

Análisis de soluciones cloud para almacenamiento de archivos y trabajo colaborativo

Autor: Javier Serrano Perelló

Tutor: Fernando Raimundo González Ladrón de Guevara

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politècnica de Valencia, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2015-16

Valencia, 28 de junio de 2016

Resumen

Con el desarrollo de Internet, el *cloud computing* se está convirtiendo en un servicio mucho más común hoy en día. Hay varios tipos diferentes de servicios en la nube, que puede dividirse en: SaaS (Software como servicio), PaaS (Plataforma como servicio), IaaS (Infraestructura como servicio). Además, de diferentes modelos de despliegue, como la nube pública, privada, híbrida o comunitaria.

Ahora, debido al aumento de la velocidad de Internet y el declive de los precios de los servicios en la nube, las empresas, especialmente las pequeñas y medianas, están provistas para utilizar servicios *cloud* para mejorar su eficiencia de trabajo y reducir los costes operativos.

En este artículo, lo que queremos hacer es presentar una visión amplia y detallada de lo que consiste el *cloud computing*, y a continuación centrarse en uno de los servicios que ofrece éste, el *cloud storage*. Por eso intentamos hacer una comparativa de los principales servicios de almacenamiento en la nube como Google Drive, Dropbox y etc, para luego poder hacer referencia a la solución de almacenamiento *cloud* más adecuada para una empresa de pequeño o mediano tamaño o un simple usuario, tras medir mediante Wireshark diversos parámetros interesantes.

La razón de que nos centremos sólo en servicios de almacenamiento en la nube es que se tarda mucho menos esfuerzos técnicos en la implementación de servicios de almacenamiento en la nube que en servicios de *cloud computing* ya que en general, no todas las empresas tienen un gran personal técnico que son capaces de desplegar la sofisticada plataforma de *cloud computing*, especialmente para las pequeñas y medianas empresas en diversos campos.

Resum

Amb el desenvolupament d'Internet, el *cloud computing* s'està convertint en un servei molt més comú avui dia. Hi ha diversos tipus diferents de serveis en el núvol, que pot dividir-se en: SaaS (Software com a servei), PaaS (Plataforma com a servei), IaaS (Infraestructura com a servei). A més, de diferents models de desplegament, com el núvol públic, privada, híbrida o comunitària.

Ara, a causa de l'augment de la velocitat d'Internet i el declivi dels preus dels serveis en el núvol, les empreses, especialment les xicotetes i mitjanes, estan proveïdes per a utilitzar serveis *cloud* per a millorar la seua eficiència de treball i reduir els costos operatius.

En aquest article, la qual cosa volem fer és presentar una visió àmplia i detallada del que consisteix el *cloud computing*, i a continuació centrar-se en un dels serveis que ofereix aquest, el *cloud storage*. Per açò intentem fer una comparativa dels principals serveis d'emmagatzematge en el núvol com Google Drive, Dropbox i etc, per a després poder fer referència a la solució d'emmagatzematge *cloud* més adequada per a una empresa de xicotet o mitja grandària o un simple usuari, després de mesurar mitjançant Wireshark diversos paràmetres interessants.

La raó que ens centrem només en serveis d'emmagatzematge en el núvol és que es tarda molt menys esforços tècnics en la implementació de serveis d'emmagatzematge en el núvol que en serveis de *cloud computing* ja que en general, no totes les empreses tenen un gran personal tècnic que són capaços de desplegar la sofisticada plataforma de *cloud computing*, especialment per a les xicotetes i mitges empreses en diversos camps.

Abstract

With the development of the Internet, cloud computing is becoming a service much more common today. There are several different types of services in the cloud, which can be divided into: SaaS (Software as a service), PaaS (Platform as a service), IaaS (Infrastructure as a service). In addition, different models of deployment, as the public cloud, private, hybrid or community.

Now, due to the increase in the speed of the Internet and the decline of the prices of the services in the cloud, enterprises, especially small and medium-sized enterprises, are equipped to use cloud services to improve its working efficiency and reduce operating costs. In this article, what we want to do is to present a broad and detailed picture of what is cloud computing, and then focus in one of the services that it offers, the cloud storage.

That is why we tried to make a comparison of the main storage services in the cloud as Google Drive, dropbox and etc, to then be able to make reference to the cloud storage solution most appropriate for a company of small or medium size or a simple user, after measure through Wireshark various parameters interesting.

The reason that we focus only on storage services in the cloud is that it takes much less technical efforts in the implementation of storage services in the cloud that in cloud-computing services since in general, not all companies have a large technical staff that are able to deploy the sophisticated cloud computing platform, especially for small and medium-sized enterprises in various areas.

Índice del contenido

| | |
|--|----|
| 1. Introducción y objetivos del trabajo..... | 3 |
| 2. Metodología de trabajo del TFG..... | 4 |
| 3. <i>Cloud computing</i> . | |
| a. Antecedentes y origen del <i>cloud computing</i> | 5 |
| b. En qué consiste y principales características..... | 8 |
| c. SMICloud y sus parámetros..... | 9 |
| d. Modelos de servicio y modelos de despliegue..... | 17 |
| e. Situación actual y futura del <i>cloud computing</i> en el mundo..... | 24 |
| 4. <i>Cloud storage</i> . | |
| a. Almacenamiento de archivos en la nube..... | 27 |
| i. Sincronización automática..... | 28 |
| ii. Herramientas colaborativas..... | 29 |
| iii. Editar archivos desde la nube..... | 30 |
| iv. Seguridad..... | 31 |
| v. Disponibilidad..... | 35 |
| vi. Privacidad..... | 35 |
| vii. Protección de datos..... | 35 |
| viii. Confidencialidad..... | 36 |
| ix. Integridad..... | 36 |
| x. Copias de seguridad..... | 36 |
| xi. Control de acceso..... | 37 |
| xii. Prevención frente a pérdidas..... | 38 |
| xiii. Precios..... | 39 |
| b. Comparación de diferentes tecnologías para el almacenamiento de archivos. | |
| i. <i>Direct Attached Storage</i> | 41 |
| ii. <i>Network Attached Storage</i> | 41 |
| iii. <i>Storage Area Network</i> | 42 |
| c. Comparación de los mejores servicios de almacenamiento en la nube (Dropbox, Google Drive, OneDrive, Mega, Box, ADrive, Amazon cloud drive). | |
| i. Estándares de seguridad..... | 45 |
| ii. Tamaño máximo de archivo..... | 47 |
| iii. Sistemas operativos..... | 47 |
| iv. Idiomas soportados..... | 48 |
| v. Cargar un archivo..... | 49 |
| vi. Descargar un archivo..... | 50 |
| vii. Mover el archivo..... | 50 |
| viii. Velocidad de sincronización..... | 50 |
| ix. Localización de los servidores..... | 50 |
| d. ownCloud. | |
| i. Descripción general y situación en la actualidad..... | 52 |
| 5. Conclusión. | |
| a. Académica..... | 54 |
| b. Personal..... | 55 |
| 6. Bibliografía..... | 56 |

Índice de figuras y tablas

| | |
|---|----|
| Figura 1. Mainframe antiguo..... | 5 |
| Figura 2. Arquitectura cliente/servidor..... | 6 |
| Figura 3. <i>Grid Computing</i> | 6 |
| Figura 4. Peer to Peer..... | 6 |
| Figura 5. Infraestructura del <i>SMICloud</i> | 12 |
| Figura 6. Distinción entre IaaS, PaaS y SaaS..... | 19 |
| Figura 7. Esquema general de las diferentes formas de desplegar una infraestructura de <i>cloud computing</i> | 19 |
| Figura 8. Forma de implementar una nube híbrida..... | 23 |
| Figura 9. Dashlane muestra la seguridad de tus contraseñas y te ayuda a recordarlas..... | 32 |
| Tabla 1. Disponibilidad de los datos en la nube (híbrida)..... | 35 |
| Tabla 2. Precios de los principales proveedores de <i>cloud storage</i> | 39 |
| Figura 10. Diferentes tarifas del servicio ADrive..... | 40 |
| Figura 11. Ejemplo DAS..... | 41 |
| Figura 12. Ejemplo NAS..... | 42 |
| Figura 13. Ejemplo SAN..... | 43 |
| Figura 14. Evolución del almacenamiento en la nube..... | 44 |
| Tabla 3. Sistemas operativos soportados por cada uno de los proveedores de <i>cloud storage</i> | 47 |
| Tabla 4. Idiomas soportados por cada uno de los proveedores de <i>cloud storage</i> | 48 |
| Figura 15. Escenario de las medidas..... | 49 |
| Tabla 5. Tiempos obtenidos tras hacer la prueba de subir un archivo al servidor oportuno..... | 49 |
| Tabla 6. Tiempos obtenidos tras hacer la prueba de descargar un archivo del servidor..... | 50 |
| Tabla 7. Velocidades de sincronización de archivos para cada uno de los proveedores..... | 50 |
| Tabla 8. Localización de los servidores donde hemos cargado y descargado archivos..... | 51 |
| Figura 16. OwnCloud en las empresas..... | 53 |

1. Introducción y objetivos del trabajo

Los servicios de almacenamiento *cloud* basados en Internet han obtenido gran atención en los últimos años. Los usuarios de almacenamiento en la nube pueden tener acceso a tanto espacio de almacenamiento como estén dispuestos a pagar por ello.

En comparación con las soluciones previas, las soluciones de almacenamiento en la nube son mucho más baratas y más fiables: los usuarios no tienen que pagar ni un gran coste inicial, ni comprar dispositivos de almacenamiento, ni de mantenimiento. El modelo de carga de pago permite a los usuarios pagar por una gran escalabilidad y flexibilidad, es decir, no tienen que preocuparse acerca de los dispositivos adicionales debido a la reducción del uso de almacenamiento o el suplemento para más dispositivos de almacenamiento, junto con el coste de emplear un especialista para gestionar la infraestructura de red y almacenamiento. Los usuarios tienen la libertad para adaptarse a la opción más adecuada en función de la situación en tiempo real.

Es difícil decir cuántos proveedores de soluciones de almacenamiento en la nube existen actualmente, pero es seguro que hay más de diez grandes jugadores en este juego. Estos proveedores ofrecen una amplia gama de opciones en sistemas funcionales, rendimiento, precios y etc. Por lo que, ¿cómo podemos hacer una buena y clara distinción si hay tantas diferencias? Para los usuarios, la respuesta de esta pregunta puede ayudarlos a elegir la solución que mejor se ajuste a una circunstancia específica.

Para los proveedores, la respuesta puede ayudar a mejorar sus soluciones existentes y por lo tanto, proporcionar mejores beneficios. Por ejemplo, son capaces de ofrecer más opciones para un uso distinto y encontrar un determinado tipo de servicios en un tipo específico de servidor de dispositivos, por lo que se puede reducir el costo, y mejorar el rendimiento, debido al diseño específico de cada tipo de hardware del servidor.

Los objetivos de este proyecto son:

- Comprender y conocer los pilares fundamentales que han dado lugar al desarrollo de la nube y todos los servicios que ello conlleva.
- Ver la situación actual del *cloud computing* en el mundo y las perspectivas de futuro que hay.
- Analizar los proveedores de soluciones de almacenamiento en la nube actualmente más populares mediante varios aspectos como el precio, el almacenamiento inicial gratuito, el tiempo de carga y descarga de un archivo, el tamaño máximo del archivo..., y entonces ofrecer el servicio más adecuado para pequeñas y medianas empresas o un usuario individual, basado en sus requerimientos específicos.

2. Metodología de trabajo del TFG

Para realizar este trabajo empezamos con él en Febrero de 2016 y acabamos a mediados de Junio de 2016. La dedicación a este trabajo a lo largo del periodo mencionado anteriormente, ha sido combinada junto con 2 asignaturas que me quedaban para acabar el grado.

Lo primero de todo fue documentarme sobre el tema a tratar y ver que tenía suficiente documentación y bibliografía para escribir sin problemas, ya que antes de empezar con el trabajo, debía tener un esquema de cómo iba a ser mi parte teórica y mi parte práctica.

Por lo que empezamos, haciendo el índice y teniendo claro cuál era mi objetivo al realizar este trabajo. Esto costó un poco ya que el tema a tratar, *cloud computing*, es bastante amplio y debíamos acotarlo para que quedase claro lo que queríamos exponer por lo que, a mi parecer, escogimos el servicio más común y usado de la computación en la nube, el *cloud storage*.

Cuando ya tuve la base del proyecto, me puso a trabajar con la bibliografía escogida para redactar la parte teórica del trabajo, aunque en unos de los apartados, situación actual del *cloud computing* en el mundo, debía estar constantemente buscando en Google, periódicos o revistas científicas, por si se publicaban artículos interesantes para tener información actualizada del tema.

Tras tener la parte teórica redactada, pasé a la parte práctica donde busqué 7 proveedores de soluciones de almacenamiento en la nube y tras hacerme la cuenta más básica y gratuita de éstos, empecé a hacer dos tareas: la primera fue encontrar toda la información posible de cada uno de los proveedores sobre precios, estándares de seguridad, tamaño máximo de archivo... y a continuación, las pruebas pertinentes para obtener los parámetros que me interesaban con el programa Wireshark.

Sobre la segunda fue la que me fue un trabajo más extenso ya que como los proveedores no tiene un único servidor y no lo tienen en un único lugar del mundo, decidí hacer 5 tests para el tiempo de carga de un archivo en un servidor, otros 5 tests para el tiempo de descarga de un archivo de un servidor en 2 horas distintas del día, unos a las 8:00 y otros a las 21:00, y hacer la media de todos los tiempos que obtuve y el número obtenido fue el resultado planteado.

Tras realizar todas las pruebas y obtener los documentos para analizar, tuve que crear un filtro para que solo viese paquetes que de una IP origen a un destino, ya que mi esquema de trabajo era tan simple como una conexión desde un ordenador a un servidor remoto. Además de los paquetes con los datos tenía paquetes con información de control del servicio, los cuales he desechado, aunque introducían un tiempo infinitamente pequeño en la realización de las pruebas. Y para comprobar que realmente estaba transmitiendo mi archivo completo, estuve haciendo cálculos ya que sabiendo que la MTU en Ethernet son 1518 bytes (1500 bytes más 18 bytes de la cabecera de Ethernet), obtenía de cada paquete los bytes que eran solo carga útil, ya que dado el tamaño de los archivos con los que trabajaba, era necesaria una fragmentación en paquetes. Partiendo de la longitud de cada uno de estos paquetes, les restaba 20 bytes de cabecera IP, 20 bytes de cabecera TCP y los campos del protocolo de aplicación del proveedor del turno o lo que sea y ya tenía lo que en cada paquete era carga útil, luego multiplicaba por el número de tramas que me quedaban tras aplicar el filtro, multiplicaba por 8 para trabajar en bits y tengo el tamaño del archivo en bits.

$$\text{Carga útil} = \text{Longitud paquete} - 2 * 20 \text{ bytes cabeceras TCP/IP} - x \text{ bytes protocolo de aplicación} \quad (1)$$

$$\text{Archivo} = \text{Carga útil} * 8 * \text{número de tramas tras aplicar el filtro} \quad (2)$$

3. Cloud computing

3.a Antecedentes y origen del *cloud computing*

Desde hace más de 40 años, tenemos antecedentes del concepto de *cloud computing* o computación en la nube, que demuestran que fue una perspectiva de futuro y tras décadas de investigación e innovación tecnológica, se llega a una nueva generación de plataformas y un nuevo horizonte, las cuales alojan un conjunto de recursos informáticos virtualizados para explotar infraestructuras, plataformas o software como servicios bajo demanda.

A continuación, se describen los pilares fundamentales para el desarrollo de la nube:

- *Mainframes*. A principios de los años 60, los ordenadores eran dispositivos muy caros, difíciles de mantener y de utilizar. Las empresas tenían grandes ordenadores, conocidos como *mainframes*, para hacer las tareas más críticas y complicadas. Generalmente, estos no estaban conectados a la red y se utilizaban para manejar grandes cantidades de datos, como censos o transacciones económicas. La capacidad de un *mainframe* estaba influenciada por su velocidad de CPU, memoria interna, capacidad de almacenamiento externo, dispositivos de E/S rápidos y su fiabilidad en el diseño de su arquitectura y soporte técnico.

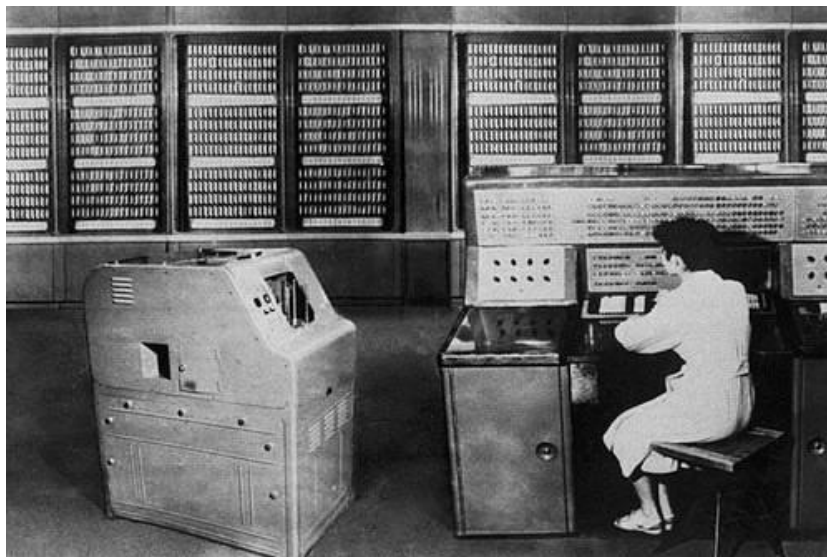


Figura 1. Mainframe antiguo [6]

- Arquitectura cliente-servidor. Entre los años 70 y 80, se generalizó el uso de ordenadores personales en los puestos de trabajo, menos costosos y potentes, pero que permitían realizar tareas básicas. Además, se disponía de un determinado número de ordenadores más potentes que se encargaban de mantener los datos más sensibles, así como las aplicaciones que necesitaban más recursos. Estos ordenadores con mayores capacidades de proceso se denominaron servidores, mientras que las máquinas con recursos más limitados de cada puesto de trabajo pasaron a llamarse clientes. Nació la arquitectura cliente-servidor.

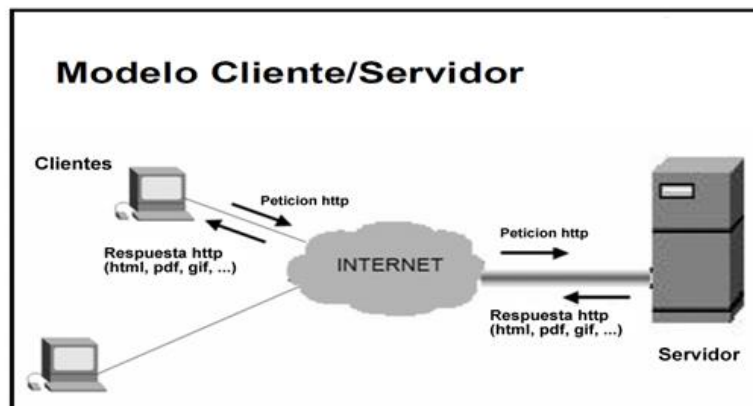


Figura 2. Arquitectura cliente/servidor [6]

• Arquitecturas colaborativas y distribuidas. Con el paso del tiempo, la complejidad de las aplicaciones informáticas ha ido creciendo y eso ha obligado a crear sistemas más complejos para solucionar de forma eficiente todas las nuevas necesidades. Por ejemplo, la *computación grid* utiliza un número variable de ordenadores de diferente hardware y software y cuyo fin es procesar una tarea que demanda una gran cantidad de recursos y poder de procesamiento. Por otra parte, la arquitectura *peer-to-peer* o p2p es una arquitectura distribuida en la que todos los nodos hacen a la vez de consumidores y suministradores de información, es decir actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados. Estas arquitecturas son ampliamente utilizadas en la actualidad, como por ejemplo en intercambio y búsqueda de ficheros (BitTorrent o Emule), sistemas de telefonía por Internet (Skype), monedas virtuales para transacciones entre partes (Bitcoin), etc.



Figura 3. Grid Computing [6]

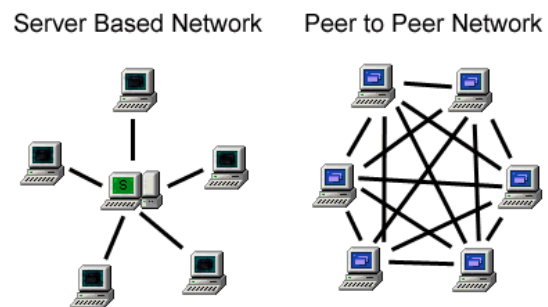


Figura 4. Peer to Peer [6]

Para conocer brevemente el origen del *cloud computing* es necesario remontarse al año 1961, con la figura de John McCarthy al que se le atribuye el concepto básico del *cloud computing* además de introducir el término inteligencia artificial y sugerir públicamente el uso de la tecnología de tiempo compartido, ya que debido a los avances en la informática y las comunicaciones, se llegaría a que algún día la computación se organizaría como un servicio público, igual que el modelo de negocio del agua o la electricidad. Esta idea era muy popular en la década de 1960, algunas empresas comenzaron a proporcionar recurso compartidos como oficina de servicios, donde se alquilaba tiempo y servicio de computo, aunque duró hasta mediados de los 70s, debido a que el hardware, software y las tecnologías de comunicación no estaban preparados.

En 1966, Douglas Parkhill escribió el libro *El desafío de la utilidad del ordenador* donde se explicaron muchas de las características actuales de la computación en nube. Pero otros investigadores afirman que las raíces de la computación en nube nos llevan hasta la década de 1950 con las observaciones de Herb Grosch, quien afirma “*la potencia de una computadora es proporcional al cuadrado de su precio*” (Ley Grosch), sin embargo, la ley de Moore se encargó de desmentir esto.

Las empresas de telecomunicaciones hasta la década de los 90s eran quienes ofrecían redes privadas virtuales (VPN) y al ser capaces de equilibrar el tráfico, pudieron hacer uso del ancho de banda total de la red con mayor eficacia.

En el año de 1999, Marc Benioff, Parker Harris y otros socios, fundaron la compañía Salesforce.com, como una empresa especializada en software como servicio (SaaS), aplicando tecnologías desarrolladas por compañías como Google y Yahoo! a diversas aplicaciones de negocio. A inicios del año 2000, Yahoo! y Google anunciaron la prestación de servicios *cloud* a cuatro de las más grandes universidades de Estados Unidos. Poco tiempo después, IBM Corp. anunció el ofrecimiento de servicios *cloud*, seguido por Microsoft, Oracle, Intel, SUN, SAS y Adobe, los cuales abarcaron la provisión de modelos IaaS, PaaS y SaaS.

Sin embargo, se considera que el inicio de *cloud computing*, puede ser debido a los servicios web de Amazon (Amazon Web Services) debido a que a finales de los años 90, los técnicos de Amazon se dieron cuenta que tenían una gran infraestructura informática pero que apenas utilizaban el 10-15% de su capacidad, y por eso iniciaron su producción en el año 2006 ofreciendo el modelo IaaS con capacidades básicas de procesamiento y almacenamiento a través de Internet.

Poco después, durante los años 2007 y 2008, grandes empresas como Google o IBM se unieron a universidades norteamericanas para iniciar una investigación a gran escala sobre el *cloud computing*. Como resultado de esta investigación, en Enero de 2009 apareció Eucalyptus, una plataforma de código abierto que permitía la creación de sistemas en la nube compatibles con los servicios web de Amazon. Microsoft entraría en el 2009 con el lanzamiento de Windows Azure. Y en 2011, Apple lanzó su servicio iCloud, un sistema de almacenamiento en la nube, para documentos, música, videos, fotografías, aplicaciones y calendarios.

3.b En qué consiste y principales características

El *cloud computing* es un modelo tecnológico que busca desplazar a los servidores físicos y utilizar servidores virtuales mediante la nube y servicios dedicados al almacenamiento de información y aplicaciones que el usuario utiliza diariamente para el desarrollo de sus labores. Por lo que podemos decir que es el conjunto “infinito” de servidores de información desplegados a lo largo del todo mundo en centros de datos (Data Centers), donde se almacenan millones de aplicaciones Web (Web Apps) y enormes cantidades de datos (Big Data) a disposición de miles de organizaciones, empresas y cientos de miles de usuarios, los cuales se descargan y ejecutan directamente los programas y aplicaciones de software almacenados en dichos servidores tales como Google, Amazon, IBM o Microsoft. Entre los servicios más conocidos del *cloud computing* se encuentra el almacenamiento de archivos en la nube (*cloud storage*), descrito más adelante.

Las principales características del *cloud computing* son:

- 1) Pago por uso: el cliente debe pagar en función del uso que realiza del servicio *cloud* contratado sabiendo que son unos costos bajos, en comparativa a los costos tradicionales por aplicación y dispositivos de almacenamiento. Además, nos permite utilizar un servicio de prueba antes de realizar la adquisición del servicio.
- 2) Abstracción: consiste en aislar los recursos informáticos contratados al proveedor de servicios *cloud* de los equipos informáticos del cliente, por lo que el mantenimiento de la infraestructura, actualización de sistemas, pruebas y demás tareas asociadas es trabajo del proveedor del servicio contratado.
- 3) Esto se consigue gracias a la virtualización, tecnología que sustenta el *cloud computing*, que consiste en la creación, a través de software, de una versión virtual de algún recurso tecnológico en lugar de una física. La diferencia esencial entre la virtualización y *cloud computing* es que con la virtualización el software manipula al hardware, mientras que el *cloud computing* consiste en el servicio resultante de tal manipulación.
- 4) Agilidad en la escalabilidad: consiste en aumentar o disminuir las funcionalidades ofrecidas al cliente y con ello el coste del servicio asociado, en función de las necesidades del negocio y de los usuarios, sin necesidad de nuevos contratos ni penalizaciones.
- 5) Multiusuario: permite a varios usuarios compartir los medios y recursos informáticos, permitiendo la optimización de su uso.
- 6) Autoservicio bajo demanda: permite al usuario acceder de manera flexible a las capacidades de computación, tales como el almacenamiento en servidores y redes, en la nube de forma automática y a medida que las vaya requiriendo, sin necesidad de una interacción humana.
- 7) Acceso sin restricciones: permite a los usuarios de acceder a los servicios contratados de *cloud computing* en cualquier lugar, en cualquier momento y con cualquier dispositivo que disponga de conexión a redes de servicio IP, tales como teléfonos móviles, dispositivos PDA u ordenadores portátiles.

- 8) Agrupación de recursos: los recursos informáticos del proveedor se agrupan para prestar servicios a diversos clientes utilizando un modelo de múltiples usuarios, con diferentes recursos físicos y virtuales asignados y reasignados de manera dinámica según la demanda. Generalmente, el cliente no tiene control o conocimiento de la ubicación exacta de los recursos proporcionados.
- 9) Elasticidad rápida: los recursos se asignan y liberan rápidamente, muchas veces de manera automática, lo que da al usuario la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.

3.c SMICloud y sus parámetros

Debido a los beneficios de negocio que ofrece la computación en la nube, muchas organizaciones han comenzado la construcción de aplicaciones en ella, y con ello hacer sus negocios ágiles, pero trasladar las aplicaciones y / o datos a la nube no es una tarea sencilla.

Existen numerosos retos para aprovechar todo el potencial que ofrece la computación en la nube, ya que a menudo las aplicaciones tienen requisitos y características específicos, que deben ser conocidos por los proveedores de la nube.

Aparte de eso, con el crecimiento de las ofertas de nube pública, para los clientes de la nube se ha vuelto cada vez más difícil decidir qué proveedor puede cumplir con su calidad de servicio (QoS). Por lo tanto, dada la diversidad de la oferta de servicios de la nube, un reto importante para los clientes es descubrir quiénes son los proveedores de la nube que mejor pueden satisfacer sus necesidades.

Para hacer frente a esta situación el Consorcio para el Índice de Medición de Servicios en la Nube (CSMIC), puesto en marcha por la Universidad Carnegie Mellon, desarrollaron el Índice de Medición de Servicios (SMI) para la evaluación de un servicio de nube. Estos índices de medición pueden ser utilizados por los clientes para comparar diferentes servicios en la nube de acuerdo con sus prioridades, hacer cálculos con la importancia de los costos, la responsabilidad, la agilidad, la seguridad y la privacidad, etc. y seleccionar lo que sea apropiado a sus necesidades.

El SMI está concebido como un marco jerárquico. El nivel superior divide el espacio de medición en 7 categorías. Cada categoría se compone por 3 o más atributos. Luego, dentro de cada atributo hay definidos un conjunto de indicadores clave de rendimiento (KPI) que describen los datos recopilados para cada medida. Algunos de estos KPI serán específicos del servicio, mientras que otros se aplican a todos los servicios. Las 7 categorías, con sus respectivos atributos son:

- 1) Financiera. ¿Cuánto cuesta?

Atributos: Adquisición & costo de transición. Costo fijo. Beneficios o participación en los gastos.

La primera pregunta que surge en la mente de organizaciones antes de cambiar a la computación en nube que si es rentable o no. Por lo tanto, el costo es claramente uno de los atributos esenciales de las Tecnologías de la Información (TI) y el negocio. El costo tiende a ser el único

más cuantificable hoy en día, pero es importante para expresar el costo en las características que son relevantes para una determinada organización empresarial.

2) Agilidad. ¿Puede ser cambiado y cómo rápidamente puede ser cambiado?

Atributos: Adaptabilidad. Capacidad. Elasticidad. Extensibilidad. Flexibilidad. Portabilidad. Escalabilidad.

La ventaja más importante de la computación en nube es que se suma a la agilidad de una organización. La organización puede ampliar y cambiar rápidamente sin mucho gasto. La agilidad en la SMI se mide como una velocidad de cambio, que muestra la rapidez con la que las nuevas capacidades se integran en lo que necesita el negocio. A la hora de considerar la agilidad de un servicio de nube, las organizaciones quieren entender si el servicio es elástico, portátil, adaptable y flexible.

3) Garantía. ¿Qué tan probable es que el servicio funcione como se espera?

Atributos: Disponibilidad. Datos geográficos / políticos. Mantenibilidad. Recuperabilidad. Confiabilidad. Resistencia / tolerancia a fallos. Estabilidad del servicio. Utilidad.

Esta característica indica la probabilidad de que un servicio en la nube que funcione como se esperaba o prometida en el SLA (Un acuerdo de nivel de servicio o ANS, en inglés *Service Level Agreement* o SLA). Cada organización busca expandir su negocio y ofrecer mejores servicios a sus clientes. Por lo tanto, la fiabilidad, resistencia y la estabilidad del servicio se convierten en un factor importante para ellos antes de que decidan pasarse a los servicios de la nube.

4) Responsabilidad. ¿Podemos contar con la organización de proveedores?

Atributos: Auditabilidad. Conformidad. Experiencia de contratación. Propiedad de los datos. Facilidad de hacer negocios. Gobernanza. Propiedad. Estabilidad de negocio del proveedor. Certificaciones de proveedor. Contrato de Proveedor. Ética del proveedor. Las necesidades de personal del proveedor. Las funciones de seguridad. La sostenibilidad.

Este grupo de atributos de calidad de servicio se utilizan para medir varias características específicas del proveedor de la nube. Ninguna organización quiere implementar sus aplicaciones y almacenar sus datos críticos en un lugar donde no hay rendición de cuentas de los riesgos de seguridad y conformidad. Las funciones críticas para la rendición de cuentas, que SMI considera al medir y puntuar, son servicios de auditoría, la conformidad, la propiedad de los datos, la ética del proveedor, sostenibilidad, etc.

5) Seguridad y privacidad. ¿El servicio es seguro y privado?

Atributos: Control de acceso & gestión de privilegio. Los datos geográficos/políticos. Integridad de los datos. Privacidad de datos & pérdida de datos. Seguridad física y ambiental. Proactiva de amenazas & gestión de vulnerabilidades. Retención/disposición.

La protección de datos y privacidad son las preocupaciones importantes de casi todas las organizaciones. El alojamiento de datos en otras organizaciones de control es siempre una cuestión crítica que requieren políticas de seguridad estrictas empleado por los proveedores de la nube. Por ejemplo, organizaciones financieras generalmente requieren un elevado cumplimiento de las regulaciones que involucran a la integridad de los datos y la privacidad. La seguridad y la privacidad son también de naturaleza multidimensional e incluyen muchos atributos tales como la confidencialidad, la integridad y la pérdida de datos.

6) Facilidad de uso ¿Es fácil de aprender y de usar?

Atributos: Accesibilidad. Necesidades del cliente. Capacidad de instalación. Facilidad de aprendizaje. Operabilidad. Idoneidad. Transparencia.

Para el uso rápido de servicios en la nube, la facilidad de uso juega un papel importante. Cuanto más fácil de usar y aprender un servicio de nube es, más rápido una organización puede cambiar a servicios en la nube. La facilidad de uso de un servicio en la nube puede depender de varios factores, tales como accesibilidad, capacidad de instalación, facilidad de aprendizaje, operabilidad.

7) Rendimiento ¿Hace lo que necesitamos?

Atributos: Exactitud. Funcionalidad. Interoperabilidad. Tiempo de respuesta del servicio.

Hay muchas soluciones diferentes que se ofrecen por los proveedores de nube abordando las necesidades de TI de las distintas organizaciones. Cada solución tiene un rendimiento diferente en términos de funcionalidad, el tiempo de respuesta del servicio y precisión. Estas organizaciones necesitan entender a través de estas propiedades cuán bien sus aplicaciones funcionarán en las diferentes nubes y si estos despliegues satisfacen sus expectativas.

La forma de medir varios atributos SMI es algo complejo, debido a que muchos de éstos varían con el tiempo. Por lo tanto, *SMICloud* utiliza mediciones históricas y las combina con los valores prometidos para averiguar el valor real de un atributo. Aunque también se da las métricas precisas para cada atributo medible.

A partir de estos atributos SMI, se debe clasificar los servicios en la nube, pero algunos de ellos no se pueden medir fácilmente dada la naturaleza de las nubes, como la seguridad y la experiencia de los usuarios. Además, cada parámetro individual afecta al servicio de una manera diferente, y su impacto en la clasificación general depende en la prioridad que se le dé en el proceso de selección en general. Para solucionar este problema, se propone un proceso analítico jerárquico (AHP: Analytic Hierarchy Process) de clasificación basado en un mecanismo para resolver el problema de asignar las ponderaciones a características considerando la interdependencia entre ellos, proporcionando así una base cuantitativa, necesaria para la clasificación de los servicios en la nube.

La infraestructura *SMICloud* ofrece características tales como servicio de selección basado en la Calidad de Servicio (QoS) y la clasificación de los servicios basado en las experiencias anteriores de los usuarios y el rendimiento de los servicios. Es una herramienta de toma de decisiones, diseñada para proporcionar una evaluación de los servicios de la nube en términos de indicadores clave de rendimiento (KPIs) y necesidades de los usuarios, por lo que los clientes

proporcionan sus requisitos de la aplicación a desplegar (esenciales y no esenciales) al marco que da una lista de servicios en la nube.

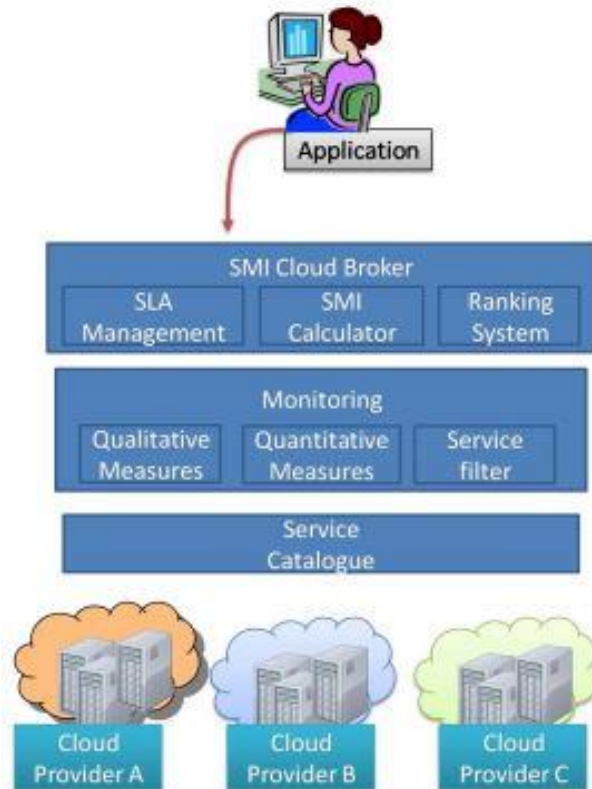


Figura 5. Infraestructura del SMICloud [11]

- *SMICloud Broker*: Recibe la solicitud del cliente para el despliegue de una aplicación. Recoge sus requisitos y lleva a cabo el descubrimiento y clasificación de servicios adecuados con otros componentes tales como *SMICalculator* y sistemas de clasificación. El gestor de SLA es el componente que realiza un seguimiento de los SLA de los clientes con los proveedores de la nube y su historial de cumplimiento. El *Ranking System* clasifica a los servicios seleccionados por la *Cloud Broker* que son apropiados para las necesidades de los usuarios. La *SMICalculator* calcula los diversos indicadores clave de rendimiento (KPIs) que son utilizados por el sistema de clasificación para priorizar los servicios en la nube.
- *Monitorización*: Este componente presenta los servicios en la nube que puede satisfacer los requisitos esenciales de calidad de servicio del usuario. Entonces, se supervisa el rendimiento de los servicios en la nube como la velocidad de la máquina virtual, la memoria, el escalado de latencia, el rendimiento del almacenamiento, la latencia de red y el ancho de banda disponible. También realiza un seguimiento de cómo los requisitos de SLA de clientes anteriores están siendo satisfechos por el proveedor de la nube.
- *Catálogo de Servicios*: almacena los servicios y sus características anunciadas por varios proveedores de la nube.

Los SMI KPI para los proveedores de IaaS son de dos tipos: cualitativos y cuantitativos, aunque este modelo puede ser ampliarse fácilmente para SaaS y PaaS. Cualitativos son aquellos indicadores clave de rendimiento (KPI) que no se pueden cuantificar y se infiere en su mayoría a partir de experiencias de usuario. Cuantitativos son los que se pueden medir utilizando herramientas de monitorización de software y hardware.

Algunos de estos parámetros dependen de aplicaciones de los clientes y algunos son independientes. Por lo tanto, es complejo definir precisamente los valores SMI para un proveedor en particular cuando hay muchos parámetros implicados y la definición del parámetro depende de muchos sub-atributos. A continuación, se define la mayoría de los indicadores clave de rendimiento cuantificables importantes sobre todo el contexto de las nubes de IaaS.

A. Tiempo de Respuesta de Servicio

La eficiencia de un servicio puede ser medido en términos de tiempo de respuesta, es decir, la rapidez con el servicio se puede hacer disponible para su uso. El tiempo de respuesta del servicio depende de varios sub-factores como el tiempo medio de respuesta promedio, el tiempo de respuesta máximo prometido por el proveedor de servicios, y el porcentaje de tiempo que este nivel es pérdida de tiempo de respuesta.

- El tiempo medio de respuesta está dado por $\sum_i T_i / n$ donde T_i es el tiempo entre el momento en que el usuario solicita un servicio IaaS y cuando está actualmente disponible y n es el número total de solicitudes de servicio IaaS.
- Tiempo de respuesta máximo es el máximo tiempo de respuesta prometida por el proveedor de la nube para el servicio.
- Error de tiempo de respuesta viene dada por el porcentaje de ocasiones en que el tiempo de respuesta fue mayor que el tiempo máximo de respuesta prometida. Por lo tanto está dado por $n' / n * 100$, donde n' es el número de ocasiones en las que el proveedor de servicios no fue capaz de cumplir su promesa.

B. La sostenibilidad

La sostenibilidad puede definirse en términos del ciclo de vida del servicio en sí o el impacto medioambiental del servicio de la nube utilizado. Por lo tanto, podemos subdividir en dos atributos: la sostenibilidad del servicio y la sostenibilidad ambiental.

- Sostenibilidad del servicio se define como el número de componentes de un servicio que pueden ser reutilizados sin cambiar con la evolución de las necesidades de los usuarios. En otras palabras, podemos decir que el servicio que sea más sostenible, tendrá muchas más funciones de las necesarias. Por lo tanto, la sostenibilidad del servicio está dada por:

$$\frac{\text{Número de características proporcionadas por el servicio}}{\text{Número de características requeridas por el cliente}}$$

- La sostenibilidad ambiental puede medirse como el promedio de la huella de carbono del servicio. La métrica de la huella de carbono es compleja y depende de muchos

factores. Por lo tanto, puede obtener los valores SMICloud usando calculadoras de carbono como PUE Calculadora.

C. La idoneidad

La idoneidad se define como el grado en que se cumplen los requisitos del cliente por un proveedor de nube. Existen dos sub casos, en primer lugar, si después del filtrado de los proveedores de nube, hay más de un proveedor de nube que satisfagan todos los esenciales y no esenciales de cliente y todos son adecuados. Y por último, si los resultados de filtrado en un proveedor de nube vacía la lista entonces, aquellos proveedores que cumplen funciones esenciales son los elegidos. En esto caso, la idoneidad será el grado de las características de servicio que se acercan a las necesidades del usuario. El resultado sería:

$$\frac{\text{número de características no esenciales proporcionados por servicio}}{\text{número de características no esenciales requeridos por el cliente}}$$

$$\begin{aligned} & \text{sólo si se satisfacen los requisitos esenciales} \\ & = 1 \text{ si todas las funciones están satisfechos} \\ & = 0 \text{ en caso contrario} \end{aligned}$$

D. La exactitud

La exactitud de la funcionalidad del servicio mide el grado de proximidad al usuario, y espera un valor real o un resultado generado por el uso del servicio. Para los recursos computacionales, tales como máquinas virtuales, el primer indicador de exactitud es el número de veces que el proveedor de la nube se desvió de una SLA prometido. Se define como la frecuencia del fracaso en el cumplimiento de SLA prometido en términos de la unidad de informática, redes y almacenamiento. Si f_i es el número de veces que el proveedor de la nube deja de satisfacer los valores prometidos para el usuario sobre el servicio tiempo T entonces, la precisión de frecuencia se define como $\sum_i \frac{f_i}{n}$ donde n es el número de usuarios anteriores. El otro indicador de precisión es el valor de precisión que se define por $\sum_i \frac{\alpha_t - \alpha_i}{T_i}$ donde α puede ser la unidad computacional, de red o de almacenamiento del servicio y T_i es el tiempo de servicio T para el usuario i.

E. La transparencia

La transparencia es una característica importante de los servicios en la nube, debido a la rápida evolución de estos servicios. Se puede inferir como un tiempo para que el rendimiento de la aplicación del usuario se ve afectada durante un cambio en el servicio. También puede ser calculado en términos de frecuencia de tales efectos. Por lo tanto, se puede medir por $\sum \frac{\text{Tiempo de servicio afectado}_i}{\text{número de tales ocurrencias}_i}$ donde n es el número de clientes que utilizan el servicio y i indica el cliente.

F. La interoperabilidad

La interoperabilidad es la capacidad de un servicio para interactuar con otros servicios ofrecidos por el mismo proveedor o de otros proveedores. Es más cualitativo y puede ser definido por la experiencia de usuario. Pero, puesto que es un parámetro importante para clientes de cloud, lo definimos como:

$$\frac{\text{número de plataformas ofrecidas por el proveedor}}{\text{número de plataformas requerida por los usuarios de interoperabilidad}}$$

G. La disponibilidad

La disponibilidad es el porcentaje del tiempo que un cliente pueda acceder al servicio. Está dada por:

$$\frac{\text{tiempo total de servicio} - \text{tiempo total para que el servicio no estaba disponible}}{\text{tiempo total de servicio}}$$

H. La fiabilidad

La fiabilidad refleja cómo opera un servicio sin fallos durante un determinado tiempo y condición dada. Por lo tanto, se define basado en el tiempo medio hasta el fallo prometido por el proveedor de la nube y fracasos anteriores experimentadas por los usuarios.

Si numfailure es el número de usuarios que han experimentado el fracaso en la cantidad de tiempo por debajo de lo prometido por el proveedor de la nube y n es el número de usuarios. Sea p_mttf el tiempo medio hasta fallo. Se mide por:

$$\text{Fiabilidad} = \text{probabilidad de violación} \times p_mttf = \left(1 - \frac{\text{numfailure}}{n}\right) * p_mttf.$$

Fiabilidad de almacenamiento puede definirse en términos de durabilidad que es la probabilidad de fallo de un dispositivo de almacenamiento.

I. La estabilidad

La estabilidad se define como la variabilidad en el rendimiento de un servicio. Para el almacenamiento, es la variación en la media del tiempo de leer y escribir. Para los recursos computacionales, es la desviación del modo indicado en el SLA es decir, $\sum \frac{\alpha_{avg,i} - \alpha_{sla,i}}{T}$ donde α puede ser unidad computacional, unidad de red o unidad de almacenamiento del recurso; $\alpha_{avg,i}$ es el rendimiento promedio observado del usuario i quien arrendó el servicio de computación en nube, $\alpha_{sla,i}$ es el valor prometido en el SLA; T es el tiempo de servicio; y n es el número total de usuarios.

J. El costo

El costo depende de dos atributos: adquisición y en curso. No es fácil comparar los diferentes precios de los servicios que ofrecen diferentes características y por lo tanto tienen muchas dimensiones. Incluso el mismo proveedor ofrece diferentes máquinas virtuales que pueden satisfacer las necesidades del usuario. Para ello, se ha definido un volumen basado en sistema métrico es decir el costo de una unidad de CPU, RAM, unidad de almacenamiento y red.

El costo de la máquina virtual es $\frac{p}{cpu^a * net^b * data^c * RAM^d}$ donde a, b, c y d son los pesos para cada atributo de recursos y $a + b + c + d = 1$. El peso de cada atributo puede variar de una aplicación a otra. Así, podemos utilizar diferentes pesos de cada atributo en función de la aplicación del usuario.

K. La adaptabilidad

La adaptabilidad es la capacidad del proveedor del servicio para ajustar los cambios en los servicios basándose en la petición del cliente. Se define como el tiempo necesario para adaptarse a los cambios o actualizar el servicio al siguiente nivel.

L. La elasticidad

La elasticidad se define en términos de cuánto un servicio en nube puede ser escalado durante las horas punta. Este es definido por dos atributos: el promedio de tiempo necesario para expandir o contraer la capacidad de servicio y la máxima capacidad de servicio. La capacidad es el número máximo de la unidad de cómputo que pueden ser provistos en las horas punta.

M. La usabilidad

La facilidad de uso de un servicio en nube está definida por los atributos de usabilidad. Los componentes tales como la operabilidad, facilidad de aprendizaje, capacidad de instalación y la comprensión pueden ser cuantificados como el tiempo promedio experimentada por los usuarios anteriores del servicio de Cloud para operar, aprender, instalar y comprender, respectivamente.

3.d Modelos de servicio y modelos de despliegue

El NIST (Instituto Nacional de Estándares y Tecnología) y la mayoría de usuarios y proveedores de la nube clasifican la computación en nube en dos modelos distintos:

-Modelos de despliegue. Se refieren a la localización y gestión de la infraestructura de la nube (pública, privada, híbrida y comunitaria).

-Modelos de servicio. Se refieren a los tipos específicos de servicios a los que se puede acceder en una plataforma de computación en la nube (software como servicio, plataforma como servicio e infraestructura como servicio).

Las tecnologías de *cloud computing* ofrecen tres modelos de servicio:

Infrastructure as a Service (IaaS)

Al usuario se le pone disposición el uso de la infraestructura informática (capacidad de computación, espacio de disco y bases de datos entre otros) como un servicio para que así, el cliente pueda ejecutar cualquier tipo de software, desde sistemas operativos hasta aplicaciones. En vez de adquirir servidores, espacio en un centro de datos o equipamiento de redes, los clientes compran todos estos recursos a un proveedor de servicios externo. Es decir, el modelo IaaS proporciona la infraestructura necesaria para ejecutar aplicaciones, por lo que los clientes renuncian a usar sus propios equipos físicos, sino que usan los recursos virtuales que le proporciona el proveedor de Servicios Cloud y sobre dichas infraestructuras el cliente es responsable de la instalación, mantenimiento, y ejecución de su propia pila de aplicaciones.

Con esta externalización, las facturas asociadas a este tipo de servicios se calculan en base a la cantidad de recursos consumidos por el cliente, basándose así en el modelo de pago por uso.

Sin embargo, el consumidor (usuario) no gestiona ni controla la infraestructura fundamental de la nube, pero tiene control sobre sistemas operativos, almacenamiento y aplicaciones desplegadas y es posible un control limitado de componentes seleccionados de red y correos, por ejemplo, los firewalls o los antispam. En la práctica el cliente IaaS alquila (pago por uso y prestaciones) recursos informáticos en su propio centro de datos, en lugar de comprarlos.

Uno de los proveedores más destacados es Amazon que ofrece Amazon Web Services (AWS) mediante servicios como EC2, S3, SimpleDB, etc. que proporcionan servidores virtuales, almacenamiento o bases de datos. El gran problema, también en los otros modelos, es la seguridad de los datos y la privacidad.

Software as a Service (SaaS)

Consiste en la entrega de aplicaciones como servicio, siendo un modelo de despliegue de software mediante el cual el proveedor ofrece licencias de su aplicación a los clientes para su uso como un servicio bajo demanda.

Los proveedores de los servicios SaaS proveen acceso a una colección de programas de aplicación. Los proveedores SaaS ofrecen a los usuarios acceso a un conjunto de aplicaciones específicas que son ejecutadas en las infraestructuras del proveedor y controladas por él. En muchas ocasiones también se le denomina “software bajo demanda” (dependiendo de la forma de pago). Es decir, el cliente no tiene acceso ni control a la plataforma subyacente ni siquiera, en general, de las capacidades y funcionalidades de la aplicación con la única posible excepción de poder modificar aquellos parámetros de configuración de la aplicación destinados de forma específica para el usuario y su personalización. Además, el usuario no tiene que instalar ningún programa de software como sí se hace en el modelo tradicional.

Es decir, SaaS es una nueva forma de distribuir software que tiene un régimen de pago mensual. El proveedor del servicio es quien tiene hospedadas las aplicaciones en sus servidores permitiendo que sus clientes accedan a las mismas a través de una conexión a Internet, estando por lo tanto disponibles en cualquier momento y desde cualquier lugar.

Ejemplos comerciales de SaaS: WebMail (Gmail, Yahoo, etc.), Salesforce, Google Docs, Office 365, etc.

Platform as a Service (PaaS)

Al usuario se le permite desplegar aplicaciones propias, ya sean adquiridas o desarrolladas por el propio usuario en la infraestructura de la nube de su proveedor, que es quien ofrece la plataforma de desarrollo y las herramientas de programación.

En este modelo el proveedor ofrece el uso de su plataforma que a su vez se encuentra alojada en sus infraestructuras. Por lo que el usuario no tiene control sobre la plataforma ni las infraestructuras, pero sí sobre sus aplicaciones. Un usuario puede adoptar uno o más de estos modelos según sus necesidades. Los sistemas PaaS son muy útiles ya que facilitan a los desarrolladores y empresas innovadoras pequeñas, desplegar aplicaciones basadas en la web sin el coste y complejidad que supondría la compra de servidores y sus correspondientes configuraciones y puestas en funcionamiento.

PaaS pertenece al mundo de desarrollo de software. Puede ser definido como una plataforma de computación para desarrollar software / aplicaciones web sin la necesidad de operar y mantener infraestructura.

PaaS es similar a SaaS, aunque el servicio es un entorno completo de desarrollo de aplicaciones y no sólo el uso de una aplicación. Las soluciones de PaaS se diferencian de SaaS en que proporcionan una plataforma de desarrollo de desarrollo virtual alojado en la nube y accesibles desde un navegador Web.

Es decir, las soluciones PaaS son plataformas de software para las cuales la herramienta de desarrollo en sí misma está alojada en la nube y se accede a través de un navegador web. Los desarrolladores pueden construir, analizar, desarrollar, testear, documentar y poner en marcha aplicaciones en un sólo proceso, sin tener que instalar ninguna herramienta adicional en sus computadoras.

Ejemplos comerciales de PaaS: Google App Engine, Force.com (de Salesforce), Microsoft Azure Services, etc.

A continuación, se deja claro el nivel de servicio, es decir hasta donde alcanzan los trabajos y responsabilidades del Proveedor de Servicios Cloud en cada uno de los 3 modelos (niveles) de servicio:

Separation of Responsibilities

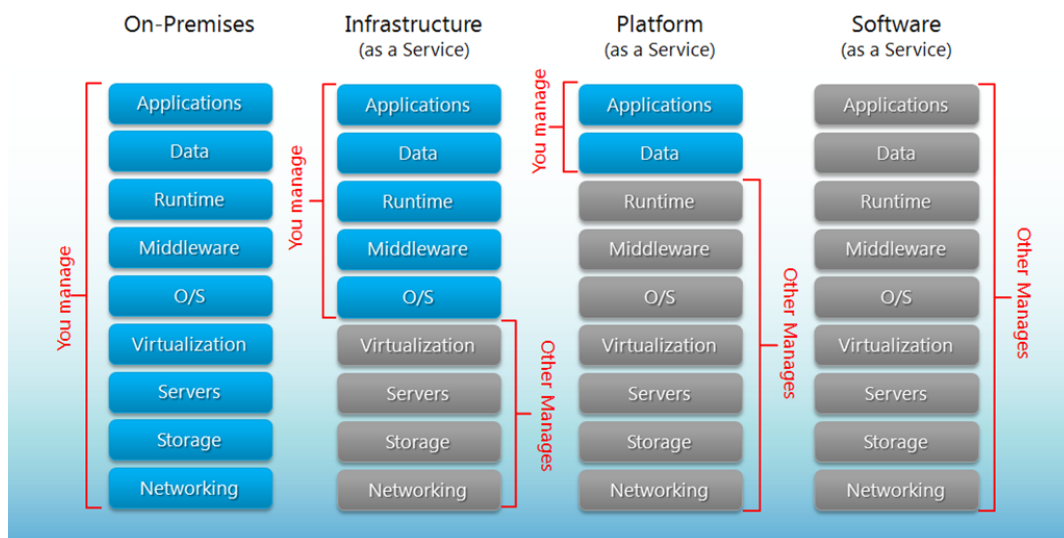


Figura 6. Distinción entre IaaS, PaaS y SaaS [15]

Según el NIST existen cuatro posibles formas de desplegar y operar una infraestructura de *cloud computing*, tomando en cuenta las necesidades de las empresas, el modelo de servicio ofrecido y cómo se despliegan, de dónde se encuentren instaladas las aplicaciones y qué clientes pueden tener acceso a ellas.



Figura 7. Esquema general de las diferentes formas de desplegar una infraestructura de *cloud computing* [13]

Cloud Público (Nube Externa)

Forma de implementación donde toda la infraestructura se encuentra en manos de un proveedor que ofrece servicios al público en general (tanto usuarios individuales como corporaciones), accediendo a los servicios a través de Internet o redes privadas virtuales (VPNs), por lo que se podría tratar como una desventaja, la dependencia de los servicios en línea y el acceso a través de Internet. Además, un despliegue de Cloud Público se caracteriza por ofrecer recursos TIC sobre infraestructuras compartidas entre múltiples clientes.

Es habitual que en las nubes públicas, el usuario acceda al servicio como cliente externo del proveedor de la infraestructura. Gracias a la virtualización y a los procesos de automatización del servicio que dicho proveedor tiene implementados, el usuario puede entonces automatizar el despliegue de máquinas preconfiguradas con un solo click, utilizando plantillas propias o del proveedor, o puede incluso integrarlas rápidamente con aplicaciones propias.

Como características a esta forma de implementación tenemos:

- Reducido plazo de tiempo para la disponibilidad del servicio.
- No se requiere una inversión para su implementación.
- Posibilita el aprovechamiento de la infraestructura de los proveedores de servicios, permitiendo adicionalmente una alta escalabilidad y flexibilidad en la modificación del dimensionamiento del servicio.
- Favorece la utilización de conjuntos de software estándar.
- Lleva asociadas unas cuotas iniciales de pago más bajas que el resto de implementaciones. Adicionalmente los costes del *cloud* público son variables, cumpliendo el principio de pago por uso
- La información corporativa se encuentra alojada en la nube pública junto a la del resto de clientes del proveedor, lo que implica, además de no poder tener localizada físicamente dicha información, imponer al proveedor una serie de requisitos de alta exigencia en temas de seguridad y protección de datos.
- Las nubes públicas pueden complementarse con otros servicios compartidos tales como servicios de balanceo y aceleración de carga, servicios de backup o de seguridad perimetral. El compartir recursos, permite un importante ahorro de costes respecto al modelo de Cloud Privado.
- Está alojada, operada y gestionada por un proveedor desde uno o más centro de datos. Los procesos de gestión, seguridad de datos y actualización del software y hardware se realizan por parte del proveedor y de forma transparente al uso diario por parte del cliente. Por lo que se tiene un control muy bajo de la seguridad física y lógica.

Por lo que, este tipo de nube está enfocada a pequeñas empresas ya que el ahorro de costes es vital para ellas. Por supuesto, puede ser útil para grandes que quieran alojar datos menos importantes.

Cloud Privado (Nube Interna)

Forma de implementación caracterizada por el suministro por parte del proveedor, de entornos virtualizados que pueden ser implementados, usados y controlados por la misma empresa contratante del servicio y además, la solución *cloud* pueden estar alojadas en las instalaciones del cliente, o en un entorno dedicado dentro de las instalaciones de un proveedor de servicios IT externo. En este último caso, pueden aprovecharse las capas tecnológicas y de servicios que el propio proveedor pueda tener desplegadas sin incurrir en inversiones adicionales. Es decir, una nube privada es aquella en la que solamente una organización, utilizando tecnologías como la virtualización, tiene acceso a los recursos que se utilizan para implementar la nube, por lo que se dice que una empresa dispone de un entorno cloud en exclusiva (un servicio a medida).

Como características propias tenemos:

- Reducido plazo de tiempo para la puesta en servicio y una alta flexibilidad en la asignación de recursos.

- Al contrario que el *cloud público*, requiere de inversión económica para la implementación de la solución contratada. A las inversiones efectuadas inicialmente deben sumarse aquellas que garanticen la evolución tecnológica de las infraestructuras adquiridas. En el caso de que esta renovación no se produzca, con el tiempo este tipo de despliegues caen rápidamente en la obsolescencia.
- Lleva asociados sistemas y bases de datos locales.
- Ofrece la posibilidad de aprovechar el personal existente y las inversiones en sistemas de información realizadas con anterioridad. Por lo que más gastos de personal y de mantenimiento de todas las infraestructuras hardware y software.
- Generan una sensación de mayor seguridad para los clientes que disponen de este tipo de despliegues, al no compartir recursos con otros usuarios.
- Se despliega considerando tecnologías afines/conocidas a las propias de la empresa o bien atendiendo a sus capacidades para interconectarse con otras nubes. La capacidad de elegir al proveedor permite seleccionar los recursos tecnológicos que más se adapten a las necesidades técnicas o económicas de la empresa, así como las tecnologías que mejor se integren con otros servicios de infraestructura ya existentes (backup, balanceadores, red, etc).
- Permite disponer de un control total de la infraestructura, de los sistemas y de la información corporativa tratada por éstos.
- Facilita el control y la supervisión de los requisitos de seguridad y protección de la información almacenada.
- La escalabilidad de la nube privada se ve mermada por los altos costes de inversión.
- La seguridad puede verse comprometida por la propia vulnerabilidad de un centro de datos interno, no especializado.

Así, las nubes privadas están especialmente orientadas a organizaciones con alta concentración de recursos y sistemas tecnológicos, tales como entidades bancarias, Administración Pública, entornos de investigación y desarrollo, consultorías y asesorías legales, tecnológicas o de negocio, etc.

Cloud Híbrido

Forma de implementación cuya infraestructura *cloud* resulta de combinar dos o más formas de *clouds* (privado, comunitario o público), y surge a partir de la necesidad de los clientes que, aunque cuentan con infraestructura propia buscan aprovechar las ventajas de los servicios de un proveedor externo. Estas diferentes formas de *clouds* continúan siendo entidades únicas interconectadas mediante tecnología estandarizada o propietaria, la cual permite la portabilidad de datos y aplicaciones entre nubes, por lo que una entidad que emplee esta forma de implementación se podría beneficiar de las ventajas asociadas a cada tipo de *cloud*.

Como principales características encontramos:

- Ofrece una mayor flexibilidad en la prestación de servicios de TI, al mismo tiempo que se mantiene un mayor control sobre los servicios de negocio y de datos.
- Con una solución de *cloud* híbrido, se consigue una rápida puesta en servicio.

- Implica mayor complejidad en la integración de la solución *cloud*, como consecuencia de ser una solución que se compone de dos formas distintas de implementación de servicios en la nube.
- Permite integrar las mejores características de las dos formas de implementación *cloud*, en cuanto al control de los datos y a la gestión de las funciones básicas de la entidad.
- Posibilita la selección por parte del proveedor, de infraestructura escalable y flexible, permitiendo una alta agilidad en el redimensionamiento de la solución.
- Permite el control interno de los servicios *cloud* desde la propia entidad.
- La inversión inicial es más moderada y permite realizar un aumento progresivo de la utilización de los servicios de la nube pública según necesidades. Para empresas con aumento de necesidades puntuales estas nubes son las que les permiten obtener servicios bajo demanda combinándolos con la nube privada.

También existen riesgos, al estar en dos nubes, es fácil a largo plazo integrar datos más sensibles en la nube pública y al contrario. Sobre todo, si estamos ante grandes corporaciones donde la información sensible para por muchas manos. Además, este tipo de infraestructuras son mucho más complejas y problemáticas porque deben combinar mucha más tecnología. Lo ideal es articular la solución híbrida que mejor responda a sus necesidades reales. Tres de cada cuatro nuevos proyectos se harán sobre este tipo de *cloud*. De esta forma, el desarrollo de aplicaciones y servicios que permanecen sobre estas infraestructuras permitirán a las empresas agilizar la toma de decisiones, así como acortar los tiempos de producción y de llegada al mercado.

Para las grandes empresas puede llegar a ser un problema más que una solución. Sin embargo, en el caso de pequeñas compañías puede ser una buena forma de proteger los datos más preciados a la vez que se ahorran costes con la combinación de un cloud público.

Las nubes híbridas aportan agilidad y reducción de costes sacrificando algo de control. Aunque son una solución compleja pues requiere coordinar una infraestructura propia con otra gestionada por otro entorno, así como una buena conectividad entre las dos plataformas, gracias a su versatilidad y a la experiencia que pueden aportar algunos integradores, están llamadas a tener un amplio protagonismo en el futuro. Entre los principales aspectos a tener en cuenta al implementar una solución de *cloud* híbrido destacan:

- Seguridad: En una *cloud* híbrida, la seguridad debe iniciarse en el sitio donde comienza la transferencia de datos. Por lo tanto, es necesario encriptar los datos antes de ser enviados para que no estén expuestos. Es necesario realizar la comunicación a través de una conexión privada (VPN).
- Hypervisor: Si el hypervisor del *cloud* público es diferente al del *cloud* privado, es necesario utilizar un software de conversión eficiente.
- Gestión y administración: Las nubes híbridas requieren niveles mayores de automatización en la gestión y administración (de lo contrario se complican los procesos de gestión de cambios).
- Visión completa y unificada del servicio: Puesto que los diferentes recursos se encuentran ubicados en CPDs (centro de procesamiento de datos) diversos y son

gestionados por organizaciones diferentes, es importante asegurar la visibilidad del conjunto a través de alguna herramienta transparente y única.

Hybrid Cloud - Ejemplo de implementación

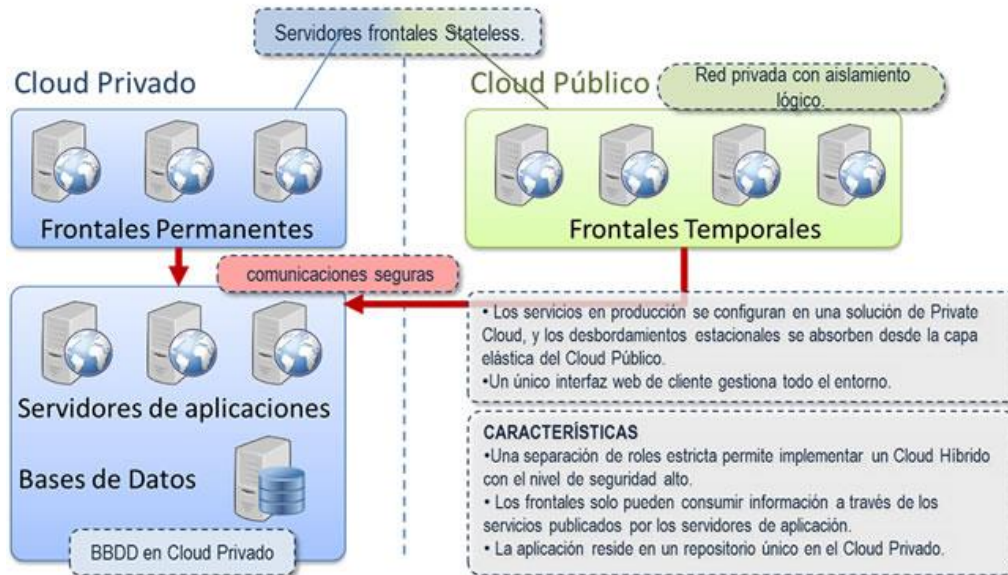


Figura 8. Forma de implementar una nube híbrida [13]

Cloud Comunitaria

Según el NIST, se define esta nube como aquella en que su infraestructura es compartida por varias organizaciones y soporta una comunidad específica que tiene características compartidas, como por ejemplo requerimientos de seguridad, política... Puede ser gestionada por las organizaciones o una tercera parte y puede existir en las dos formas pública y privada.

3.e Situación actual y futura del *cloud computing* en el mundo

Puede que el término *cloud computing* nos suene un poco ajeno, pero en mayor o menor medida, estamos haciendo uso del *cloud computing* o computación en la nube en nuestro día a día, con servicios de correo electrónico, almacenamiento de archivos, etc.

Cada vez son más las empresas que optan por el *cloud computing*, ya que ayuda a mejorar la productividad y la competitividad de las pequeñas y medianas empresas, algo a lo que antes solo podían acceder grandes empresas. Por esta razón, cada vez son más los estudios que analizan la comparativa entre los mejores *cloud computing* del mercado. Además, el *cloud computing* ahorra el 40% de los costes informáticos de las pymes, datos reflejados en el “Informe 2015 Cloud Computing” realizado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), e indican que la implantación de tecnologías de *cloud computing* favorece la productividad y reduce costes de las empresas que las adoptan. Además, su potenciación tiene un impacto positivo y directo en la economía y la generación de empleo, podría suponer la creación de más de 3,8 millones de empleos en Europa hasta el año 2020.

En Abril de 2016 el Ministerio de Industria, Energía y Turismo, a través de la Entidad Pública Empresarial Red.es, organismo dependiente de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, con un presupuesto total de 40 millones de euros presenta el “Programa de fomento de la demanda de soluciones de computación en la nube para PYMEs”, que se engloba dentro de las líneas de actuación estructurales de la Agenda Digital para España y cuyo objetivo es el de fomentar la digitalización y mejora la competitividad de la PYME española adoptando soluciones basadas en *cloud computing*. Éstas garantizan el ahorro de costes, la accesibilidad y la eficiencia energética de los sistemas de información para posicionar a la PYME estratégicamente en el mercado.

Las principales conclusiones obtenidas por el ONTSI serían:

- **Movilidad:** Al hacer uso de los servicios de computación en la nube, no es necesaria la instalación de software en los terminales. El acceso se realiza a través de Internet desde cualquier equipo conectado, y con las integraciones móviles desde cualquier lugar.
- **Flexibilidad:** El paso de software como producto a software como servicio fomenta la fórmula de pago por uso. Permite dimensionar los servicios contratados a las necesidades puntuales de la pyme.
- **Productividad:** La flexibilidad en la organización, el acceso remoto y los equipos conectados y colaborativos, asociados al uso de soluciones en la nube, actúan como impulsores de la productividad de las empresas.
- **Ahorro:** Se ha demostrado que tienen un efecto directo en el ahorro de costes informáticos de las pymes. Hasta un 40% de la inversión en hardware y software, un 31% en los costes de personal TIC, y hasta un 80% en consumo energético.
- **Seguridad:** Las empresas proveedoras de servicios de *cloud computing* ofrecen unos estándares de seguridad muy elevados. Por encima de lo que pueden alcanzar, por medios y conocimientos, la mayoría de las pymes. El uso de esta tecnología permite que

las empresas pequeñas y medianas experimenten esos niveles de seguridad en sus comunicaciones, datos y equipos.

Por lo que esta tendencia podría llevarnos a esperar una migración en masa de la mayoría de aplicaciones y datos de las empresas al *cloud* en 2016, pero sin embargo no va a ser así hasta que mejoren algunos aspectos que preocupan mucho a los usuarios, como la seguridad. Los presupuestos de seguridad en IT van a subir entorno a un 20% en 2016 debido a la creciente complejidad del *cloud computing*. Algunos de los principales retos en seguridad son: el control de las descargas, la compartición externa o las grietas de seguridad en aplicaciones que permiten el acceso a dispositivos no autorizados.

Sin embargo, hacer una copia de seguridad y almacenar datos en la nube presenta sus propios desafíos, sobre todo a las empresas que carecen de grandes equipos de TI. Los datos son por lo general el mayor activo de una organización, y por lo tanto requiere protección frente a desastres, pérdida o robos. En la economía digital en tiempo real, los datos también deben ser de fácil acceso –para el personal autorizado–, de cara a que los empleados sean productivos y sirvan mejor a los clientes. Proporcionar backup y una adecuada protección de datos al mismo tiempo que se permite un acceso fácil y rápido a los datos de forma controlada puede ser difícil, incluso si éstos están en un solo lugar. Hoy en día, sin embargo, este tipo de entornos simples de TI están desapareciendo. Las empresas de cualquier tamaño indistintamente almacenan datos en múltiples ubicaciones; un centro de datos interno, servidores físicos y virtuales, almacenamiento fuera del edificio, en la nube (a menudo con múltiples proveedores), ordenadores en red, dispositivos móviles, aplicaciones móviles y cuentas cloud de los empleados como Dropbox... Las empresas están procesando cada vez más una amplia gama de cargas de trabajo en entornos mixtos, incluyendo las aplicaciones físicas y virtuales, y dispositivos móviles. Por lo que para los profesionales IT que administran redes para pequeñas y medianas empresas, tratar de gestionar y proteger los datos en varios lugares utilizando múltiples soluciones puntuales puede convertirse rápidamente en una frustrante pesadilla que consuma buena parte de su tiempo.

Si se usa sólo almacenamiento en la nube se puede complicar el acceso a los datos, protección y seguridad ya que los datos se almacenan en un lugar remoto gestionado por un tercero y conectados por una red. Si se interrumpe la red, los datos no serán accesibles a menos que se haya hecho un backup en las instalaciones, ya sea en un centro de datos o algún otro almacenamiento local, por ejemplo, una estación de trabajo de los empleados. Además, una empresa que utiliza solamente almacenamiento en la nube estará delegando en un tercero buena parte de la protección física de sus datos. Los acuerdos de servicios pueden implicar niveles de protección de datos y tiempo de actividad de la nube, pero con apenas garantías.

“Como una persona IT, el trabajo se vuelve cada vez más desafiante: cada vez hay más datos localizados en distintos lugares y uno no puede perder de vista donde están, además de asegurarse de que estén protegidos en todo momento”, dice Frank Jablonski, vicepresidente de producto de Acronis, proveedor de soluciones híbridas de protección de datos en la nube para las empresas.

Europa es la mayor productora de datos científicos del mundo, pero la insuficiencia y fragmentación de las infraestructuras impiden que se aproveche plenamente el potencial de esos macrodatos. La Comisión Europea tiene previsto reforzar e interconectar las actuales infraestructuras de investigación para crear una nueva “Nube Europea de la Ciencia Abierta”, que ofrecerá a los 1,7 millones de investigadores y los 70 millones de profesionales de la ciencia y la tecnología europeos un entorno virtual para almacenar, compartir y reutilizar sus datos entre las diversas disciplinas y a través de las fronteras.

Dicha nube se basará en la infraestructura europea de datos, que desplegará las redes de banda muy ancha, los mecanismos de almacenamiento a gran escala y la capacidad de supercomputación necesarios para poder acceder a grandes conjuntos de datos almacenados en la nube y tratarlos. Estas infraestructuras de categoría mundial permitirán que Europa participe en la carrera mundial por una informática de alto rendimiento de forma conmensurable con su potencial económico y sus conocimientos.

Centrada inicialmente en la comunidad científica, en Europa y entre sus socios mundiales, la base de usuarios se ampliará con el tiempo al sector público y a la industria. Esta iniciativa forma parte de un conjunto de medidas para reforzar la posición de Europa en el ámbito de la innovación impulsada por los datos, aumentar la competitividad y la cohesión y contribuir a la creación de un mercado único digital en Europa.

La Comisión implantará progresivamente la Iniciativa Europea de Computación en la Nube a través de una serie de acciones, entre ellas:

A partir de 2016: creación de una Nube Europea de la Ciencia Abierta destinada a los investigadores europeos y sus colaboradores científicos mundiales mediante la integración y consolidación de las plataformas de infraestructuras electrónicas, la agrupación de las nubes científicas e infraestructuras de investigación existentes, y el apoyo al desarrollo de los servicios basados en la nube.

2017: apertura por defecto de todos los datos científicos producidos por los futuros proyectos en el marco del programa de investigación e innovación Horizonte 2020, con una dotación de 77 000 millones EUR, para garantizar que la comunidad científica pueda reutilizar la enorme cantidad de datos que generan.

2018: puesta en marcha de una iniciativa emblemática para acelerar el incipiente desarrollo de las tecnologías cuánticas, que constituyen la base para la próxima generación de superordenadores.

De aquí a 2020: desarrollo y despliegue de una infraestructura europea a gran escala de computación, almacenamiento de datos y redes de alto rendimiento que incluya la adquisición de dos prototipos de superordenadores de nueva generación, uno de los cuales se sitúe entre los tres primeros del mundo, la creación de un centro europeo de macrodatos, y la mejora de la red básica para la investigación y la innovación (GEANT).

Se estima que serán necesarias inversiones públicas y privadas por valor de 6 700 millones EUR para implantar la Iniciativa Europea de Computación en la Nube. La Comisión calcula que, globalmente, se destinarán a dicha iniciativa 2.000 millones de euros procedentes de los fondos de Horizonte 2020. Se estima, además, que las inversiones públicas y privadas suplementarias para el período de cinco años ascenderán a 4.700 millones.

Esta iniciativa se enmarca dentro del plan que ha presentado el Ejecutivo comunitario en el marco de la estrategia europea hacia el mercado único digital. En conjunto, Bruselas confía en que el paquete digital movilice inversiones públicas y privadas por valor de 50.000 millones de euros para la digitalización de la industria europea.

Además de la nube europea, la Comisión ha propuesto armonizar estándares en cinco ámbitos prioritarios: las redes 5G, las nubes informáticas, el llamado 'Internet de las cosas', las tecnologías de datos y la ciberseguridad.

4. *Cloud storage*

4.a Almacenamiento de archivos en la nube

El Almacenamiento en la nube es un modelo nuevo tecnológico que consiste en almacenar muchos datos en varios servidores virtuales, los cuales están administrados por terceros. Estos proveedores gestionan y operan grandes centros de datos y los usuarios finales adquieren o alquilan espacio dentro de sus servidores, dependiendo de las necesidades de cada uno. Los operadores de dichos centros, virtualizan los recursos de acuerdo a los requerimientos de los usuarios para que a su vez ellos puedan utilizar este servicio para el almacenamiento de sus datos.

El almacenamiento en la nube o *cloud storage* proporciona seguridad a los datos que en él se almacenan debido a la independencia de los datos y demás información de los propios equipos. Esta característica permite que los datos estén siempre disponibles independientemente del equipo de trabajo, protegiendo de esta manera estos ante indisponibilidad de dichos equipos, así como proporcionando acceso a la información desde cualquier ubicación o dispositivo.

El *cloud storage*, evidentemente, necesita de recursos de disco, estos recursos pueden pertenecer a distintos proveedores que han de garantizar la disponibilidad y backup de los datos, o servidores propios, en tal caso han de adoptarse las medidas oportunas para la protección y disponibilidad de los mismos, según la criticidad de los datos y las leyes de protección de los mismos vigentes. El aumento de las necesidades de disco, tanto en ámbitos empresariales como personales, está provocando que la solución de almacenamiento en la nube se implante en numerosas empresas y usuarios, que contratan almacenamiento con distintos proveedores pagando sólo el coste por uso del servicio disminuyendo así la adquisición y mantenimiento de nuevas infraestructuras.

Existen actualmente una gran variedad de compañías que se dedican a dotar de este servicio a los usuarios y empresas, tales como Dropbox, SugarSync, etc. Estos proveedores brindan sus servidores y sus unidades de disco para el uso de clientes, para que estos puedan almacenar en ellos sus datos y por tanto, acceder a los mismos desde cualquier dispositivo con conexión a Internet. El software desarrollado es de código cerrado, es decir, el cliente no tendrá acceso a este y por tanto no podrá realizar modificaciones sobre el desarrollo software de la plataforma de almacenamiento en la nube, aunque existe ownCloud de código abierto descrito más adelante. Los servicios que ofrecen este tipo de proveedores son similares, siendo principalmente la disponibilidad, compartición de archivos, sincronización de directorios mediante la instalación de un cliente de la plataforma usada un dispositivo. La capacidad de almacenamiento y servicios que pueden disfrutar los usuarios difiere de un proveedor a otro, siendo común ofertar una determinada capacidad de almacenamiento sin coste a los usuarios cuando estos crean su cuenta.

A su vez, existen opciones de almacenamiento en la nube open source, es decir, software de código abierto que permite adaptar la tecnología de almacenamiento en la nube a las distintas necesidades de los usuarios. Este código libre es usado por compañías que ofrecen a los usuarios servicios de almacenamiento haciendo uso de este software, como es el caso de Owncube. La alternativa de uso de almacenamiento en la nube mediante software libre haciendo

uso de un servidor propio, proporciona gran versatilidad y adaptación a los usuarios y a las empresas, ya que pueden adaptar el software creado bajo esta licencia a las necesidades propias, así como garantizar la localización de sus datos. Esta alternativa necesitará la inversión en infraestructura por parte de la empresa que permita su despliegue. Algunas de estas alternativas de software libre son ownCloud, Ubuntu One, etc.

El acceso a la información almacenada en una plataforma *cloud* puede hacerse por varias vías. Por un lado, se puede acceder directamente al espacio de almacenamiento mediante protocolos comunes (por ejemplo WebDAV) y trabajar con este espacio de igual forma que si lo estuviéramos haciendo con un disco duro local. Otra posibilidad es acceder al espacio de almacenamiento utilizando una interfaz Web, que permite de una forma sencilla, “subir” ficheros a la nube o borrar documentos. La mayoría de interfaces Web actuales para este tipo de servicios, permiten *drag and drop*, facilitando la subida de archivos. Las plataformas de *cloud storage* profesionales también permiten el acceso a través de una API especialmente construida, y ofrecen funciones básicas que permiten copiar archivos, borrarlos o moverlos por medio de programación. De esta manera se pueden integrar las ventajas del almacenamiento remoto en cualquier aplicación empresarial que se ejecute en los terminales de los usuarios. El sistema de almacenamiento se convierte en el soporte o infraestructura del sistema de información o ficheros implantado. La empresa se despreocupa de los límites físicos y almacena la información que necesita, sin límites.

Al elegir un servicio en la nube, es importante tener en cuenta las necesidades individuales del negocio, en vez de mirar las mejores soluciones globales de almacenamiento en la nube; por lo que una lista de características importantes sería:

4.a.i Sincronización automática

El proceso es transparente: cuando hay nuevos archivos o se han modificado, se suben a la red automáticamente. Por lo que los datos están siempre actualizados y siempre accesibles desde cualquier dispositivo conectado a la red. La sincronización de carpetas en varios equipos es muy útil, pero también arriesgada porque lo que borremos en uno de ellos se verá reflejado en el resto de dispositivos en el momento que se conecten a Internet. Por ello, deberemos tener mucha precaución con el borrado de archivos y especialmente con su sobrescritura. Si en algún momento detectamos que hemos actuado erróneamente en uno de los equipos, podemos mantener cualquiera de los otros sin conexión hasta recuperar los archivos deseados. También debemos saber que la mayoría de nubes cuentan con su papelera de reciclaje donde se guardan los archivos borrados mientras haya espacio suficiente. Esta opción es muy útil cuando borramos algo por error.

Los mejores servicios de almacenamiento en la nube también permiten a los usuarios programar copias de seguridad permanentes en una unidad externa que se produzca en intervalos de tiempo especificados. Por ejemplo, según los datos de Western Digital publicados en 2013, la forma más fiable de realizar copias de seguridad en la actualidad son los discos duros con un 59% de fiabilidad, seguidos por las memorias Flash con un 41%, los soportes ópticos (CD o DVD) con un 30% y en último lugar la nube y sus múltiples servicios con un 22%.

Hoy en día sería imposible pensar un mundo sin datos sincronizados entre nuestros dispositivos... salvo que sólo uses uno para conectarte a Internet.

4.a.ii Herramientas Colaborativas

Si disponemos de unos archivos completamente actualizados, podemos compartirlos entre nuestros compañeros de trabajo y para ello necesitamos unas herramientas colaborativas que nos permitan compartir archivos con un usuario autorizado en cualquier dispositivo de múltiples maneras y además, se pueden elaborar flujos de trabajo y revisiones por parte de varias personas de un equipo de trabajo. Poniendo unos ejemplos, podríamos mencionar:

1. Google Apps

Google reúne su servicio de almacenamiento en la nube a Google Drive, Google+ y Gmail, tres herramientas que juntas ofrecen 15GB de capacidad gratuita.

Esta aplicación evita que el usuario se preocupe por la capacidad del servicio. Incluso, hay archivos que no ocupan espacio en Google Drive.

Google Apps también incluye Google Calendar, una herramienta que permite planificar actividades en grupo.

2. Dropbox

Es un sitio de almacenamiento en carpetas en línea que cuenta con el respaldo de casi 200 millones de usuarios en todo el mundo. Tiene varias características beneficiosas, entre ellas la disponibilidad del servicio en dispositivos móviles.

Dropbox adquirió recientemente Mailbox, una aplicación de gestión de correo electrónico que organiza rápido y eficientemente la bandeja de entrada.

3. Diigo

Esta herramienta crea una librería personal de archivos, en donde se almacena material de lectura, archivos, documentos y enlaces.

Tiene una opción de autoguardado de tuits y también la posibilidad de importar marcadores. Diigo tiene interesantes aplicaciones para iPad, Android y Mac, lo que la convierte en una aplicación móvil de primer nivel.

4. VoiceThread

Es una herramienta gratuita y bastante útil para el trabajo colaborativo, ya que ofrece facilidades para la recolección de ideas en diferentes formatos.

Puedes almacenar archivos de video, audio y de texto de manera sencilla.

5. Evernote

Evernote ayuda a organizar ideas y archivos de texto, audio, imágenes y páginas web. Una vez que estos documentos son subidos a la nube, se puede agregar etiquetas para que el trabajo con el material sea más ordenado.

La aplicación está disponible de forma gratuita, pero con la suscripción premium se adquiere mayor capacidad de almacenamiento y otras funcionalidades como la búsqueda en documentos PDFs.

6. Instapaper

Esta herramienta funciona sin necesidad de estar en línea, por lo tanto el usuario tiene la facilidad de tener sus archivos a disposición incluso si no está conectado a Internet.

Dentro de Instapaper, los miembros de un equipo pueden compartir archivos y enlaces de manera rápida.

7. Dipity

Dipity es una herramienta que nos sirve para crear líneas de tiempo, las cuales podemos elaborar con más usuarios. El servicio ofrece incluir fotografías y texto, y generar resultados que pueden ser insertados en otras plataformas.

8. Skydrive

Este servicio sirve para compartir y almacenar material multimedia en carpetas. La plataforma se descarga al escritorio y también trabaja con dispositivos móviles.

Skydrive incluye las principales aplicaciones de Office (Word, Excel y PowerPoint) de manera gratuita.

9. OneNote

Es una herramienta excelente para el almacenamiento y la organización de archivos. Se puede sincronizar con Skydrive, ya que ambos son productos de Microsoft.

Funciona como un blog portátil de notas que reúne archivos y documentos que luego pueden insertarse en otros sitios.

10. Blendspaced

Tiene como principal ventaja guardar videos de YouTube. La aplicación también almacena archivos, diapositivas, texto e imágenes.

Es una excelente alternativa para profesores que buscan acostumbrar a sus alumnos al manejo y almacenamiento de contenido multimedia.

4.a.iii Editar archivos desde la nube

A veces, no solo se basa en compartir archivos, sino también en poder verlos y editarlos desde la propia plataforma, y que estos cambios se sincronicen en todos los dispositivos a la vez.

La gran mayoría de estos servicios permite a los usuarios ver y editar archivos desde la nube en cualquier ordenador, smartpone, tableta u otro dispositivo conectado a Internet.

Los editores de texto en la nube más conocidos:

- Google Drive, o anteriormente conocido como Google Docs. Permite crear y editar documentos de manera colaborativa, es decir, podremos estar varias personas editando el mismo documento a la vez, en tiempo real. En mi opinión, uno de los más completos y con más funcionalidades. Disponible también en iOS y Android.

- Office Web Apps. Prácticamente todos conocemos la suite de productos Office: Word, Excel, PowerPoint y OneNote. Éstos mismos están también disponibles para usar directamente desde el navegador, sin necesidad de instalar nada en nuestro ordenador. Usando una cuenta Microsoft podremos acceder a todos los servicios y características que nos ofrece Office Web Apps, casi idéntico a su versión de escritorio.
- Evernote. ¿Quién no conoce Evernote? Prácticamente no necesita presentaciones. Evernote es un servicio que nos permite guardar ideas, artículos, anotaciones, imágenes, etc. Disponible tanto en versión web como en aplicaciones para Android e iOS.
- Springpad. Servicio muy curioso y práctico, una especie de cuaderno de anotaciones (como un notebook) donde podemos guardar textos en diferentes formatos, como por ejemplo recetas, un libro de fotos, ideas, tareas, cualquier cosa que tengamos en mente. Es una libreta *everywhere* en formato digital donde podremos optar por mostrar nuestros cuadernos públicamente o de forma privada. Disponible para iOS y Android.
- Zoho. Similar a Google Drive. Dispone de una serie de aplicaciones online para la edición de documentos: Writer (procesador de texto), Sheet (hojas de cálculo) y Show (editor de presentaciones y diapositivas). El uso de la aplicación es gratuito con registro, aunque dispones de planes de pago para obtener herramientas adicionales.
- Pinfolio. Herramienta muy útil para crear múltiples notas de texto. Permite colocar marcadores, guardar en diferentes formatos (incluido para eBook), insertar en cualquier sitio Web mediante *embed* y QR, comparar con otros documentos, etc. Para crear documentos necesitaremos obligatoriamente una cuenta en el servicio, algo que nos podría echar para atrás en ciertas ocasiones.
- Memonic. Se trata de un anotador online colaborativo, o lo que es lo mismo, varias personas al mismo tiempo podrán realizar modificaciones simultáneamente. Realmente no se trata de un servicio para crear documentos, sino más bien de un Web Clipper que nos permite guardar una Web y realizar anotaciones en ella posteriormente con una cuenta Memonic.

4.a.iv Seguridad

La seguridad es una de las principales preocupaciones de las empresas, respecto a la nube. Los datos privados de una empresa podrían verse comprometidos si el servicio que utiliza carece de las características adecuadas. Por lo que es importante proteger los archivos con una contraseña, en particular cuando se accede a ellos desde un dispositivo móvil, así como la capacidad para establecer diferentes niveles de acceso para diferentes empleados. Pero además de esto, es conveniente elegir un servicio que encripte los datos, e incluso que le permita elegir su propia clave de cifrado.

Más de la mitad de las empresas europeas coloca la seguridad de los datos (54%) y las soluciones cloud (52%) como las áreas de inversión prioritarias por parte de los departamentos de Tecnologías de la Información (TI) para 2016, según un estudio elaborado por Toshiba en colaboración con la consultora ICM.

Según el informe, realizado entre más de 400 directivos senior de TI de Europa, estas prioridades de inversión están relacionadas con la proliferación del número y tipos de dispositivos y aplicaciones IoT (Internet of Things) que usan los profesionales.

En este contexto, el 62% de los empleados de toda Europa utilizan sus smartphones (42%) y tabletas (31%) para conectarse a los datos de la empresa, lo que genera mayor complejidad en la gestión de las infraestructuras TI y mayores riesgos para la seguridad

El reciente caso del robo de fotos de celebridades de Hollywood, conocido como «Celebgate» y la consecuente violación de su intimidad desde la plataforma en la nube de Apple iCloud, saca de nuevo a la luz una problemática sobre la que los expertos de seguridad advierten constantemente. «Los usuarios, bien por desconocimiento o bien por un exceso de confianza, a menudo exponen información personal desde diferentes dispositivos, sobre todo smartphones, y cada vez más lo hacen a través de aplicaciones o plataformas en la nube, lo que supone un riesgo añadido», ha destacado en un comunicado Mario García, director general de Check Point.

La compañía recomienda tomar una serie de medidas básicas, que mitigarán los riesgos para la información que tengamos en la nube:

- Contraseñas

Las contraseñas representan la primera línea de protección en materia de seguridad, no obstante, un informe de SplashData desveló hace pocos meses que entre las 25 claves más habituales se siguen encontrando, sorprendentemente, algunas como password, 12345678, abc123 o 123123. Es necesario usar contraseñas largas (al menos de 8 caracteres) y complejas, es decir, que incluyan minúsculas, mayúsculas, números y caracteres no alfanuméricos, usar siempre contraseñas distintas y seguras, aunque más recientemente se ha aceptado como estándar que es una mejor idea tener contraseñas difíciles de adivinar, pero fáciles de recordar. También es bastante recomendable que uses un gestor de contraseñas. Los hackers comienzan su trabajo buscando nombres de usuario, contraseñas y preguntas de seguridad. Si aun así te parece muy difícil recordar contraseñas únicas, te recomendamos usar un gestor de contraseñas.

Comprobar la seguridad del proveedor Cloud, no usar la misma contraseña para estos sistemas, cambiar las contraseñas periódicamente y no recordar las contraseñas en equipos que utilicen otras personas son otras recomendaciones que se han de tener en cuenta.



Figura 9. Dashlane muestra la seguridad de tus contraseñas y te ayuda a recordarlas [20]

- Limitar y clasificar la información

Una norma de sentido común consiste en separar aquellos archivos que consideramos más sensibles y no alojarlos en la nube. Realizar un sencillo ejercicio de clasificación de nuestros datos podría ahorrarnos muchos problemas en caso de un ataque o de una fuga de información.

Hace unos diez años, si alguien adivinaba la contraseña que sueles usar en la red no podría hacer mucho comparado con lo que sucede en la actualidad.

Hoy en día, compartimos carpetas enteras llenas de documentos de todo tipo, contraseñas, marcadores, contactos, mensajes privados, historial de navegación, búsquedas, todas las fotos que has tomado con el teléfono...

La cantidad de información privada y confidencial que nosotros mismos colgamos en la red crece y crece sin parar. Por lo que el botín que conseguirá un hacker es cada vez más cuantioso.

- Encriptar

Si se usan sistemas Cloud, asumir que el contenido que se envía dejará de ser totalmente privado, por lo que es recomendable encriptarlo antes de enviarlo, incluyendo copias de seguridad. Algunos proveedores de almacenamiento, como Mega, ofrecen cifrado automático para tus archivos. Si el servicio que usas no lo ofrece, es una buena idea cifrar tus archivos por ti mismo antes de subirlos a la nube. Existen herramientas de cifrado que pueden sincronizarse con algunos proveedores de almacenamiento para funcionar de manera automática, como Cloudfogger, Viivo o boxcryptor.

Si te parece demasiado problemático, considera cifrar al menos tus archivos más sensibles que aun así necesites respaldar, como aquellos que contengan información bancaria, direcciones u otros datos personales.

- Servicios conectados entre sí

Muchos servicios y aplicaciones permiten el inicio de sesión con redes de terceros, como tu cuenta de Facebook, Google o Microsoft. Por tanto, la misma llave abre cada vez más y más puertas.

- Revisar las configuraciones por defecto

Es importante, a juicio de los expertos, poner atención cuando aceptamos las condiciones y no «Aceptar y olvidarse» como sucede en la mayoría de las ocasiones. En el caso de la plataforma iCloud de Apple los afectados desconocían que habían aceptado que se realizasen por defecto tres copias de seguridad de sus datos de forma automática, una de las razones que permitió que los hackers accediesen a datos borrados de los dispositivos hacía meses, pero que se mantenían en la nube.

- Un sistema de seguridad

Es posible disminuir el riesgo de tener malware/troyanos en los dispositivos que pueden robar las credenciales de usuario si vigilamos el software antivirus y velamos porque se actualice regularmente. Utilizar un software específico acorde a nuestras necesidades y mantenerlo actualizado en todos nuestros dispositivos es un requisito básico a la hora de evitar cualquier brecha de seguridad.

- Habilita la verificación en dos pasos

La importancia de la verificación en dos pasos, es que añade una capa adicional de seguridad al momento de acceder tu cuenta. Con la verificación en dos pasos, cualquier persona que intente ingresar necesitará dos piezas diferentes de información (por lo general, una contraseña y un código distinto y aleatorio que te es proporcionado mediante otro mecanismo).

Muchos servicios de almacenamiento en la nube, como Dropbox y Google Drive ofrecen verificación en dos pasos. Este proceso adicional implica que, además de tu usuario y contraseña, también debes indicar un código que se te envía por SMS. Lo cierto es que solventa parte del problema, pero no lo evita totalmente.

Los posibles problemas que puedan surgir con el marco legal vigente. En este aspecto hay que tener en cuenta varias cosas, como conocer el contenido del contrato con el servicio o asegurarnos de cumplir con la LOPD o *Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal*.

Si revisamos la Ley Orgánica de Protección de Datos de Carácter Personal, veremos que el artículo 12 dice que "*la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato*", así como debe establecerse expresamente que el encargado del tratamiento "*únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento*". Y en el mismo apunta la directiva europea de protección de datos personales.

El 25 de enero de 2012, la Comisión Europea publicó sus propuestas de modificación de la Directiva sobre protección de datos de la UE en un intento de armonizar el marco legislativo actual sobre protección de datos, considerado "fragmentado y anticuado". Entre los cambios propuestos figuran los siguientes:

- Las autoridades de reglamentación nacionales estarán facultadas para tomar medidas contra las organizaciones de otros Estados Miembros cuando concurren determinadas circunstancias, y podrán imponer multas de hasta 1 millón EUR o, si se trata de una empresa, de hasta el 2% de su volumen de negocios anual en algunos casos.
- La definición del concepto de datos personales se ampliará para abarcar toda información relativa al interesado y la normativa requerirá el consentimiento expreso del individuo para autorizar la captura de datos.
- La normativa se aplicará más allá de la UE con objeto de incluir a entidades no comunitarias que procesen datos personales pertenecientes a ciudadanos de la UE.
- Las organizaciones deberán informar sin dilación sobre las violaciones de la seguridad de los datos, a ser posible, dentro de las 24 horas siguientes a la comisión de la infracción.
- Los responsables del tratamiento de datos estarán obligados a llevar a cabo informes de evaluación de impacto de la protección de datos, nombrar a delegados de protección de datos e informar a terceros sobre cualquier infracción.
- En determinadas circunstancias, se concederá a los interesados el "derecho al olvido" y dejarán de estar obligados a pagar para acceder a sus datos.
- Las transferencias internacionales de datos estarán sujetas a un marco normativo más exhaustivo que requerirá la adopción de salvaguardias, la realización de controles previos

por parte de las autoridades y la restricción de las excepciones aplicables a los responsables del tratamiento de datos.

El carácter polémico que presentan las reformas propuestas ha suscitado un proceso de cabildeo y debate que podría demorar ampliamente su aplicación.

4.a.v Disponibilidad de los datos en la nube (híbrida)

Recordemos que la disponibilidad de los sistemas es una probabilidad de que se entregue el servicio en el momento solicitado. Se considera que cuando el sistema falla, este debe ser reparado y restaurado para seguir ofreciendo el servicio y se expresa en términos de “nueves”. Y no hay que confundirla con la fiabilidad, que es la probabilidad de que el sistema realizará su función durante un período determinado de tiempo bajo ciertas condiciones y no incluye el tiempo de mantenimiento o reparación.

| % Disponibilidad | Cantidad de tiempo de caída anual |
|------------------|-----------------------------------|
| 99% | 88 horas |
| 99,9% | 8,8 horas |
| 99,99% | 53 minutos |
| 99,999% | 5,3 minutos |
| 99,9999% | 32 segundos |

Tabla 1. Disponibilidad de los datos en la nube (híbrida) [16]

4.a.vi Privacidad

La información es el activo más importante de las organizaciones. Asegurar la privacidad de la información durante su ciclo de vida es crucial a la hora de utilizar servicios de *cloud computing*.

4.a.vii Protección en los datos

El ciclo de vida que siguen los datos que son procesados en la nube es el siguiente:

Los datos son preparados para poder adaptarse a la nube adaptando su formato o creando un fichero que contenga toda la información necesaria.

Los datos “viajan” a la nube a través de una conexión a Internet, mediante un correo electrónico, una aplicación específica para importarlos o la transferencia a la nube de la copia de seguridad obtenida de un servidor en la organización.

Los datos son procesados en la nube, desde su almacenamiento hasta el cálculo de complejas operaciones matemáticas. Es importante mencionar que los datos pueden almacenarse en copias de seguridad en la nube para facilitar futuros accesos.

Los datos finales “viajan” de vuelta al usuario. Una vez terminado el procesamiento, el resultado debe volver al usuario con el valor añadido de la información generada en la nube.

4.a.viii Confidencialidad

Pero si la disponibilidad es importante, la confidencialidad es otro de los pilares. De nada sirve estar siempre con los sistemas activos si estamos enviando información a quien no debe verla o utilizando passwords que en una hora se han visto comprometidos.

Siempre hay que ser extremadamente cuidadosos con los sistemas, ya estén en la nube o en el mundo físico. Un error en la confidencialidad es un error de negocio. Imaginemos enviar un email con información crítica a quien no se debe. Así que en la transferencia de información será fundamental utilizar herramientas de encriptación de datos.

Mucho se habla de la seguridad en la nube, de dónde se alojan los servidores, de quién tiene acceso a ellos. Sin embargo, si nos paramos a pensar, estas mismas preguntas nos las tenemos que hacer en la parte física. Quién accede a los servidores, quién conoce nuestras contraseñas, quién realiza el mantenimiento de los equipos.

En muchas ocasiones, utilizar servicios en la nube va a ser incluso más seguro que dejarlo en los propios sistemas in house donde el acceso a los servidores donde reside la información queda en manos de más personas.

4.a.ix Integridad

Mantener una correcta integridad de los datos significa que estos permanecen idénticos durante las operaciones de transferencia, almacenamiento o recuperación. En el ámbito del *cloud computing*, la integridad de los datos es especialmente crítica: los datos están siendo transferidos constantemente entre los servicios en la nube y los distintos usuarios que acceden a ellos.

Debido a las características de la computación en la nube, varios usuarios pueden estar accediendo simultáneamente y modificando determinada información. Por ello, deben implementarse los mecanismos que garanticen la correcta integridad de los datos.

Para evitar que los datos en la nube no puedan utilizarse o que no estén disponibles se utilizan principalmente tres mecanismos: control de integridad, gestión de cambios y copias de seguridad.

El control de integridad hace uso de funciones matemáticas (funciones resumen o *hash*) para verificar que los datos no han sufrido modificaciones durante su traslado. El proceso consiste en obtener un valor para la función *hash* antes de mover el dato y otro cuando se ha terminado de mover. Si dichos valores no coinciden es que ha habido un problema en la transacción y debe ser repetida. En el caso del *cloud computing* no se utilizan funciones resumen solo para ficheros, sino también para máquinas virtuales completas o para las copias de seguridad.

La gestión de cambios mantiene un historial de modificaciones de los datos o ficheros almacenados en la nube. Cada modificación lleva asociada un sello de fecha y el usuario que lo produjo. Si se detecta que varios usuarios han modificado el recurso a la vez se puede analizar el sello de fecha para comprobar qué versión tiene validez. Del mismo modo, si se detecta un error de integridad en el recurso se puede volver a una versión anterior que sea correcta.

4.a.x Copias de seguridad

Las copias de seguridad son la última línea defensiva para garantizar la integridad de los datos. Utilizando adecuadamente las herramientas en la nube se pueden programar copias de seguridad cada cierto tiempo. Si se detecta un fallo de integridad a nivel general, la forma de solucionarlo es volver a una versión anterior del sistema almacenada en la copia de seguridad.

- Ventajas de guardar archivos en la nube

Las copias se hacen automáticamente del ordenador a un servicio remoto de backup online.

No es necesario estar grabando cada cierto tiempo. Se hace una copia todos los días de todo lo que has hecho nuevo.

Se pueden prevenir problemas repentinos.

Puedes acceder en cuestión de minutos y recuperar los datos desde otro ordenador.

Tus archivos se guardan de modo seguro, con cifrado de datos, ya que se hace a través de un servicio que cumple a rajatabla con la LOPD y especialmente pensado para empresas.

- Desventajas de las copias de seguridad online

La nube implica poner tus archivos en manos de un servidor externo.

Si suceden fallos de seguridad o utilizan tus datos, es responsabilidad suya.

No todos los servicios de backup te facilitan cumplir con la LOPD para alojar archivos de terceros con seguridad.

- Ventajas de usar un disco duro externo

Es sencillo de utilizar y permiten almacenar una gran cantidad de ficheros. Hay muchos por 1 Terabyte que pueden resultarnos útiles.

Tienes los archivos en un dispositivo físico y transportable.

No necesitas depender de una empresa externa.

Con un programa como Time Machine (para Mac), se hacen copias de seguridad cada día.

- Desventajas de utilizar un disco duro externo

Si la unidad de disco duro se estropea, es difícil que se pueda recuperar. Sometimiento a altas temperaturas, introducción de virus, rotura, etc.

Para que tenga sentido usarlo, debe estar conectado a tu PC permanentemente. Eso implica mayor riesgo de seguridad si no se acompaña de otras alternativas.

En una red se pueden usar 1 o más discos duros, pero siempre es conveniente comprar varios.

4.a.xi Control de acceso

Igual que sucede con las arquitecturas tradicionales, el control de acceso también juega un papel importante en el *cloud computing*. Aunque esta tecnología se represente informalmente como una nube a la que se conecta todo el mundo desde sus equipos (tanto fijos como dispositivos móviles), no significa en absoluto que cualquier persona pueda acceder a cualquier dato o proceso en la nube.

Cuando una empresa o entidad utiliza las capacidades de la computación en la nube, necesita que el administrador del sistema establezca un correcto control de acceso para garantizar que los usuarios solo utilizan los datos o procesos para los que han sido autorizados.

4.a.xii Prevención frente a pérdidas

Uno de los mayores riesgos a los que se enfrenta todo sistema informático es la pérdida de datos, ya sea porque un usuario ha borrado información accidentalmente, porque haya un fallo en algún dispositivo hardware o por culpa de un ataque informático. Perder los datos no solo significa tener que rehacer parte del trabajo realizado, sino que en muchos casos puede significar cuantiosas pérdidas económicas. La solución a este problema se enfoca desde dos puntos de vista principales

Por un lado, una correcta política de seguridad limita la libertad de los usuarios para borrar elementos del sistema, protege los equipos ante el ataque de software malintencionado y además impide que personas ajenas a la organización accedan o corrompan los datos. El proveedor de servicios se encarga de solucionar todos los problemas relacionados con los componentes electrónicos. Si detecta un fallo en uno de los equipos dentro de sus instalaciones, automáticamente lo aísla y todos los procesos que se ejecutan en él se migran a otra máquina que no tenga problemas. Este proceso puede durar tan solo unos minutos e incluso realizarse sin cortar el servicio, permitiendo una disponibilidad ininterrumpida de los servicios en la nube.

Por otra parte, una correcta política de copias de seguridad permite recuperar los datos aun cuando todas las medidas de seguridad han fallado o cuando se produce una avería en un componente hardware. Todos los proveedores de servicios en la nube ofrecen sistemas de copias de seguridad de forma completamente transparente para el usuario. Tan solo es necesario seleccionar los activos que se quieren proteger y la periodicidad con la que se desean estas copias. La recuperación frente a un ataque puede ser tan sencilla como la restauración de un *snapshot* (copia instantánea de volumen) anterior de la máquina virtual.

Las características anteriormente expuestas permiten disponer de un sistema robusto preparado para realizar una correcta recuperación frente a desastres, es decir, asegurando la continuidad del negocio. Por último, existe otra ventaja relativa a los dispositivos portátiles, cada vez más utilizados en las empresas y desde los que se accede a la información de la organización: ordenadores portátiles, USBs, móviles, etc. Estos dispositivos pueden ser robados u olvidados exponiendo grandes cantidades de datos a personas completamente ajenas a la organización. Si se utilizan sistemas en la nube, aunque se pierda un teléfono móvil o alguien robe un portátil, la información permanecerá inaccesible para terceros.

4.a.xiii Precios

Una de las características que define el *cloud computing* es la escalabilidad, entendida en este caso como una capacidad de almacenamiento flexible a las necesidades de cada usuario, a un precio asequible, sin necesidad de instalar costosos dispositivos físicos.

| Servicio | Gratis | 20GB | 50 GB | 100 GB | 200 GB | 500 GB | 1 TB | Más de 1 TB |
|--------------------|----------------------------|--------|-----------|-----------------------|-----------|-----------|---|--|
| Amazon cloud drive | 5GB | 8€/año | 20€/año | 40€/año | 80€/año | 200€/año | 400€/año | - |
| iCloud | 5 GB | - | 0.99€/mes | - | 2.99€/mes | - | 9.99€/mes | - |
| Dropbox Basic | 2 GB ampliables hasta 16GB | - | - | - | - | - | 9.99€/mes (Pro) | Ilimitado: 12€/usuario (Business) |
| OneDrive | 5 GB | - | 2€/mes | - | - | - | 10€/mes. Con Microsoft Office365, 1 TB gratis un año. | - |
| Google Drive | 15 GB | - | - | 1.99\$/mes | - | - | 9.99\$/mes | 10 TB por 99,99\$/mes, 20 TB por 199,99\$/mes y 30 TB por 299,99\$/mes |
| Box Personal | 10 GB | - | - | 8€/mes (Personal Pro) | - | - | - | Ilimitado: 12€/mes por usuario (Business) |
| Mega | 50 GB | - | - | - | - | 9.99€/mes | - | 2 TB por 19,99€/mes y 4 TB 29,99€/mes |

Tabla 2. Precios de los principales proveedores de *cloud storage* [22]

Además, de los más conocidos tenemos otros servicios de almacenamiento en la nube menos conocidos:

1. ADrive: ADrive ha decidido eliminar su cuenta 50 GB de almacenaje en la nube gratis con cuentas personales. Ahora te dan una versión de prueba de 60 días eligiendo previamente el plan que mejor se te adapta con cuentas personales o empresariales.

| Personal Premium | | | | | Business | | | | |
|------------------|----------|------------|------------|------------|------------|----------|------------|-------------|------------|
| Size | Monthly | Yearly | 2 Year | 3 Year | Size/Users | Monthly | Yearly | 2 Year | 3 Year |
| 100GB | \$2.50 | \$25.00 | \$45.00 | \$60.00 | 200GB/10 | \$7.00 | \$70.00 | \$126.00 | \$168.00 |
| 250GB | \$6.25 | \$62.50 | \$112.50 | \$150.00 | 500GB/25 | \$17.50 | \$175.00 | \$315.00 | \$420.00 |
| 500GB | \$12.50 | \$125.00 | \$225.00 | \$300.00 | 1TB/50 | \$35.00 | \$350.00 | \$630.00 | \$840.00 |
| 1TB | \$25.00 | \$250.00 | \$450.00 | \$600.00 | 2TB/100 | \$70.00 | \$700.00 | \$1,260.00 | \$1,680.00 |
| 2TB | \$50.00 | \$500.00 | \$900.00 | \$1,200.00 | 10TB/500 | \$350.00 | \$3,500.00 | \$6,300.00 | Contact |
| 3TB | \$75.00 | \$750.00 | \$1,350.00 | Contact | 20TB/1000 | \$700.00 | \$7,000.00 | \$12,600.00 | Contact |
| 5TB | \$125.00 | \$1,250.00 | \$2,250.00 | Contact | | | | | |
| 10TB | \$250.00 | \$2,500.00 | \$4,500.00 | Contact | | | | | |

Figura 10. Diferentes tarifas del servicio ADrive [Web ADrive]

2. **Bitcasa:** Bitcasa es un servicio de almacenamiento en la nube que pone el énfasis sobre la intimidad de tus datos. Todos los datos que tu almacenes en Bitcasa son cifrados antes de cargarlos y sólo tú puedes verlos, nadie más. Bitcasa proporciona 5 GB de almacenaje de nube gratis durante 60 días y puedes tener acceso a tus datos desde 3 dispositivos diferentes. Y con cuentas Premium tenemos 1TB por 10\$/mes y con cuentas Pro 10 TB por 99\$/mes y puedes tener acceso a tus datos desde 5 dispositivos diferentes.
3. **SpiderOak:** Este es otro servicio de almacenamiento en la nube gratis que se centra en ofrecer mayor seguridad sobre la intimidad de tus datos almacenados. SpiderOak proporciona tan solo 2 GB de almacenaje en la nube gratis que puede ser ampliado hasta 10 GB por invitar a tus amigos (tu cuenta aumenta en 1 GB por cada amigo que se abre cuenta en el servicio).
4. **Tencent Weiyun:** Tencent es una enorme empresa china de Internet que ofrece 10 TB de almacenaje en la nube gratis a cada nuevo usuario.

Algunas compañías de telefonía quieren facilitar la vida a sus clientes y les ofrecen espacio en la nube para guardar fácilmente todos los archivos de tu teléfono sin tener que recurrir a otro tipo de servicios.

- **Orange Cloud:** Mediante este servicio de Orange podrás guardar tu música, fotos, contactos y vídeos. Si tienes una tarifa Canguro (Sin Límites o Familia), Ballena o Delfín, Canguro o Sin Límites, posees 25 GB gratis. Las tarifas Canguro ahorro, Canguro 35, Tucán, Ballena 32 y Ballena 22 pueden contratarlo por 2,42€ al mes. Si 100GB por 6,05€ al mes.
- **Buckup+ de Vodafone:** En colaboración con Dropbox, te permite guardar el contenido de tu teléfono y acceder a él a través de otros dispositivos. Gracias a esta colaboración, todas las tarifas móviles de Vodafone (incluido Vodafone One) disponen de 25 GB gratis durante un año asociando una nueva cuenta de Dropbox, y si contratas la tarifa Red XL, esta oferta se amplía a los dos años.
- **Movistar Cloud:** Este servicio no está incluido en ninguna de las tarifas de Movistar, sino que tendrás que pagar por él. Por 1 euro al mes dispones de la modalidad de 20 GB, por 2 euros de la de 100 GB y, si prefieres optar por un almacenamiento ilimitado, solo tendrás que pagar 5 euros al mes. Las condiciones es que, lógicamente, debes ser cliente de móvil de Movistar (incluyendo Movistar Fusión).

4.b Comparación de diferentes tecnologías para el almacenamiento de archivos

Existen tres modelos de almacenamiento tradicionales que son usados actualmente en diferentes situaciones o entornos de red los cuales son:

4.b.i *Direct Attached Storage*

Almacenamiento de conexión directa (DAS, del inglés, Direct Attached Storage), hace referencia al sistema de almacenamiento tradicional en el cual el dispositivo que contiene la información sea este un disco duro o cualquier otro dispositivo va conectado directamente al equipo sea este un cliente o un servidor es un método de almacenamiento local y económico. Una desventaja importante de DAS incluyen incapacidad para compartir datos o recursos no usados con otros servidores.

Finalmente, el modo de almacenamiento DAS utiliza la misma forma de comunicación que SAN, a través de protocolos SCSI, SAS y Fibre Channel, aunque en este caso se conecta directamente al servidor a través de un “host bus adapter” (HBA). Las peticiones de datos al igual que en SAN se hacen directamente al sistema de ficheros.

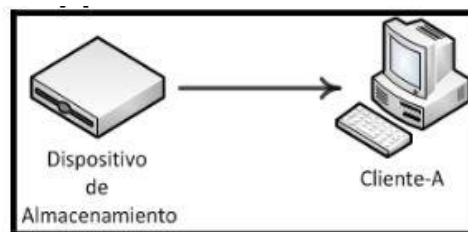


Figura 11. Ejemplo DAS [16]

4.b.ii *Network Attached Storage*

Almacenamiento de conexión en red (NAS, del inglés, Network Attached Storage), es un sistema de almacenamiento multiplataforma dirigido a un entorno de red ya que la información se la guarda en un servidor centralizado dedicado para tareas de almacenamiento el cual cuenta con políticas de acceso, seguridad, administración de clientes, etc. debido a esto es perfecto incluso para un entorno sin dominio. Las soluciones NAS utilizan la consolidada tecnología de red IP a través de una “Local Area Network (LAN)”.

En la tecnología NAS, las aplicaciones y programas de usuario hacen las peticiones de datos a los sistemas de archivos de manera remota mediante protocolos CIFS, NFS, FTP o TFTP y el almacenamiento es local al sistema de archivos. Sin embargo, DAS y SAN realizan las peticiones de datos directamente al sistema de archivos.

Las ventajas del NAS sobre la conexión directa (DAS) son la capacidad de compartir las unidades, un menor coste, la utilización de la misma infraestructura de red y una gestión más sencilla. Por el contrario, NAS tiene un menor rendimiento y confiabilidad por el uso compartido de las comunicaciones.

Al ser los dispositivos de almacenamiento direccionables a través de una LAN, el almacenamiento es liberado de un servidor específico proporcionando una conectividad “any-to-any” usando dicha LAN. En principio, muchos usuarios ejecutarán múltiples sistemas operativos accediendo a los ficheros a través de un dispositivo de almacenamiento remoto, accesible a través de la red mediante el uso de un protocolo de acceso común. Un dispositivo de almacenamiento no puede unirse directamente a la red. Él necesita “inteligencia” que gestione la transferencia y la organización de los datos que se almacenan o almacenarán en dicho dispositivo. La “inteligencia” es proporcionada por un servidor dedicado que se une a los dispositivos de almacenamiento comunes. Un NAS está compuesto por tanto, por un servidor, un sistema operativo y almacenamiento que es compartido a través de la red por muchos otros servidores y clientes. Así, un NAS es un dispositivo y no una arquitectura de red, y el almacenamiento que comparte es interno o unido a dicho dispositivo (NAS).

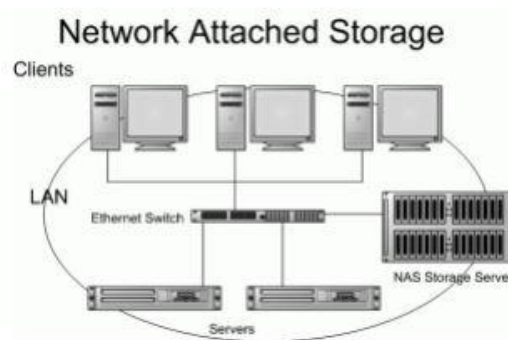


Figura 12. Ejemplo NAS [16]

Beneficios de usar un sistema NAS:

- Agrupación de recursos.
- Explotación de la infraestructura existente.
- Fácil de implementar.
- Independencia al escoger servidor y dispositivos de almacenamiento según las necesidades
- Conectividad.
- Escalabilidad.
- Compartición de archivos heterogéneos.
- Backup mejorado.
- Gestión mejorada.

4.b.iii Storage Area Storage

Red de área de almacenamiento (SAN, del inglés, Storage Area Network), refiere a un tipo de red ideada para el transporte de información a alta velocidad entre servidores o equipos de red. Para alcanzar estas altas velocidades de transferencia generalmente la SAN funciona en un ambiente de fibra óptica separada de la LAN de tal manera que no afecte al tráfico de los usuarios en ésta.

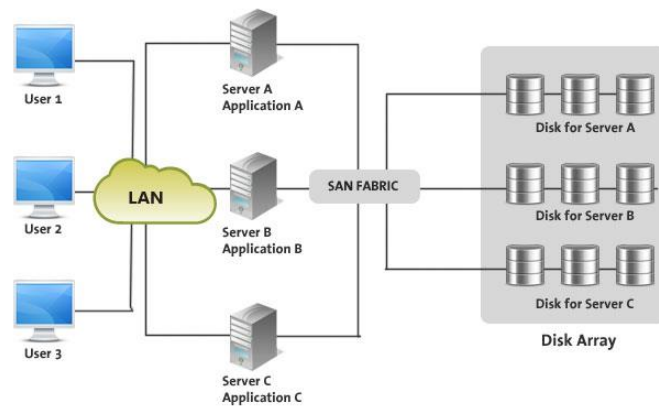


Figura 13. Ejemplo SAN [16]

Dicho en términos simples, una SAN es un organismo especializado, de alta velocidad de red que conecta servidores y dispositivos de almacenamiento. Una SAN permite conexiones “any-to-any” a través de una red, usando elementos de interconexión como routers, gateways, hubs, switches y directores. Se elimina la tradicional conexión dedicada entre un servidor y el almacenamiento, y el concepto de que el servidor, de manera efectiva, “posee y gestiona” los dispositivos de almacenamiento. También elimina cualquier restricción a la cantidad de datos que un servidor puede tener acceso, anteriormente limitado por el número de dispositivos conectados al servidor. En su lugar, una SAN introduce flexibilidad en las redes permitiendo que un servidor, o varios servidores heterogéneos, compartan una utilidad de almacenamiento común, que puede comprender muchos dispositivos de almacenamiento, incluyendo discos, cintas y almacenamiento óptico. Además la unidad de almacenamiento puede encontrarse alejada físicamente de los servidores que la utilicen.

Puede ser vista como una extensión del concepto de almacenamiento, que permite a los dispositivos de almacenamiento y servidores ser interconectados usando elementos similares que una red de área local y una red de área extensa.

Una SAN se puede considerar una extensión de Direct Attached Storage (DAS).

Donde en DAS hay un enlace punto a punto entre el servidor y su almacenamiento, una SAN permite a varios servidores acceder a varios dispositivos de almacenamiento en una red compartida.

Tanto en SAN como en DAS, las aplicaciones y programas de usuarios hacen sus peticiones de datos al sistema de ficheros directamente. La diferencia reside en la manera en la que dicho sistema de ficheros obtiene los datos requeridos del almacenamiento.

En DAS, el almacenamiento es local al sistema de ficheros, mientras que en SAN, el almacenamiento es remoto.

SAN utiliza diferentes protocolos de acceso como Fibre Channel y Gigabit Ethernet. En el lado opuesto se encuentra la tecnología Network-Attached Storage (NAS), donde las aplicaciones hacen las peticiones de datos a los sistemas de ficheros de manera remota mediante protocolos Server Message Block (CIFS) y Network File System (NFS).

Una SAN tiende a maximizar el aprovechamiento del almacenamiento, puesto que varios servidores pueden utilizar el mismo espacio reservado para crecimiento.

Las rutas de almacenamiento son muchas, un servidor puede acceder a uno o "n" discos y un disco puede ser accedido por más de un servidor, lo que hace que aumente el beneficio o retorno de la inversión.

Una ventaja primordial de la SAN es su alta disponibilidad de los datos y su compatibilidad con los dispositivos SCSI ya existentes, aprovechando las inversiones ya realizadas y permitiendo el crecimiento a partir del hardware ya existente. Mediante el empleo de dispositivos modulares como *hubs*, *switches*, *bridges* y *routers*, se pueden crear topologías totalmente flexibles y escalables, asegurando la inversión desde el primer día y, lo que es más importante, aprovechando dispositivos SCSI de costo considerable como subsistemas RAID-SCSI a SCSI, librerías de cintas o torres de CD-ROM, ya que a través de un *bridge Fibre Channel* a SCSI podemos conectarlos directamente a la SAN. Puesto que están en su propia red, son accesibles por todos los usuarios de manera inmediata.

El rendimiento de la SAN está directamente relacionado con el tipo de red que se utiliza. En el caso de una red de canal de fibra, el ancho de banda es de aproximadamente 100 megabytes/segundo (1.000 megabits/segundo) y se puede extender aumentando la cantidad de conexiones de acceso.

La capacidad de una SAN se puede extender de manera casi ilimitada y puede alcanzar cientos y hasta miles de terabytes. Una SAN permite compartir datos entre varios equipos de la red sin afectar el rendimiento porque el tráfico de SAN está totalmente separado del tráfico de usuario. Son los servidores de aplicaciones que funcionan como una interfaz entre la red de datos (generalmente un canal de fibra) y la red de usuario (por lo general Ethernet).

Por otra parte, una SAN es mucho más costosa que una NAS ya que la primera es una arquitectura completa que utiliza una tecnología que todavía es muy cara. Normalmente, cuando una compañía estima el TCO (coste total de propiedad) con respecto al coste por byte, el coste se puede justificar con más facilidad.

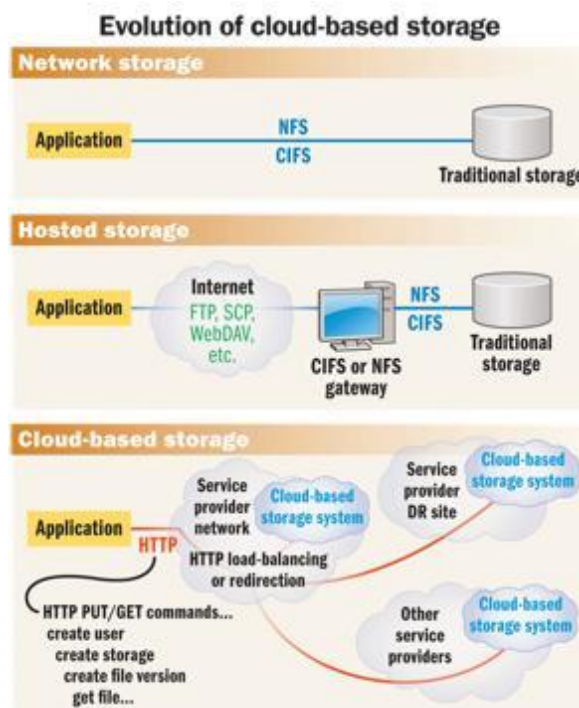


Figura 14. Evolución del almacenamiento en la nube [16]

4.c Comparación de los mejores servicios de almacenamiento en la nube

4.c.i Estándares de seguridad

Dropbox

Los archivos de Dropbox almacenados se cifran mediante el estándar Advanced Encryption Standard (AES) de 256 bits.

Para proteger los datos en tránsito entre las aplicaciones de Dropbox y los servidores, Dropbox se emplea las tecnologías Secure Sockets Layer (SSL)/Transport Layer Security (TLS), que crean un túnel seguro protegido por un cifrado con Advanced Encryption Standard (AES) de 128 bits o superior.

Además, la verificación en dos pasos ofrece una capa adicional de seguridad al iniciar sesión. Ya que se puede elegir entre recibir códigos de seguridad mediante mensajes de texto o mediante aplicaciones de contraseñas de un solo uso (TOTP).

Google Drive

Los datos se cifran en diferentes niveles. Google aplica el protocolo HTTPS (Protocolo seguro de transferencia de hipertexto) para todas las transmisiones entre los usuarios y los servicios de Google Apps, este protocolo se activa por defecto para todos los usuarios, lo cual ayuda a asegurar que nadie excepto el usuario tiene acceso a sus datos, y emplea Perfect Forward Secrecy (PFS) en todos los servicios.

Además, la conectividad SSL (Capa de conexión segura) / TLS (Seguridad en la capa de transporte) está disponible para todos los clientes de Google Apps y se habilita de forma predeterminada para los nuevos clientes. Por lo que Google cifra las transmisiones de mensajes con otros servidores de correo mediante TLS de 256 bits y utiliza claves de cifrado 2048 RSA en las fases de validación e intercambio de claves.

OneDrive

El transporte de archivos en OneDrive también se realiza mediante el protocolo SSL, pero a diferencia de otros servicios como Dropbox, no mantiene encriptados los archivos que almacena -aunque si el tráfico-.

De nuevo OneDrive tiene habilitada la posibilidad de acceder a tu cuenta mediante una verificación en dos pasos, una medida de seguridad muy importante para evitar el pirateo de las cuentas.

La comunicación en OneDrive para la Empresa a través de Internet usa conexiones SSL/TLS. Todas las conexiones SSL se establecen con claves de 2048 bits. Además, el cifrado por archivo incluye una clave de cifrado única para cada archivo. Además, cada actualización de cada archivo se cifra mediante su propia clave de cifrado. Antes de almacenarse, las claves del contenido cifrado se cifran y almacena en una ubicación físicamente independiente del contenido. Cada paso de este cifrado usa el Estándar de cifrado avanzado (AES) con claves de 256 bits y es compatible con el Estándar federal de procesamiento de información (FIPS) 140-2.

Box

El servicio cifra los archivos en tránsito con SSL/TLS de alta calidad y cifrado multicapa en reposo mediante AES de 256 bits, aunque también permite que sea el usuario el que decida el tipo de cifrado en el caso de pagar la versión Enterprise de Box. Las claves de cifrado se almacenan de forma segura en ubicaciones independientes que cambian con regularidad.

Box es un servicio similar a Google Drive que incorpora su propia suite ofimática para poder trabajar y compartir documentos y hojas de cálculo entre usuarios.

Mega

La empresa utiliza protocolos de cifrado AES para proteger los archivos antes de transferirlos desde el ordenador del usuario. A continuación, los archivos permanecen cifrados durante el tránsito y, una vez que se guardan en los servidores de Mega, utilizando un sistema de claves pública/privada.

Lo primero que hace cuando nos registramos es generar un par de claves pública/privada RSA de 2048 en nuestro ordenador. Se guardan en nuestro espacio de almacenamiento del navegador, pero también se envían a los servidores de Mega. También se genera una clave simétrica maestra, que permanece en los servidores de Mega. Esta clave está cifrada con un *hash* derivado de nuestra contraseña. Esta es la clave que se usa para proteger nuestra clave privada.

Cuando se sube un archivo:

- Se genera una clave simétrica aleatoria de 128 bits para el archivo.
- Se cifra el archivo con esa clave.
- Se genera otra clave para enviar el archivo. Probablemente se use el intercambio de claves Diffie-Hellman con tu par de clave pública/privada y un secreto compartido.
- Se envía el archivo cifrado a Mega, junto con la clave de cifrado del archivo, todo ello protegido con la clave que habíamos generado antes.
- Mega guarda el archivo cifrado (sin descifrar sus contenidos) por un lado. Por otro, guarda la clave del archivo cifrada con tu clave maestra.

ADrive

El acceso a los archivos ubicados en los servidores ADrive *cloud* se permite mediante cualquier cliente FTP, pero no se hace a través de un servidor seguro, por lo que el tráfico podría ser fácilmente interceptado esto se soluciona en las versiones de pago al usar SSL. Se puede usar AUTH TLS para transferir archivos de forma segura. Además, los datos están seguros al transferir archivos a y desde el ADrive *cloud*. Se proporciona cifrado de datos SSL para todos los usuarios de pago. SSL es un protocolo criptográfico que proporciona comunicaciones seguras a través de Internet para las transferencias de datos.

Amazon cloud drive

La diferencia básica de Amazon Cloud Service con otros servicios similares es que el usuario escoge el nivel de encriptación de sus archivos y transferencias, y el servicio permite dejar esta tarea en manos del servidor, o hacerlo el usuario directamente en su propio ordenador antes de subirlo a la nube.

El servicio en la nube de Amazon dispone de un sistema de cifrado flexible que incluso dispone de una biblioteca que nos permite gestionar nuestras propias claves para así poder adaptar el

cifrado de los archivos a nuestras necesidades. Los usuarios más avanzados disfrutarán con el control y la documentación de la que dispone el servicio y que permite cierto grado de personalización.

4.c.ii Tamaño máximo de archivo

- Dropbox: Los archivos subidos en dropbox.com no deben superar los 20 GB.
- Google Drive: 5 TB
- OneDrive: Si usamos Internet Explorer 10 o una versión reciente de otros exploradores web populares, podemos cargar archivos en OneDrive con un tamaño máximo de 10 GB. Si usamos un explorador web antiguo, no podemos cargar archivos con un tamaño superior a 300 MB.
- Box: Depende del plan que escojamos, como por ejemplo si escogemos el plan Free personal, el tamaño máximo de archivo es de 250MB, para el plan Starter: 2GB y para los planes Business/Enterprise: 5GB.
- Mega: El único límite son los 50GB por la cuenta gratuita. O más si pagas por ampliar el espacio disponible.
- ADrive: Se ha aumentado las limitaciones de tamaño de un archivo de 2 GB a 16 GB.
- Amazon cloud drive: 2 GB

4.c.iii Sistemas operativos

| | Windows | OSX | Linux | iOS | W Phone 8 | Android | Blackberry 10 |
|--------------------|---------|-----|-------|-----|-----------|---------|---------------|
| Dropbox | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Google Drive | Yes | Yes | | Yes | | Yes | Yes |
| OneDrive | Yes | Yes | | Yes | Yes | Yes | Yes |
| Box | Yes | Yes | | Yes | Yes | Yes | Yes |
| Mega | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| ADrive | Yes | Yes | Yes | Yes | | Yes | |
| Amazon cloud drive | Yes | Yes | Yes | Yes | | Yes | |

Tabla 3. Sistemas operativos soportados por cada uno de los proveedores de *cloud storage*

4.c.iv Idiomas soportados

| | Dropbox | Google Drive | OneDrive | Box | Mega | ADrive | Amazon cloud drive |
|-----------|---------|--------------|----------|------|------|--------|--------------------|
| Español | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Inglés | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Chino | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Alemán | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Francés | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Italiano | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Portugués | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Ruso | Yes | Yes | Yes | Yes | Yes | Yes | |
| Japonés | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Malayo | Yes | Yes | Yes | | | | |
| Coreano | Yes | Yes | Yes | Yes | Yes | Yes | |
| Polaco | Yes | Yes | Yes | Yes | Yes | | |
| Indonesio | Yes | Yes | Yes | | Yes | Yes | |
| Sueco | Yes | Yes | Yes | Yes | Yes | | |
| Danés | | Yes | Yes | Yes | | | |
| TOTAL | 14 | 15 * | 15 * | 13 * | 13 * | 11 | 8 |

Tabla 4. Idiomas soportados por cada uno de los proveedores de *cloud storage*

*A parte de los que se han puesto en la tabla, existen soporte a otros lenguajes

Escenario de las medidas

Red de transporte: Telefónica de España

Ubicación de la prueba: Valencia, España.

Ubicación del servidor: Valencia, España.

Ping: 32 ms

Velocidad de subida: 306.65 Mbps

Velocidad de bajada: 32.16 Mbps



Figura 15. Escenario de las medidas [<http://www.speedtest.net/es/>]

4.c.v Carga del archivo

El resultado del test es la media de 5 tests, limpiando la cache antes de cada test

| | Amazon cloud drive | Dropbox | Google Drive | OneDrive | Box | Mega | ADrive |
|--------|--------------------|-----------|--------------|-----------|---------|----------|----------|
| 1 MB | 1.45 s | 2.63 s | 1.33 s | 1.46 s | 1.53 s | 1.71 s | 3.04 s |
| 5 MB | 3.38 s | 4.8 s | 4.93 s | 3.74 s | 3.95 s | 4.9 s | 4.4 s |
| 10 MB | 5.57 s | 10.1 s | 5.28 s | 6.35 s | 6.2 s | 7.87 s | 9.43 s |
| 20 MB | 7.19 s | 16.17 s | 9.63 s | 12.95 s | 10.78 s | 14.43 s | 30.81 s |
| 50 MB | 19.7 s | 30.64 s | 18.77 s | 47.72 s | 17.63 s | 35.65 s | 62.68 s |
| 100 MB | 34.11 s | 82.71 s | 36.3 s | 107 s | 35.69 s | 80.2 s | 137.78s |
| 200 MB | 101.8 s | 201.09 s | 86.97 s | 314.97 s | 67.99 s | 126.35 s | 351.8 s |
| 512 MB | 212.49 s | 516.9 s | 178.65 s | 715.73 s | - | 310.85 s | 991.1 s |
| 1 GB | 395.8 s | 1044.13 s | 347.87 s | 1258.22 s | - | 577.29 s | 2042.3 s |

Tabla 5. Tiempos obtenidos tras hacer la prueba de subir un archivo al servidor oportuno

4.c.vi Descarga del archivo

El resultado del test es la media de 5 tests, limpiando la cache antes de cada test

| | Amazon cloud drive | Dropbox | Google Drive | OneDrive | Box | Mega | ADrive |
|--------|--------------------|---------|--------------|----------|---------|----------|----------|
| 1 MB | 0.92 s | 0.18 s | 0.38 s | 0.53 s | 3.17 s | 0.86 s | 4.39 s |
| 5 MB | 1.85 s | 0.6 s | 0.78 s | 1.72 s | 5.17 s | 2.68 s | 6.6 s |
| 10 MB | 1.89 s | 1.16 s | 0.97 s | 2.02 s | 5.92 s | 3.26 s | 7.04 s |
| 20 MB | 2.75 s | 1.51 s | 1.21 s | 3.31 s | 7.53 s | 6.54 s | 8.12 s |
| 50 MB | 4.42 s | 2.59 s | 2.54 s | 6.78 s | 10.37 s | 7.77 s | 13.91 s |
| 100 MB | 5.36 s | 7.18 s | 3.66 s | 14.77 s | 18.16 s | 13.34 s | 24.47 s |
| 200 MB | 11.86 s | 12.32 s | 7.51 s | 29.77 s | 27.34 s | 22.59 s | 33.96 s |
| 512 MB | 20.21 s | 27.9 s | 16.85 s | 93.76 s | - | 51.68 s | 69.18 s |
| 1 GB | 42.08 s | 5.53 s | 30.71 s | 168.03 s | - | 102.95 s | 109.93 s |

Tabla 6. Tiempos obtenidos tras hacer la prueba de descargar un archivo del servidor

4.c.vii Mover el archivo

Todas las soluciones de almacenamiento en la nube acabaron el test inmediatamente.

4.c.viii Velocidad de sincronización

| Amazon cloud drive | Dropbox | Google Drive | OneDrive | Box | Mega | ADrive |
|--------------------|---------|--------------|----------|-----------|------|--------|
| 2 s | 2 s | 2 s | 10 s | Inmediato | 2 s | 2 s |

Tabla 7. Velocidades de sincronización de archivos para cada uno de los proveedores

4.c.ix Localización de los servidores

Sabiendo que las soluciones escogidas de almacenamiento en la nube no tienen un único servidor y que los archivos almacenados en ellos se van moviendo entre los distintos servidores, hemos podido rellenar la siguiente tabla de los diferentes tests realizados y de las diferentes IP de los servidores que me han salido al subir o descargar un archivo a cualquiera de las soluciones *cloud* planteadas.

Análisis de soluciones cloud para almacenamiento de archivos y trabajo colaborativo

| | Dropbox | Google Drive | OneDrive | Box | Mega | ADrive |
|--------------------------|----------------------------------|--|-------------------------------------|--|---|---------------------------------|
| Stops | 16 | 9 | 11 | 10-14 | 8 - 12 | 12 |
| Localización del destino | Reston, Virginia, United States. | Mountain View, California, United States | Redmond, Washington, United States. | Los Altos, California, United States Palo Alto, California, United States | Datacenter Luxembourg S.A.en Luxembourg | Oregon, Portland, United States |
| Ping | 118 ms | 9 ms | 13 ms | 249 – 254 ms | 34 – 41 ms | 244 ms |

Tabla 8. Localización de los servidores donde hemos cargado y descargado archivos

(*)Algunos sitios populares como amazon.com, microsoft.com, slashdot.org y otros sitios donde se han tenido ataques de denegación de servicio en el pasado pueden deshabilitar ICMP para evitar solicitudes de ping.

Respecto a la localización de los servidores de Amazon cloud drive, se encuentran principalmente en Amazon Technologies en Dublin, Dublin, Ireland.

4.d ownCloud

4.d.i Descripción general y situación en la actualidad

OwnCloud, un programa multiplataforma, muy similar al popular DropBox, el cual al instalarlo sincroniza los archivos que queramos con la nube, a los cuales también podremos acceder desde un dispositivo móvil o cualquier ordenador conectado a Internet ya que presenta clientes para GNU/Linux, Mac OS X, Windows, iPhone y Android, donde podremos compartir nuestros archivos públicamente con o sin contraseñas, pero existe una gran diferencia frente a DropBox, OwnCloud se aloja en nuestro propio servidor, con lo que la seguridad y privacidad está asegurada. Por lo que es un servicio que nos proporciona nuestra propia nube personal, siendo una alternativa libre a las soluciones privadas presentes en el mercado, donde podremos almacenar en nuestro servidor toda la información que queramos, vídeos, música, imágenes... debido a que la capacidad de almacenamiento solo estará limitada por el espacio que tengamos disponible en el disco duro.

OwnCloud puede ser instalado dentro de un servidor que disponga de una versión reciente de PHP (mayor o igual a 5.3) y soporte de SQLite (base de datos por defecto), MySQL o PostgreSQL.

El proyecto fue lanzado en enero del 2010 por Frank Karlitschek, un desarrollador del proyecto KDE, con el objetivo de dar a los usuarios el control de sus datos en la nube. OwnCloud formó parte de la comunidad KDE pero luego se independizó. Concretamente el 13 de diciembre de 2011 ha sido creada una entidad comercial fundada bajo el proyecto OwnCloud.

OwnCloud es una aplicación web basada en PHP y de libre distribución, es una herramienta muy útil ya que es compatible con la mayoría de las bases de datos para facilitar su implantación. Esta aplicación no solo nos proporciona un almacenamiento seguro de nuestros datos, también podemos encontrar en su web gran cantidad de *plugins* que facilitan la experiencia del usuario, como un reproductor multimedia online, un visor y editor de archivos, un servidor de archivos WebDAV, un calendario de eventos (permite la sincronización CalDAV) y la posibilidad de administrar nuestra agenda de contactos (CardDAV).

La primera vez que accedamos al servicio tendremos que configurar la base de datos y el usuario que vamos a utilizar para administrar y configurar el servicio. Primero deberemos crear una base de datos nueva con PhpMyAdmin, luego podremos usar la interfaz del ownCloud para utilizarla para guardar la información acerca de los usuarios.

Además, ownCloud pone a disponibilidad "ownCloud 2012 Business and Enterprise", dos ofertas dedicadas a las empresas, que les permite administrar su propia nube segura para facilitar el trabajo de los colaboradores móviles.

Las versiones Business and Enterprises se dirigen a las pequeñas y medianas empresas. Estos servicios permiten el acceso a los archivos en la nube, desde dispositivos fijos y móviles, ofreciendo a los clientes una sincronización para Linux y Windows y aplicaciones móviles para Android e iOS.

La tarifa de ownCloud Enterprise cuesta 15 000 dólares al año (1500 dólares al mes) para un máximo de 250 usuarios.

La tarifa de ownCloud Business cuesta 999 dólares al año (100 dólares al mes) para un máximo de 50 usuarios.

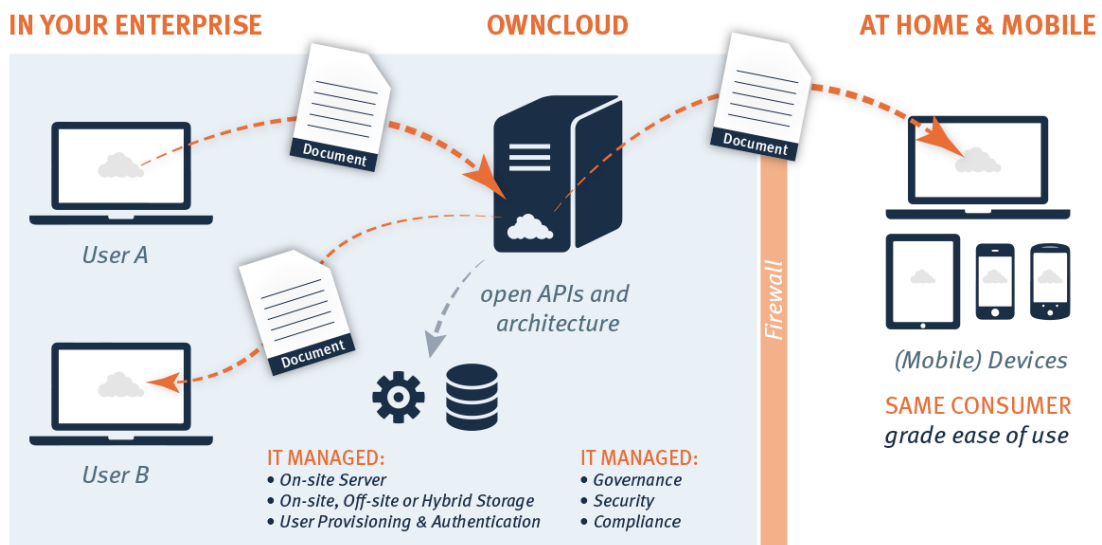


Figura 16. ownCloud en las empresas [28]

Los clientes del servicio de ownCloud se encuentran en diferentes sectores:

- Educación.
- Tecnologías.
- Servicios financieros.
- Telecomunicaciones.
- Fabricación.
- Atención sanitaria.
- Gobiernos.
- Otros sectores.

Finalmente, OwnCloud ha sufrido la pérdida de buena parte de sus integrantes más conocidos desde el lanzamiento de la versión 9. Parece ser que las personas que abandonaron ownCloud han decidido bifurcarlo y crear NextCloud.

Además de la sincronización y compartición de ficheros, NextCloud también incorporará soporte total para Spread.ME, una plataforma de comunicación de última generación basada en WebRTC para realizar conferencias y chats de texto. También se añadirá aplicaciones de calendario y contacto para enriquecer la experiencia de usuario en otras áreas.

Parece que NextCloud tendrá dos objetivos en mente. Uno, hacer más transparentes sus productos y servicios con respecto a lo ofrecido por ownCloud. Segundo, ofrecer una perspectiva más abierta, un salto ya dado por motivos más o menos similares por MariaDB frente a MySQL y LibreOffice frente a OpenOffice.

5.a Conclusión Académica

Como se muestra en los resultados, los servidores, principalmente, están en un continente diferente de donde se realizó la prueba. El resultado debe variar si la prueba se lleva a cabo en diferentes lugares o en un momento diferente ya que el tiempo es un factor de influencia, debido a que en todas partes del mundo, la velocidad de las conexiones a Internet no siempre es estable, y en realidad fluctúa en cierta medida. Y además, la distancia entre el lugar de la prueba y la localización de los servidores es también un factor de influencia, debido a la rapidez de respuesta y la velocidad de conexión. Sin embargo, el resultado es representativo en gran medida y las razones se enumeran a continuación:

a) El número de paradas representa el número de saltos que un paquete de datos tiene que hacer para llegar al servidor de destino. Cuanto menor sea el número, la posibilidad será menor de que un paquete de datos se considere perdido y por tanto haya que reenviarlo.

Se obtiene mediante el comando `tracert` o `tracert`, el cual envía paquetes eco (igual que el ping) pero éste nos muestra la ruta que toma hacia el destino al que queremos llegar, mostrándonos en ese camino datos como los host por los que pasa y el tiempo que se toma en cada salto hasta llegar al destino. El `tracert` tiene una ventaja contra el ping, y es que aquí podemos ver hasta qué punto y host llegamos en caso de que tengamos un fallo en la comunicación con el destino.

b) El tiempo de ping representa el tiempo de respuesta de una solicitud, que es extremadamente importante en la experiencia de usuario. Menos tiempo de ping significa menos tiempo de espera. El ping es una pequeña línea de código y lo que hace es enviar desde nuestra posición un paquete de información de 32 bytes al destino que hayamos seleccionado, para comprobar que tenemos comunicación con el destino. Lo que hace es enviar pequeños paquetes, el destino los escucha y responde de la misma forma, esperando solo hasta un segundo por cada envío. Pero si el ping falla es porque hay pérdidas por el camino.

c) Para los pequeños paquetes de datos, la velocidad de transferencia no es un factor importante de influencia, ya que la mayoría tiempo se dedica a las peticiones HTTP y la respuesta. Es decir, para los que quieren utilizar el sistema de almacenamiento en la nube para transferir pequeños paquetes de datos, los que tienen menos tiempo de ping deben ser las mejores opciones.

A pesar de los impactos ambientales, también pueden ser causas de diferencia en los resultados que grandes empresas como Google y Microsoft inviertan mucho más dinero en los servidores, en comparación con aquellos competidores que sólo tiene que preocuparse por cumplir la función más básica. Además, otro factor pueden ser las leyes y políticas locales.

Para la realización de las pruebas de cargar y descargar un archivo en los servicios elegidos de almacenamiento en la nube, hemos utilizado el programa Wireshark donde hemos visto las marcas temporales del primer y último paquete enviado y luego las resto para ver el tiempo que me interesa de carga y de descarga del fichero completo, aunque hemos tenido que añadirle un filtro para que solo vea paquetes que de una IP origen a una IP destino. Además, me fijo en la columna Info, en los paquetes donde dice Continuation Data, Application Data, TCP segment of a reassembled PDU y los respectivos ACK, para restar tiempos y obtener lo que necesito.

El filtro escogido era: `ip.src == x.x.x.x && ip.dst == y.y.y.y && tcp`, donde al cargar un archivo en un servidor `x.x.x.x` era la IP de mi ordenador (192.168.1.38) y `y.y.y.y` era la IP del servidor con el cual iniciaba la transferencia del archivo, y si estábamos en el caso de descargar un archivo `x.x.x.x` era la IP del servidor y `x.x.x.x` era mi IP. Aunque cabe destacar que Google Drive trabaja sobre UDP, no TCP.

En resumen, podemos ver como en este trabajo se ha podido comprender y conocer los pilares fundamentales que han dado lugar el desarrollo de la nube y todos los servicios que ello conlleva, es decir, todos los antecedentes al *cloud computing* que han ido evolucionando, bajo mucho trabajo científico y tecnológico, para luego poderlo implementar en la vida personal y profesional de las personas. También se puede apreciar en el trabajo, como hemos dado una visión actual y futura del tema del *cloud computing* ya que no para de crecer, en el sentido que las empresas que ofrecen servicios *cloud* intentan mejorar constantemente sus servicios a los clientes para hacer un uso correcto, fácil y seguro de éstos e incluso gobiernos internacionales destinan parte de presupuestos para fomentar el uso de este tipo de tecnologías en las empresas y así éstas tener mejor beneficios y una mejor organización.

Respecto a la parte más práctica de este trabajo, se puede ver como existen diversos factores que hacen que lo calculado varíe, pero lo que he querido aportar es ver que existen muchos proveedores de servicios de almacenamiento en la nube los cuales permiten dejar nuestra información en sus servidores, situados principalmente en Estados Unidos, y tener acceso a ellos cuando queramos de una manera rápida, dependiendo del tamaño del archivo, y seguro. Las diferencias de tiempo, se podrían decir que se debe en la cantidad de saltos que se debe hacer para llegar al destino y a la fragmentación que se les aplica a estos archivos y luego al ensamblaje en el destino. Además, lejos de necesitar los servidores de una empresa de terceros o tener que pagar una inscripción para usar un alojamiento en la nube podemos usar nuestros propios servidores, gracias a ownCloud.

Como trabajo futuro, podemos plantear varios aspectos:

- Ampliar la elección de los proveedores de almacenamiento de archivos en la nube.
- Hacer las mismas pruebas con archivos de menor tamaño e incluso de mayor.
- Hacer las mismas pruebas con otro tipo de conexión a Internet o en otra zona geográfica.
- Montar nuestro propio servidor cloud y hacer las mismas pruebas expuestas anteriormente.

Conclusión Personal

Este trabajo me ha parecido muy interesante y productivo ya que, es un tema de actualidad, donde muchas empresas están invirtiendo grandes cantidades de dinero para poder migrar y trabajar en la nube, lo que significa que van a necesitar a gente, principalmente ingenieros, para ponerlo en marcha. Además, he podido poner conocimientos prácticos de materias estudiadas en mi carrera y ver como la tecnología avanza a pasos agigantados.

Para finalizar, me gustaría mostrar mi mayor agradecimiento a mi tutor Fernando Raimundo González Ladrón de Guevara por sus ideas y ayuda constante, para poder sacar el trabajo adelante. Además, agradecerle también su preocupación y observación en mis estudios. Debo agradecer también a otros profesores que me ayudaron en la parte práctica de este trabajo: José Óscar Romero Martínez y Antonio León Fernández. Por último, pero no menos importante, agradecer a todos mis amigos y familiares que animan y me apoyan durante los días.

Bibliografía

[1] Buyya R.; Broberg J. and Goscinski A. *Cloud Computing: Principles and Paradigms*. John Wiley & Sons INC. Publication, 2011.

[2] Joyanes Aguilar, L. *Computación en la nube: estrategias de Cloud computing en las empresas*. Alfaomega y Marcombo, 2013.

[3] Rhoton, J. and Haukioja R. *Cloud computing architected*. Recursive Press, 2011.

[4] Gnanasundaram, S. and Shrivastava, A. *Information storage and management: storing, managing, and protecting digital information in classic, virtualized, and cloud environments*. John Wiley & Sons INC. Publication, 2012.

[5] Hwang, K; Fox, G.C and Dongarra, J.J. *Distributed and cloud computing: from parallel processing to the Internet of things*. ELSEVIER, 2012.

[6] Deng, P. Undergraduate Project Report 2013/2014. *Analysis of Cloud computing solutions for file storage*.

[7] Cloud Computing: Antecedentes

<http://cloud-fi.blogspot.com.es/2012/11/antecedentes-cloudcomputing-no-es-un.html>

[8] El origen de: El Cómputo en la Nube

<https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/>

[9] Cloud Computing. Lic. Guillermo Montenegro VicePresidente CPCIPC

<http://www.cervantes.edu.ar/news/pdf/cloudconsejo.pdf>

[10] Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374

[11] Cloud Services Measurement Initiative Consortium (CSMIC) Overview (November 2011)

http://csmic.org/downloads/SMI_Overview_TwoPointOne.pdf

[12] SMICloud: A Framework for Comparing and Ranking Cloud Services. Saurabh Kumar Garg, Steve Versteeg and Rajkumar Buyya

<http://www.buyya.com/papers/SMICloud2011.pdf>

[13] A survey on quality attributes in service-based systems. David Ameller, Matthias Galster, Paris Avgeriou and Xavier Franch

<http://www.cs.rug.nl/paris/papers/SQJ15.pdf>

[14] Modelos de despliegue cloud: Cloud privado, cloud público y cloud híbrido

<https://www.nexica.com/es/blog/modelos-de-despliegue-cloud-cloud-privado-cloud-p%C3%BAblico-y-cloud-h%C3%ADbrido>

[15] MuyCloud. Información sobre Cloud Computing

<http://muycloud.com/>

[16] Cloud computing por Oscar Mendoza Ricci

<http://www.monografias.com/trabajos-pdf5/cloud-computing/cloud-computing.shtml>

[17] Cloud storage - Administración de Sistemas Operativos

http://www.adminso.es/recursos/Proyectos/PFM/2011_12/PFM_cloud_storage.pdf

[18] Top 20 Best Cloud Storage Providers – Reviews and Comparison of the Top Secure Solutions and Services. Find Unlimited Cloud Based Data Storage Services and Options

<http://cloudnewsdaily.com/cloud-storage/>

[19] 30 servicios gratis para almacenar archivos en la nube

<http://ignaciosantiago.com/mejores-servicios-almacenamiento-gratis-nube/>

[20] 5 características que debe tener un buen servicio de almacenamiento en la nube

<http://www.revistacloudcomputing.com/2015/06/5-caracteristicas-que-debe-tener-un-buen-servicio-de-almacenamiento-en-la-nube/>

[21] Retos de seguridad en el almacenamiento en la nube

<http://www.muycomputerpro.com/2015/01/20/seguridad-almacenamiento-nube>

[22] Protección de datos y privacidad en la nube ¿Quién es el propietario de la nube?

<https://itunews.itu.int/Es/3702-Proteccion-de-datos-y-privacidad-en-la-nube-BR-Quien-es-el-propietario-de-la-nube.note.aspx>

[23] Comparativa de precios para guardar tus archivos en la nube

<http://www.adslzone.net/2015/09/10/comparativa-de-precios-para-guardar-tus-archivos-en-la-nube/>

[24] Almacenamiento en la nube. El mejor gratis y de pago

<http://discodurobarato.com/almacenamiento-en-la-nube/>

[25] 10 herramientas útiles para trabajar en la nube

<http://www.clasesdeperiodismo.com/2013/09/03/10-herramientas-utiles-para-trabajar-en-la-nube/>

[26] Siete alternativas para crear y editar documentos de texto desde el navegador

<http://www.genbeta.com/ofimatica/siete-alternativas-para-crear-documentos-de-texto-desde-el-navegador>

[27] Internet de las cosas: Desarrollo de un servidor Domótico. Trabajo Fin de Grado. Grado en Ingeniería Informática

<https://riunet.upv.es/bitstream/handle/10251/56081/SORIANO%20-%20Internet%20de%20las%20cosas%3a%20Desarrollo%20de%20un%20servidor%20Dom%C3%B3tico.pdf?sequence=2&isAllowed=y>

[28] ownCloud

<https://es.wikipedia.org/wiki/OwnCloud>

[29] Access, Sync and Share Your Data, Under Your Control

<https://owncloud.org/features/>

<https://owncloud.com/sync-share-files/>

