Cloud Report.*

Tal y como es posible observar, en el Gráfico 6 y 7 se encuentran muchos productos/servicios de la nube pública que están comentados o mencionados en los apartados anteriores. *AWS* sigue siendo la primera opción de los consumidores de la nube pública. Sin embargo, el porcentaje de adopción de *Microsoft Azure* ha experimentado un incremento significativo durante los últimos años.

AWS ha tenido la mayor cuota del mercado entre las empresas grandes y ha obtenido

un incremento del 6%. No obstante, entre las pequeñas y medianas, el porcentaje de adopción de *AWS* se ha reducido ligeramente, mientras que el de *Microsoft Azure* ha aumentado. Asimismo, las preferencias de los CSPs por parte de las empresas grandes, pequeñas y medianas también son distintas. De acuerdo con el Gráfico 6 y 7, aunque ambos *AWS* y *Microsoft Azure* son sus primeras opciones, la segunda preferencia de las empresas grandes se inclina a *VMware vCloud Air* y *IBM SoftLayer*, mientras que para las empresas pequeñas y medianas son *Google App Engine* y *DigitalOcean*.

- **La adopción de la nube privada entre las empresas grandes, pequeñas y medianas**

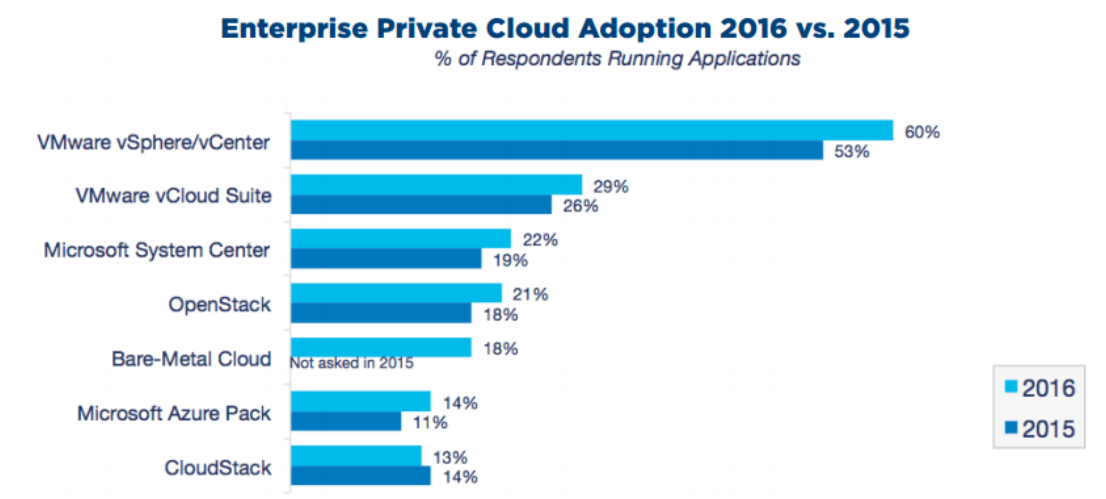

Gráfico 8. Comparación de la adopción de la nube privada en las empresas grandes entre los años 2015 y 2016.
Fuente: *RightScale 2016 of the Cloud Report.*

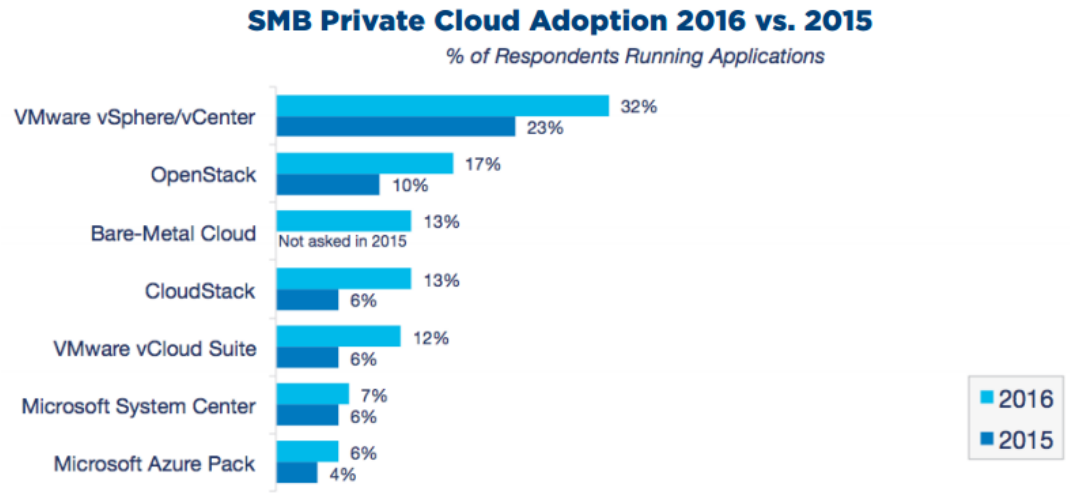

Gráfico 9. Comparación de la adopción de la nube privada en las empresas pequeñas y medianas entre los años 2015 y 2016.
Fuente: *RightScale 2016 of the Cloud Report.*

A pesar de que la nube pública tiene muchos clientes, la nube privada aún mantiene su cuota del mercado. La investigación de RightScale muestra que, tal y como se pueden observar en el Gráfico 8 y 9, la proporción del cliente de la nube privada está aumentando constantemente, y que ocurre en casi todos los tipos de productos de la nube privada.

En cuanto a la comparación de la selección de productos de la nube privada entre las

empresas grandes, pequeñas y medianas, la primera opción para las empresas grandes es utilizar las tecnologías de *VMware* para construir la nube privada, mientras que *OpenStack* es la cuarta. La proporción de la utilización de la nube privada en las empresas pequeñas y medianas es menor que las empresas grandes, y para ellas *OpenStack* es la segunda opción. Sin embargo, RightScale también indica en en informe que existe una parte de usuarios que considera el entorno de *VMware* como la nube privada, aunque normalmente no se correspondería con la definición exacta de la misma.

- **El rol del departamento central de la TI**

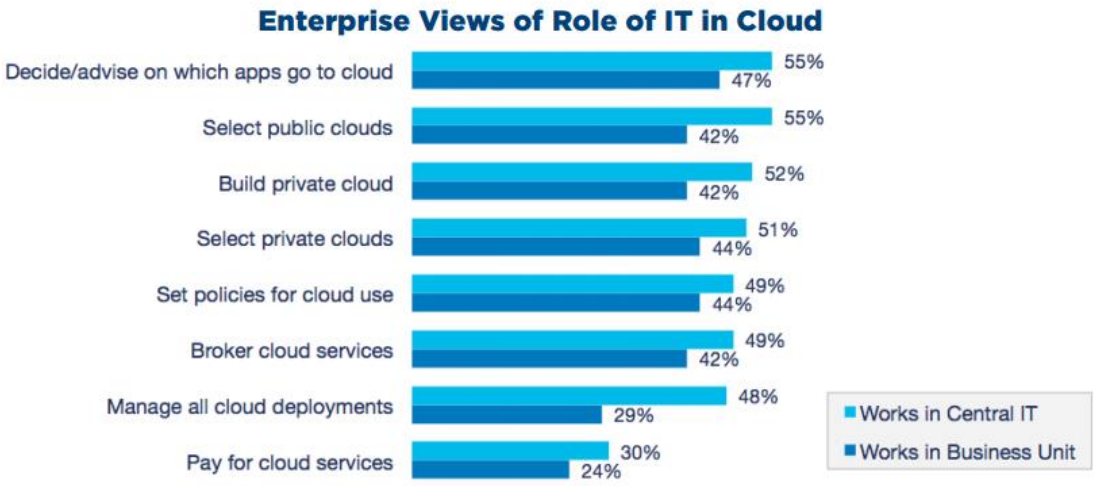

Gráfico 10. La visión de las empresas grandes sobre el rol del departamento central de la TI en la nube.

Fuente: *RightScale 2016 of the Cloud Report.*

En el Gráfico 10 podemos observar que, el departamento central de la TI está desempeñando un papel cada vez más importante en la toma de decisiones sobre las políticas del *cloud computing*.

Ese fenómeno acontece por variadas razones. Por ejemplo, en numerosas empresas, los que inicialmente utilizan las plataformas de la nube son principalmente los equipos individuales de desarrollo, ya que para desarrollar los proyectos o las aplicaciones tienen que basarse en la nube pública.

A medida que las plataformas empresariales de la nube cada vez se adoptan más ampliamente, el departamento central de la TI empieza a desempeñar un rol de intermediario de los servicios en la nube, con el fin de garantizar la gestión, distribución y el control de los mismos. Sin embargo, atendiendo a los informes de investigación de los últimos años, los encuestados de las unidades de negocio han expresado su disgusto ante la transferencia de los derechos de control al departamento central de la TI.

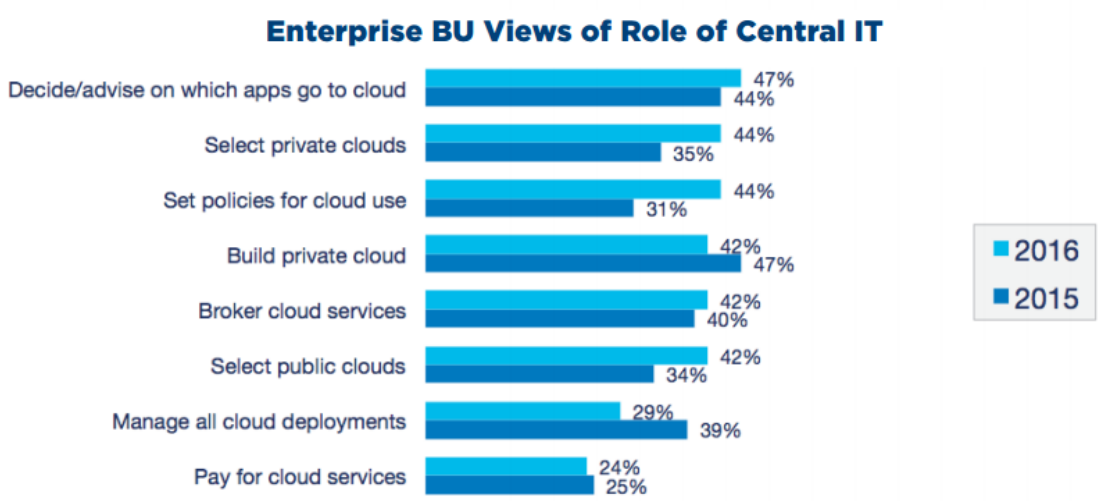

Gráfico 11. La visión de las unidades de negocio en las empresas grandes sobre el rol del departamento central de la TI.
Fuente: *RightScale 2016 of the Cloud Report.*

No obstante, esta animadversión ha mudado durante el último año. Actualmente, el departamento de la TI ha participado insistentemente en la selección de plataformas de la nube, en la construcción de la nube privada, en el establecimiento de políticas de la nube y en la oferta de sugerencias a los otros departamentos sobre esta materia.

Según el Gráfico 11, entre los encuestados de las unidades de negocio, existe un 42% que considera que el departamento central de la TI tiene que seleccionar la nube pública, y un 44% piensa que él tiene que encargarse del establecimiento de las políticas de los asuntos asociados a la nube. Dichas proporciones del año pasado son el 31% y el 34%, frente a las ratios anteriores. También habría que tener en cuenta que, el porcentaje de los encuestados de las unidades de negocio que considera que el departamento central de la TI tiene que gestionar el despliegue de la nube se ha reducido de un 39% hasta un 29%. Quizá lo que podría significar es que los otros equipos prefieren que departamentos ajenos no procesen su propio sistema.

3.2.2 Comentarios

Tras el análisis del informe *State of the Cloud* podemos detectar dos tendencias fundamentales del desarrollo del *cloud computing* en las empresas: la alta proporción de la adopción de la nube pública y el papel que desempeña el departamento central de la TI.

Por un lado, la relación competitiva entre la nube pública y la nube privada está convirtiéndose en una relación complementaria. Es decir, una empresa puede beneficiarse simultáneamente de las ventajas de ambos tipos de nube. De acuerdo con lo que se ha mencionado en el Capítulo 1, estos beneficios pueden ser la seguridad y la fiabilidad en la nube privada, y la compatibilidad y la flexibilidad en la nube pública. Por ejemplo, una empresa puede desplegar los datos o las aplicaciones menos importantes en la nube pública para aprovechar al máximo posible el ahorro del coste y las ventajas en la escalabilidad o compatibilidad, mientras que procesa aquellos que son claves o nucleares en la nube privada para garantizar la seguridad de la información. Además, aunque esas plataformas de la nube son individuales, mediante cierta técnica o estandarización se pueden realizar la migración mutua de datos sin ningún tipo de inconveniente. Por lo tanto, cada vez hay más empresas que adoptan más de un tipo de la nube para la mejora de la eficiencia de la gestión de recursos de la TI, el despliegue del desarrollo de nuevas aplicaciones, así como las necesidades de la automatización de la TI.

Por otro lado, el desarrollo de la nube también ha favorecido enfatizar la importancia del departamento central de la TI, especialmente en convertirse desde un departamento pasivo de apoyo y de servicio e incluso de gasto a un departamento de toma de decisiones. Obviamente, este cambio ha promovido la centralización del poder sobre los asuntos de la nube por parte del mismo y podría causar la insatisfacción de los otros departamentos. Sin embargo, dado que el departamento central de la TI domina una cantidad de datos operativos y sensibles de la empresa y está familiarizado con los procesos de operaciones de negocio, en cierto sentido tiene más competitividad que los otros departamentos. El departamento central de la TI no debería simplemente centralizar el poder de la toma de decisiones sobre los asuntos de la nube, sino que, tendría que liberarse de los servicios básicos de mantenimiento/operación para integrarse en el sistema de negocio nuclear competitivo de la empresa y así poder aportar mayores beneficios.

3.3 Conclusiones del capítulo 3

En este capítulo hemos conocido las últimas tendencias del desarrollo de la nube, tanto sobre las políticas nacionales relacionadas con el sector público de algunos países como la renovación de la estructura industrial de una serie de empresas más prestigiosas del mundo. Además, mediante el análisis del informe de investigación realizado por RightScale sobre la situación de la adopción de los productos/servicios de la nube hemos tenido una visión sobre la tendencia interna de la misma en las empresas grandes, pequeñas y medianas.

Resulta evidente que, en comparación con la TI tradicional, la gestión de la información mediante la nube tiene sus propias ventajas insustituibles tanto en el sector público como en las empresas, tales y como se muestran a continuación:

- **Reducción de costes**
  El precio de los servicios en la nube es muy atractivo. El coste de los servidores, las licencias de software, los gastos de mantenimiento, el espacio de datos, la electricidad y del personal de la TI se puede reducir considerablemente, ya que la forma de utilizarlos es bajo demanda. Esto ha sustituido el alto coste de las inversiones iniciales de la TI. Por lo tanto, el impacto positivo sobre los aspectos financieros del *cloud computing* es obvio.

- **Flexibilidad**
  El *cloud computing* puede ofrecer recursos flexibles para satisfacer a las distintas necesidades de la gestión de la información en nube. Por ejemplo, se pueden añadir más capacidades para procesar cálculos complicados o reducirlas cuando no se necesitan. Por lo tanto, da igual que sea un trabajo ocasional o periódico de gestión de la información, la nube puede adaptarse eficazmente y realizar cantidades de trabajos de tratamiento de datos de forma rápida. Además, la nube puede ofrecer refuerzos a los sistemas tradicionales cuando la necesidad de cálculo excede su capacidad máxima. En comparación, siendo una inversión de capital, los sistemas tradicionales tienen que enfrentarse con los procesos de examen y de ratificación de las adquisiciones, mientras que los servicios de la nube, dado que todo ello se puede virtualizar (los recursos de cálculo como IaaS, la virtualización del desarrollo/prueba/despliegue/operación/mantenimiento de las aplicaciones como PaaS, el desarrollo de software como SaaS, etc.), se podrá considerar como un gasto de operación, por lo que será más fácil de adquirir, con el fin de responder de manera flexible y eficaz a las diversas demandas.

- **Velocidad**
  La tecnología de la nube puede ayudar a los programadores a crear servicios y softwares con un coste muy bajo. Como resultado, las empresas u organizaciones públicas pueden mejorar la flexibilidad del funcionamiento, obtener la capacidad de respuesta rápida y de la normalización del proceso. Para aquellas aplicaciones

que requieren el apoyo de una gran cantidad de infraestructura de la TI (los servidores y los equipos de almacenamiento), el *cloud computing* puede reducir significativamente el tiempo que tarda en la adquisición, entrega e instalación. En general, si se despliega adecuadamente la estructura de la nube, las empresas u organizaciones públicas podrán conseguir los servicios innovadores de la TI con el tiempo y costes más bajos.

A la par que se resaltan las oportunidades que aporta el *cloud computing*, la dirección de las empresas u organizaciones públicas también tendrían que considerar los siguientes aspectos para planificar los servicios en la nube:

- **Infraestructura**
  La utilización de la CPU, la memoria y la capacidad del disco tiene que basarse fundamentalmente en la demanda real. Esto podrá ayudar a obtener grandes beneficios.

- **Aplicaciones**
  Las aplicaciones diseñadas para el sector público y basadas en la nube comercial podrán ofrecer excelentes funciones. Estas aplicaciones se mejorarán a medida que la nube se populariza en el sector público.[41]

- **Servicios**
  Los servicios en la nube pueden proporcionar capacidades para fortalecer la competitividad del sector público y hacerlo más flexible y eficiente en responder a los cambios del mercado.

Observadas las ventajas del *cloud computing*, en el capítulo de conclusiones pasaremos a enumerar, desde el punto de vista preservador, sus principales desventajas en la gestión de la información, así como aquellas oportunidades que deberíamos aprovechar y que nos ofrece esta tecnología tan potencial.

[41] Material de referencia:
Microsoft Hohm Energy (dado de baja en 2011):
Disponible en: http://www.cnet.com/news/microsoft-kills-hohm-energy-app/

Google PowerMeter (dado de baja en 2011):
Disponible en: http://www.cbsnews.com/news/why-googles-home-energy-product-powermeter-failed/

"Many organisations are in a better security position by being on the cloud than on their internal networks."

- Azeem Aleem Christopher Ryan Sprott

CAPÍTULO 4
CONCLUSIONES

En el capítulo de conclusiones se presentarán los puntos débiles del *cloud computing,* las oportunidades que tendríamos que aprovechar, así como las futuras líneas de investigación.

4. Capítulo 4: Conclusiones

En este último capítulo se presentarán, por un lado, los posibles puntos débiles que deberían considerarse cuidadosamente cuando se emplean cualquier tipo de tecnología del *cloud computing*; y, por otro lado, las otras tecnologías o tendencias de la TI asociadas a la tecnología de la nube que tendríamos que aprovechar para poder conseguir el uso máximo de la misma.

4.1 Puntos débiles del *cloud computing* en la gestión de la información

Tras la realización de los capítulos 1, 2 y 3, hemos conocido las principales características y la estructura básica del *cloud computing*, su marco jurídico-normativo, la tendencia de desarrollo y sus ventajas en la gestión de la información y en la mejora del rendimiento de las organizaciones. Sin embargo, evidentemente, el *cloud computing* también tiene sus puntos débiles intrínsecos. A continuación, se mostrarán las principales desventajas de la tecnología de la nube que hemos considerado importantes respecto a la gestión de la información.

- **Imprescindible la conexión a Internet**
  La conexión a Internet es la premisa de todas las tareas que se llevan a cabo en la nube. Sin ella, es imposible realizar el *cloud computing*, ya que la necesitamos para poder conectarnos a las aplicaciones o los documentos desplegados en la nube. La falta de la conexión a Internet podrá suspender todos los trabajos durante un período de tiempo, aspectos que condiciona de modo definitivo la aplicación del *cloud computing* especialmente en las zonas que no tienen conexión a Internet o la tienen muy inestable. Es decir, cuando estamos *offline*, el *cloud computing* no funciona.

- **Bajo rendimiento cuando la velocidad de la conexión a Internet es baja**
  De la misma manera, la velocidad de la conexión a Internet también afecta al rendimiento del *cloud computing*. Normalmente, el procesamiento de las aplicaciones basadas en la web requiere un ancho de banda muy grande, lo mismo que ocurre en el tratamiento de datos enormes. Si estamos en un Internet con baja velocidad, es muy difícil conectarnos a los servicios en la nube con diversas funciones. El *cloud computing* no se podrá aplicar en entornos de ancho de banda insuficiente.

- **Las funciones pueden ser limitadas**
  Muchas aplicaciones de la nube basadas en la web tienen menos funciones que las mismas basadas en el escritorio. Por ejemplo, cuando se comparan la aplicación *Documentos de Google* con *Microsoft PowerPoint*, aunque las dos

tienen funciones muy similares, *Microsfot PowerPoint* tienen más funciones avanzadas que *Documentos de Google*, que está basada en la nube. A pesar de que con el paso de tiempo se han añadido nuevas funciones en *Documentos de Google*, en calidad de usuario avanzado se tendría de considerar cuidadosamente si las aplicaciones basadas en la nube podrían facilitar todas las funciones que se necesitan cuando se decide abandonar los softwares tradicionales

- **La seguridad y la privacidad de la información**
  Quizás las cuestiones de la seguridad y la privacidad de la información almacenada en la nube deberían ser el primer reto de la gestión de la información en todos los campos. El *cloud computing* está gestionando la información clave de las empresas y de los individuos. ¿Ellos más propensos a convertirse en objetivo de los *hackers*? ¿Es recomendable que las empresas u organizaciones que tienen datos sensibles, como los de asistencia sanitaria y económicos, utilicen la tecnología de la nube? ¿Es segura la realización de la copia de seguridad de los datos de los clientes por parte de los CSPs? ¿Se puede confiar totalmente en el tratamiento de los datos que realizan los empleados de los CSPs? Estas preguntas son muy difíciles de contestar de forma contundente y precisa.

Entonces, ¿deberíamos utilizar la tecnología del *cloud computing*? Sí. Aunque conlleva ciertas desventajas, sus puntos fuertes tampoco pueden ser ignorados. De acuerdo con Beagrie et al. (2014), los pasos básicos que se siguen al contratar un servicio en la nube deberían ser: establecer las necesidades, elegir el servicio, elegir el CSP, definir el proceso de adquisición (en el que se incluyen la firma del contrato y la adquisición de servicios) y el desarrollo del proyecto de negocio. Lo que puede ser llamativo es la orden de la selección del servicio y la selección del CSP. Es decir, los clientes tienen que analizar lo que realmente necesitan en vez de confiar en el prestigio del CSP. Además, da igual que sea un cliente o CSP, lo más fundamental es respetar las normativas asociadas a la contratación, seguridad y privacidad de la nube para poder regular todos los procesos que se realizarán en ella. Estos aspectos se han explicado detalladamente en el Capítulo 2.

4.2 *Cloud computing* y la externalización de la TI

El *cloud computing* es un modelo para el suministro y el consumo de las capacidades de la TI bajo demanda. Esto ayuda en el cambio de la estructura de costos desde gastos de capital a gastos de funcionamiento, así como sirve de apoyo a los sistemas de la TI para ser más ágiles. Este modelo innovador de adquisición de servicios relacionados con la TI ha promovido que las organizaciones revisen su infraestructura y las estrategias de servicios, y que optimicen los gastos en la TI al tiempo que mejoran la agilidad de modo general.

El *cloud computing* representa un cambio fundamental en cómo las organizaciones pagan y cómo se accede a los servicios de la TI. Se han creado nuevas oportunidades para los CSPs y los proveedores de externalización. El *cloud computing* tendrá un impacto significativo en estos últimos, quienes deberían adoptar nuevas estrategias para incluir servicios en la nube como parte de sus ofertas para mantener su competitividad en la era de cambios profundos en la industria de servicios de la TI. También debería experimentar con los servicios en la nube y entender cuáles son los modelos adecuados para sus clientes. Esto les ayudará a aprovechar nuevas oportunidades de negocio que surgirían a partir del *cloud computing*.

Los CIOs (*Chiel Information Officer*) tienen que analizar los beneficios del *cloud computing* junto con los impactos comerciales. Deben tener simultáneamente un plan de desarrollo a corto plazo y otro a largo plazo. También tienen que realizar un plan de transición para todos sus clientes que proceden de sistemas antiguos y aportan el nuevo concepto de *computing*. Además, deben aplicar un programa de formación para los usuarios, siempre que sea necesario.

Los CSPs deben de ser conscientes de que la seguridad es una gran preocupación para la mayoría de las organizaciones. Las cuestiones de protección de datos están limitando la profundidad de la aplicación del *cloud computing* en las empresas. Estos retos deben abordarse mediante el desarrollo de las políticas de seguridad, la reducción de riesgo y la creación de una infraestructura robusta de fiabilidad y alta disponibilidad junto con la garantía de ejecución.

Se puede decir que, actualmente la industria de los servicios de la TI está enriqueciéndose mediante la integración de nuevos servicios en la nube por parte de los proveedores de externalización. Las últimas tendencias tendrán un impacto en el futuro de los servicios de la TI y el *cloud computing* que incluyen la integración de nuevos servicios con los ya existentes, el incremento del número de aplicaciones que utilizan la infraestructura de la nube y los modelos globales de entrega a petición del usuario. El despliegue de servicios innovadores en la nube con modelos de negocio atractivos podrá satisfacer a las necesidades del cliente y la adopción sin precedentes de los servicios en la nube en las empresas.

4.3 El *cloud computing* y la preservación digital en centros de información

La preservación digital se refiere principalmente a la gestión de contenidos digitales para garantizar su acceso continuo durante el tiempo que sea necesario, independientemente de los cambios tecnológicos u organizativos. Por tal motivo, atendiendo a sus diversos campos, la tecnología de la nube podrá beneficiar,

especialmente, a los centros de información, que son las principales organizaciones que deberían planificar estrategias adecuadas para garantizar la preservación digital de sus colecciones. Beagrie et al. (2014) nos ofrecen una serie de recomendaciones que se muestran a continuación:

- Los servicios en la nube pueden proporcionar la replicación con característica fáciles y automatizadas para múltiples ubicaciones y accesos a espacios de almacenamiento gestionados profesionalmente. Como resultado, la situación de la preservación de la información digital será mejor (o por lo menos asegurarlo del mismo modo) aquello que realizan localmente.

- Los centros de información pueden añadir acceso a herramientas dedicadas, procedimientos, acuerdos de flujo de trabajo y de servicios, todo ello se adapta a los requisitos de la preservación digital a través de los proveedores especializados.

- El coste se puede reducir considerablemente gracias a la forma más rápida y fácil de adquisición, especialmente en los centros de información pequeños.

- La flexibilidad del *cloud computing* permite realizar pruebas de los CSPs relativamente rápidas y a bajo coste.

- Actualmente existe mucha flexibilidad y más opciones del despliegue de servicios en la nube. Por lo tanto, los centros de información están desempeñando un papel más relevante que antes. En particular, la implementación de la nube privada y la nube híbrida son las mejores opciones en solucionar las preocupaciones de la seguridad del almacenamiento de materiales sensibles frente a las actuaciones de la nube pública.

- También se pueden implementar estrategias eficaces para abordar preocupaciones sobre la estabilidad y la durabilidad de los CSPs. Por ejemplo, se pueden sincronizar contenidos entre dos CSPs o crear una nube externa con almacenamiento local. O, como alternativa, realizar una copia de seguridad de la información digital almacenada en la nube que está controlada independientemente por un tercero de confianza.

Al diferenciarse de la perspectiva de Beagrie et al., que se ofrecen las recomendaciones desde el punto de vista organizativo, Stančić et al. (2012) nos abordan 4 planes que consideran "*probably the best way to ensure long-term protection, preservation and usage of electronic content created and archived today*[42]" sobre el archivo en la nube desde el enfoque de la relación entre los servicios, archivos

[42] Traducción al español: (estos 4 planes) son probablemente las mejores técnicas en garantizar la protección a largo plazo, la preservación y la utilización de los contenidos electrónicos que se han creado y archivados de hoy en día.

y los CSPs. Estos planes se listan a continuación:

- Los CSPs tienen la responsabilidad de controlar los contenidos archivados sin intervenir los controles de los mismos por parte de los creadores o las instituciones de archivo.

- Los creadores de contenidos tendrían que esforzarse más en el control adicional de los servicios no estandarizados.

- Los servicios tendrían que ser estandarizados con buenas prácticas y los creadores de contenidos tienen que tener la conciencia de la importancia de elegir CSPs consistentes con ellas.

- La comunidad archivística tendría que participar activamente en el nuevo concepto de archivo e influir en las prácticas de los CSPs.

Tomando como base lo anteriormente citado, quizás es posible observar que, el mayor reto que está afectando al grado de adopción del *cloud computing* es el conjunto de amenazas vinculadas a la seguridad de la información y aspectos asociados a dicha seguridad. Afortunadamente, esa situación podrá ser mejorada significativamente si podemos respetar estrictamente al marco jurídico-normativo correspondiente, tanto para los clientes como para los CSPs. El *cloud computing* podrá enriquecer y fortalecer en gran medida nuestra capacidad de gestión de la información siempre que convirtamos sus amenazas en oportunidades. Para ello, se precisa, por supuesto, profesionales de la información activos y con conocimiento y habilidades para actuar.

4.4 Futuras líneas de investigación

Con respecto a la ventaja de este trabajo, se puede decir que ha abordado una introducción detallada del *cloud computing* desde un enfoque preservador que podría considerarse útil como base a partir de la cual se podrían desarrollarse diversos trabajos adicionales. Es posible localizar información introductoria, detallada sobre el *cloud computing* en el Capítulo 1, el marco jurídico-normativo exhaustivo y especializado en las principales preocupaciones sobre la gestión de la información en la nube en el Capítulo 2, y el panorama de la tendencia internacional, incluyendo, tanto el cambio de la industria de las TIs relacionado con la tecnología de la nube, como la situación de adopción y de desarrollo del *cloud computing* en las empresas, en el Capítulo 3.

Sin embargo, tal y como es factible observar, este trabajo es generalista y totalmente teórico. Para futuras líneas de investigación, sería recomendable realizar estudios más específicos, tales como por ejemplo, a partir del estudio del *cloud computing* en

sentido general, un enfoque específico en la preservación en la nube o la externalización de la misma para enriquecer los conocimientos asociados. En este sentido, sería aconsejable, igualmente, realizar investigación del mercado, análisis estadístico o cuestionarios en instituciones.

Tras la realización de este trabajo como Trabajo de Fin de Máster esperamos haber aportado nuestro grano de arena para que la tecnología de la nube sea reconocida como una de las herramientas más potenciales en el campo de la gestión de la información.

5. Bibliografía y fuentes consultadas

Bibliografía

Aleem, A., & Ryan Sprott, C. (2013). Let me in the cloud: analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime, 20*(1), págs. 6-24. doi:http://dx.doi.org/10.1108/13590791311287337

B. Horrigan, J. (2008). *Pew Internet & American Life Project: Use of Cloud Computing Applications and Service 1.* Recuperado el 11 de mayo de 2016, de http://www.pewinternet.org/pdfs/PIP_Cloud.Memo.pdf

Beagrie, N., Charlesworth, A., & Miller, P. (2014). *How cloud storage can address the needs of public archives in the UK.* The National Archives. Recuperado el 20 de julio de 2016, de http://www.nationalarchives.gov.uk/documents/archives/cloud-storage-guidance.pdf

Breeding, M. (2011). A cloudy forecast for libraries. *Computers in Libraries, 31*(7), págs. 4-32. Recuperado el 21 de mayo de 2016, de http://www.infotoday.com/cilmag/sep11/breeding.shtml

CCN - Centro Criptográfico Nacional. (2014). *Guía de seguiridad de las TIC (CCN-STIC-823).* Recuperado el 12 de abril de 2016, de https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html

Cloud Security Alliance. (2011). *CSA Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.* Recuperado el 20 de mayo de 2016, de https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Debois, P. (2011). Devops: A software revolution in the making. *Journal of Information Technology Management, 24*(8), págs. 3-39.

Dhar, S. (2012). From outsourcing to Cloud computing: evolution of IT services. *Management Research Review, 35*(8), págs. 664-675. doi:http://dx.doi.org/10.1108/01409171211247677

Érica, S. (2014). *La aplicación de la nube en bibliotecas universitarias públicas en Brasil.* Recuperado el 15 de mayo de 2016, de http://orff.uc3m.es/bitstream/handle/10016/19199/EricaSaito_TFM_MBSID_2014.pdf?sequence=1

ESPAÑA. (1999). Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de

Carácter Personal. *(298)*, 43088-43099. Bolentín Oficial del Estado. Recuperado el 6 de junio de 2016, de https://www.boe.es/diario_boe/txt.php?id=BOE-A-1999-23750

GIMÉNEZ CHORNET, V. (2015). Archivos electrónicos: criterios de preservación con la norma UNE-ISO 14641-1. *SíMILE*, 4-6. Recuperado el 23 de mayo de 2016, de http://vicentgimenez.net/archivos%20electronicos.pdf

Goldner, M. (2011). Winds of change: libraries and cloud computing. *Multimedia Information and Technology, 37*(3), págs. 8-24. Obtenido de http://www.oclc.org/content/dam/oclc/events/2011/files/IFLA-winds-of-change-paper.pdf

Han, Y. (2010). On the clouds: a new way of computing. *Information Technology and Libraries, 29*(2), págs. 87-92. Recuperado el 12 de mayo de 2016, de http://athena.rider.edu:2928/login.aspx?direct¼true&db¼eft&AN¼502992329&site¼ehost-live

ISO 14641-1. (2012). Electronic archiving -- Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation. Recuperado el 10 de junio de 2016, de http://www.iso.org/iso/catalogue_detail.htm?csnumber=54911

ISO/IEC 27017. (2015). Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Recuperado el 10 de junio de 2016, de http://www.iso.org/iso/catalogue_detail?csnumber=43757

ISO/IEC 27018. (2014). Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Recuperado el 10 de junio de 2016, de http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

Kwame Adjei, J. (2015). Explaining the role of trust in cloud computing services. *info, 17*(1), págs. 54-67. doi:http://dx.doi.org/10.1108/info-09-2014-0042

McKemmish, S. (2013). *Recordkeeping and archiving in the cloud. Is there a silver lining.* Recuperado el 21 de julio de 2016, de http://infoz.ffzg.hr/INFuture/2013/papers/1-02%20McKemmish,%20Recordkeeping%20and%20Archiving%20in%20the%20Cloud.pdf

Mell, P., & Grance, T. (2011). *SP 800-145.* The NIST Definition of Cloud Computing, National Institute of Standards & Technology, Gaithersburg, MD.

National Archives and Records Administration. (mayo de 2010). *NARA Bulletin 2010-05*. Recuperado el 9 de abril de 2016, de National Archives:

http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html

Ojala, A., & Tyrväinen, P. (2011). Value networks in cloud computing. *Journal of Business Strategy, 32*(6), págs. 40-49. doi:http://dx.doi.org/10.1108/02756661111180122

Peña-López, I. (2013). Guía para clientes que contraten servicios de Cloud Computing.

Pérez San-José, P., Gutiérrez Borge, C., Álvarez Alonso, E., De la Fuente Rodríguez, S., & García Pérez, L. (2011). *Guía para empresas: seguridad y privacidad del cloud computing.* Instituto Nacional de Tecnologías de la Comunicación, INTECO.

Real Decreto 1720/2007. (2007). De 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *(17)*, 4103-4136. Bolentín Oficial del Estado. Recuperado el 6 de junio de 2016, de https://www.boe.es/buscar/doc.php?id=BOE-A-2008-979

RightScale. (2016). *STATE OF THE CLOUD REPORT: Hybrid Cloud Adoption Ramps as Cloud Users and Cloud Providers Mature.* Recuperado el 15 de julio de 2016, de http://assets.rightscale.com/uploads/pdfs/RightScale-2016-State-of-the-Cloud-Report.pdf

Sánchez, C., & Recio, M. (2015). UNE-ISO/IEC 27018: privacidad elevada a la nube. *AENOR: Revista de la normalización y la certificación*(309), págs. 20-23. Obtenido de http://www.aenor.es/revista/pdf/nov15/20nov15.pdf

Stančić, H., Arian Rajh, A., & Milošević, I. (2013). "Archiving-as-a-Service". Influence of Cloud Computing on the Archival Theory and Practice. *The Memory of the World in the Digital Age: Digitization and Preservation*, (págs. 108-125). Recuperado el 22 de julio de 2016, de http://1seminariopreservacaopatrimoniodigital.dglab.gov.pt/wp-content/uploads/sites/19/2015/08/recurso_25.pdf

Wolf, R. (2010). Cloud computing. *North Carolina Libraries, 68*(2), págs. 1-30. Recuperado el 11 de mayo de 2016, de http://www.ncl.ecu.edu/index.php/NCL/article/view/326

Yang, S. Q. (2012). Move into the Cloud, shall we? *29*(1), págs. 4-7. doi:http://dx.doi.org/10.1108/07419051211223417

Fuentes consultadas

Amazon (s.f.). Amazon WorkSpaces. Recuperado el 15 de junio de 2016. Disponible en: https://aws.amazon.com/es/workspaces/?nc1=h_ls

CA Tecnologies (2012). Do you want to run your mainframe software from CA Technologies on IBM Rational Development and Test Environment for System z? Recuperado el 18 de junio de 2016. Disponible en: http://www.ca.com/us/~/media/Files/SolutionBriefs/1368-mfsuite-ibm-rational-dev-sys-zunit-test-sb-final.pdf

CBS (2011). Why Google's Home-Energy Product PowerMeter Failed. Recuperado el 18 de junio de 2016. Disponible en: http://www.cbsnews.com/news/why-googles-home-energy-product-powermeter-failed/

CNET (2011). Microsoft kills Hohm energy app. Recuperado el 18 de junio de 2016. Disponible en: http://www.cnet.com/news/microsoft-kills-hohm-energy-app/

Department of Finance and Deregulation, Australian Government (2013). Australian Government Cloud Computing Policy: Maximising the Value of Cloud. Recuperado el 12 de junio de 2016. Disponible en: http://www.finance.gov.au/files/2012/04/Australian-Government-Cloud-Computing-Policy-Version-2.0.pdf

Dell (s.f.). Wyse Thin Clients, VDI Appliances and Software. Recuperado el 18 de junio de 2016. Disponible en: http://www.dell.com/us/business/p/cloud-client

Department of Finance and Deregulation, Australian Government (2013). The Australian Public Service Big Data Strategy: Improved understanding through enhanced data-analytics capability. Recuperado el 12 de junio de 2016. Disponible en: https://www.finance.gov.au/files/2013/06/Draft-Big-Data-Strategy.pdf

Enterprise Business (s.f.). Cloud Servicies. Recuperado el 18 de junio de 2016. Disponible en: https://www.business.att.com/enterprise/Portfolio/cloud/

European Commission (2012). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Unleashing the Potential of Cloud Computing in Europe. Recuperado el 12 de junio de 2016. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

European Commission (2015). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND

SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: A Digital Single Market Strategy for Europe. Recuperado el 12 de junio de 2016. Disponible en: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX%3A52015DC0192

HP (s.f.). Plataforma de big data. Recuperado el 18 de junio de 2016. Disponible en: http://www8.hp.com/es/es/software-solutions/big-data-platform-haven/

IBM (2015). IBM Cloud Manager with OpenStack. Recuperado el 15 de junio de 2016. Disponible en: https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W21ed5ba0f4a9_46f4_9626_24cbbb86fbb9

IBM (2013). IBM to Acquire Aspera to Help Companies Speed Global Movement of Big Data. Recuperado el 15 de junio de 2016. Disponible en: http://www-03.ibm.com/press/us/en/pressrelease/42782.wss

ISO (2015). Security toolbox protects organizations from cyber-attacks. Recuperado el 12 de junio de 2016. Disponible en: http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref2032

Kundra, Vivek (2011). Federal Cloud Computing Strategy. Recuperado el 12 de junio de 2016. Disponible en: https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

Microsoft (s.f.). Windows Azure Pack. Recuperado el 15 de junio de 2016. Disponible en: http://www.microsoft.com/es-es/server-cloud/products/windows-azure-pack/overview.aspx

NSW Government (2013). Cloud Services Policy and Guidelines. Recuperado el 12 de junio de 2016. Disponible en: https://11217-presscdn-0-50-pagely.netdna-ssl.com/wp-content/uploads/2013/09/NSW-Government-Cloud-Services-Policy-and-Guidelines.pdf

Oracle (2016). Oracle Buys NetSuite. Recuperado el 15 de junio de 2016. Disponible en: https://www.oracle.com/corporate/acquisitions/netsuite/index.html

Oracle (2016). Oracle Buys Opower. Recuperado el 15 de junio de 2016. Disponible en: https://www.oracle.com/corporate/pressrelease/oracle-buys-opower-050216.html

Oracle (2016). Oracle Buys Textura. Recuperado el 15 de junio de 2016. Disponible en: https://www.oracle.com/corporate/pressrelease/oracle-buys-textura-042816.html

RightScale (2015). State of the Cloud Computing: Central IT Is Taking the Lead to Broker Cloud Services to the Enterprise. Recuperado el 18 de junio de 2016. Disponible en: http://assets.rightscale.com/uploads/pdfs/RightScale-2015-State-of-the-Cloud-Report.pdf