UNIVERSIDAD DE SALAMANCA

FACULTAD DE TRADUCCIÓN Y DOCUMENTACIÓN

GRADO EN INFORMACIÓN Y DOCUMENTACIÓN

Trabajo Fin de Grado

COMPUTACIÓN EN LA NUBE

Contratos: un estudio comparativo

CLOUD COMPUTING

Contracts: a comparative study

Alumno: Pedro Cortés García

Tutor: María Manuela Moro Cabero

Salamanca, 2017

ASIENTO CATALOGRÁFICO ISDB

CORTÉS GARCÍA, Pedro

Computación en la nube. Contratos: un estudio comparativo / Pedro Cortés García, María Manuela Moro Cabero . – Salamanca : Universidad de Salamanca. Facultad de Traducción y Documentación, 2017

50 h.
Trabajo de Fin de Grado – Grado en Información y Documentación

1. Computación en la nube. 2. Informática – Sistemas de información. 3. Universidad de Salamanca. Informática I. Moro Cabero, María Manuela, dir. II. Título

RESUMEN: Con el auge de la computación en la nube como nuevo sistema de almacenamiento de información surgen dudas sobre su gestión, funcionamiento y legislación. Este trabajo intenta dar respuesta a dichas dudas con definiciones y descripciones del denominado cloud computing y se focaliza en el sistema de obtención de productos y la relación (normativas, deberes y derechos) con los proveedores mediante un estudio comparativo de los contratos de varias entidades.

Palabras clave: computación en la nube, contrato

ABSTRACT : With the rise of cloud computing as a new information storage system, doubts arise about its management, operation and legislation. This paper tries to answer these doubts with definitions and descriptions of the so-called cloud computing and focuses on the system of obtaining products and the relationship (regulations, duties and rights) with suppliers through a comparative study of the contracts of several entities.

Keywords: cloud computing, contract

SUMARIO

1. INTRODUCCIÓN

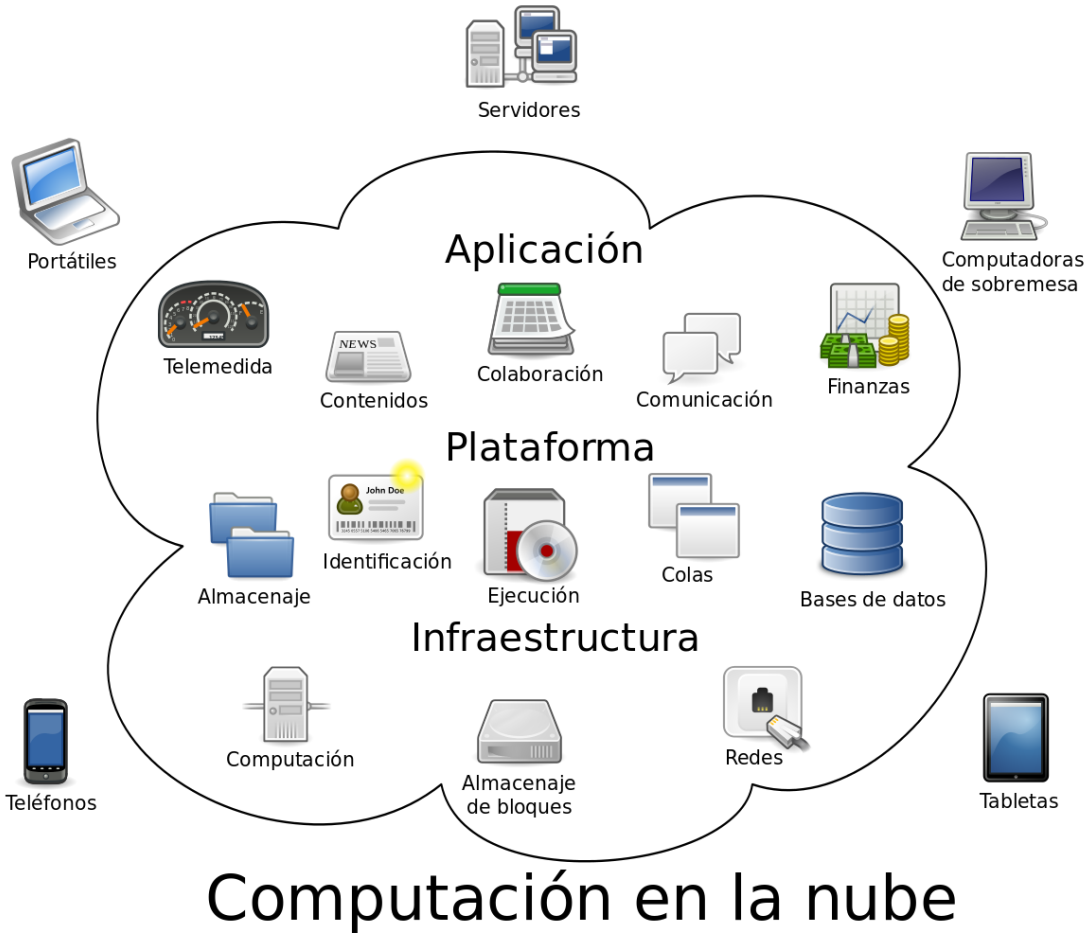

Figura 1.- Esquema de la computación en nube

1.1. OBJETO

El objetivo del presente trabajo es definir el concepto de "computación en la nube" (cloud computing), enumerar sus distintos tipos y modelos describiendo sus características y tratar de explicar la forma de contratación de dicho servicio complementada con su legislación vigente. Para verificar eficazmente dicha contratación se ha realizado una comparación y evaluación de varios proveedores de servicios cloud computing. Finalmente, el trabajo se complementa con unas conclusiones.

1.2. JUSTIFICACIÓN

La computación en la nube es una tendencia que cada vez va ganando más fuerza entre las empresas que prestan servicios a través de la web y usuarios y entidades que acceden a ellos a través de Internet. El aumento en el uso de la computación en la nube se debe entre otras a que no hay necesidad de conocer la infraestructura detrás de ésta, ya que pasa a ser “una nube” donde las aplicaciones y servicios pueden fácilmente crecer y funcionar rápidamente. Además otro de los aspectos que más llaman la atención es la reducción de los costos, ya que el capital de trabajo de la empresa se convierte en un gasto operacional, no hay que preocuparse por armar un excelente y confiable data center, ya que ésto es responsabilidad directa de la empresa a la cual se le compra un espacio en sus servidores, también se reduce notablemente su consumo de energía eléctrica.

Es por el creciente interés (y para muchos el desconocimiento) que provoca este servicio que se justifica este trabajo ya que busca dar a entender que es el cloud computing, características, ventajas, desventajas y su esquema de funcionamiento y modelos de contratación ya que el futuro está en la nube y los sistemas de información han venido experimentando un cambio radical en la manera en la que accedemos a ellos y cómo son gestionados.

1.3. METODOLOGÍA

Para la realización del presente trabajo (y siempre bajo la dirección de la tutora) se ha tomado como fuente principal Internet y su acceso a distintos artículos del tema a tratar. Para la compresión y elaboración de los primeros pasos nos hemos ayudado de la "Guía para clientes que contraten servicios de Cloud Computing[1]" creada por la Agencia Española de Protección de Datos. Se ha completado dicha información apoyándonos en los artículos descritos en la bibliografía. Para conocer las características y términos de contrato de los distintos proveedores de servicio se ha acudido a sus respectivos sitios *web*. Para la realización de la comparativa se ha tomado como herramienta la "Lista de verificación para los contratos de servicio en la nube[2]" creada por InterPARES Trust Project. Dicha lista de verificación para los contratos de servicios en la nube es un producto final de investigación que llevó a cabo el Proyecto InterPARES Trust sobre contratos comunes de servicio desde una perspectiva de administración de archivos, archivística y jurídica. InterPARES Trust (2013-2018) es un proyecto de investigación multinacional, interdisciplinario que explora cuestiones relacionadas con los documentos de archivo y datos en el ambiente en línea. Las audiencias objetivo para este documento son los gestores o administradores de documentos, archivistas, funcionarios de servicios de información y otros interesados que evalúan los servicios de nube dentro de una organización. El objetivo del mismo es proporcionar una herramienta para:

- Adquirir un conocimiento de un texto estándar o modelo de contratos.

- Verificar si los contratos potenciales de servicios en la nube cumplen con los requerimientos.

- Clarificar a las áreas de tecnologías de la información y jurídicas las necesidades de gestión documental y archivísticas

- Comunicar las necesidades de gestión documental y archivística a los proveedores de servicio de nube.

Esta lista de verificación es solo una herramienta para tomar en cuenta, no constituye una propuesta jurídica. No se recomienda su uso para o en contra de cualquier proveedor de servicio de nube en particular (o uso de servicios de nube en general). Los individuos y las organizaciones deberán solicitar el apoyo jurídico en caso de que lo requieran para un contrato en particular. De dicha comparativa extraeremos unas conclusiones.

[1]https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf
[2] https://interparestrust.org/assets/public/dissemination/ABAITRUSTNA14_FINAL_checklist_julio-29_2016TRAD.AB_.pdf

2. DESARROLLO

2.1. DEFINICIÓN Y CARACTERÍSTICAS DE CLOUD COMPUTING

Para definir el concepto de "computación en la nube" o "cloud computing", acudiremos a la definición oficial ofrecida por el NIST (National Institute of Standards and Technology), que es la entidad encargada de desarrollar estándares y guías para favorecer la innovación y la competitividad industrial. El NIST define cloud computing de la siguiente manera[3]:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

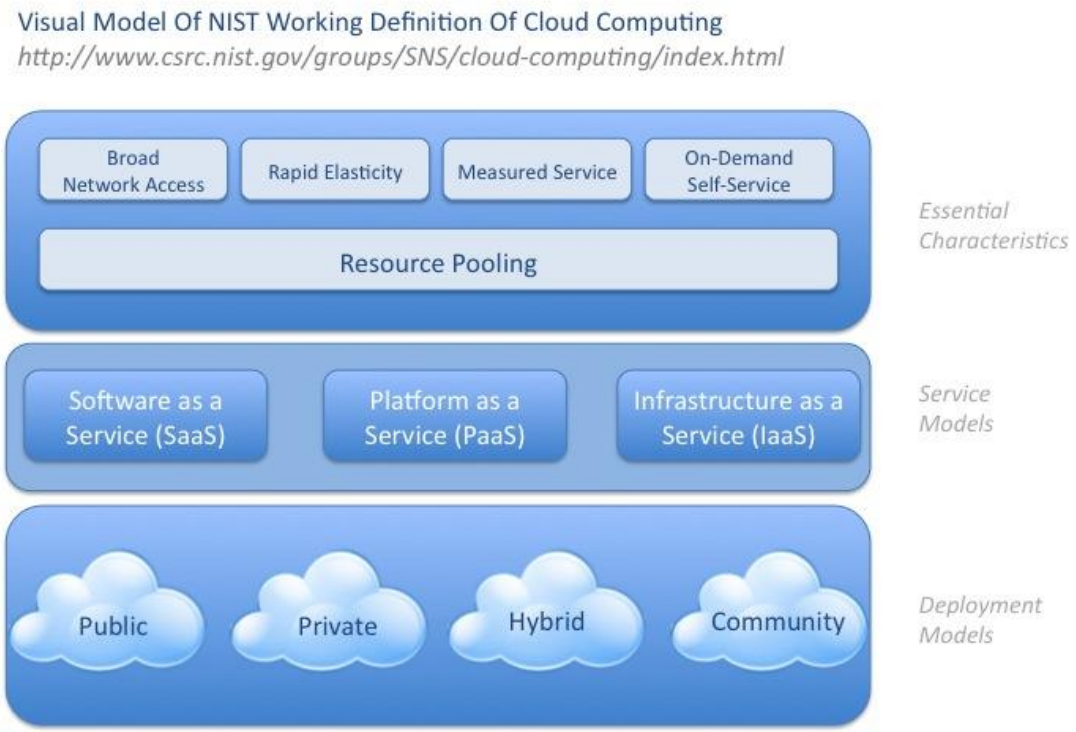

Figura 2.- Definición del concepto Cloud Computing, por NIST

En otras palabras y apoyándonos en la Guía para clientes que contraten servicios de Cloud Computing[2] podemos entender que la computación en nube es una nueva forma

[3] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como para un particular y, también, para la Administración Pública.

Una solución cloud computing permite al usuario optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información. El usuario no tiene necesidad de realizar inversiones en infraestructura sino que utiliza la que pone a su disposición el prestador del servicio, garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecoste asociado a dichas situaciones.

En un entorno de cloud computing la gestión de la información está de forma virtual en manos del cliente que contrata los servicios de la nube, que la trata a través de Internet accediendo a soluciones de bases de datos, correo electrónico, nóminas o gestión de recursos humanos de acuerdo a sus necesidades. En función del modelo utilizado, los datos pueden no estar realmente en manos del contratista, toda vez que la propiedad, el mantenimiento y gestión del soporte físico de la información, los procesos y las comunicaciones pueden encontrarse en manos de terceros. El proveedor del servicio puede encontrarse en, prácticamente, cualquier lugar del mundo y su objetivo último será proporcionar los servicios citados optimizando sus propios recursos a través de, por ejemplo, prácticas de deslocalización, compartición de recursos y movilidad o realizando subcontrataciones adicionales.

De esta forma, el cloud computing representa una nueva forma de utilizar las tecnologías de la información y las comunicaciones, que se basa en emplear técnicas ya existentes de una forma innovadora y, sobre todo, a una nueva escala. Esto último es lo que la hace realmente distinta, ya que permite el uso de recursos de hardware, software, almacenamiento, servicios y comunicaciones que se encuentran distribuidos geográficamente y a los que se accede a través de redes públicas, de forma dinámica, cuando se necesita, mientras se necesita y abonando una tarifa (cuando no es gratuita) sobre lo que se consume; es decir, proporcionando a sus clientes un servicio de tecnologías de información bajo demanda.

Como consecuencia de lo anterior, el mismo contratista puede desconocer la localización precisa de sus datos y no disponer del control directo de acceso a los mismos, de su borrado y de su portabilidad, ya que la información no está físicamente en su poder aunque, si esa información contiene datos de carácter personal, sí está bajo su responsabilidad desde el punto de vista de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD).

En resumen, se puede entender como un modelo de uso de los equipos informáticos, en el que lo que normalmente estaría en nuestro propio equipo, pasa a estar en un conjunto de servidores – la nube - a los que se puede acceder a través de Internet. El concepto fundamental y que lo hace realmente interesante, es que todo lo que ocurre dentro de la nube es transparente para el usuario, y además no se necesita ningún tipo de conocimiento técnico para utilizarla.

La computación en nube tiene las siguientes cinco características esenciales:

— Autoservicio bajo demanda. El usuario puede acceder a capacidades de computación «en la nube» de forma automática conforme las necesita sin necesidad de una interacción humana con su proveedor o sus proveedores de servicios Cloud.

— Múltiples formas de acceder a la red. Los recursos son accesibles a través de la red y por medio de mecanismos estándar que son utilizados por una amplia variedad de dispositivos de usuario, desde teléfonos móviles a ordenadores portátiles o PDAs.

— Compartición de recursos. Los recursos (almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) de los proveedores son compartidos por múltiples usuarios, a los que se van asignando capacidades de forma dinámica según sus peticiones. Los usuarios pueden ignorar el origen y la ubicación de los recursos a los que acceden, aunque sí es posible que sean conscientes de su situación a determinado nivel, como el de CPD o el de país.

— Elasticidad. Los recursos se asignan y liberan rápidamente, muchas veces de forma automática, lo que da al usuario la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.

— Servicio medido. El proveedor es capaz de medir, a determinado nivel, el servicio efectivamente entregado a cada usuario, de forma que tanto proveedor como usuario tienen acceso transparente al consumo real de los recursos, lo que posibilita el pago por el uso efectivo de los servicios.

Como se indica en el informe «Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal[4]», las ventajas técnicas y económicas del modelo son inmediatas para los usuarios. No es necesario que los pequeños negocios cuenten con personal informático propio dedicado al mantenimiento de los servidores y las aplicaciones. Por otra parte, los servicios tecnológicos pasan a ser un gasto operativo, obviándose la necesidad de inversiones en infraestructuras de breves ciclos de vida y rápida obsolescencia. El acceso a los servicios está garantizado desde cualquier lugar del mundo en el que se disponga de una conexión a Internet, y el proveedor de servicios asegura la disponibilidad del servicio y la actualización permanente de aplicaciones y sistemas.

4 https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/informe_CLOUD.pdf

2.1.1. MODELOS DE "NUBES"

Según la citada Guía para clientes que contraten servicios de Cloud Computing anteriormente no todos los servicios y proveedores de computación en la nube son iguales, ni lo son las posibles relaciones que se establecen entre clientes y proveedores. Las nubes se pueden clasificar de muchas formas atendiendo a varios criterios y lo que más interesa, desde el punto de vista de la normativa española de protección de datos, es cómo afectan dichas modalidades de implementación al tratamiento de datos de carácter personal.

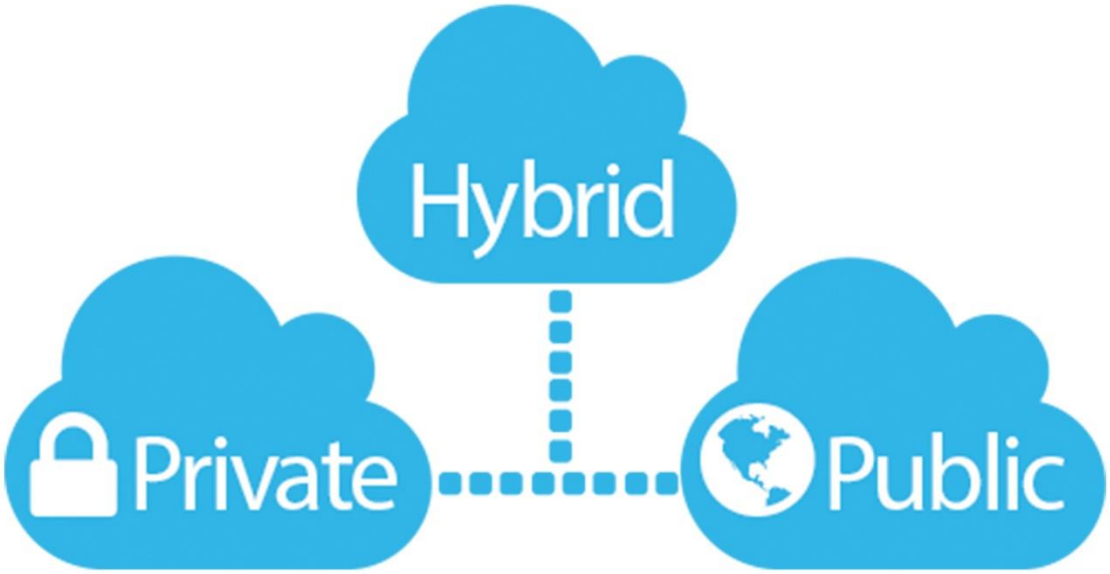

Figura 3.- Esquema de los tipos de nubes

Nube pública

Hablamos de un servicio de Nube Pública cuando el proveedor de servicios de cloud proporciona sus recursos de forma abierta a entidades heterogéneas, sin más relación entre sí que haber cerrado un contrato con el mismo proveedor de servicio. Existen diversas y numerosas soluciones en Nube Pública y prestan sus servicios desde particulares a grandes corporaciones, ya que cualquiera puede contratar con ellos. Algunos ejemplos de proveedores de nubes públicas son Amazon, Google, Apple o Microsoft.

Nube privada

En el otro extremo podemos hablar de Nube Privada, que la encontramos cuando una entidad realiza la gestión y administración de sus servicios en la nube para las partes que la forman, sin que en la misma puedan participar entidades externas y manteniendo el control sobre ella. Una Nube Privada no necesariamente se implementa por la misma entidad que la utiliza, sino que puede contratarse a un tercero que actuará bajo su supervisión y en función de sus necesidades.

Las entidades que optan por las Nubes Privadas son aquellas que son complejas y necesitan centralizar los recursos informáticos y, a la vez, ofrecer flexibilidad en la disponibilidad de los mismos, por ejemplo, administraciones públicas y grandes corporaciones, aunque hay ejemplos de Nubes Privadas implementadas en entidades de enseñanza. Son muchos los proveedores de nubes privadas; algunos de ellos son VMware, OpenStack o CloudStack.

Otros modelos

Entre ambos modelos se encuentran soluciones intermedias que tomarán distintos nombres, como pueden ser las Nubes Híbridas, en las que determinados servicios se ofrecen de forma pública y otros de forma privada; las Nubes Comunitarias, cuando dichos servicios son compartidos en una comunidad cerrada; o las Nubes Privadas Virtuales, cuando sobre Nubes Públicas se implementan garantías adicionales de seguridad.

2.1.2. TIPOS DE SERVICIOS

Los proveedores de la nube proporcionan acceso a recursos informáticos a través de la red, y ofrecen una serie de servicios adicionales de valor añadido que acercarán la oferta del proveedor a las necesidades de su cliente. En función de lo completo que sea ese valor añadido podemos decir que tenemos una solución de Infraestructura como Servicio, Plataforma como Servicio o Software como Servicio. Esta división no puede considerarse rígida, ya que hay proveedores que proporcionan soluciones mixtas en las que se combinan características de todas ellas.

Cabe destacar, antes de entrar más a fondo en cada uno de estos modelos, que un usuario tendrá más flexibilidad con IaaS, y menos con SaaS. Del mismo modo, con esta flexibilidad que aporta IaaS viene el tener que administrar, monitorizar y gestionar todo el entorno cloud, cosa que nos ahorra SaaS a costa de ofrecernos mucha menos flexibilidad. Dependiendo de la aplicación que queramos desplegar, tendremos que usar

un modelo de servicio u otro, ya que no hay uno que sea mejor o peor, cada uno se adapta mejor a unas necesidades concretas.

De manera resumida, podemos decir que con IaaS, el usuario construye el servidor (virtual) comenzando en la capa del sistema operativo; con PaaS, el consumidor construye la base de datos y la aplicación, así como las reglas de negocio, y carga los datos; por último, con SaaS, el usuario final sólo tiene que cargar los datos en la aplicación preconstruida.

También es importante saber que las fronteras entre los modelos de servicio no son estrictas, es decir, que hay plataformas que pueden ser consideradas, por ejemplo, IaaS y PaaS al mismo tiempo, ya que tienen características propias de ambos modelos.

Software como servicio

Podemos hablar de una Nube de Software (modelo de servicio *Software as a Service* o SaaS), cuando el usuario encuentra en la *nube* las herramientas finales con las que puede implementar directamente los procesos de su empresa: una aplicación de contabilidad, de correo electrónico, un *workflow*, un programa para la gestión documental de su empresa, etc.

Infraestructura como servicio

Si el valor añadido es nulo, se puede hablar de una Nube de infraestructura (IaaS). En ese caso el proveedor proporciona capacidades de almacenamiento y proceso en bruto, sobre las que el usuario ha de construir las aplicaciones que necesita su empresa prácticamente desde cero. Tal vez se pueda decir que éste es el modelo más primitivo de *nube*, que se inició con los sitios de Internet que proporcionaban capacidad de almacenamiento masivo a través de la red y los servidores de alojamiento web.

Plataforma como servicio

Entre estas dos aproximaciones se pueden encontrar otras intermedias llamadas PaaS (Plataforma como Servicio), en las que se proporcionan utilidades para construir aplicaciones, como bases de datos o entornos de programación sobre las que el usuario puede desarrollar sus propias soluciones.

Con el objetivo de dejar muy claro el concepto de IaaS, PaaS y SaaS, y las diferencias entre ellos, nos apoyaremos en una tabla comparativa desarrollada por Arsys, proveedor europeo de servicios de presencia en Internet, hosting gestionado, cloud computing y soluciones de infraestructura TIC.

	¿Qué es?	Conocimientos IT necesarios	Proveedor gestiona	Cliente gestiona
SaaS	Aplicación empresarial - 'llave en mano' - lista para utilizar	-	Todo	Parametrización básica
PaaS	Plataforma (hardware + software) sobre la que desplegar aplicaciones de forma sencilla	Programación	Datacenter, hardware, sistema operativo y software base	Código y datos de la aplicación
IaaS	Infraestructura (servidores y almacenamiento) para alojar aplicaciones con control total	Programación y administración de sistemas	Datacenter y hardware	Todo el software (sistema operativo y aplicaciones)

Figura 4.- Comparativa modelos de servicio cloud, por Arsys

2.1.3. BENEFICIOS Y RIESGOS DEL USO DE LA NUBE

Como bien explica Rafael García del Poyo «…las ventajas que ofrece la nube son muchas, el hecho de que la empresa -en principio- no va a verse en la necesidad de instalar ningún hardware adicional y, por lo tanto, se requerirá de una inversión inicial menor de la que debería haberse realizado en el pasado para obtener unos rendimientos productivos similares, se producen mayores compatibilidades y capacidades de integración con el resto de aplicaciones informáticas, proporcionando una mayor capacidad de recuperación en caso de desastre y reduciendo los tiempos de inactividad del sistema. Otra de las grandes ventajas de la nubes es que se permite en paralelo por parte del cliente un seguimiento continuo de su actividad, lo que contribuye a realizar una gestión transparente que repercute en un mayor "bienestar contractual" de las partes».

Si bien es cierto que la contratación de servicios en la nube entraña ciertos riesgos y límites dentro de la gestión de la empresa, algunos aducen que limita la libertad de gestión de las empresas clientes y las hace excesivamente dependientes de su proveedor de servicios y, a su vez, ello redunda en que se limita tanto la libertad como la creatividad de la empresa cliente para estructurar y organizar de una cierta manera su información.

Se ha advertido acerca de los riesgos para la confidencialidad, disponibilidad, integridad, y portabilidad de los datos, ya que a través del cloud computing se pone en peligro la libertad de disposición de la información de las empresas, argumento este especialmente digno de consideración si aceptamos que en la sociedad de la información el activo más valioso de una compañía es precisamente su información. Los riesgos fundamentales son:

- Disminución de disponibilidad debido a la merma en la interoperabilidad (cautivos de un sólo proveedor): Si un cliente contrata exclusivamente con una solo proveedor de servicios en la nube que le garantiza un servicio completo puede ser complicado transferir datos y documentos entre diferentes sistemas de proveedores de nubes (data portability) o intercambiar información con otras entidades que utilizan un sistema diferente de nubes (interoperabilidad).

- Disminución de la integridad de los sistemas por operar con recursos compartidos: Las infraestructuras de las nubes se realizan a través de sistemas y recursos compartidos. De forma que los datos personales de personas físicas u organizaciones estén dentro de infraestructuras de seguridad más complicadas.

- Disminución de confidencialidad: Es el riesgo que entraña que los servidores donde se aloje la información de la nube no se encuentren dentro del ámbito territorial de la UE y por lo tanto no cumplan con la normativa de seguridad que exige la UE en materia de protección de datos.

- Disminución de la capacidad de control debido a la complejidad de las dinámicas de la externalización de los servicios: Los proveedores de servicios de nube suelen utilizar a su vez otros proveedores que pueden cambiar a lo largo del contrato, dificultando el control sobre los mismos y pudiendo provocar cambios durante la prestación del servicio.

De este modo se advierte que mediante el funcionamiento del modelo cloud las compañías depositan sus informaciones de negocio más valiosas y los datos personales de los que disponen en manos de terceros, y esta información recorre diferentes nodos para llegar a su destino, cada uno de ellos y sus respectivos canales de acceso pueden convertirse en un foco permanente de inseguridad y por esta razón, se deben utilizar protocolos seguros. Otro riesgo reside en la velocidad de acceso a la información que puede llegar a disminuir drásticamente, debido a la sobrecarga que requieren este tipo de protocolos lo cual puede llegar a producir un excesivo grado de dependencia tanto de los proveedores de servicios de cloud computing como de los proveedores de acceso a Internet, o que la externalización de los servicios cloud puede implicar que la información acabe alojándose en países que no pertenecen a la Unión Europea sin las garantías que esta exige en materia de protección de datos.

Finalmente, si nos centramos exclusivamente en los proveedores de servicios altamente especializados, la prestación completa de los servicios al cliente que los solicita puede llegar a tardar meses o incluso años. Y, por otro lado, si tenemos en cuenta que la madurez funcional de las aplicaciones informáticas hace que continuamente deban incorporarse modificaciones, puede ocurrir que, para aquellas empresas cliente de baja intensidad en la utilización de recursos tecnológicos, la curva de aprendizaje puede alcanzar un exiguo rendimiento.

2.1.4. PARTES QUE INTERVIENEN

En el ámbito de la protección de datos es muy importante evaluar el papel de las partes que intervienen en la computación en nube. Para efectuar este estudio es muy importante el análisis del documento elaborado por el Grupo de Protección de Datos del Artículo 29 (G-29 a partir de ahora) sobre los conceptos de responsable del tratamiento y encargado del tratamiento[5], si bien encontramos las definiciones generales de ambas figuras en el artículo 2 de la Directiva:

— Responsable del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario.

— Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Según el documento antes indicado del G-29, «el papel primero y primordial del concepto de responsable del tratamiento es determinar quién debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera los interesados pueden ejercer sus derechos en la práctica. En otras palabras, debe asignar la responsabilidad». Por otra parte, el encargado del tratamiento deberá cumplir dos condiciones básicas:

— Ser una entidad jurídica independiente del responsable.

— Realizar el tratamiento de datos personales por cuenta de éste.

En el Dictamen 05/2012 del G-297, se estudia la posición que ocupan clientes y proveedores de servicios de computación en nube. Para el G-29, el cliente determina el objetivo último del tratamiento y decide sobre la externalización de este tratamiento y la delegación de la totalidad o de parte de las actividades de tratamiento a una organización externa. El cliente actúa por tanto como responsable del tratamiento, y por lo tanto debe aceptar la responsabilidad de respetar la legislación sobre protección de datos, y es responsable y está sujeto a todas las obligaciones legales que figuran en la Directiva 95/46/CE.

El proveedor es la entidad que presta los servicios de computación en nube de las distintas formas que se han mencionado. Cuando el proveedor suministra los medios y

[5] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

la plataforma, actuando en nombre del cliente, se considera que es el encargado del tratamiento es decir, será como antes ya hemos definido, «la persona física o jurídica, autoridad pública, servicio cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento».

En la computación en nube es frecuente que los encargados de tratamiento (proveedores del servicio) subcontraten subencargados del tratamiento adicionales. Esta subcontratación se ha estudiado por el G-29 en el Dictamen 1/2010 antes mencionado, llegando a la conclusión de que «no hay nada en la Directiva que impida que, por exigencias organizativas, se pueda designar a varias entidades como encargadas (o subencargadas) del tratamiento de datos, incluso subdividiendo los cometidos en cuestión. Ahora bien, todas ellas tienen que ajustarse a las instrucciones dadas por el responsable del tratamiento de los datos al llevar a cabo el tratamiento».

2.1.5. ASPECTOS CLAVE A CONSIDERAR

Armonización

Como servicio transfronterizo, resulta necesaria una armonización de la legislación de protección de datos a nivel global a fin de evitar las grandes divergencias en implementación, lo cual evidentemente supone un reto a superar.

Interoperabilidad

Es de suponer que las empresas que estén considerando el uso de sistemas/servicios basados en la Nube les puedan interesar soluciones que les permitan distribuir el trabajo a través de múltiples proveedores. Puede entenderse la interoperabilidad como la capacidad de los diferentes ambientes de servicios en la Nube (proveedores, servicios en la Nube, infraestructura en la Nube) puedan sin ningún problema trabajar juntos, transferir las cargas de trabajo, etc... La mayoría de los aspectos de interoperabilidad en la capa de IaaS (infraestructura) ya se están considerando, existen formatos comúnmente admitidos, tales como el formato de virtualización abierto (OVF) para las máquinas virtuales, que permite el exportar/importar una máquina virtual entre servicios. La Interoperabilidad es necesaria, por un lado para evitar que los clientes de la Nube puedan ser bloqueados por los proveedores de la nube, y por otro, para que los proveedores de la Nube no puedan ser bloqueados por los productores de tecnología de la nube.

Normalización

La normalización es crucial para garantizar la interoperabilidad en la Nube y esta debe seguir estando liderada por la industria. Los consorcios industriales en los organismos de normalización están y deberían seguir liderando el desarrollo de estándares para la Nube, por otro lado, es deseable que futuras alianzas entre los operadores de

telecomunicaciones garanticen la interoperabilidad de los servicios en la Nube. La función de los reguladores está en garantizar que los consorcios de la industria garanticen procedimientos abiertos, acceso no discriminatorio y transparente, así como una política de los derechos de propiedad intelectual legalmente segura y equilibrada.

Portabilidad

Es de suponer que las empresas que estén utilizando sistemas/servicios basados en la Nube quieran disponer de la libertad de poder cambiar de proveedor evitando las "ataduras" a un proveedor determinado. La portabilidad es la capacidad del consumidor de servicios de nube para cambiar sus datos y servicios de un proveedor a otro evitando problemas de incompatibilidad.

Subcontratación

Por el contrario, puede no tratarse de un prestador final cuando el servicio que ofrece directamente al usuario se construye sobre la subcontratación a terceros de elementos necesarios para implementarlos (hardware, almacenamiento, comunicaciones, etc.), como es el caso de los partners. A su vez, los subcontratistas pueden subcontratar de nuevo parte del servicio que proporcionan al prestador final a terceras y sucesivas compañías. Este es un modelo de cadena de subcontrataciones que en teoría podría no tener fin, y cuyo objeto es redimensionar continuamente los recursos de la nube de forma dinámica y en función de las condiciones del mercado.

Localización

A la hora de decantarse por la utilización de un servicio de cloud computing, hay otros condicionantes que hay que tener en cuenta desde el punto de vista de los derechos de los ciudadanos y del ejercicio de las responsabilidades del cliente de dichos servicios. Es importante identificar qué proveedores de cloud están localizados dentro del Espacio Económico Europeo o en países que de una u otra forma garanticen un nivel adecuado de protección de los datos de carácter personal. Esta localización afecta no sólo a la sede del proveedor de cloud, sino también a la localización de cada uno de los recursos físicos que emplea para implementar el servicio, de forma directa o subcontratada. Y hay que enfatizar que hay que tener en cuenta la localización de todos los recursos pues, por la misma naturaleza del servicio de cloud, los datos pueden estar en cualquier momento en cualquier sitio, pero los derechos y obligaciones relativos a dichos datos han de garantizarse siempre.

Transparencia

En relación al control de la localización de los datos de un usuario, un servicio de cloud puede ser auditable o transparente (en el sentido de la palabra inglesa accountable) cuando el contratista puede reclamar información precisa de dónde, cuándo y quién ha almacenado o procesado sus datos (dentro de los recursos propios del proveedor o de

la cadena de subcontrataciones), y en qué condiciones de seguridad se ha producido. En otro caso, nos encontraremos con un servicio opaco al usuario, en el que éste no tiene opción alguna de obtener información precisa de qué ha ocurrido con sus datos ni herramientas para auditar el servicio que se le está proporcionando y en el que su propia información escapa a su control.

2.2. EL CONTRATO

Volviendo a Rafael García del Poyo, la prestación de servicios de cloud computing se articula a través de un elemento básico y fundamental: la firma de un contrato entre las partes.

Si bien es cierto en nuestro ordenamiento jurídico no se regula expresamente la materia del cloud computing, no es menos cierto que tanto el derecho español como la legislación europea aportan una respuesta general y suficiente a los interrogantes de carácter normativo que se plantean en la operativa diaria de este modelo. De ahí que surja la necesidad de regular este tipo de actividades por vía contractual, con independencia de que ello sea o no una práctica lo suficientemente habitual.

El encuadramiento de este tipo de contratos dentro de una u otra clase vendrá determinado exclusivamente por la normativa que le fuera de aplicación, sin que el dotarle de un nombre concreto tenga mayor relevancia. Normalmente, los contratos utilizados para regular los servicios de cloud computing suelen ser contratos de adhesión en los que los proveedores de servicios en la nube imponen sus propias condiciones (a pesar de que lo más deseable sería que fuesen contratos específicamente negociados entre las partes) con el consiguiente riesgo para la parte contratante ya que no posee capacidad de negociación respecto del reparto de responsabilidad en la seguridad de la conservación de los contenidos, la obligatoriedad del cumplimiento en materia de datos etc…

La información, los datos y las aplicaciones propietarias de un consumidor de cloud computing deben considerarse como bienes activos, ya que poseen un valor económico intangibles, por lo que se hace necesaria la instalación de controles destinados a su protección. Para adquirir servicios en cloud computing, las organizaciones deben depositar estos activos en los recursos físicos de los proveedores de servicio. Por lo tanto, los acuerdos de servicios y contratos deben estar cuidadosamente escritos, contemplando todos los detalles posibles de transferencia, almacenamiento, recuperación y acciones al término del contrato. Además se debe contemplar, las acciones a tomar si ocurre algún evento como el robo, pérdida y corrupción de la información, como también los mecanismos de encriptación y protección de la propiedad intelectual. Se debe tener en cuenta que donde estén alocados los datos es

donde se deberá respetar la legislación y por lo tanto consultar los marcos regulatorios de la jurisdicción donde se realice el almacenamiento y procesamiento de datos.

Las características básicas de seguridad que deben estar contempladas en un contrato de servicio son: a) autenticidad: es la garantía de que el origen y el destino de la información son de usuarios o procesos debidamente autorizados; b) integridad: aseguramiento de que el contenido de los datos y servicios permanecen invariable a menos que sea modificado por un usuario o un proceso debidamente autorizado, es decir que la información fue adulterada o destruida; c) operatividad: los servicios y la datos son accesibles durante el tiempo estipulado que dura el contrato; y d) confidencialidad: la garantía que la información es conocida por los usuarios y procesos debidamente autorizados.

Existen dos tipos de modelos de contratos para la adhesión y adquisición de servicios de cloud computing: modelo unilateral y modelo negociable.

Contrato Unilateral de Adhesión a Servicios

Este modelo de contrato es muy común en aquellos usuarios de Internet, que utilizan servicios estándares y servicios de proveedores gratuitos (cuentas de e-mails, redes sociales, álbum fotográfico, repositorio de almacenamiento, etc.). Generalmente la suscripción a estos servicios gratuitos, permite que el consumidor del servicio pueda acceder a sus datos y a los servicios provistos desde cualquier dispositivo, utilizando mecanismos sencillos de autenticación y protocolos de acceso a Internet.

Los proveedores de estos tipos de servicios ofrecen contratos estáticos y predefinidos para todos los consumidores de servicio. Como contrapartida, estos tipos de contratos protegen los intereses propios de la parte proveedora y pueden restringir severamente el monitoreo en los mecanismo de entrega del servicio. Al mismo tiempo, estos acuerdos pueden ser incompletos y presentar términos ambiguos que hacen difícil la evaluación de los riesgos asociados al optar por un determinado proveedor. Por ejemplo, en los términos de contrato el proveedor puede indicar que escaneará los datos del consumidor almacenados en sus servidores y utilizará la información adquirida para ofrecer publicidades a medida.

Además, en estos tipos de contratos, el proveedor puede restringe su responsabilidad ante las fallas ocasionadas durante los cortes programados de servicios, los eventos de fuerza mayor fuera de su alcance, y las violaciones de seguridad. También reservan el derecho de cambiar el acuerdo de servicio, y modificar los servicios, sin previo aviso y publicando las modificaciones directamente en su página web. Sin embargo, se exige a los consumidores respetar los términos de servicio, abstenerse de almacenar contenidos ilegales en los entornos del proveedor y comprometerse a no realizar ningún tipo de

acciones fraudulentas, cumpliendo con la jurisdicción donde se encuentran los dispositivos físicos del proveedor.

La mayoría de estos servicios se encuentran en nube públicas y las conexiones a las interfaces del servicio se realizan mediante la utilización de navegadores. El nombre del dominio o URL ("Uniform Resource Locator"), que se coloca en el navegador, es traducido mediante los servidores DNS ("Domain Name System") a etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz ("API") de un dispositivo dentro de una red que utilice el protocolo IP ("Internet Protocol").

Sin embargo, es probable que un atacante o usuario malicioso se valga de la dirección IP de los recursos de determinado servicio de cloud computing, para acceder a los datos del consumidor. En los últimos años se han registrado estos tipos de accesos fraudulentos a las cuentas de usuario, robos de identidad, y violaciones de la privacidad, acciones maliciosas que aprovecharon la brecha de seguridad en los servidores de servicios. Algunos ataques pueden hasta generar un gran número de “botnet”, que son algoritmos que enciende un gran número de máquinas "zombie" para enviar paquetes a la web del servidor generando congestión en la comunicación.

Por lo tanto, el navegador y la red de acceso del consumidor de servicio deben estar libre de vulnerabilidades en la seguridad, tráfico malicioso y atacantes. Aunque los servicios sean estándares o gratuitos, es recomendable adoptar siempre el mayor nivel posible de seguridad, y realizar un estudio minucioso de riesgos e impactos. Por ejemplo, se podría acceder a la interfaz del proveedor utilizando algún protocolo de cifrado en los navegadores ("Security Socker Layer"), registrar los accesos y monitorear el tráfico de la red.

Contrato Negociable de Adquisición de Servicios

Los contratos negociables o personalizados de adquisición de servicio son adecuados para clientes de cloud computing que necesitan algún trato especial en sus operaciones o trabajan con datos sensibles. Estos consumidores potenciales de servicios deben consultar con brókeres, consultores tecnológicos y agentes especializados en contratos.

Probablemente, exista la necesidad de implementar cloud privadas para localizar las aplicaciones propietarias del consumidor del servicio y proteger los datos confidenciales, mientras se beneficia de las bondades que ofrece cloud computing como paradigma de negocio. El consumidor de servicio se debe asegurar que existen cláusulas de confidencialidad y políticas de seguridad en estos contratos.

Debido a la especialización de los términos de servicios que se requieren para este tipo de contrato, uno de los riesgos asociados es "provider lock in", técnica que utilizan la mayoría de los proveedores de servicios para que un consumidor se mantenga

dependiente de los servicios que estos proveen. Por lo tanto, se recomienda indicar explícitamente los mecanismos adicionales de transferencia de datos, migración de entornos y despliegue de servicios hacia otros proveedores, en el periodo de extinción del contrato. Del mismo modo, el consumidor de servicio debe estar atento de los cambios que realice el proveedor en sus entornos, ya que podría traer asociado complejidad para cambiar de proveedor.

En esto tipos de contratos se debe identificar todos los aspectos contractuales (funcionales, calidad, jurídicos y legales), al mayor detalle posible. Estos contratos deben evitar interpretaciones ambiguas y limitar las responsabilidades de las partes. También deben incluir cláusulas de acceso de datos, seguridad de información, monitoreo y control de los servicios, medidas de resguardo de datos y recuperación del servicio.

Todas las políticas y procedimientos que se llevarán a cabo para el transporte, almacenamiento y procesamiento de datos, durante el contrato y el periodo de extinción del mismo (destrucción de la información del cliente en los entornos del proveedor).

En se indican una lista de partes del contrato donde el consumidor de servicio debe centrar especial atención al momento de la negociación. Las más relevantes son: nivel de servicio; confidencialidad; disponibilidad; rendimiento; seguridad; plan de continuidad y recuperación ante desastres; facturación de servicios suspensión del servicio; servicios de soporte; terminación o modificación del contrato; privacidad y cumplimiento normativo; notificaciones de brechas de seguridad y procesos legales; uso de datos del cliente; y compensación e indemnización.

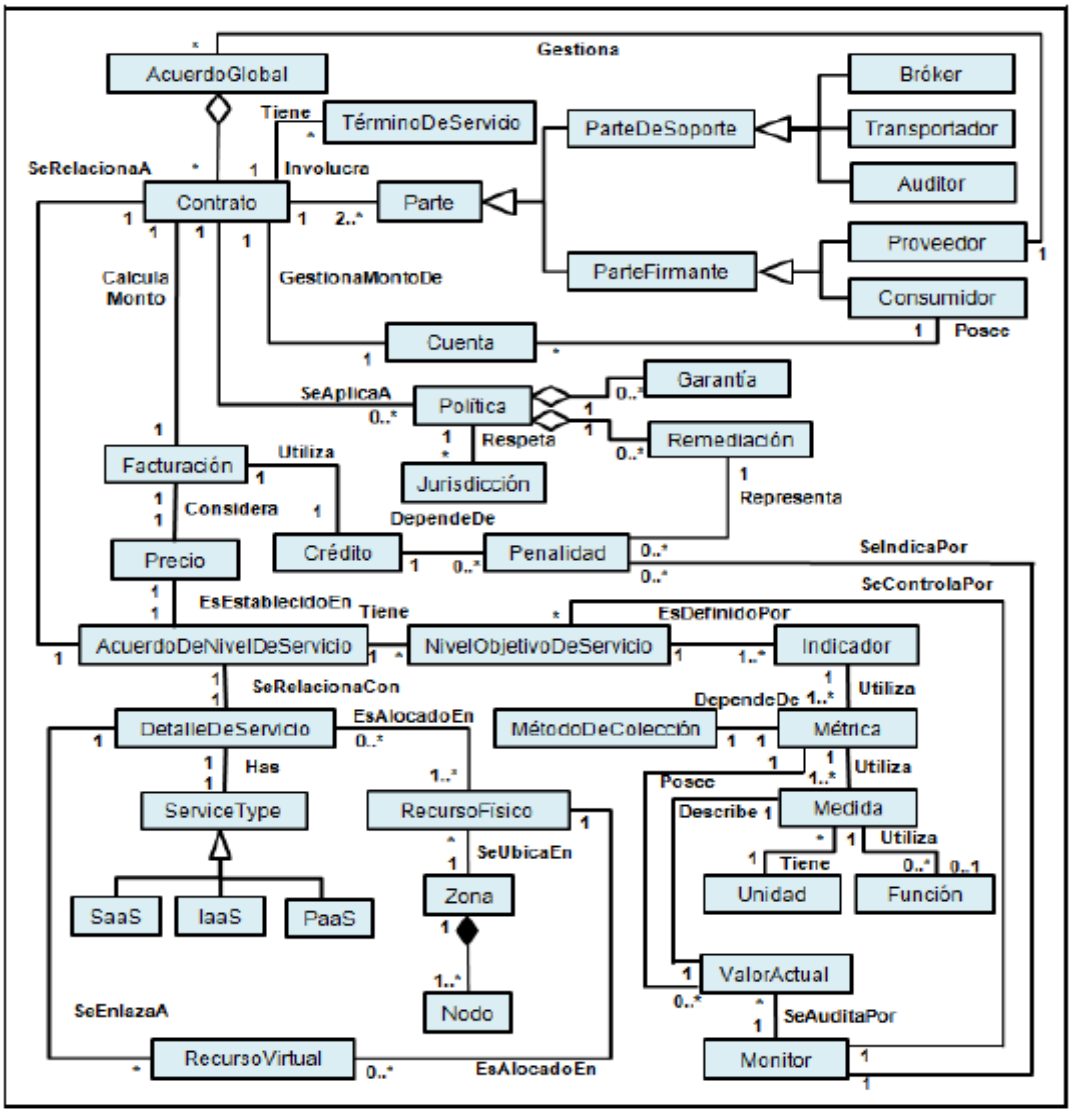

Figura 5.- Modelo conceptual de la contratación de servicios

2.2.1. RECOMENDACIONES LEGALES PARA LA CONTRATACIÓN

En el documento publicado por ENISA[6] se presentan las recomendaciones legales para los clientes reales y potenciales de los servicios de cloud computing. A continuación se resumen estas recomendaciones, que deben ser analizadas en todas las contrataciones de servicios en cloud computing:

• Protección de datos. Control de medidas técnicas de seguridad adecuada y medidas organizativas de protección de datos. El cliente debería analizar cuidadosamente este apartado en el contrato, para determinar si el proveedor ofrece las suficientes garantías

[6] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

de tratamiento lícito y las compensaciones acordes a los daños potenciales de la violación de estas cláusulas.

• Seguridad de los Datos. Respetar las medidas obligatorias a escala nacional y supranacional de seguridad de los datos. En el terreno legal, un lugar físico se refiere a una jurisdicción y las autoridades pueden confiscar los datos si no se cumplen las leyes locales. El proveedor debe estar obligado a notificar a sus clientes cuando existen amenazas o incidentes de seguridad que involucren sus datos, principalmente que afecten la integridad, la confidencialidad y la disponibilidad de la información del cliente.

• Transferencia de información. Se debe prestar atención a la transferencia e intercambio de información, dentro y fuera de la jurisdicción de los consumidores y los proveedores. Garantizar la protección adecuada de los datos, aun cuando el origen/destino de la transferencia sea de diferente jurisdicción.

• Acceso a las autoridades policiales. Analizar las restricciones y requisitos necesarios de las autoridades policiales sobre la jurisdicción en la que los datos pueden almacenarse, procesarse y evaluar cualquier riesgo derivado a esto.

• Confidencialidad y no divulgación. Funciones y obligaciones referidas a esta cuestión. El cliente potencial debería analizar las políticas de confidencialidad y no divulgación de sus datos y saber qué información del cliente circulará en los entornos de cloud computing.

• Propiedad intelectual. Explicitar que se respeta los derechos del cliente de cloud computing, sobre cualquier propiedad intelectual o trabajo original. Esta cláusula deberá ser lo suficientemente detallada y las infracciones deben ser sustanciales, para que el proveedor garantice la protección de la información del cliente.

• Asignación de riesgos y limitación de la responsabilidad. Considerar las obligaciones que plantean los riesgos y los límites de responsabilidad, incluyendo cláusulas de compensación económica y obligaciones de indemnización por la parte que no cumpla con los contratos. Los errores en los servicios pueden tener impacto en la capacidad del cliente y sus obligaciones para con sus propios clientes, por lo que debe analizarse las responsabilidades contractuales por negligencia. También debe evaluarse las condiciones del contrato que atribuyen responsabilidad al cliente por cualquier actividad ilegal realizada utilizando las cuentas autenticadas por el cliente, sin que este las realice.

• Servicios de subcontratación y cambio de control. Capacidad para continuar las obligaciones contractuales en caso de producirse un cambio de control, o bien la posibilidad de rescindir el contrato. El cliente puede exigir que los cambios de control o subcontratación estén sujetas a su autorización previa.

2.2.2. LEY APLICABLE

No se consideran necesarias acciones legislativas o regulatorias específicas de cara a la Computación en la Nube, el marco(s) regulatorio(s) actual(es) proporcionan la libertad y flexibilidad suficiente para el desarrollo de la Nube por lo que regular podría generar efectos adversos. En particular, no deberían introducirse nuevos derechos del consumidor en el ecosistema de la Nube, es suficiente con la aplicación de las normas generales de protección de datos y protección del consumidor a todos los actores.

Tampoco son aspectos menores la determinación de la legislación y jurisdicción aplicables a cualquier contrato. Es más, en ocasiones puede resultar un aspecto clave debido a que no es improbable la aparición de un conflicto entre jurisdicciones por encontrarse la información ubicada físicamente en un territorio distinto de aquel en que se encuentren los contratantes y, como consecuencia, resulte aplicable un régimen jurídico distinto, y competentes unas autoridades distintas, un sistema judicial distinto a los que a priori podamos pensar como "lógicos u obvios".

El lugar físico de ubicación de los servidores en un Estado concreto viene a determinar, como norma general, tanto la legislación como la jurisdicción aplicables. Sin embargo, aunque pueda resultar complicado determinar dónde se ubican los servidores en los que se aloja la información y resulta complejo determinar qué norma puede llegar a aplicarse en cada momento, este hecho no debe servir para excusar el incumplimiento por parte de las empresas que prestan servicios de cloud computing de los principios jurídicos de la protección de datos y la privacidad que protegen a los ciudadanos.

Un potencial problema que no debe pasar inadvertido consiste en que las autoridades de un determinado país pueden llegar a tener competencia para “confiscar” tal información. Una posible solución a este potencial conflicto puede pasar por que el proveedor de servicios de cloud computing se obligue contractualmente a no transferir en ningún caso información a otros países sin el previo consentimiento expreso del cliente.

En este apartado nombraremos la legislación vigente, que se aplica a esta nueva tecnología, tanto dentro del territorio español, como en el resto del mundo. Como ya hemos dicho en los apartados anteriores, es el cliente el responsable del tratamiento de los datos personales que se van a usar en el desarrollo de su actividad empresarial. A pesar de que el contrato que firme indique que la responsabilidad es del proveedor, esta no se desplaza y seguirá siendo del cliente.

Si la empresa trata con datos personales, en un entorno en la nube, es muy importante conocer la ubicación de estos, debido a que las garantías que se exigen para su

protección son distintas dependiendo del país en el que se encuentren alojados. Si el traspaso de datos se realiza entre los países de la Unión Europea, Islandia, Liechtenstein y Noruega, no se considera que se esté realizando una transferencia internacional de datos, pero entre el resto de países, sí, por lo que se deben proporcionar garantías jurídicas adecuadas para el tratamiento y la transferencia de estos datos. Actualmente existen varios países de fuera de la Unión Europea, con un nivel adecuado de protección.

Algunas de las leyes vigentes que afectan a cualquier entorno cloud son las que se indican y explican en los siguientes apartados:

Ley Orgánica de Protección de Datos - LOPD

En el territorio español, se aplica la Ley Orgánica de Protección de Datos[7] y su reglamento de desarrollo (RLOPD[8]) que establecen medidas para la regulación de la seguridad y las técnicas a la hora de tratar con datos de carácter personal.

Esta ley también regula la transferencia internacional de datos, la subcontratación y la atención de los derechos ARCO, que son los de acceso, rectificación, cancelación y oposición. Para poder considerar que se está cumpliendo esta ley, se deben tener en cuenta los siguientes aspectos:

- Si el contrato con el proveedor incluye datos o activos de carácter personal, el proveedor debe garantizar e indicar la ubicación de los mismos, y en caso de que la ubicación o sea reconocida como un emplazamiento de puerto seguro, se deberá solicitar una autorización a la agencia.
- Deben establecerse las condiciones de acceso a los datos, las medidas de seguridad a implementar, las reglas de devolución en caso de cierre del contrato y las subcontrataciones a terceros.
- Se debe garantizar el borrado de los datos tras el fin del contrato.
- Cláusulas de penalización, responsabilidad civil y procedimientos y directrices de seguridad.

Ley de Servicios de la Sociedad de Información y de Comercio Electrónico - LSSI

La Ley de Servicios de la Sociedad de Información y de Comercio Electrónico[9], o LSSI, es una ley de origen español, que surge en 2002. Tiene como objetivo la regulación del régimen jurídico de la sociedad de la información y de la contratación por vía electrónica, como su nombre indica, el comercio electrónico y los servicios de intermediación. Esta ley se aplicará solo en caso de que la actividad constituya una actividad económica o lucrativa para el prestador. De esta manera, se considerará

[7] https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf
[8] https://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf
[9] https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf

prestador tanto a los operadores de red y servicios de comunicaciones, ISP y empresas y ciudadanos con página *web* propia.

Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos – LAECSP
Es la ley[10] que reconoce el derecho que tienen los ciudadanos para poder relacionarse con las administraciones públicas por medios electrónicos. Además de esto, es la que regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa del as entidades y en las relaciones entre entidades, entre otras cosas.

Gracias a esta ley, se facilita el acceso de los ciudadanos a las diferentes plataformas públicas y se aumenta la transparencia administrativa. Asimismo, se mejora la comunicación, el intercambio de datos y de servicios entre entidades administrativas.

Ley de Firma Electrónica
La firma electrónica[11] es un concepto jurídico, es el equivalente electrónico a la firma manuscrita. Algunos ejemplos de firma electrónica son la firma digital, usuario y contraseña, firma con lápiz electrónico, etc.

La ley que se aplica a este concepto tiene como objeto regular la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación. Según esta ley, la firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Cláusulas contractuales tipo de la Unión Europea
Las cláusulas contractuales tipo adoptadas por la Comisión Europea han contemplado dos posibles supuestos: transferencias internacionales de datos entre responsables del tratamiento o entre un responsable y un encargado del tratamiento.

Las cláusulas contractuales tipo entre responsables de tratamiento cubren la transferencia de datos personales por responsables del tratamiento establecidos en la UE a destinatarios establecidos fuera del territorio de la Unión que actúen también como responsables del tratamiento:

—Decisión 2001/497/CE.
—Decisión 2004/915/CE (por la que se modifica la Decisión 2001/497/CE).

[10] https://www.boe.es/buscar/pdf/2007/BOE-A-2007-12352-consolidado.pdf
[11] https://www.boe.es/buscar/pdf/2003/BOE-A-2003-23399-consolidado.pdf

Las cláusulas contractuales tipo entre un responsable y un encargado del tratamiento cubren la transferencia de datos personales por responsables del tratamiento establecidos en la UE a destinatarios establecidos fuera del territorio de la Unión que actúen solamente como encargados del tratamiento, ya que estas transferencias no exigen las mismas garantías, porque el encargado del tratamiento actúa exclusivamente en nombre del responsable:

—Decisión 2002/16/CE (derogada a partir de 15 de mayo de 2010).
—Decisión 2010/87/UE.

Como ya se había indicado anteriormente, en la computación en nube el cliente actúa como responsable del tratamiento, y por lo tanto debe aceptar la responsabilidad de respetar la legislación sobre protección de datos, y es responsable y está sujeto a todas las obligaciones legales que figuran en la Directiva 95/46/CE. El proveedor es la entidad que presta los servicios de computación en nube y por regla general se considera que es el encargado del tratamiento.

Si la relación se produce entre un responsable y un encargado de tratamiento, las cláusulas tipo de conformidad con la Decisión 2010/87/CE de la Comisión son un instrumento que puede ser utilizado como base para que la computación en nube ofrezca garantías adecuadas en el contexto de las transferencias internacionales.

La Decisión 2010/87/UE debe entenderse sin perjuicio de las autorizaciones nacionales que puedan conceder los Estados miembros de conformidad con las disposiciones nacionales de aplicación del artículo 26.2 de la Directiva 95/46/CE. La Decisión tendrá como efecto únicamente exigir a los Estados miembros que no se nieguen a reconocer que las cláusulas contractuales tipo establecidas en ella proporcionan las garantías adecuadas, por lo que no afectará de ninguna manera a otras cláusulas contractuales.

Anteriormente a la Decisión 2010/87/UE ya existía la Decisión 2002/16/CE de la Comisión. La anterior Decisión se adoptó para facilitar la transferencia de datos personales de un responsable del tratamiento de datos establecido en la Unión Europea a un encargado del tratamiento de datos establecido en un tercer país que no ofrezca el nivel adecuado de protección. Sin embargo, la Decisión 2002/16/CE necesitaba una actualización que abordase entre otros temas, algunos problemas que no fueron regulados por dicha Decisión.

La Decisión 2010/87/UE contiene cláusulas contractuales tipo específicas para la subcontratación por un encargado del tratamiento de datos establecido en un tercer país (el importador de datos) de sus servicios de tratamiento a otros encargados (subencargados del tratamiento de datos) establecidos en terceros países. Además

establece las condiciones que ha de cumplir el subtratamiento para garantizar que los datos personales que se están transfiriendo sigan protegidos con independencia de la sucesiva transferencia a un subencargado del tratamiento.

El subtratamiento no podrá exceder de las operaciones acordadas en el contrato entre el exportador de datos y el importador de datos. No se referirá a operaciones de tratamiento o finalidades diferentes para respetar así el principio de limitación de la finalidad establecido en la Directiva 95/46/CE. Además, si el subencargado del tratamiento de datos no cumple sus propias obligaciones de tratamiento de datos, el importador de datos seguirá siendo responsable frente al exportador de datos. La transferencia de datos personales a encargados del tratamiento establecidos fuera de la Unión Europea se hará sin perjuicio de que las actividades de tratamiento se rijan por la legislación de protección de datos aplicable.

Las cláusulas contractuales tipo serán exigibles no solamente por las organizaciones que sean parte en el contrato, sino también por los interesados, en particular cuando estos sufran un daño como consecuencia del incumplimiento del contrato. El interesado tendrá derecho a emprender acciones y, en su caso, percibir una indemnización del exportador de datos que sea el responsable del tratamiento de los datos personales transferidos. Excepcionalmente, bajo ciertas condiciones, también tendrá derecho a emprender una acción y, en su caso, percibir una indemnización del importador de datos o del subencargado del tratamiento de datos. El contrato se regirá por la legislación del Estado miembro de establecimiento del exportador de datos.

La Decisión 2010/87/UE solo se aplica a la subcontratación por un encargado del tratamiento establecido en un tercer país, de sus servicios de tratamiento a un subencargado establecido en un tercer país, por lo que no se aplicará a la situación en la que un encargado del tratamiento establecido en la Unión Europea y que realice el tratamiento de datos personales en nombre de un responsable del tratamiento establecido en la Unión Europea subcontrate sus operaciones de tratamiento a un subencargado del tratamiento establecido en un tercer país.

Aparece entonces el problema de cómo encuadrar jurídicamente las transferencias de datos de un responsable del tratamiento establecido en el EEE hacia un encargado del tratamiento establecido en el EEE y luego a un subencargado del tratamiento establecido fuera del EEE. Mientras no se adopte ningún instrumento específico para este caso, el G-29 encuentra tres posibles soluciones:

a) Un contrato directo entre el responsable del tratamiento y el subencargado del tratamiento establecido fuera del EEE, conforme a la Decisión 2010/87/UE.

b) Un mandato expreso por el cual el responsable da al encargado del tratamiento establecido en el EEE el poder de utilizar las cláusulas tipo de la Decisión 2010/87/UE por su cuenta.

c) Un contrato ad hoc. Tal como se indica en el Considerando 23 de la Decisión 2010/87/UE, «en tales situaciones, los Estados miembros son libres de tener en cuenta el hecho de que los principios y las garantías de las cláusulas contractuales tipo establecidas en la presente Decisión se hayan utilizado para subcontratar a un subencargado establecido en un tercer país con la intención de prestar la adecuada protección de los derechos de aquellos interesados cuyos datos personales se estén transfiriendo para operaciones de subtratamiento».

La Decisión 2010/87/UE se aplica desde el 15 de mayo de 2010, quedando derogada la Decisión 2002/16/CE con efectos a partir de la misma fecha.

2.2.3. RELACIÓN DE PRESTADORES DE SERVICIOS

Generales

- **Dropbox**

Dropbox es un servicio de alojamiento de archivos multiplataforma en la nube, operado por la compañía Dropbox. El servicio permite a los usuarios almacenar y sincronizar archivos en línea y entre ordenadores y compartir archivos y carpetas con otros usuarios y con tabletas y móviles. Existen versiones gratuitas y de pago, cada una de las cuales tiene opciones variadas. La versión móvil está disponible para Android, Windows Phone, Blackberry e iOS (Apple). Actualmente cuenta con más de 500 millones de usuarios registrados. *Recursos on-line:*

https://www.dropbox.com/privacy

- **Amazon**

Amazon ofrece una gama completa de servicios de almacenamiento en la nube para respaldar los requisitos de conformidad de las aplicaciones y el archivado. Se puede seleccionar entre servicios de almacenamiento de objetos, archivos y por bloques, así como opciones de migración de datos a la nube para comenzar a diseñar las bases de su entorno de Tecnologías de la Información en la nube. *Recursos on-line:*

http://aws.amazon.com/es/whitepapers/?nc1=f_cc

- **Google Cloud Storage**

Google Cloud Storage (creado por Google) es el sistema de almacenamiento de objetos unificado para desarrolladores y empresas, que abarca desde el suministro de datos activos hasta el aprendizaje automático y el análisis de datos, pasando por el archivado. *Recursos on-line:*

https://cloud.google.com/security/

Específicas

- **DSpace**

DSpace es uno de los programas de código abierto preferidos por las instituciones académicas para gestionar repositorios de ficheros (textuales, audio, vídeo, etc.), facilitando su depósito, organizándolos en comunidades, asignándoles metadatos y permitiendo su difusión en recolectores o agregadores. El manual que aquí presentamos no es el típico manual genérico sobre su funcionamiento (cómo se consulta, cómo se depositan documentos, cómo se revisan, etc.), sino uno de específico para gestores de la información y la documentación, centrado en aquellas funciones del programa que se encuentran más directamente relacionadas con nuestra profesión (esquema de metadatos, vocabularios controlados, interfaces de consulta, herramientas de difusión, estadísticas, etc.). *Recursos on-line:*

http://wiki.duraspace.org/display/DSDoc18

- **Preservica**

Empresa especializada en tecnología de preservación digital, consultoría e investigación. *Recursos on-line:*

http://preservica.com

Especializadas en Información y Documentación

- **Archivemática**

Archivematica es una solución *opensource* que permite disponer de un sólido sistema de preservación digital, construido de acuerdo a los principios que definen el modelo funcional de la ISO-OAIS. Permite dar respuesta al conjunto de requerimientos inherentes a los procesos de transferencia, ingesta, archivo y difusión de los paquetes de información a la vez que proporciona mecanismos para garantizar su adecuación en materia de preservación.

En Archivematica se defiende la premisa de garantizar la disponibilidad tanto de los archivos originales como de las versiones de preservación que se generan si se opta por el seguimiento de la totalidad del proceso de gestión que propone la plataforma. El mantenimiento de los formatos originales conjuntamente con las versiones de preservación se lleva a cabo en aras de poder asistir en procesos futuros tanto de migración como de emulación de formatos. *Recursos on-line:*

https://www.archivematica.org/es/

- **Ex – Libris: Rosetta**

Rosetta, el sistema de preservación digital de ExLibris, representa un nuevo modo de conservar la herencia cultural y el conocimiento. Esto es así porque hoy en día, la mayor parte del material utilizado para la investigación está creado en formato digital. Además, existe una gran cantidad de material antiguo, no creado en formato digital, que es digitalizado para asegurar una mejor conservación y accesibilidad.

Centradas en la conservación del conocimiento, las bibliotecas y otras instituciones de todo el mundo, son cada vez más conscientes de la necesidad de preservar la información digital. Para ayudar a estas instituciones a alcanzar su misión y asegurar la preservación y accesibilidad de sus fondos en el futuro, Rosetta proporciona un sistema de preservación sumamente escalable, seguro, y fácilmente manejable. *Recursos on-line:*

http://www.exlibrisgroup.com/category/RosettaOverview&prev=search

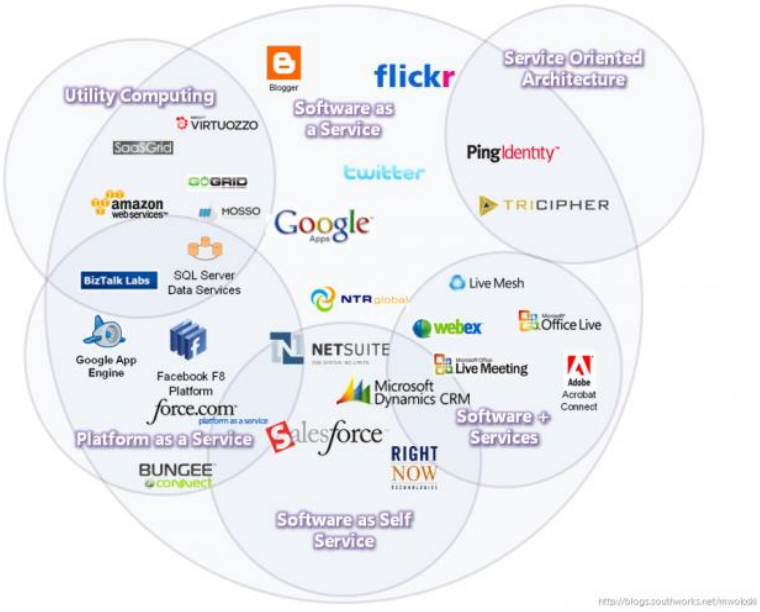

Figura 6.- Proveedores de servicios cloud computing

2.2.4. TABLA COMPARATIVA DE PROVEEDORES

Leyenda:

DB = Dropbox ; AZ = Amazon ; G = Google Cloud Storage ; DS = DSpace ;

P = Preservica ; AR = Archivematica ; R = Rosetta

Verde = Sí ; Rojo = No ; Amarillo = Parcialmente

La interrogación "?" indica una situación en la cual el contrato no es claro o la cuando pregunta no aplica al contrato en particular.

Lista de verificación para contratos de servicios en la nube Público objetivo: Gestores documentales y archivistas[1]							
Preguntas	**DB**	**AZ**	**G**	**DS**	**P**	**AR**	**R**
1. Convenio							
▪ ¿Se encuentra claramente establecida la fecha efectiva de inicio del contrato?							
▪ ¿Existe una explicación sobre las circunstancias por las cuales el servicio podría suspenderse?							
▪ ¿Existe una explicación sobre las circunstancias por las cuales el servicio podría darse por concluido? (ver también sección 8)							
▪ ¿Existe una explicación de notificación o una opción para suscribir un servicio de notificación en el caso de cambios realizados a los términos que regulan el servicio?[2]			?	?	?	?	?
2. Propiedad de la información y uso							
▪ ¿Se retiene la propiedad de los datos que almacena, transmite, y/o produce en el servicio de nube?							
▪ ¿Se reserva el proveedor el derecho para usar los datos para propósitos de operar y mejorar los servicios?							
▪ ¿Se reserva el proveedor el derecho para usar los datos con propósitos de mercadotecnia?							
▪ ¿Se reserva el proveedor el derecho para usar o disponer de sus datos como datos abiertos anónimos (a través de aplicaciones API's)?							

▪ ¿El proveedor restringe el tipo de contenido que usted almacena en cumplimiento a legislación sobre derechos de autor y otros derechos de propiedad intelectual?							
▪ Los términos del proveedor ¿Aplican a metadatos?[3]	?	?	?			?	
▪ ¿Se adquiere la propiedad de los metadatos generados por el sistema de servicio de nube, durante los procedimientos para subir, administrar, recuperar y migrar datos?	?	?	?			?	
▪ ¿Se tienen derechos para acceder a estos metadatos durante la relación contractual (ver también la sección 8)	?	?	?			?	
3. Disponibilidad, recuperación y uso							
▪ ¿Son precisos los indicadores proporcionados respecto de la disponibilidad del servicio?							
▪ ¿Se cumplen las necesidades de la organización en cuanto al grado de disponibilidad de datos?							
▪ ¿Permite el grado de disponibilidad de datos cumplir con las leyes de acceso a la información?[4]							
▪ ¿Permite el grado de disponibilidad de los datos cumplir con el derecho de las personas para acceder a sus datos personales?[5]							
▪ ¿Permite el grado de disponibilidad de los datos cumplir con el derecho de las autoridades para acceder legalmente a la investigación de sus datos para fines de investigación, control o propósitos judiciales?							
▪ ¿Se encuentran claramente establecidos los procedimientos, el tiempo y el costo para restaurar los datos después de una interrupción del servicio?							
4. Almacenamiento de datos y preservación							
4.1. Almacenamiento de datos							
▪ ¿El proveedor genera copia de seguridad[6] de los datos de la organización?							
▪ En el caso de que la organización maneje documentos de archivo externos (ejem. Datos del cliente), ¿El proveedor genera copia de seguridad de sus clientes?							
▪ Los términos del proveedor ¿Aplican a cualquier copia de seguridad generado?[7]	?	?	?	?	?	?	?

▪ En el caso de supresión accidental de datos, ¿tiene el proveedor la responsabilidad de la recuperación de datos?							
4.2. Preservación de datos							
▪ ¿Existen procedimientos definidos para indicar que sus datos serán manejados al paso del tiempo de manera que preserven su usabilidad, fiabilidad, autenticidad e integridad?[8]							
▪ ¿Existen procedimientos para asegurar la integridad del archivo durante la transferencia de los datos dentro y fuera del sistema? (ejem. "checksums")	?	?	?	?	?	?	?
▪ ¿Se proporciona alguna explicación acerca de cómo evolucionará el servicio en el tiempo (es decir actividades de migración y/o emulación?	?	?	?	?	?	?	?
▪ ¿Proporciona el sistema acceso a bitácoras de auditoría[9] respecto de las actividades relacionadas con la evolución del servicio?							
▪ ¿Habrá una notificación del proveedor sobre los cambios realizados a sus datos debido a la evolución del servicio?							
▪ ¿Puede solicitarse una notificación de cambios inminentes al sistema respecto de la evolución del servicio que puedan impactar a sus datos?							
5. Retención y Disposición de datos							
▪ ¿Está informado acerca del procedimiento y condiciones para la destrucción de sus datos?[10]							
▪ ¿Sus datos (y todas las copias, incluyendo respaldos) serán destruidos en cumplimiento con las disposiciones establecidas (disposición documental)?							
▪ Si es así, ¿Serán destruidos inmediata y permanentemente de tal manera que su reconstrucción no sea posible, de acuerdo con la política o lineamiento para una destrucción segura que asegure la confidencialidad de los datos hasta su eliminación completa?	?	?	?	?	?	?	?
▪ ¿Existe información disponible acerca de la naturaleza y contenido de los metadatos asociados que son generados por el sistema de servicio de nube?							
▪ ¿El proveedor destruirá los metadatos asociados al momento de disposición final de sus datos?							

▪ ¿El proveedor enviará y/o proporcionará acceso a las bitácoras de auditoría de la actividad de destrucción?							
▪ ¿El proveedor proporcionará una certificación, reporte o declaración de eliminación (si es requerido por las políticas legales de destrucción)?							
6. Seguridad, confidencialidad y privacidad							
6.1 Seguridad							
▪ ¿Impide el sistema acceso, uso, alteración o destrucción de sus datos?							
▪ ¿Están seguros los datos durante los procedimientos de transferencia dentro y fuera del sistema?							
▪ ¿Proporciona y da acceso el sistema a las bitácoras de auditoria, metadatos, y/o bitácoras de acceso[11] para demostrar las medidas de seguridad?							
▪ ¿Se notificará en el caso de una violación a la seguridad o un mal funcionamiento del Sistema?							
▪ ¿Usa el proveedor servicios de un subcontratista?	?	?	?	?	?	?	?
▪ ¿Ofrece información el proveedor acerca de la identidad del subcontratista y sus tareas?	?	?	?	?	?	?	?
▪ ¿Se encuentran los subcontratistas en el mismo nivel de obligaciones legales de las del proveedor del servicio de nube?	?	?	?	?	?	?	?
▪ ¿Existe un plan de recuperación de desastres disponibles, o el contrato considera qué pasa en el evento de un desastre?							
▪ ¿Ofrece el proveedor cualquier información relacionada con resultados anteriores respecto de los procedimientos de recuperación de desastres?							
6.2 Confidencialidad							
▪ ¿Cuenta el proveedor con una política de confidencialidad respecto de sus empleados, socios y subcontratistas?							
6.3 Privacidad							
▪ ¿Los términos del proveedor incluyen políticas de privacidad, confidencialidad o seguridad para datos sensibles, confidenciales, personales o de otro tipo especial?							

▪ ¿Está claramente establecido cuál información (incluyendo información personal) es coleccionada acerca de la organización, por qué es coleccionada y cómo será usada por el proveedor?							
▪ ¿Comparte el proveedor esta información con otras compañías, organizaciones o individuos sin su consentimiento?							
▪ ¿Establece razones legales el proveedor por las cuales ellos compartirían la información con otras compañías, organizaciones o individuos?[12]							
▪ Si el proveedor comparte esta información con sus afiliados por razones de procesamiento, ¿esto se lleva a cabo en cumplimiento con la política de privacidad, confidencialidad o seguridad existente?							
6.4.Certificación y auditoría							
▪ ¿Está el proveedor acreditado en un programa de certificación de terceros?							
▪ El proveedor ¿Es auditado de forma sistemática, regular e independiente por un tercero para demostrar el cumplimiento con políticas de seguridad, confiabilidad y privacidad?							
▪ ¿Está documentada la certificación o proceso de auditoría?							
▪ ¿Se tiene acceso a la información de los organismos de auditoría o certificadores y la fecha de vencimiento de la certificación?							
7. Ubicación de los datos y flujo de datos transfronterizos							
7.1 Ubicación de los datos							
▪ ¿Se sabe dónde se localizan los datos y sus copias durante su almacenamiento en el servicio de nube?			?			?	?
▪ ¿Se cumple con los requisitos del lugar que pueden ser impuestos a los datos de la organización por ley, especialmente aplicables por la ley de privacidad?			?			?	?
▪ ¿Se tiene la opción de especificar la ubicación, en la cual sus datos y sus copias serán almacenados?							
▪ ¿Se sabe dónde se almacenan los metadatos y si éstos están almacenados en la misma ubicación de los datos?	?	?	?	?	?	?	?
7.2 Flujo transfronterizo de datos							
▪ ¿Se notificará si la ubicación de los datos se mueve fuera de la jurisdicción del cliente?							

▪ ¿Se tienen cuestiones o problemas acerca de los datos almacenados que están sujetos a órdenes de apertura emitidas por autoridades de seguridad nacionales o extranjeras?							
▪ ¿Establece el proveedor claramente la jurisdicción legal en la cual el convenio será cumplido y las disputas potenciales serán resueltas?							
8. Fin del servicio – Terminación del contrato[13]							
▪ En el caso de que el proveedor termine el servicio, ¿Existirá una notificación?							
▪ ¿Existe un procedimiento establecido para contactar al proveedor si se desea terminar el contrato?							
▪ Si el contrato es terminado, ¿Se transferirán los datos a la organización o a otro proveedor de su elección en un formato utilizable e interoperable?							
▪ ¿Está claramente establecido el procedimiento, costo y periodo para devolver/transferir los datos al final del contrato?				?	?		?
▪ Al final del contrato, ¿Se tiene el derecho para acceder a los metadatos generados por el sistema del servicio de nube?							
▪ Al final del contrato y después de completar el reconocimiento de restitución de los datos ¿Serán los datos y los metadatos asociados inmediata y permanentemente destruidos de tal forma que se impida su reconstrucción?	?	?	?	?	?	?	?
▪ ¿Se tiene una opción para confirmar la eliminación de documentos de archive y metadatos por la organización antes de la terminación de los servicios con el proveedor?	?	?	?	?	?	?	?
▪ ¿Se cuenta con la opción para el cliente para terminar el acuerdo de servicio sin penalidad en el caso de que el proveedor del servicio de nube cambie?							

[1] La lista de verificación es principalmente una herramienta para apoyar a las organizaciones a evaluar cuestiones típicas de un formato estándar para convenios de cómputo en la nube, en los cuales la organización tiene que negociar con convenios propuestos por el proveedor. Una segunda aplicación de la lista es proporcionar un panorama de cuestiones sobre gestión documental que son relevantes para los servicios de cómputo en la nube y que deberían estar incluidos en los términos del convenio. Se hace énfasis que cualquier organización en proceso de adquisición de servicios de

cómputo en la nube, donde se el contrato del cliente se está elaborando, deberá revisarse cuidadosamente y contar con el consejo jurídico necesario sobre los términos de uso específicos.

[2] Algunos convenios de servicios de nube, especialmente servicios en la nube pública, incluyen cláusulas que permiten al proveedor cambiar los términos del convenio en cualquier momento y a su discreción. Por tanto, si es posible las organizaciones deberían considerar eliminar este derecho o hacer que el mismo esté sujeto al acuerdo de la organización para hacer cualquier cambio, o asegurar que el proveedor esté obligado a notificar a la organización con bastante anticipación de cualquier cambio.

[3] Los metadatos aseguran que los documentos de archivo puedan ser hallados, recuperados y utilizados. Son críticos para asegurar la autenticidad de los mismos al paso del tiempo. Pueden ser generados por la organización o por el proveedor. Es por lo tanto importante abordar específicamente los metadatos en el contrato a fin de clarificar cuestiones tales como propiedad, acceso, retención y disposición durante el servicio y después de su terminación.

[4] En general, las leyes de acceso a la información permiten el acceso por cualquier persona a la información guardada por los gobiernos en los países.

[5] En algunos países existe una ley de privacidad que protege la privacidad de los individuos con respecto a su información personal acerca de ellos mismos guardada por organismos públicos y/o privados y que les da derecho a acceder a esa información.

[6] Nota de traducción. En español el término “backup” también se traduce como: “respaldo de datos”, “respaldo de información” o “copia de información”.

[7] Específicamente en términos de propiedad, acceso, seguridad, retención y disposición durante el servicio y después de su conclusión.

[8] La usabilidad, fiabilidad, autenticidad e integridad se pueden definir en el contrato (por ejemplo en una sección de definiciones o en el glosario). Se recomienda verificar si la organización y el proveedor tienen un entendimiento común de estos conceptos.

[9] Nota de traducción. En español el término “audit trail” también se traduce como “pista de auditoría”.

[10] Por ejemplo, ¿La operación es automática o requiere autorización de la organización? ¿Ofrece el proveedor la función de “congelamiento” para suspender temporalmente la disposición de un grupo de datos y/o metadatos en contraposición de las instrucciones de la tabla de vigencias? ¿Se hará saber a la organización o podrá especificar el método de disposición?

[11] Nota de traducción. En español el término “bitácoras de acceso” también se utiliza como anglicismo parcial “logs de acceso”.

[12] Por ejemplo, ¿se sabe que su información puede estar accesible por cumplimiento legal y por autoridades se seguridad nacional de jurisdicciones diferentes?

[13] El final del servicio es un momento clave que necesita ser abordado en el contrato a fin de especificar el procedimiento a seguir, las obligaciones y responsabilidades de la organización y del proveedor y el destino de todos los datos antes de terminar la relación contractual.

3. CONCLUSIONES

El hecho de que los entornos cloud proliferen de forma exponencial obliga a los posibles usuarios a comprender mejor estos entornos y sus principales problemáticas. El termino cloud computing es amplio y su definición poco precisa. Por ello, a la hora de la elección de servicios cloud se ha de tener claro el tipo de infraestructura que lo soporta y el tipo de servicio que se ofrece.

Tras el análisis realizado en este informe se obtiene una visión global de esta problemática y se extraen conclusiones comunes a todos los puntos de vista.

La seguridad y la propiedad de los datos es uno de los aspectos clave. Los informes muestran una gran preocupación por la propiedad y el tratamiento de los datos dado que estas infraestructuras pueden gestionar los datos en múltiples países lo que puede generar conflictos en cuanto al marco legal en el que son tratados. También se plantea que estos entornos, al manejar gran cantidad de datos, pueden ser objeto de fugas de información, ya sean intencionadas o fortuitas.

El cumplimiento normativo también es uno de los pilares de la seguridad en entornos cloud. En este caso el problema se presenta debido a la falta de transparencia de estas infraestructuras, por lo que es muy recomendable que el suscriptor del servicio se informe claramente de cómo se gestiona el entorno.

Para la creación de un servicio cloud interviene multitud de software de distintos proveedores. Es decir, son entornos complejos por lo que se ha de poner especial atención a las posibles vulnerabilidades del mismo e implantar procedimientos de parcheado.

Otro de los aspectos considerados importantes es la identidad y el control de acceso. Por lo general, la mayoría de las infraestructuras son compartidas por múltiples empresas o usuarios y la mala definición de los controles de acceso puede provocar accesos no autorizados a datos confidenciales. La definición de una buena política de identidad y control de acceso basada en políticas de mínimo privilegio es esencial en entornos cloud.

Por último, existe un denominador común a todos estos aspectos mencionados. Se trata de los contratos de acuerdo de servicio. Todas las recomendaciones en cuanto a este asunto indican que éstos deben de ser revisados y creados específicamente, detallando los controles, las normativas, las medidas de protección, los plazos de recuperación del servicio, etc. Y como hemos visto en la comparativa aún falta camino que recorrer.

4. BIBLIOGRAFÍA

- 1. **Mell, P., Grance, T**.: The NIST Definition of Cloud Computing. National Institute of Standards and Technology. *NIST Special Publication 800-145* (2011)
- 2. **Guasch Portas, V., Soler Fuensanta, J.R**.: Cloud Computing, cláusulas contractuales y reglas corporativas vinculantes. *Revista de Derecho UNED*, num. 14, 2014
- 3. **García del Poyo, R**.: Cloud Computing: Aspectos jurídicos claves para la Contratación de estos Servicios. *Revista Española de Relaciones Internacionales* (2012) 48-91.
- 4. **Pérez San-José, P., Gutiérrez Borge, C., Álvarez Alonso, E., De la Fuente Rodríguez, S., García Pérez, L.**: Guía para empresas: seguridad y privacidad del cloud computing. Instituto Nacional de Tecnologías de la Comunicación, INTECO (2011)
- 5. **Zalazar, A. S., Gonnet, S., Leone, H.**: Un Modelo para Contratos de Cloud Computing. 42JAIIO – 14 Simposio Argentino de Ingeniería de Software (ASSE 2013) Argentina (2013) 303-317
- 6. **Zalazar, A. S., Gonnet, S., Leone, H**.: Aspectos Contractuales de Cloud Computing INGAR (UTN-CONICET) Argentina (2013)
- 7. **InterPARES/ICA**. Los Caminos de los Documentos de Archivo Digitales: Tópicos en Preservación Digital. Módulo 8: Introducción al Cómputo en la Nube
- 8. **INTECO-CERT.** Riesgos y amenazas en Cloud Computing. (marzo 2011) https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf [última visualización el 15 de junio de 2017]
- 9. **Centro de Estudios de telecomunicaciones de América Latina**. Computación en la Nube Desafío y oportunidad en la sociedad conectada.

5. ÍNDICE DE FIGURAS

6. GLOSARIO

CC: Cloud Computing

NIST: National Institute of Standards and Technology

IaaS: Infrastructure as a Service

SaaS: Software as a Service

Paas: Platform as a Service

TIC: Tecnología de la Información y Comunicación

7. Anexo I. Modelo de contrato SaaS Zikzakmedia

Contrato de Servicio SaaS ofrecidos por Zikzakmedia

Los servicios detallados en el anexo A son prestados por ZIKZAKMEDIA S.L., con C.I.F. B64425879 y domicilio en C / Dr. Fleming, 28 bajos de Vilafranca del Penedès, Catalunya.

El contratante del servicio o servicios, en adelante "CLIENTE", acepta las condiciones detalladas en el presente contrato. El uso de este/os servicio/s conlleva la aceptación plena de las condiciones del presente contrato.

CONDICIONES GENERALES

1. Política de protección de datos

ZIKZAKMEDIA, siguiendo la normativa vigente de protección de Datos de Carácter Personal (Ley reguladora de la privacidad de datos, Ley 15/1999 de 13 de diciembre), informa:

1.1. Que los datos recogidos a través de los formularios situados en www.zikzakmedia.com o de www.zzsaas.com se incluyen en ficheros automatizados de uso interno, cuyo responsable y titular es ZIKZAKMEDIA, con el fin de poder prestar los servicios contratados por el CLIENTE, o en caso contrario, poder facilitarle cualquier información que éste requiera de una forma personalizada.

1.2. ZIKZAKMEDIA garantiza la confidencialidad de todos los datos recogidos desde www.zikzakmedia.com o www.zzsaas.com, adoptando las medidas técnicas que sean necesarias para garantizar la seguridad e integridad de las mismas.

1.3. ZIKZAKMEDIA se compromete a no vender, ceder o transferir los datos recogidos bajo ningún concepto. No obstante ZIKZAKMEDIA revelará a las autoridades públicas competentes los Datos Personales o cualquier otra información que sea requerida de conformidad a las disposiciones legales y reglamentarias aplicables en cada caso.

1.4. ZIKZAKMEDIA asegura que protegerá la confidencialidad del correo electrónico intercambiando con el CLIENTE.

1.5. El CLIENTE tiene reconocidos sus derechos, y podrán ejercitar sus derechos de acceso, cancelación, rectificación y oposición en cualquier momento, solicitándolo por correo postal a ZIKZAKMEDIA o por correo electrónico en la dirección soporte[arroba]zikzakmedia.com

1.6. El CLIENTE garantiza y responde, en cualquier caso, de la veracidad, exactitud, vigencia y autenticidad de los Datos Personales facilitados, y se compromete a mantenerlas debidamente actualizadas.

1.7. El CLIENTE autoriza de forma inequívoca a ZIKZAKMEDIA el tratamiento informático de los datos facilitados bajo las condiciones descritas en este documento y exclusivamente para poder facilitar y facturar de forma correcta los servicios contratados.

2. Soporte técnico o consultas

2.1. ZIKZAKMEDIA ofrecerá soporte técnico o funcional según el servicio contratado a través del correo electrónico de atención al CLIENTE soporte[arroba]zikzakmedia.com durante toda la vigencia del contrato.

2.2. El tiempo de respuesta es de menos de 4 horas en casos de incidencias y soporte técnico o funcional. Si se ha contratado el servicio de resolución de errores o bugs, el tiempo de respuesta es de 1 día en caso de errores graves (imposibilidad de trabajar), 5 días en caso de errores medios (dificultad de trabajar) y 15 días en caso de errores menores (no afecta al trabajo diario). En el cómputo de tiempo no se considerarán los sábados, domingos y festivos oficiales de Catalunya.

2.3. El servicio se prestará dentro del horario laboral de ZIKZAKMEDIA: de lunes a viernes de 9:00h. a 19:00h. excluyendo los festivos oficiales de Catalunya.

2.4. Los servicios de mantenimiento, actualizaciones y resolución de errores en los servidores del CLIENTE se realizarán de forma remota desde las oficinas de ZIKZAKMEDIA. Estos servicios no incluyen desplazamientos a las instalaciones del CLIENTE. El CLIENTE ha de proporcionar los datos de conexión remotos (nombre o IP del servidor, puertos, usuarios, contraseñas) y tener el servidor y router encendidos y bien configurados.

3. Precios, facturación y pagos del servicio prestado

3.1. ZIKZAKMEDIA informará al CLIENTE el precio inicial del servicio o servicios contratados.

3.2. El pago de los servicios prestados son a cuenta y de carácter mensual. Se emitirá una factura el día de alta cada mes con un importe del mes próximo y el pago podrá efectuarse por transferencia bancaria, TPV virtual o recibo domiciliado. Al inicio del servicio se emitirá una factura del mes en curso. Cuando el CLIENTE se dé de baja del servicio se emitirá una factura de abono para abonar los días naturales desde la baja del servicio hasta el final del mes en curso.

3.3. El precio del servicio podrá ser modificado por parte de ZIKZAKMEDIA avisando con 30 días de antelación a través de los medios que considere necesarios, incluido Internet. En el caso de que haya una modificación de tarifas por parte de ZIKZAKMEDIA, un vez notificado este cambio, si el CLIENTE no rechaza la variación solicitando la baja del servicio, se entenderá que acepta

las nuevas tarifas. En todo caso, ZIKZAKMEDIA se compromete a hacer una variación del precio del servicio cada año, como mucho.

3.4. En caso de devolución, retraso o impago de recibo de 5 días posterior a la fecha de alta de cada mes, ZIKZAKMEDIA suspenderá el servicio, avisando previamente al CLIENTE, hasta la confirmación del pago debido. En caso de devolución del recibo se cargará al CLIENTE seis (6) € + IVA adicionales por coste de comisiones bancarias.

3.5. Después de reiterados retrasos o impagos, ZIKZAKMEDIA se reserva el derecho a solicitar al CLIENTE una fianza, con importe igual a la cuota que esté pagando.

3.6. Si diera el caso de tener que cancelar un servicio por impago, ZIKZAKMEDIA no será responsable de los perjuicios que eso le pueda ocasionar al CLIENTE, o a los clientes del CLIENTE.

4. Baja del servicio prestado

4.1. El contrato mínimo es de seis meses, excepto acuerdo en caso contrario. Este contrato se prorroga automáticamente pasado este tiempo.

4.2. El CLIENTE podrá anularlo solicitando con 5 días de antelación al inicio del nuevo período de abono mediante correo electrónico o por escrito. Una vez pasada esta fecha, ZIKZAKMEDIA podrá reclamar el pago del período completo.

4.3. La baja se efectuará en un día laborable (de lunes a viernes) y se activará entre las 8:00 h. y las 9:00 h. El servicio completo de baja sólo lo activará un miembro de ZIKZAKMEDIA.

4.4. En caso de interceptar cualquier conducta o actividad ilegal, ZIKZAKMEDIA se reserva el derecho a denegar o cesar los servicios contratados sin previo aviso.

4.5. En el hipotético caso que ZIKZAKMEDIA cancelara el servicio prestado sin que el CLIENTE haya infringido alguna de las condiciones aquí descritas, le sería devuelto el importe correspondiente a la parte proporcional del período no consumido.

4.6. En cualquier caso ZIKZAKMEDIA no será responsable de las consecuencias que puedan derivarse de la interrupción del servicio.

Garantías del servicio prestado

5.1. ZIKZAKMEDIA se responsabilizará del correcto funcionamiento del hardware y software que esté a su cargo según el servicio contratado, asumiendo los costes de las incidencias producidas en el servicio que sean responsabilidad de ZIKZAKMEDIA. En este caso ZIKZAKMEDIA compensará al CLIENTE el coste equivalente al tiempo sin servicio. En ningún otro caso puede haber ningún otro tipo de compensaciones económicas por estos problemas.

5.2. El CLIENTE deberá comunicar la avería o incidencia por correo electrónico a la dirección soporte[arroba]zikzakmedia.com y después reclamar la compensación. El período a compensar se contará desde el momento de la recepción del aviso. La compensación será en tiempo adicional de servicio sin coste.

5.3. En caso de que las incidencias puedan derivar de un mal uso por parte del CLIENTE se reserva el derecho a facturar al CLIENTE estos gastos.

5.4. ZIKZAKMEDIA no se hace responsable de la adecuación de los servicios que ofrece a las necesidades del CLIENTE. Su inadecuación no podrá ser causa de resolución del contrato ni de impago de las cuotas.

6. Responsabilidades

6.1. ZIKZAKMEDIA no será responsable de pérdidas de beneficios y daños como consecuencia del uso, funcionamiento o rendimiento del software, siendo responsable únicamente de los actos realizados que sean necesarios para el cumplimiento de sus obligaciones de acuerdo con este contrato.

6.2. ZIKZAKMEDIA no será responsable del incumplimiento de sus obligaciones definidas en el presente contrato, si la realización de estas obligaciones ha sido impedida, interferida o retrasada razonablemente por circunstancias que escapen al control de ZIKZAKMEDIA. Estos eventos serán, por ejemplo y entre otros, los actos de fuerza mayor, actos fortuitos, huelgas, motines, cierres patronales, actos de guerra, epidemias, actos o reglamentaciones oficiales, incendios, fallos de comunicaciones, fallos de suministro eléctrico, rayos, terremotos, inundaciones, catástrofes y otros eventos.

Modificaciones

7.1. Las condiciones de este contrato podrán ser modificadas por parte de ZIKZAKMEDIA, notificándolo por los medios que considere necesarios, con 30 días de antelación. Si durante este periodo de tiempo no se rechaza expresamente la variación de las condiciones por parte del CLIENTE se entenderá que aceptan las modificaciones de las condiciones del contrato.

Fuero

8.1. Ambas partes (CLIENTE y ZIKZAKMEDIA) se someten a los Juzgados y Tribunales de Vilafranca del Penedès, Catalunya para la resolución de cualquier controversia que con motivo de este contrato pudiera surgir, renunciando a su fuero si éste fuese otro.

CONDICIONES ESPECÍFICAS DE LOS SERVICIOS SaaS EN SERVIDORES DE ZIKZAKMEDIA

Política de protección de datos

ZIKZAKMEDIA, siguiendo la normativa vigente de protección de Datos de Carácter Personal (Ley reguladora de la privacidad de datos, Ley 15/1999 de 13 de diciembre), informa:

9.1. El CLIENTE se compromete a cumplir las obligaciones derivadas de las Leyes de Protección de Datos o cualquier otra que sean aplicables a cada momento. El CLIENTE es responsable de comunicar y hacer cumplir la ley vigente de protección de datos de carácter personal si en su aplicación WEB o ERP se recogieran datos personales. Si se cumpliera este hecho, el CLIENTE, en su condición de responsable de su archivo, indemnizará a ZIKZAKMEDIA por cualquier pérdida, daños, perjuicios, intereses, sanciones o indemnizaciones que ZIKZAKMEDIA se vea obligado a satisfacer, pueda sufrir, o en las que pueda incurrir como consecuencia de un mal uso, o incumplimiento por parte del CLIENTE de las obligaciones de la presente clausula y/o del incumplimiento por su parte de las obligaciones vigentes en cada momento en materia de protección de datos.

9.2. El CLIENTE es responsable de comunicar y hacer cumplir la ley vigente de protección de datos de carácter personal si en su aplicación WEB o ERP se recogieran datos personales de los clientes del CLIENTE, así como de advertir a sus clientes de la ubicación de los servidores de ZIKZAKMEDIA.

9.3. En el caso de alojamiento WEB, el CLIENTE deberá publicar en su sitio web un aviso legal con sus datos legales: NIF, dirección, ubicación de los servidores, licencia de los contenidos web... y, en caso de recoger datos personales de los clientes del CLIENTE, un aviso sobre el cumplimiento de la ley vigente de protección de datos. En caso contrario se le publicará unos avisos por defecto.

9.4. En el caso de registros de dominio, el CLIENTE autoriza a ZIKZAKMEDIA a facilitar sus siguientes datos (nombre, apellidos, dirección completa y teléfono) ante el organismo de dominios (ICANN) con la finalidad que los nombres de dominio queden registrados a nombre del CLIENTE. Esta autorización es necesaria para que los dominios estén registrados a nombre del propietario legal que los solicita.

Contenidos del servidor

10.1. ZIKZAKMEDIA no será responsable de los contenidos alojados en el/los servidor/es contratado/s en ningún caso, ya sean propiedad del CLIENTE o de los clientes del CLIENTE.

10.2. Queda totalmente prohibido utilizar los servidores para fines ilegales. ZIKZAKMEDIA se reserva el derecho de desconectar un servidor si éste se estuviera utilizando para fines ilegales, avisando a las autoridades pertinentes. En ningún caso se podrá:

- Alojar contenido ilegal, ya sea pornografía infantil o contenido con derechos reservados de copia (música, vídeos, software, etc. con licencia que limite la copia).

- Utilizar el servidor para realizar SPAM (envío masivo e indiscriminado de e-mails).

10.1. Se notifica al CLIENTE que el servidor donde se aloja la información y las aplicaciones WEB y ERP se encuentra en España, dentro del territorio de la Unión Europea, aceptando el CLIENTE de forma inequívoca este hecho.

Uso del servidor

11.1. El contrato y el soporte correspondiente quedará anulado si:

- Si el CLIENTE instala cualquier tipo de software en el servidor sin el consentimiento de ZIKZAKMEDIA.

-Se accede vía Telnet o SSH para hacer modificaciones en el servidor.

- Uso malintencionado o erróneo del servicio continuo en el tiempo.

11.1. Todos los servidores funcionan sobre sistemas GNU/Linux y sólo se instalará software con licencia libre GPL o similar para evitar problemas de licencias.

11.2. El CLIENTE puede solicitar la instalación de software en el servidor, siempre bajo presupuesto aparte y siempre que el software instalado no afecte al rendimiento del servidor.

11.3. El acceso al servidor por parte del CLIENTE será únicamente mediante WEB (HTTP) o, en caso de alojamiento ERP, mediante cliente de Tryton o OpenERP asignado.

11.4. No hay límite en el uso del espacio de disco duro del servidor. Sin embargo, si la aplicación web o ERP ha de ofrecer un mayor número de registros y conexiones simultáneas, se acordará con ZIKZAKMEDIA sobre la mejora de hardware y red del servidor, presentando presupuesto previamente.

Direcciones IP

12.1. Según el tipo de servicio contratado le serán asignadas un número de direcciones IP para poder configurar sus DNS o sus clientes Tryton o OpenERP.

12.2. El CLIENTE reconoce que las IP no son de su propiedad, y en el momento de dar de baja su servicio será el responsable de liberarlas de sus DNS antes de los cinco (5) primeros días de la baja efectiva del servidor.

12.3. Si el CLIENTE se niega a realizar la liberación de las direcciones IP prestadas, se le cargará el importe de 200 € + IVA en concepto del tiempo requerido por ZIKZAKMEDIA para efectuar estos trabajos.

Baja del servicio prestado

13.1. El día de la baja se ofrecerá al cliente el código fuente de las aplicaciones (licencia GPL) y los datos (SQL) para ser descargado por el cliente (archivo comprimido en formato tgz o similar). Si el cliente quiere una copia en soporte digital (CD, DVD...) deberá abonar la gestión y envío según las tarifas vigentes.

13.2. Al cabo de 5 días laborables de la baja, el código fuente de las aplicaciones y los datos, serán borrados completamente de los servidores.

Garantías del servicio prestado

14.1. El CLIENTE deberá poner sus propias condiciones de uso del servicio a sus clientes, si los hubiere, así mismo será el responsable de dar soporte técnico a sus clientes.

14.2. ZIKZAKMEDIA efectúa copias de seguridad de todos sus servidores con las que se pueda restablecer el servicio en caso de incidencia técnica grave. Así mismo, ZIKZAKMEDIA no se responsabiliza de las posibles pérdidas de datos o errores en el servicio prestado.

14.3. El CLIENTE deberá velar por el secreto de las palabras (contraseñas) de acceso al servicio, modificándolas si tiene la menor sospecha de que terceras personas las conocen.

NOTAS

Los alojamientos WEB o ERP incluyen el mantenimiento y actualizaciones del servidor.

Se entiende por alojamiento WEB el funcionamiento de aplicaciones tipo gestores de contenidos web (CMS), wikis, tiendas virtuales, aulas virtuales... en un servidor compartido de ZIKZAKMEDIA. No se considerará alojamiento WEB el correo electrónico, el flujo o streaming de audio y/o vídeo ni servidores de ficheros.

Se entiende por alojamiento ERP el funcionamiento de una aplicación de gestión de una empresa u organización y los módulos correspondientes en un servidor compartido de ZIKZAKMEDIA. No se considerará alojamiento ERP las aplicaciones WEB (excepto el cliente-servidor WEB de Tryton o OpenERP), correo electrónico, el flujo o streaming de audio y/o vídeo ni servidores de ficheros.