Cloud computing

Una guía de aproximación para el empresario

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

Cloud computing

Una guía de aproximación para el empresario

INCIBE_PTE_AproxEmpresario_009_CloudComputing-2017-v1

Índice

1 Introducción

La evolución de la tecnología, y en particular la irrupción de Internet, está provocando cambios en los hábitos de consumo, en los modelos de negocio y en los mercados. Estos cambios empujan a las empresas hacia una **transformación digital** para adaptarse y aprovechar las oportunidades de negocio que ofrecen la movilidad, la analítica, la nube o las redes sociales.

La nube, en algunos casos considerada la quinta revolución del mundo TIC [1], permite a las pymes y autónomos adoptar las últimas tecnologías a un coste reducido, alcanzando así **mayor productividad con el mínimo esfuerzo**. Al utilizar servicios en la nube no sólo ahorran costes sino que también pueden crecer de forma eficiente ya que los servicios en la nube aportan **agilidad** al negocio nivelando volumen con capacidad. Emprendedores y *start-ups* han sido las pioneras en utilizar servicios en la nube para extender su negocio llegando sin grandes inversiones a tener un gran número de usuarios, en muchos casos a nivel internacional.

Los proveedores de servicios en la nube (en inglés *cloud*) prometen a los empresarios reducir las inversiones destinadas a hardware y software sustituyéndolas por gastos en servicios en un atractivo esquema de «pago por uso», a la vez que ofrecen otras ventajas como **acceso** a los servicios contratados **desde cualquier lugar**, **flexibilidad**, **escalabilidad**, etc.

Pero, aunque sigue creciendo la oferta de servicios en la nube para pymes y autónomos, todavía existe un gran desconocimiento sobre este concepto, y muchas dudas sobre si es seguro utilizarla. De hecho muchos usuarios disfrutan los servicios en la nube sin ni siquiera ser conscientes de ello.

En esta guía se explicarán:

- los conceptos básicos para comprender este tipo de servicios
- sus características
- sus ventajas e inconvenientes
- las opciones de contratación y los tipos de servicios en la nube
- los riesgos y amenazas
- los aspectos legales a tener en cuenta
- los pasos que tenemos que dar
- las medidas que podemos tomar para contratar servicios en la nube con seguridad.

La oferta de los proveedores en la nube abarca todo tipo de servicios: almacenamiento, *backup*, aplicaciones de oficina, servidores de correo, alojamiento web, gestión de contactos, etc.

Con esta variedad de servicios de **pago por uso**, las pymes no tecnológicas empiezan a valorar las ventajas que supone para sus negocios el poder evitar importantes inversiones en hardware, software y personal técnico propio y el tener acceso a la expansión de sus negocios.

1 Introducción

"Los proveedores de servicios en la nube permiten sustituir las inversiones en hardware y software a cambio de servicios de pago por uso."

Por si fuera poco, estos servicios en la nube aportan interesantes oportunidades para el trabajo **colaborativo**. Además, ofrecen **mejoras en la seguridad** si los comparamos con la opción tradicional aunque no están exentos de riesgos.

2 ¿Qué es *cloud computing*?

El *cloud computing*, o computación en la nube, es un modelo de computación que permite al proveedor tecnológico ofrecer servicios informáticos a través de internet. De esta forma los recursos, es decir, el hardware, el software y los datos se pueden ofrecer a los clientes **bajo demanda**.

Esta prestación de servicios permite al cliente el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor. En resumen, permite acceder a los servicios y recursos contratados proporcionando flexibilidad de dimensionamiento y acceso.

El cliente, bien sea una empresa o un particular, se abstrae de la infraestructura tecnológica necesaria para poder utilizar una determinada aplicación, ya que simplemente se requiere un navegador web con conexión a la red para tener acceso a los procesos o a los datos. El cliente puede acceder a los servicios contratados desde cualquier lugar y todos los días del año, adaptándolos a sus necesidades de forma dinámica. Todo ello sin realizar inversiones en equipos y software, y sin los gastos derivados de su mantenimiento.

La evolución e implantación de este modelo ha sido propiciada por la convergencia de los siguientes avances tecnológicos:

- El crecimiento de la **capacidad de procesamiento y de cálculo** de los sistemas desde la aparición de la informática hasta nuestros días ha hecho posible tener ordenadores conectados entre sí en redes de alta velocidad (también conocido como *cluster*) que multiplican exponencialmente la capacidad de procesamiento. De esta forma los proveedores *cloud* pueden «alquilar» esta capacidad (número de procesadores y memoria) y el cliente pagar por su uso.

- La eficiencia de los sistemas de **almacenamiento** con ratios crecientes de **capacidad** y velocidad de **transferencia,** hacen posible igualmente su abastecimiento desde centros de datos en la nube.

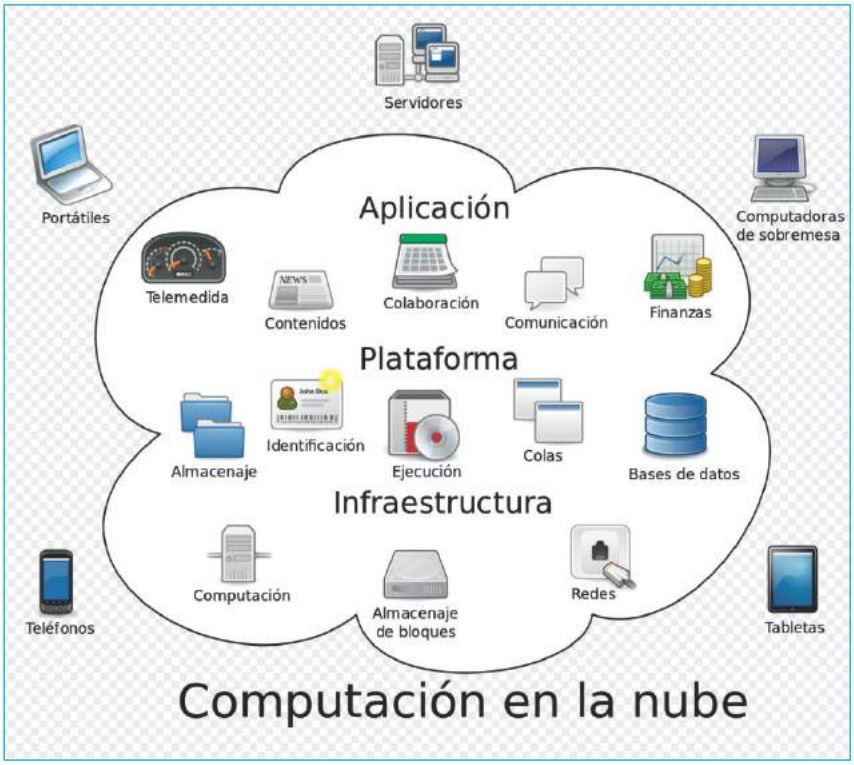
- La **extensión y abaratamiento del acceso a Internet** amplifica la **conectividad** que hace posible no sólo aplicaciones cómo el comercio electrónico o las redes sociales, sino también el acceso ágil desde cualquier lugar a los centros de datos y de proceso.

2 ¿Qué es *cloud computing*?

La proliferación de **dispositivos móviles** conectados a la red hace posible que empresarios y trabajadores estemos conectados en cualquier situación, de viaje, en clientes o fuera de la oficina. Muchas aplicaciones *cloud* aprovechan la **movilidad** que permiten los dispositivos para ofrecer servicios en cualquier lugar o incluso adaptados al lugar dónde se encuentre el usuario (gestión de flotas, partes de obra,...)

La flexibilidad que ofrece la virtualización1 de sistemas operativos, servidores y redes que permite a los proveedores cloud aprovisionar los recursos de acuerdo con las demandas de sus clientes.

"El cloud computing permite al proveedor tecnológico ofrecer servicios informáticos bajo demanda a través de internet."



Para el proveedor, la esencia de este modelo de computación reside en ofrecer recursos estándar a los clientes a través internet. Esto quiere decir que despliega, para un servicio, las mismas versiones de hardware y software para todos los clientes que podrán configurarlos para adaptarlos a sus necesidades. Con esto el proveedor consigue, y ofrece a sus clientes, **ventajas** en cuanto a **fiabilidad, flexibilidad y escalabilidad, y mejoras en el rendimiento** frente a configuraciones *ad-hoc*. Esto permite también que los distintos servicios sean **interoperables**, es decir, que se puedan integrar con mayor facilidad y rapidez con otras aplicaciones empresariales.

Algunos ejemplos de servicios que se pueden contratar en la nube son: puestos de trabajo, bases de datos, servidores de correo electrónico, almacenamiento, servidores web, servidores de aplicaciones, entornos de desarrollo, redes, etc. Además, las empresas pueden contratar a los proveedores *cloud* el despliegue conjunto de varias de las aplicaciones de la empresa, como servicios de correo y web, CRM y ERP.

1 La virtualización es un mecanismo software que permite utilizar un equipo para «hospedar» otra u otras máquinas diferentes comportándose como ellas.

2 ¿Qué es *cloud computing*?

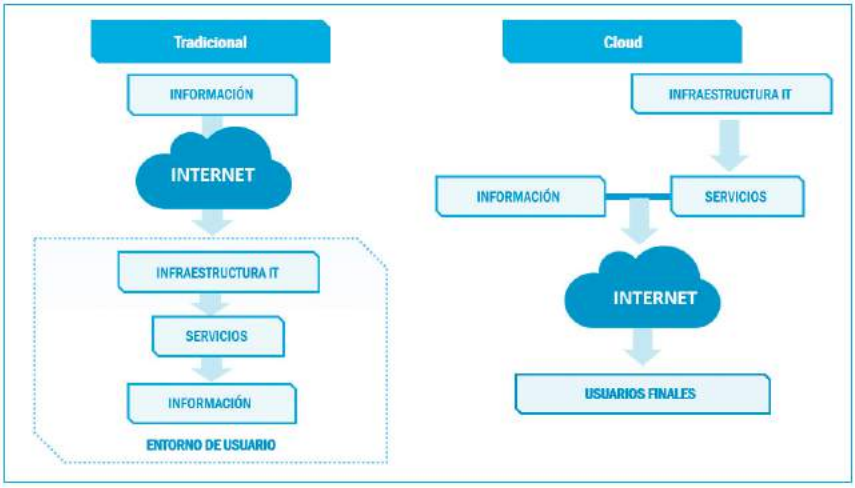
Para el empresario, si lo comparamos con los modelos tradicionales como son el alquiler de equipos o los centros de proceso de datos internos, el *cloud computing* pone a su alcance sistemas y aplicaciones informáticas sin necesidad de adquirirlos, sólo **contratándolos como un servicio**. En este esquema se sustituye la compra o alquiler de máquinas y software exclusivo por un gasto, por un «suministro», como el agua o la energía eléctrica, al pagar por el uso de los sistemas y aplicaciones que necesitemos.

Este nuevo modelo evita al cliente, en particular a la pyme o al autónomo, la preocupación de comprar y mantener la infraestructura y los elementos técnicos de la misma ya que son ofrecidos por el proveedor como un servicio.

En este escenario de pago por uso, el empresario no tendrá que preocuparse de hacer nuevas inversiones o quedarse con sistemas y aplicaciones obsoletas o sobredimensionadas si cambian sus necesidades de recursos informáticos, por ejemplo si tiene que aumentar o reducir su infraestructura por que cambie su plantilla o varíe la magnitud de su negocio o si cesa el soporte de una aplicación. Tampoco tendrá que comprar nuevos sistemas y aplicaciones si abre una nueva oficina o si decide migrar a otra aplicación más moderna. En estos casos solo tendría que modificar su suscripción al servicio para adecuarlo al nuevo contexto.

"El cloud computing pone al alcance del consumidor sistemas y aplicaciones sin necesidad de adquirirlos."

La siguiente imagen muestra gráficamente las diferencias entre el modelo tradicional y la computación en la nube.



En cualquier caso, como veremos más adelante, de cara a la seguridad va a ser clave el establecimiento de **acuerdos de nivel de servicio** entre el proveedor y el cliente (o SLA del inglés *Service Level Agreements*). En ellos se definen los compromisos de ambas partes. Estos acuerdos deben contener clausulas en las que se defina la responsabilidad del proveedor en algunos aspectos relacionados con la seguridad: el mantenimiento, las actualizaciones, las incidencias, la disponibilidad y la recuperación de los servicios contratados por el cliente.

2.1 Características de los servicios en la nube

Cuando contratamos servicios en la nube seleccionamos una serie de **recursos computacionales** como servidores, sistemas de almacenamiento, aplicaciones o equipos de comunicaciones, y los dimensionamos según nuestras necesidades. Así elegimos por ejemplo: el número de procesadores, la memoria, la capacidad del almacenamiento o el número de usuarios. El precio variará según nuestra selección, pero podremos cambiarla más adelante, si cambian nuestras necesidades.

"La escalabilidad, el pago por uso y el acceso desde la red son algunas de las características que definen el modelo de cloud computing."

Estas propiedades el **pago por uso** y la **escalabilidad** son dos características que definen este nuevo modelo de computación. La siguiente tabla describe e ilustra con un ejemplo estas y otras características de los servicios en la nube.

Característica	Descripción	Ejemplo
Pago por uso	El precio del servicio varía en función de las necesidades del cliente de manera flexible.	Si necesito más capacidad de proceso por un pico de trabajo solicitaré más recursos y sólo tendré que pagar más por el tiempo de uso extra.
Acceso desde la red	Como los recursos están alojados en la red, se puede acceder a los mismos desde cualquier lugar.	Es posible acceder al panel de gestión de nuestras aplicaciones, y como usuarios, desde distintas oficinas o desde el teléfono móvil.
Recursos compartidos	Los recursos están en reservas comunes a no ser que se contraten servicios de nube privada, es decir, se comparte hardware y software.	Las pymes pueden disponer de recursos, por tamaño o precio, antes sólo destinados a la gran empresa.
Recursos a la carta o escalabilidad	Los clientes pueden redimensionar los recursos que contratan de manera rápida y eficaz en casi cualquier momento.	Si aumenta nuestra necesidad de recursos podemos cambiarla desde el panel de control de *cloud* y estará a nuestra disposición en un plazo razonable.
Servicio supervisado	El control y la optimización de los recursos se automatizan por el proveedor de los servicios en la nube siendo este proceso, transparente para el cliente.	No tenemos que prever la compra de más equipos o de nuevas licencias de software, ni tendremos que contratar técnicos para mantenimiento de equipos.

Tabla 1: Características de los servicios en la nube

2.2 Ventajas e inconvenientes

Los servicios *cloud* ponen al alcance de la pyme las ventajas y funcionalidades de la tecnología que de otra forma no podrían permitirse. Los proveedores de estos servicios ofrecen **escalabilidad y flexibilidad** para adaptarse sobre la marcha (*pay as you go*) a nuestras necesidades. También nos permiten tener siempre disponibles y accesibles desde cualquier lugar nuestras aplicaciones. Todo esto con la posibilidad de contratar no solo la infraestructura o el software, sino también su mantenimiento. La siguiente tabla ilustra las ventajas e inconvenientes de este modelo.

"Los proveedores de cloud computing permiten tener siempre disponibles y accesibles nuestras aplicaciones."

VENTAJAS	
Ahorro de costes	Este ahorro se debe a la reducción de los costes de infraestructura y su mantenimiento, licencias de uso, personal, etc. Se paga por uso de recursos.
Optimización de recursos	Los recursos (equipos, técnicos, etc.) se utilizan cuando se necesitan y se paga por este uso. Si tenemos un pico pagaremos más. Esto supone un ahorro en la infraestructura que tendríamos que comprar si queremos cubrir esos picos.
Recuperación ante desastres	La información y las aplicaciones están almacenadas en la nube y en distintas ubicaciones. Si se produjera algún incidente grave, esa información seguiría estando accesible.
Tecnología actualizada y segura	El proveedor del servicio en la nube es el encargado de realizar las tareas de mantenimiento, que son transparentes para el cliente.
Dedicación al negocio	Al reducir la carga de trabajo para la administración de los sistemas TIC podemos dedicar mayor esfuerzo en la gestión de nuestro negocio.

INCONVENIENTES	
Pérdida de control	Como cliente de servicios *cloud* no tendremos acceso a las instalaciones donde se están ejecutando nuestras aplicaciones. Dejamos nuestros datos y aplicaciones en manos del proveedor. Debemos leer con detalle el contrato de suministro: ubicación, disponibilidad, responsabilidades, etc.
Confidencialidad y seguridad en los datos	La información de nuestra empresa (datos de clientes, facturas,...) va a estar almacenada en los servidores del proveedor y, en caso de que sufra un problema técnico o de seguridad, nuestra información puede verse comprometida.
Disponibilidad del servicio	La nube, como cualquier otro servicio, no está exenta de problemas y puede ocurrir que se caiga. Como consecuencia de ello los servicios que ofrece podrían no estar disponibles.
Acceso a internet	El acceso a las aplicaciones está condicionada a que tengamos acceso a Internet. Si no tenemos acceso por algún motivo, no tendremos acceso a las aplicaciones.

Tabla 2: Ventajas e Inconvenientes de los servicios en la nube

2.3 Opciones de contratación

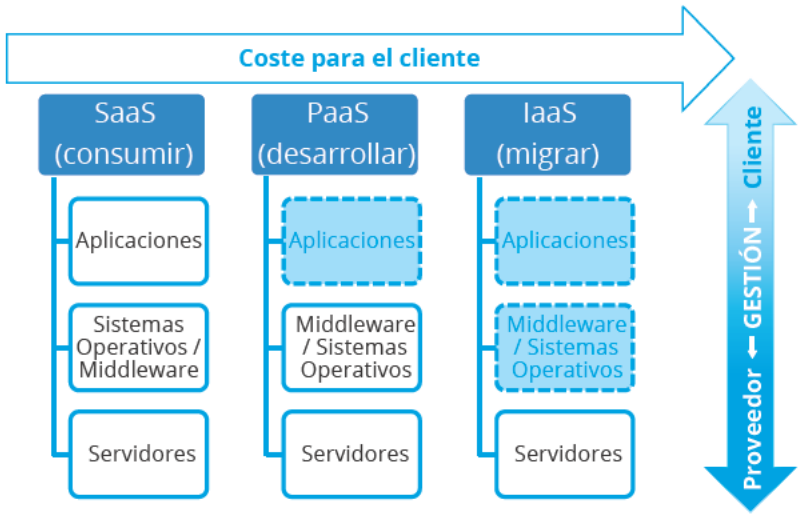
Para comprender el funcionamiento del *cloud computing* es fundamental conocer las tres opciones o tipos de servicio en *cloud*:

SaaS (*Software as a Service*) o **software como servicio**, **directo para su consumo por los usuarios finales.** Por ejemplo CRM, ERP o correo electrónico bajo demanda, escritorio virtual, comunicación, juegos,...

PaaS (*Platform as a Service*) o **plataforma como servicio para actividades de desarrollo o despliegue de aplicaciones** como servidores web, herramientas de desarrollo, bases de datos, big data,...

IaaS (*Infrastructure as a Service*) o **infraestructura como servicio para administradores TIC**: máquinas virtuales, servidores, almacenamiento, balanceadores de carga, equipos de comunicaciones, cortafuegos,...

"Hay tres tipos de opciones en cloud computing: software como servicio, plataforma como servicio e infraestructura como servicio."



2.3.1 Software como Servicio

En los servicios del tipo ***SaaS*** el proveedor entrega al cliente el software instalado en sus instalaciones para su uso a través de Internet, siempre que lo demande el usuario (bajo demanda). El correo web, las suites ofimáticas o los paquetes de desarrollo de negocio a los que se puede acceder online son un buen ejemplo de este tipo de servicios.

Permite el acceso a la aplicación utilizando un navegador web o una app, **sin necesidad de instalar programas adicionales** en el ordenador o teléfono móvil. Es adecuado para usuarios que solamente necesitan utilizar las aplicaciones. Los usuarios aportan sus datos y pueden personalizar la aplicación dentro de los límites que marca el

proveedor. No existen costes tecnológicos de hardware, software o soporte técnico.

VENTAJAS	INCONVENIENTES
• Reducción drástica de costes • Reducción de tiempos debido a que el software ya está instalado • Escalabilidad • Facilidad de uso	• Integración con aplicaciones existentes en la organización • Incertidumbre en relación al dueño de las aplicaciones • Gran dependencia del proveedor

En cuanto a la seguridad, como es el proveedor quien gestiona toda la infraestructura sobre él recaen la mayoría de las obligaciones de poner las medidas de seguridad para garantizar la seguridad de los datos de los clientes. Los clientes deben leer y aceptar las políticas de seguridad del proveedor, y utilizar el servicio bajo esas premisas, siendo conscientes de cuál es su responsabilidad en la seguridad del servicio.

"En los servicios SaaS el proveedor entrega al cliente el software ya instalado para su uso a través de internet bajo demanda"

2.3.2 Plataforma como Servicio

En los servicios del tipo ***PaaS*** el proveedor entrega una plataforma al cliente con el hardware, el sistema operativo y el middleware[2] o las API (interfaces de programación de aplicaciones) necesarias **para que el cliente pueda instalar software y desarrollar un servicio o una aplicación.**

Es adecuado para empresas que deseen desarrollar o lanzar sus propias aplicaciones sobre la plataforma que proporciona el proveedor, despreocupándose del hardware y del sistema operativo. El cliente despliega sus propias aplicaciones sobre la plataforma, las puede configurar y tiene el control sobre el entorno que instala y las aplicaciones que desarrolla. Para el empresario conlleva costes de soporte y software adicional.

Algunos ejemplos son:

- el servidor web preinstalado y el alojamiento para crear una página web que mantenemos nosotros, instalando el gestor de contenidos o CMS;
- el servicio contratado para crear o subir BBDD cuando el cliente instala su propio gestor de base de datos en la plataforma alquilada;
- los servicios que se contratan para poder instalar una aplicación que sirva contenidos como por ejemplo videos en *streaming*;
- las plataformas para la creación de aplicaciones como cuadros de mando, sistemas de *reporting* (BI *Business Intelligence*) o analítica Big Data.

2 Software que permite el intercambio de información entre aplicaciones, programas, redes, hardware o sistemas operativos.

VENTAJAS	INCONVENIENTES
• Facilidad para administrar la plataforma • Sencillez a la hora de permitir un desarrollo propio • Facilidad de integración con el resto de la plataforma	• Dependencia del proveedor • Dudas sobre la confidencialidad de los datos

"Los servicios PaaS son adecuados para empresas que deseen desarrollar sus propias aplicaciones sin preocuparse del hardware y del sistema operativo."

En cuanto a la seguridad en este tipo de servicios está repartida entre proveedor y cliente. El proveedor gestiona la plataforma y debe garantizar su seguridad, pero el cliente es responsable de las aplicaciones que instala o desarrolla. Los proveedores tomarán medidas para garantizar la calidad del servicio, la disponibilidad del mismo o el acceso seguro. Los clientes deben poner las medidas para que las aplicaciones que despliegan tengan *backup*, estén actualizadas y el acceso a las mismas sea seguro.

2.3.3 Infraestructura como Servicio

En los servicios del tipo ***IaaS*** el proveedor entrega al cliente el acceso a la infraestructura de computación bajo demanda. Es adecuado para empresas que necesitan una mayor versatilidad ya que permite ejecutar prácticamente lo que la organización desee. Presenta un coste elevado, ya que la empresa es la encargada de mantener todo el software que instale.

Algunos ejemplos son los centros virtuales de datos o los sistemas de respaldo. El proveedor utiliza entornos de virtualización para entregar al usuario el espacio en disco o la capacidad de proceso o los *routers* solicitados por el cliente como si fueran un servicio.

VENTAJAS	INCONVENIENTES
• Flexibilidad en relación a la infraestructura necesaria por el cliente • Rapidez de instalación • Facilidad al desplegar las aplicaciones del cliente	• Soporte ofrecido ya que al estar externalizado el servicio es más complicado solucionar el problema de una forma rápida

En cuanto a la seguridad en este caso también está repartida. El proveedor gestiona la infraestructura y debe garantizar su seguridad que será principalmente física, pero el cliente es responsable de los sistemas y aplicaciones que despliega en ella. Los proveedores tomarán medidas para garantizar por ejemplo la disponibilidad de la infraestructura o el acceso seguro a la misma. Los clientes deben poner las medidas para que sus sistemas y aplicaciones sean seguros.

2.4 Modelos de despliegue en la nube

Los proveedores pueden ofrecernos los servicios *cloud* en tres modelos de despliegue:

- **nube pública:** si los clientes, varias empresas o particulares, «comparten» los recursos tecnológicos;
- **nube privada**: cuando los recursos se ofrecen de forma exclusiva, es decir, sólo para nuestra empresa;
- **nube híbrida:** mezclando servicios de forma exclusiva con otros compartidos.

"En los servicios de nube pública el proveedor ofrece el mismo servicio a muchos clientes desde el mismo centro de datos compartiendo los recursos."

2.4.1 Servicios en nube pública

El proveedor ofrece el mismo servicio a muchos clientes desde el mismo centro de datos de forma que comparten recursos (de almacenamiento, de proceso,...). Esto hace posible una gran escalabilidad y eficiencia y generalmente un precio asequible.

VENTAJAS	INCONVENIENTES
• Escalabilidad • Ahorro de tiempo y costes • Mayor eficiencia de los recursos	• La infraestructura es compartida • Hay poca transparencia para el cliente de cloud ya que no se sabe el resto de recursos que se puede estar compartiendo

Los clientes utilizan los servicios que son procesados en el mismo servidor y pueden compartir espacio en disco u otras infraestructuras de red con otros clientes.

Son ejemplos los servicios de almacenamiento o correo que se ofrecen generalmente en formato gratuito o *fremium*, es decir, el servicio básico es gratuito pero se paga por un servicio avanzado, por ejemplo más espacio de almacenamiento o más cuentas de correo.

Se reconocen porque en estos casos el contrato y el ANS (Acuerdo de Nivel de Servicio) suelen ser cerrados e innegociables. Es decir tenemos que aceptar las condiciones del proveedor.

2.4.2 Servicios en nube privada

Son servicios en los que los recursos se entregan de forma exclusiva, privada, al cliente, al que se lo ofrece el control sobre el servicio que alquila.

En estos casos seguimos disfrutando de la flexibilidad de escalar el servicio si necesitamos contratar más recursos. Además, al ser un servicio privado, el proveedor garantiza la separación de los recursos que alquilamos y de los que alquilan otros clientes.

VENTAJAS	INCONVENIENTES
• Cumple con las políticas internas, ofreciendo mayor seguridad que la pública • Control total de los recursos	• Elevado coste • Dependencia de la infraestructura contratada

Los servicios en nube privada tienen ventajas en cuanto al control de la seguridad y privacidad de los datos y procesos. También son más costosos.

En este caso los contratos y los ANS son negociables o parcialmente negociables.

"Los servicios den nube privada permiten mayor control sobre la seguridad y privacidad de datos pero son más costosos."

2.3.4 Servicios en nube **híbrida**

Combinan servicios en nube pública y en nube privada con una administración única, es decir, gestionados desde un mismo panel de gestión. También se integran con servicios en nuestras oficinas (*on premise*). Con la mezcla entre servicios públicos y privados se consiguen reducir costes frente a la nube privada.

VENTAJAS	INCONVENIENTES
• Maximiza el valor al utilizar recursos privados y compartidos • Reducción de costes	• Riesgo al combinar dos modelos de implementación diferente • Control de la seguridad entre ambas nubes

Un ejemplo de servicios en nube híbrida se da cuando una empresa contrata un servicio de CRM en la nube pública pero el servicio de ERP e la nube privada. De este modo nuestros datos sensibles permanecen bajo nuestro estricto control mientras que el servicio CRM puede ser administrado por el proveedor que se encarga de mantenerlo online, vigilar que tenga suficientes recursos para soportar los picos de usuarios, etc.

Este enfoque no soluciona el problema de tener que contratar servicios en una nube privada asumiendo las obligaciones derivadas de su mantenimiento, pero puede disminuir considerablemente su complejidad y coste.

3 Seguridad en la nube

Elegir la forma de contratación y el modelo de despliegue que nos interesa, va a depender del servicio que queramos subir a la nube y **de sus requisitos de seguridad**. Así, no es lo mismo contratar un servicio para el correo electrónico, para almacenar y compartir ficheros o alojar una web, que migrar por completo nuestra empresa a la nube.

Utilizar servicios en la nube conlleva un cambio en la forma de entender la seguridad informática ya que deja de estar completamente bajo nuestro control y pasa a estar parcial o totalmente delegada en los proveedores.

Una parte importante de la seguridad del cualquier servicio *cloud* recae sobre la empresa proveedora pues será la encargada de garantizar la **seguridad física** en sus centros de procesos de datos. Del mismo modo, deberá **mantener sus equipos actualizados** tanto a nivel hardware como software para hacer frente a las amenazas existentes en Internet.

Esto no significa que el proveedor de servicios se encargue de todo y que ya no sean necesarios los administradores del sistema en nuestra organización. Tanto si se utiliza un servidor en la nube (*IaaS*) como si se utiliza un entorno de desarrollo (*PaaS*), somos responsables de mantener el sistema operativo y las aplicaciones que instalemos correctamente configuradas, actualizadas a las últimas versiones y con todos los parches de seguridad que vayan apareciendo.

Sea cual sea la forma de contratación y el modelo de despliegue en la nube, tendremos que **mantener las políticas de seguridad que aplicaban a los servicios que hemos trasladado a la nube**. Tendremos que cumplirlas o revisar su cumplimiento por parte del proveedor. Por ejemplo realizaremos periódicamente una copia de seguridad, controlaremos los accesos de los usuarios y borraremos las cuentas que ya no se utilizan; o verificaremos que lo hace el proveedor si así lo hemos acordado.

El proveedor de servicios se encarga de solucionar todos los problemas relacionados con los componentes electrónicos, si detecta un fallo en uno de los equipos dentro de sus instalaciones, automáticamente este equipo queda aislado y todos los procesos que se ejecutasen en él se migran a otra máquina que no tenga problemas. Este proceso puede durar tan solo unos minutos e incluso realizarse sin cortar el servicio permitiendo una **disponibilidad ininterrumpida** de los servicios en la nube.

En este aspecto, las ventajas del *cloud computing* frente a las arquitecturas tradicionales son abrumadoras. Gracias a las técnicas de virtualización y a la deslocalización de datos, se puede realizar una **copia de seguridad de la máquina virtual al completo**. De este modo, se almacena cada cierto tiempo el estado actual de todo el sistema incluyendo el sistema operativo, todas las aplicaciones instaladas con sus correspondientes actualizaciones y todos los datos.

Las responsabilidades de seguridad y los requisitos de seguridad de los procesos que migremos a la nube, que no recaigan directamente sobre nosotros como clientes, tenemos que trasladarlos al proveedor, y exigir poder verificar su cumplimiento.

Como clientes de los proveedores *cloud,* firmaremos **ANS o Acuerdos de Nivel de Servicio**, en los que se han de reflejar todos estos aspectos para cumplir nuestros requisitos de seguridad para cada servicio que contratemos. Antes de contratar tendremos que valorar las opciones que hay en el mercado para cada servicio que queramos subir a la nube. Unos tendrán más requisitos de seguridad que otros, en particular si tratan cono datos personales o confidenciales.

Lo que está claro es que antes de lanzarse a firmar con un proveedor en la nube, sea para una aplicación, una plataforma o una infraestructura, tenemos que hacer un **análisis**

detallado de los objetivos de negocio que queremos conseguir, incluidos los de seguridad. Cuando tengamos claro estos objetivos, escucharemos a los proveedores para ver cuáles de ellos entienden nuestra necesidad, los requisitos de ciberseguridad y nuestro mercado.

"Utilizar la nube conlleva un cambio en la forma de entender la seguridad informática ya que deja de estar completamente bajo nuestro control."

3.1 Amenazas y riesgos

Toda la información que se recibe, se genera o se conserva en la empresa en el desarrollo de su actividad son **activos de negocio, de conocimiento, intelectuales**, etc. Parte de esta información se almacena durante un tiempo porque supone una evidencia de que se ha realizado una transacción comercial o profesional, es decir, está sujeta a algún tipo de obligación legal. Por ejemplo los contratos de servicios o de personal, las facturas, presupuestos, etc.

Esta información requiere un tratamiento específico durante todo su ciclo de vida, ya que se deben preservar sus **propiedades de autenticidad, fiabilidad y usabilidad** y en algunos casos **confidencialidad**. Pueden ser ficheros de documentos, hojas de cálculo o pdf, bases de datos, formularios web, ficheros de imagen, video o multimedia, ficheros CAD, xml, sms, páginas web, ficheros de log, etc. Además si utilizamos servicios en la nube es fácil que estén gestionados desde todo tipo de dispositivos: PC, portátiles, tabletas o móviles. Por eso si, utilizamos servicios *cloud* tenemos que cerciorarnos de que se conservan estas propiedades esté donde esté nuestra información.

El uso del *cloud computing* lleva asociados **amenazas y riesgos** que es necesario tener en cuenta y gestionar. Su conocimiento y su gestión van a hacer posible que mantengamos el control sobre nuestra información que debe permanecer protegida y disponible en cualquier momento.

3.1.1 Amenazas

Las amenazas dependen del tipo de servicio contratado y de su forma de contratación y de despliegue. También será distinta la forma de afrontarlas según el grado de control sobre el servicio que recae en el proveedor y en el cliente acordado en el ANS. Por ejemplo, la responsabilidad de hacer *backup* o la de actualizar las aplicaciones pueden recaer en el proveedor o en el cliente (la empresa) del servicio en la nube dependiendo del modelo del contratado. No obstante, a pesar de las diferencias, las más importantes son:

Accesos no autorizados: si proveedor y cliente no toman conjuntamente las medidas de seguridad adecuadas, no habrá posibilidad de controlar los accesos a la información de la organización. Los accesos no autorizados pueden provocar robo de datos, inyección de código malicioso, etc.

3 Seguridad en la nube

"Las amenazas dependen del tipo de servicio contratado, de su forma de contratación y de su despliegue."

Amenazas internas: empleados insatisfechos o exempleados pueden provocar situaciones de riesgo si no se gestionan los permisos y privilegios de acceso. Por ejemplo cuando algún trabajador que usa un servicio en la nube deja la empresa (por fin de contrato o por despido), se debe notificar al proveedor de servicios *cloud* su baja para evitar que sigan teniendo acceso a la información.

Interfaces inseguras: si las interfaces que proporciona el proveedor para acceder a la plataforma en la nube no son del todo seguras y presentan fallos de seguridad, estos pueden ser explotados por terceros para acceder a nuestra información.

Problemas derivados de uso de las tecnologías compartidas: si contratamos una infraestructura compartida existe la amenaza de que por un fallo de seguridad usuarios de otras empresas puedan acceder a nuestra información.

Fuga de información: como resultado de un ataque de ingeniería social o por una infección con malware, un delincuente puede conseguir que algún usuario envíe información confidencial. También en el caso de que las operaciones de transferencia de datos no estén cifradas puede producirse una fuga de información.

Suplantación de identidad: Si los ciberdelincuentes consiguen, por ingeniería social, fuerza bruta o descuido, las credenciales de algún usuario podrán acceder a la plataforma suplantándole, pudiendo manipular la información, actuar en su nombre, etc.

Desconocimiento del entorno: si el personal encargado de implantar las políticas de seguridad no conoce el entorno *cloud*, las políticas estarán mal configuradas y no serán eficaces.

Ataques de hacking: suceden cuando una persona maliciosa intenta robar o acceder a la información que maneja alguno de los empleados de nuestra organización o el administrador de la plataforma.

3.1.2 Riesgos

Las amenazas pueden transformarse en incidentes si se dan las circunstancias para ello, provocando daños en la reputación y pérdidas económicas. Para ser consciente de estas circunstancias es necesario realizar una **evaluación de los riesgos** que afectan al servicio que vamos a contratar para así poder poner las medidas adecuadas para tratarlos.

"Es necesario realizar una evaluación de los riesgos que afectan al servicio que vamos a contratar para tomar medidas adecuadas para tratarlos."

De las características de los servicios en la nube y conociendo las amenazas, se derivan estos riesgos que tenemos que valorar para darles el tratamiento adecuado:

Acceso de usuarios con privilegios: este riesgo (pérdida de confidencialidad, integridad e incluso disponibilidad) aparece cuando un empleado con privilegios de administrador accede cuando no debería o actúa de forma maliciosa (empleados descontentos por ejemplo) alterando datos o configuraciones. También es posible que se den privilegios por error a empleados que no deban tenerlos y estos por desconocimiento provoquen daños.

Incumplimiento normativo: este tipo de riesgos, que puede tener consecuencias administrativas o penales, aparece cuando el proveedor no cumple, o no nos permite cumplir con nuestras obligaciones legales. Por este tipo de infracciones nos podemos enfrentar a sanciones legales.

Desconocimiento de la localización de los datos: cuando se contratan servicios a un proveedor que aloja nuestros datos en un Centro de Datos del cual desconocemos su ubicación, ponemos a riesgo la seguridad de los mismos al desconocer la legislación de otros países. Por ejemplo, si tratamos con datos de carácter personal, en caso de alojarse fuera del Espacio Económico Europeo es necesario que se proporcionen las garantías jurídicas necesarias sobre la privacidad de los mismos.

Falta de aislamiento de los datos: en los servicios en los que nuestra empresa comparte la infraestructura en la nube con otras es necesario que el proveedor gestione que los datos de las distintas empresas no se mezclen y que cada empresa sólo tenga acceso a los suyos.

Indisponibilidad del servicio en caso de desastre o incidente: si nuestro proveedor sufre un incidente grave o un desastre y no tiene un plan de continuidad por ejemplo, los servicios y los datos replicados en otro centro de datos, no nos podrá seguir dando servicio.

Carencia de soporte investigativo: en caso de que ocurra un incidente, necesitamos revisar los accesos a los datos para saber qué ha ocurrido. En este caso, no podremos actuar si el proveedor no nos garantiza el acceso a los *logs* o registros de actividad.

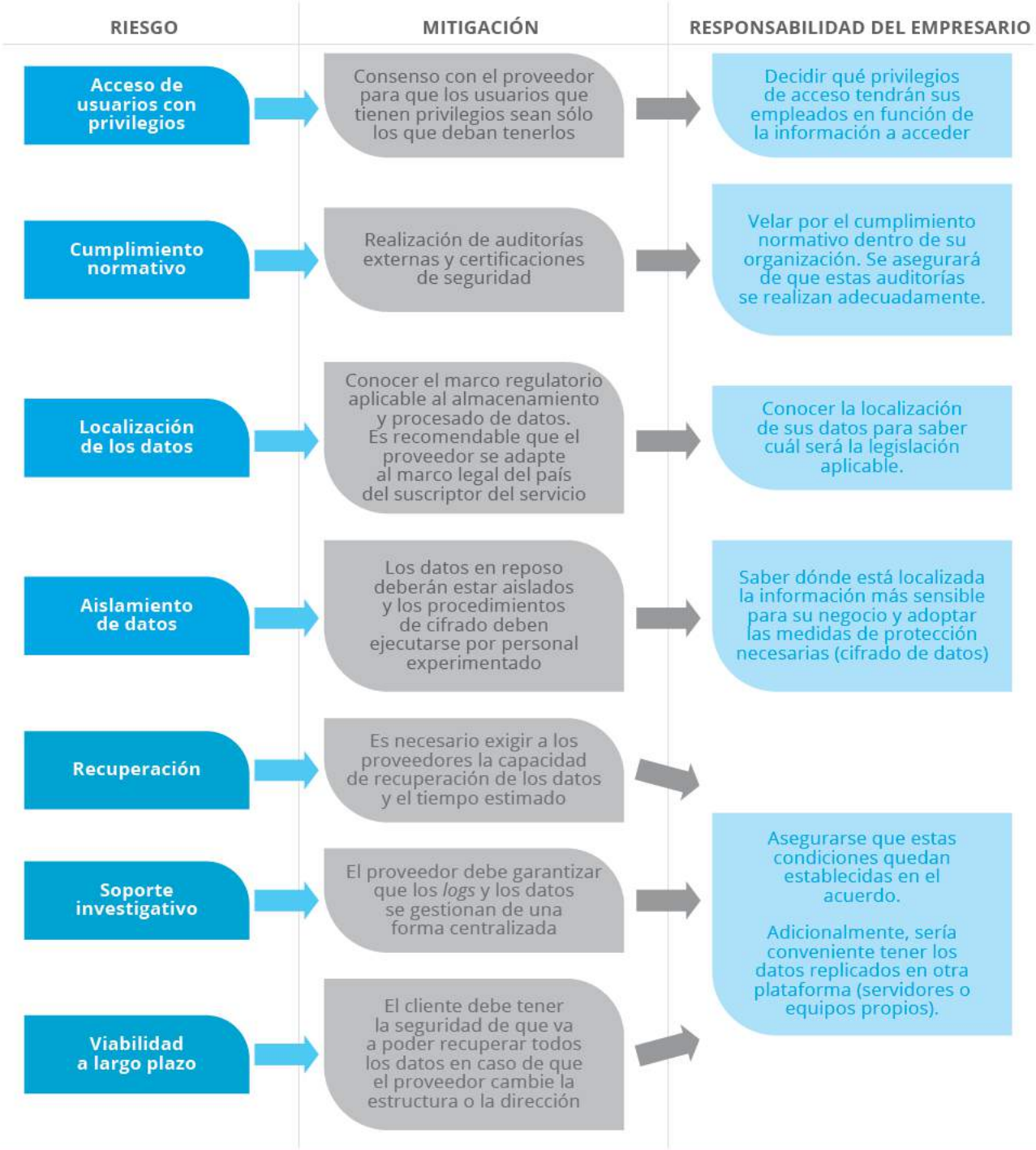
Viabilidad a largo plazo: existe el riesgo de que las condiciones del contrato sufran alguna modificación debido al cambio de estructura del proveedor, de la alta dirección, a la entrada en situación de quiebra del mismo o a que decida externalizar parte de sus servicios. Por ello es recomendable asegurarse el acceso a los datos y su recuperación.

"Tienes que trasladar a tu servicio en la nube la misma seguridad que exiges a tus instalaciones en local."

3.1.3 ¿Cómo reducir los riesgos?

Tanto si contratas en la nube un servidor de correo, un servidor web, un CRM o un servicio de almacenamiento como si decides contratar capacidad de proceso para instalar tus propias aplicaciones tienes que **trasladar la seguridad que exiges a tus instalaciones en local, a la nube**. No olvides que tus activos de información siguen siendo igual de confidenciales y tienen que mantenerse íntegros y estar disponibles cuando los necesites.

La siguiente ilustración muestra algunas estrategias para mitigar los riesgos que en su mayoría van de estar reguladas por el contrato y los acuerdos de nivel de servicio o ANS.



4 Aspectos legales y contractuales

Cuando se decide implementar una solución *cloud* es necesario tener en cuenta el marco legal existente, tanto del país donde reside la organización como del país del proveedor del servicio en la nube. En el caso de España será de aplicación la Ley Orgánica de Protección de Datos (LOPD), que se cumple gracias a la actuación de la Agencia Española de Protección de Datos.

4.1 La privacidad en servicios *cloud*

En un mundo donde los datos circulan de manera global, las empresas tenemos que prestar atención a la protección de la **privacidad** pues todas en mayor o menor medida tratamos con datos personales, ya sean de clientes o de empleados. Es decir, tratamos con datos e información que deben ser protegidos.

Por ello tenemos que considerar **dónde están ubicados los centros de datos** del proveedor de servicios *cloud*, ya que la legislación sobre seguridad y privacidad varía de unos países a otros. En concreto, para cumplir la legislación en materia de protección de datos personales, los proveedores con centros de datos en el EEE nos ofrecen más garantías en materia de protección de datos. En cualquier caso si el proveedor, a su vez, **subcontrata** servicios a terceros que hace que pueda cambiar la ubicación de nuestros datos, tendremos que saberlo.

No debemos olvidar que como empresa, si utilizamos datos personales somos los «responsables del tratamiento» según la LOPD [3], incluso aunque contratemos a proveedores *cloud* algún servicio en el que se manejen estos datos. En este caso el proveedor sólo será un «encargado del tratamiento».

En caso de que estén fuera de la UE podría tratarse de una transferencia internacional de datos, y en este caso sería necesario asegurar que dicho país ofrece unos niveles jurídicos de protección de datos equivalentes a las del EEE (Espacio Económico Europeo).

Las transferencias internacionales de datos tienen que contar con la autorización expresa del Director de la Agencia Española de Protección de Datos [5].

4.2 Contrato, ANS y condiciones de uso

Como en todo acuerdo empresarial, la relación entre el proveedor de servicios en la nube y el cliente debe estar regulada por un **contrato** [6] y en muchos casos por un **Acuerdo de Nivel de Servicio o ANS**. Estos documentos deben definir claramente la posición de cada una de las partes así como sus responsabilidades y obligaciones.

En el contrato se fijará el servicio contratado, su duración, condiciones de finalización y desistimiento, precio y otras condiciones. Entre ellas, las **condiciones de uso** son una parte importante y de obligada lectura. Definen las características del servicio y su forma de entrega, el uso aceptable que se espera del cliente, la descarga de responsabilidad y la legislación aplicable en caso de conflicto.

4 Aspectos legales y contractuales

"La relación entre el proveedor de servicios en la nube y el cliente debe estar regulada por un contrato donde se establezcan las condiciones del acuerdo."

Cuando se contratan servicios en la nube surgen muchas dudas relativas a la seguridad de la información, a su confidencialidad, integridad y disponibilidad. Si se cumple la LOPD, dónde estarán alojados los servicios, qué medidas de seguridad tienen, etc. Estas dudas se resuelven al negociar los **acuerdos de nivel de servicio** ANS o, en inglés, SLA (*Service Level Agreements*). Más concretamente, la calidad del servicio establece los niveles de rendimiento y disponibilidad garantizados por el proveedor.

Los **ANS** describen las responsabilidades de ambas partes, en particular del proveedor, y las penalizaciones si las hubiera, en cuanto a:

- **Rendimiento**: disponibilidad, tiempo de respuesta, capacidad, soporte, proceso de finalización y rescisión.
- **Seguridad**: fiabilidad, autenticación y autorización, criptografía, gestión de incidentes y su notificación, monitorización y registro de actividad (*logging*), auditorías y verificación de la seguridad, gestión de vulnerabilidades y gobernanza.
- **Tratamiento de datos**: clasificación, *backup,* ciclo de vida y portabilidad.
- **Privacidad**: códigos de conducta, estándares y mecanismos de certificación, minimización de datos, uso, retención y limitación de revelado, transparencia, intervención, ubicación geográfica y control de accesos.

Los contratos de prestación de servicios y los ANS entre proveedor y cliente pueden ser:

- **De adhesión**: los proveedores de servicios *cloud* muestran las condiciones fijas en las que prestan su servicio para todos los clientes. Cada empresa tiene que estudiar la oferta del mercado hasta encontrar la que mejor satisface sus necesidades.
- **Negociado**: el cliente puede fijar las condiciones de contratación en cuanto a medidas de seguridad, localización de los datos, portabilidad, etc.
- **Mixto**: una parte de las condiciones son fijas y otras se pueden negociar.

El primero de ellos es el más común si utilizamos servicios de *cloud* pública, aquellos en los que el proveedor de servicios ofrece sus recursos (aplicaciones, almacenamiento,...) al público en general a través de Internet. En estos casos el proveedor dispone de un acuerdo tipo y no podemos hacer nada por cambiarlo. Vienen acompañados por la conocida frase: «Acepto los términos y condiciones de uso», o similar.

En el otro extremo, los completamente negociables son los más parecidos a los contratos de externalización de servicios. Son los necesarios si se maneja información muy sensible con altos niveles de confidencialidad o integridad, se requiere alta disponibilidad o se ha de cumplir con normativa sectorial específica (entidades bancarias, Administración Pública, entornos de investigación y desarrollo, clínicas, consultorías y asesorías legales, tecnológicas o de negocio, etc.).

4 Aspectos legales y contractuales

"Es importante revisar que el cloud tenga las medidad técnicas y organizativas adecuadas para que nuestra información no se pierda, dañe o corrompa."

Los parcialmente negociables están entre ambos modelos, son los que permiten modificar o añadir algunas cláusulas al modelo no negociable. Son poco comunes.

Estos dos últimos modelos se asocian a modelos de *cloud* privada, es decir entornos *cloud* en exclusiva para su empresa y *cloud* híbrida (entre pública y privada).

Aunque depende mucho del servicio que se contrate, en general y **en cuanto a la seguridad debemos revisar**:

- que el prestador del servicio *cloud* tenga e implemente las medidas técnicas y organizativas adecuadas para que la información que es almacenada en la nube no se pierda, dañe o corrompa;
- si la ubicación del centro de datos cumple con los requisitos de protección de la privacidad adecuados a los datos personales que allí se alojen, según su tratamiento por la LOPD;
- las medidas de seguridad adoptadas por el proveedor para conservar nuestros datos, como actualizaciones, *backups*, auditorías, medidas contra incendios, etc.;
- que los datos y procesos que se almacenan en las instalaciones del prestador del servicio no sean accedidos o utilizados por terceras personas y que ofrece garantías de que nuestros datos están separados y no accesibles por otros clientes de la nube;
- que los datos que almacena el prestador del servicio no sean accedidos o utilizados por éste para fines distintos a los que establece el contrato;
- que los datos viajen de forma segura cuando están siendo comunicados entre el prestador del servicio y su empresa, es decir, la seguridad que aplican en las transacciones y transferencias de datos;
- que la calidad del servicio y su disponibilidad sea la necesaria para la actividad de la empresa;
- las condiciones del servicio de atención al cliente que nos ofrecen, si es por teléfono, en nuestro idioma, 24x7, etc.;
- su flexibilidad o cómo escala los servicios si aumentan o disminuyen nuestras necesidades;
- las opciones de portabilidad cuando termine el servicio o si cambian las condiciones;
- que implanta medidas de continuidad de negocio para garantizar la continuidad en caso de incidente o de desastre que afecte a sus instalaciones.

En ocasiones el proveedor permite la realización de auditorías de seguridad conjuntas para revisar que todo el sistema está protegido frente a posibles amenazas.

5 Pasos necesarios para dar el salto a la nube

Desde la perspectiva de muchas pequeñas y medianas empresas el modelo de *cloud computing* es atractivo para externalizar sus necesidades tecnológicas. Desde el correo electrónico hasta el alquiler de servidores y redes pasando por el almacenamiento de información, aplicaciones empresariales, de gestión y contabilidad, CRM, ERP y otras para compartir información los socios comerciales, sin olvidar el alojamiento web y la tienda online, toda la actividad del negocio puede subirse a la nube.

Una vez que se ha entendido cómo funciona la tecnología y las distintas posibilidades que nos brinda, es el momento de pensar en si realmente mi empresa o negocio se puede beneficiar de ellos. Estos serían los distintos pasos que se deberían seguir para dar el salto a la nube:

5.1 Estudio de las necesidades del negocio

Lo primero que tenemos que plantearnos es si nuestro negocio necesita una aplicación en la nube y el ahorro que supone frente a otras opciones. Si, por ejemplo, tenemos que implantar:

- herramientas de oficina (procesador de textos, hoja de cálculo, presentaciones, etc.), almacenamiento;
- una página web, un portal colaborativo, una red social interna;
- un sistema de correo electrónico, de gestión de clientes CRM o de productividad ERP;
- soluciones de gestión de movilidad, servicios de seguridad;
- o herramientas de BI (inteligencia de negocio) y analítica predictiva;

Podemos valorar contratarlos en la nube, si esto supone ahorros en equipos, en compra de licencias software o en desarrollo.

Por otra parte hay otros factores que pueden hacer que nos decantemos por soluciones en la nube. Por ejemplo si se estima que el número de usuarios va a tener grandes fluctuaciones, o prevemos que se incrementará rápidamente, deberíamos optar por una solución en la nube. Del mismo modo, resulta interesante optar por un servicio de *cloud computing* si los usuarios van a estar dispersos geográficamente o si la aplicación hace un uso intensivo de los recursos computacionales.

5.2 Estudio de las ofertas de los distintos proveedores de servicios en la nube

Si se decide que las características de nuestro negocio requieren una solución basada en el *cloud computing*, el siguiente paso obligatorio es tomarse el tiempo necesario en estudiar las distintas opciones existentes en el mercado.

Por ejemplo, hay muchas empresas especializadas en servicios de *cloud hosting* que llevan años trabajando con esta tecnología mientras que hay empresas de hosting tradicional que están empezando a ofertar distintos paquetes de funcionalidades en la nube.

Por otra parte, las grandes multinacionales del software como Microsoft, Amazon o Google disponen de una gran oferta de servicios en la nube que pueden ser aplicados rápidamente a nuestras necesidades.

"Antes de tomar una decisión sobre nuestro proveedor de cloud computing hay que estudiar las distintas opciones existentes."

5.3 Estudio de las cláusulas legales y términos de uso

Por supuesto, una de las claves que decidirá qué solución de *cloud computing* elegida será el precio de los servicios. Sin embargo, no debe ser la única, ya que las consideraciones legales son igualmente importantes. Aunque la publicidad sea estupenda y prometa los mejores precios, la calidad de los servicios que se compromete a ofrecer el proveedor viene estipulada claramente en el contrato o los términos de uso. Del mismo modo, es necesario comprobar que el proveedor nos ofrece la seguridad que necesitamos para el servicio y se encarga de cumplir las regulaciones legales establecidas por nuestro país o por la Unión Europea.

5.4 Utilización de mecanismos de migración

Lo más importante a la hora de utilizar los servicios en la nube es tener claro qué parte de nuestros activos informáticos van a ser migrados. Conviene hacer un estudio de las implicaciones de migrar todos los datos y procesos a la nube.

Durante los primeros momentos de uso del *cloud computing*, una opción muy inteligente sería mantener los datos o procesos más sensibles bajo nuestro estricto control mientras que las aplicaciones más pesadas, computacionalmente hablando, se migran a la nube. Una vez comprobada si la fórmula funciona se podría realizar una migración total a la nube. Todos los proveedores de servicios ofrecen mecanismos para facilitar la migración de nuestros sistemas a la nube. Conviene realizar un estudio completo de estas funcionalidades antes de realizar la migración para aprovecharse de sus posibilidades reduciendo significativamente la complejidad de la tarea.

5.5 Continuidad de negocio

También debemos plantearnos qué pasa si el proveedor sufre un incidente grave que le impida seguir operando. Por eso revisaremos si el **Plan de Continuidad** del proveedor cumple nuestros requisitos de continuidad de negocio.

5 Pasos necesarios para dar el salto a la nube

"Recuerde contar con un plan de recuperación de desastres que facilite la migración en caso de que falle el proveedor."

El proveedor debe permitirnos:

- verificar de forma automática la integridad de sus datos en cualquier momento;
- configurar los puntos objetivo de recuperación en sus copias de seguridad, es decir, los intervalos de las copias completas o el alcance de las copias incrementales para proteger los procesos más críticos;
- el acceso a un portal personalizado para la recuperación de ficheros, discos, sistemas o el sitio completo.

Negociaremos en los ANS por adelantado verificando:

- la documentación y el alcance de las certificaciones que el proveedor pueda tener sobre continuidad de negocio (ISO 22301);
- los compromisos que adquieren los proveedores para asegurar la continuidad del servicio externalizado, en particular si se tratan datos de carácter personal que puedan acarrear tratamientos específicos según la LOPD (Medidas de seguridad AEPD);
- que los proveedores cuentan con herramientas para restaurar los sistemas y acuerdos con otros proveedores de plataformas, en el caso de que contrate Infraestructura en *cloud* o *IaaS* (*Infrastructure as a Service*).

Solicitaremos información puntual o periódica para comprobar:

- que el proveedor tiene implantados los controles necesarios para mantener la continuidad de negocio pactada, incluso presencialmente;
- los resultados de las pruebas de continuidad y recuperación pactadas (por ejemplo restauración de *backups*) cuando se realicen;
- los niveles de cumplimiento de los ANS.

Si el ANS no es negociable recuerde contar con un Plan de recuperación de desastres que facilite la migración en caso de que falle algún proveedor. Y aunque estas precauciones son básicas, no olvide:

- respaldar siempre la información contenida en la nube
- evitar la dependencia en exclusiva de un único proveedor de servicios *cloud* también llamada *vendor lock-in* revisando antes de firmar si ofrece herramientas o servicios para migrar grandes cantidades de datos

6 Checklist de seguridad para contratar en la nube

A pesar de que los proveedores *cloud* ofrecen cada vez más información sobre la seguridad de sus servicios, es necesario como clientes **entender también cuáles son nuestras oportunidades y riesgos cuando contratamos servicios en la nube**.

La Guía de Seguridad en Cloud para pymes [7] de la Agencia Europea de Seguridad (ENISA) propone estas doce preguntas que debemos plantear al proveedor:

Para el servicio que quiero contratar: ¿cómo gestiona el proveedor los riesgos de seguridad de la información?

Como clientes tendremos que tener una idea de la eficacia de la gestión de la seguridad del proveedor. Una buena respuesta tendría:

- un punto de contacto para incidentes de seguridad;
- la política de seguridad del proveedor y sus dependencias con terceros (si a su vez externalizan);
- los informes de auditoría o sus certificaciones (como ISO27001) que incluyan el servicio en el alcance;
- los informes de cumplimiento o adherencia a estándares de buenas prácticas.

¿Qué tareas de seguridad hace el proveedor?, ¿qué tipo de incidentes de seguridad son mitigados por él? (y qué tareas e incidentes permanecen bajo nuestra responsabilidad)

Cada servicio *cloud* es diferente y también lo será el reparto de responsabilidades y obligaciones en cuanto a la seguridad. Pero en el contrato o en los acuerdos de nivel de servicio (*SLA*) se debe especificar:

- los activos cuya seguridad vigilará el proveedor y los que vigilaremos nosotros;
- las tareas de seguridad (parcheado, actualización,...) que realizará el proveedor y las que realizaremos nosotros;
- una clasificación de incidentes con sus objetivos de tiempos de respuesta o recuperación;
- las obligaciones contractuales, por ejemplo compensaciones financieras por pérdidas, etc.

¿Cómo maneja el proveedor los desastres que afecten a los centros de datos o a las conexiones? y ¿de qué datos se hace *backup* y dónde?

En el caso que un terremoto, una tormenta eléctrica o una inundación afecten al proveedor tendremos que saber en qué medida el servicio *cloud* que contratamos permanecerá activo, y cómo y dónde se hacen las copias de seguridad. Para ello tendremos que poder revisar:

6 Checklist de seguridad para contratar en la nube

- los planes de recuperación ante desastres y continuidad de negocio del proveedor;
- los mecanismos de *backup*, tolerancia a fallos y tiempos de recuperación;
- si tienen redundancia de sus centros de datos.

¿Cómo se garantiza la seguridad del servicio cloud en lo que concierne a disputas administrativas y aspectos legales?

Si el proveedor tuviera algún problema administrativo o legal (bancarrota, embargo, denuncias...) interno o con terceros, como clientes querremos saber qué ocurrirá con nuestros datos y con la continuidad del servicio. Debemos comprobar que aún en estos casos el servicio está garantizado. En los SLA o las cláusulas del contrato se incluirán las que nos garanticen el acceso a los datos y a las copias de seguridad en estos casos.

"Si vamos a depositar nuestros datos en manos de un proveedor tendremos que comprobar que son responsables con ellos."

¿Cómo asegura que su personal trabaja con medidas de seguridad?

Si vamos a depositar nuestros datos en sus manos tendremos que comprobar que son responsables. Algunas de las formas que tiene el proveedor de demostrar esto es:

- con certificados profesionales;
- con sus políticas de incorporación y formación de empleados;
- mediante ataques simulados a sus empleados con mecanismos de ingeniería social.

¿Cómo se protegen nuestros procesos y datos de los accesos lógicos y físicos no autorizados?

Nuestros datos y procesos estarán en sus instalaciones. El proveedor debería mostrarnos:

- las medidas de control de acceso físico y lógico (roles, privilegios,...) que tiene implantados;
- los mecanismos de autenticación en uso;
- su cumplimiento con criterios de buenas prácticas.

¿Cómo asegura la seguridad del software? y ¿qué software permanece bajo nuestra responsabilidad?

Como clientes tendremos que conocer cómo el proveedor garantiza la seguridad del software, en particular solicitaremos:

- informes de escaneos de *vulnerabilidades*;
- procedimientos de *parcheado* y actualización;
- auditorías externas del software.

6 Checklist de seguridad para contratar en la nube

"Desde nuestras instalaciones debemos poder monitorizar el rendimiento y las alertas de seguridad del servicio de cloud."

¿Cómo se protege el acceso a los interfaces de usuario y de programación de aplicaciones?, y ¿existen medidas adicionales para los perfiles con privilegios especiales y administradores?

Para acceder a los servicios *cloud,* los clientes y administradores utilizan interfaces web. La protección de estos interfaces es clave pues a través de ellos se pueden llegar a nuestros datos y procesos. En este caso el proveedor debe proporcionarnos los detalles técnicos de los interfaces y sus protecciones (métodos de autenticación, restricciones de acceso, privilegios,...)

¿Cómo podemos monitorizar el servicio, qué registros de actividad (logs) se toman y cómo podemos obtenerlos cuando necesitemos analizar un incidente?

Desde nuestras instalaciones tendremos que poder acceder a cuadros de mandos en los que monitorizar el rendimiento, las alertas y todo lo relativo a la seguridad del servicio. Igualmente en los SLA se podrá incluir una cláusula para poder recuperar los *logs* en caso de incidente, de manera que podamos saber qué ocurrió y depurar responsabilidades.

¿Es el servicio cloud portable e interoperable?

Como nada es para siempre y ante la posibilidad de tener que migrar, en el futuro, a otro proveedor o si quisiéramos integrar el servicio con otras aplicaciones, el proveedor del servicio *cloud* debería proporcionarnos los detalles técnicos del software instalado como los interfaces, formatos de datos, *máquinas virtuales* y formatos de exportación de datos.

¿Cómo gestionan picos de uso y cuáles son los costes asociados?

La elasticidad del uso de los recursos es la base de los servicios *cloud* en los que se paga por uso. Como clientes querremos saber cómo se va a gestionar los aumentos de demanda (disponibilidad) y cuánto van a costarnos. Los SLA deben incluir cláusulas que lo definan, escenarios y forma de calcular los costes. Podremos solicitar datos del rendimiento de estos mecanismos.

¿Qué legislación nacional o de otras naciones aplica?

Hay proveedores *cloud* que trabajan desde centros de datos fuera de nuestras fronteras, lo que pueden ocasionar fricciones entre legislaciones nacionales. Un ejemplo reciente es lo ocurrido con el puerto seguro en materia de protección de datos personales. Como clientes debemos asegurarnos de qué legislación aplica en cada caso. Para ello solicitaremos esta información al proveedor, en particular si recabamos datos personales de nuestros usuarios, tratamos con productos con propiedad intelectual y si realizamos actividades de comercio electrónico.

7 Productos y servicios de seguridad en *cloud*

El catálogo de empresas y soluciones de ciberseguridad de INCIBE [16] recoge las soluciones de seguridad, productos y servicios, que están disponibles en el mercado español. En el caso los **productos de seguridad en la nube** son, en general, **herramientas** registradas por los proveedores dentro de las siguientes categorías y subcategorías de la taxonomía [17]:

- **Anti-malware**: destinadas a la protección de servidores, ordenadores de sobremesa, portátiles, dispositivos móviles, etc., frente a todo tipo de software malicioso que pueda afectarles (virus, troyanos, gusanos, spyware, etc.). Detectan y eliminan todo tipo de malware.

- **Contingencia y continuidad**: cuyo objetivo es planificar planes de actuación y contingencia destinados a mitigar el impacto provocado por cualquier incidente de seguridad, con estas subcategorías:

  - **copias de seguridad**: destinadas al almacenamiento de datos o información con el fin de disponer de un medio para poder recuperarlos en caso de pérdida accidental o intencionada;

  - **infraestructura de respaldo**: destinadas a posibilitar el despliegue rápido de infraestructura de respaldo en caso de pérdida, con el objetivo de reducir al mínimo los tiempos de interrupción de la actividad.

- **Prevención de fuga de información**: garantizan la confidencialidad, la disponibilidad y la integridad de la información. Tienen la función de identificar, monitorizar, detectar y prevenir fugas de información desde y hacia el exterior de la organización, implementando políticas de uso de la información, de los dispositivos y periféricos.

- **Protección de las comunicaciones**: destinadas a proteger los sistemas y dispositivos conectados a una red. Permiten controlar el tráfico generado y recibido, realizando un control sobre el uso de ancho de banda, el tráfico y el rendimiento.

- **Seguridad en dispositivos móviles**: destinadas a la protección y gestión de la seguridad en los dispositivos móviles. Proporcionan protección y seguridad no sólo a los dispositivos móviles sino a las infraestructuras a las cuales se conectan.

En cuanto a los **servicios** registrados para seguridad en la nube se encuentran principalmente bajo las categorías [17] de servicios:

- **Contingencia y continuidad**: para realizar acciones encaminadas a contrarrestar y evitar interrupciones de las actividades del negocio y proteger sus procesos críticos ante incidentes y desastres de seguridad, garantizando la continuidad de los procesos de negocio, con estas subcategorías:

  - **Copias de seguridad remotas** (*backup*): son servicios de almacenamiento de datos fuera de la organización, permitiendo la restauración de la información de forma inmediata en caso de robos o pérdida de datos.

  - **Custodia y archivo seguro**: son servicios de almacenamiento con fuertes medidas de seguridad y en un emplazamiento distante de la organización.

7 Productos y servicios de seguridad en *cloud*

- **Centros de respaldo**: son servicios diseñados de réplica y almacenamiento que permiten a las organizaciones disponer de infraestructuras secundarias ante incidentes de seguridad.

- **Análisis de impacto en el negocio** (*Business Impact Analysis*, *BIA*): servicio destinado a la identificación de los procesos o actividades de cada una de las áreas del negocio, cuantificando el impacto ante incidentes de seguridad que puedan afectar al negocio.

Gestión de incidentes: destinados a prevenir, detectar y solucionar incidentes de seguridad de la información. Tienen el objetivo de obtener información y ayudar y detectar las amenazas de forma rápida, identificar vulnerabilidades y priorizar riesgos. Permiten llevar la gestión antes, durante y después de cualquier incidente de seguridad. Tienen esta subcategorías:

- **Prevención de incidentes de seguridad**: son servicios destinados a prevenir incidentes de seguridad, para ello se llevan cabo servicios de concienciación, definición de buenas prácticas y políticas de seguridad, definición de planes de contingencia.

- **Detección de incidentes de seguridad**: son los servicios destinados a la detección de incidentes de seguridad, consisten en la instalación de herramientas de seguridad, anti-malware, IDS, gestión de *logs* y eventos de seguridad.

- **Respuesta de incidentes de seguridad**: son servicios destinados a resolver incidentes de seguridad que hayan ocurrido, consisten en procedimientos de restauración de *backups*, eliminación de malware y auditoría forense.

Implantación de soluciones: destinados a la planificación, diseño e implantación de infraestructuras y soluciones de ciberseguridad.

Seguridad en la nube: destinados a la protección de las infraestructuras y servicios alojados en la nube. Permiten el uso de recursos de hardware, software, almacenamiento y comunicaciones proporcionado a las empresas un servicio adicional de seguridad.

8 Referencias

[1]. Telefónica - A un clic de las TIC - Cloud: ¿estás en las nubes o vives en la nube?)
http://aunclicdelastic.blogthinkbig.com/ebook-cloud/

[2]. ONTSI. Red.es Cloud computing. Retos y oportunidades
http://www.ontsi.red.es/ontsi/es/estudios-informes/cloud-computing-retos-y-oportunidades

[3]. Ley de Protección de Datos de Carácter Personal:
https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

[4]. Agencia Española de Protección de datos:
https://www.agpd.es

[5]. AGPD - Países con un nivel adecuado de protección de datos
https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

[6]. Incibe – Protege tu empresa – Contratación de servicios
https://www.incibe.es/protege-tu-empresa/que-te-interesa/contratacion-servicios

[7]. ENISA Guía de Seguridad en Cloud para pymes (en inglés) de la Agencia Europea de Seguridad
https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

[8]. España - Portal administración electrónica - Estrategia Europea de Cloud Computing
http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_lineas_ccoperacion/pae_Cooperacion_Internacional/pae_Estrategia_Europea_de_Cloud_Computing.html#.WGUkdvk8oVp

[9]. EU Digital Single Market – Cloud Computing (en inglés)
https://ec.europa.eu/digital-single-market/en/cloud

[10]. Incibe – Protege tu empresa – Blog - 12 preguntas de seguridad que has de hacer antes de contratar en la nube
https://www.incibe.es/protege-tu-empresa/blog/12-preguntas-seguridad-antes-contratar-cloud

[11]. Incibe – Protege tu empresa – Blog - ¿Qué seguridad le pides a tu proveedor *cloud*?
https://www.incibe.es/protege-tu-empresa/blog/seguridad-le-pides-tu-proveedor-cloud

[12]. Incibe – Protege tu empresa – Blog - Con la movilidad y la nube, ¿dónde está el perímetro?
https://www.incibe.es/protege-tu-empresa/blog/con-movilidad-y-nube-donde-esta-el-perimetro

[13]. Incibe – Protege tu empresa – Blog – Sube a la nube, pero no estés en «las nubes» sin continuidad de negocio
https://www.incibe.es/protege-tu-empresa/blog/no-estes-en-las-nubes

[14]. Incibe – Protege tu empresa – Blog - Pasos a seguir antes de subir a la nube (infografía)
https://www.incibe.es/protege-tu-empresa/blog/pasos-seguir-subir-nube#overlay-context=protege-tu-empresa/blog

8 Referencias

[15]. Incibe – Protege tu empresa – Sellos de confianza - *cloud*
https://www.incibe.es/protege-tu-empresa/sellos-confianza/cloud

[16]. Incibe – Protege tu empresa – Catálogo -
https://www.incibe.es/protege-tu-empresa/catalogo-de-ciber-seguridad/

[17]. Incibe – Protege tu empresa – Taxonomía de soluciones de seguridad
https://www.incibe.es/sites/default/files/contenidos/guias/doc/taxonomia_ciberseguridad.pdf

[18]. ByteTI - Toda la empresa en la nube. Especial Cloud Computing
http://www.revistabyte.es/cloud-computing-byte-ti/toda-la-empresa-la-nube-especial-cloud-computing/

[19]. Incibe - CERTSI - Arquitecturas de seguridad en la nube para la industria
https://www.certsi.es/blog/arquitecturas-seguridad-nube-industria

[20]. Incibe - CERTSI - Mi SCADA en las nubes
https://www.certsi.es/blog/mi-scada-nubes


GOBIERNO
DE ESPAÑA
MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL


incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD