## ¿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, adaptándose 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 como el comercio electrónico o las redes sociales, sino también el acceso ágil desde cualquier lugar a los centros de datos y de proceso.
* 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, etc)**
* La flexibilidad que ofrece la virtualización de sistemas operativos, servidores y redes que permite a los proveedores cloud aprovisionar los recursos de acuerdo con las demandas de sus clientes



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 para 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.

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 porque 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.

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 Leve/Agreements)**. En ellos se definen los compromisos de ambas partes.

Estos acuerdos deben contener cláusulas 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.**

## 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

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.

**Tabla 1. 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 pick de trabajo, solicitará 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 destinado 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.  |

## 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.

|  |
| --- |
| **VENTAJAS** |
| **Ahorro de costos** | Este ahorro se debe a la reducción de los costos 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 pick pagaremos más. Esto supone un ahorro en la infraestructura que tendríamos que comprar si queremos cubrir esos picks |
| **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 |

**Tabla 2. Ventajas e Inconvenientes de los servicios en la nube**

|  |
| --- |
| **INVONVENIENTES** |
| **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 condicionado a que tengamos acceso a internet. Si no tenemos acceso por algún motivo, no tendremos acceso a las aplicaciones |

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



## 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 costos
* 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.

## PLATAFORMA COMO SERVICIO

En los servicios del tipo **Paas** el proveedor entrega una plataforma al cliente con el hardware, el sistema operativo y el middleware2 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 contraten 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 lntelligence)** 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
 |

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

## INFRAESTRUCTURA COMO SERVICIO

En los servicios del tipo loas 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.

## 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.

## 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 costos
* 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.

## SERVICIOS EN NUBE PRIVADA

Son servicios en los que los recursos se entregan de forma exclusiva, privada, al cliente, al que se le 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 costo
* 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.

## SERVICIOS CON 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 costos
 | * 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** en 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.

## 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 de 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 **(laaS)** 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 ejecutarán 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 migramos 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 como 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.

## 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 lag**, 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

## 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.
* **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 del 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 suplantando, 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.

## 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.

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 tener­ los 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.
* **lndisponibilidad 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.