

La nube

1. Introducción

Migrar a la **nube**, o **cloud computing**, se está convirtiendo para las empresas en algo común, debido a que aumenta la velocidad de los procesos. De este modo, las compañías de cualquier sector, aparte de volverse más innovadoras, se hacen más ágiles. Esta tecnología no solo aumenta la potencia, las aplicaciones y el almacenamiento, sino que transforma por completo la forma de comunicarse y colaborar de los trabajadores.

Toma nota: Una de las ventajas de migrar a la **nube** es la escasa inversión necesaria en el primer momento para obtener servicios seguros. En principio, es el proveedor del servicio el que se encarga de dotar de **seguridad** al sistema y de mantener los equipos.

Los responsables de muchas empresas se dan cuenta en poco tiempo de que, utilizando **cloud computing**, sus sistemas se ven mejorados. Alrededor del **80%** tienen una visión positiva de esta tecnología durante los seis primeros meses tras la implantación. Entre sus ventajas o beneficios, destacan los que siguen:

- No es necesario adquirir ningún hardware, dado que el proveedor del servicio se hace cargo de ello. Además, se puede mejorar (upgrade) o empeorar (downgrade) el servicio cambiando la configuración del cliente.
- Para las empresas, este tipo de servicio es sumamente rentable, porque no hace falta llevar a cabo una inversión inicial en servidores o **centros de datos**. En ocasiones, estas inversiones empiezan a rentabilizarse más tarde, mientras que los sistemas cloud son ventajosos desde el minuto uno.
- Las empresas que ofrecen servicios cloud pueden ofrecer precios muy competitivos, porque se benefician de la **economía a gran escala**. Cuantos más clientes tenga la compañía, más baratos puede ofertar los servicios.
- No es necesario disponer de equipos que consuman electricidad las veinticuatro horas, todos los días. Tampoco hace falta que la compañía cuente con un gran centro de procesamiento de datos, ni con oficinas sobredimensionadas.
- Se facilitan la **deslocalización** y el **teletrabajo**. Las aplicaciones en la **nube** son ideales para este tipo de sistema productivo.
- Cuando se teletrabaja, las **latencias** y el acceso son más rápidos que cuando los servidores y el servicio se hallan en la propia compañía.



2.Cloud o nube. Niveles y funciones

Las empresas eligen el tipo de servicio en la **nube** dependiendo de sus necesidades. Existen empresas que necesitan tener un control más riguroso de los datos y, para obtenerlo, eligen un tipo de servicio **IaaS**. Otras empresas prefieren entregar el control de la infraestructura, los sistemas operativos y el software al proveedor de servicios; estas compañías se ocupan únicamente del negocio y, por ello, utilizan un servicio **SaaS**.

Recurso web: Los servicios en la **nube** se distribuyen en los modelos **IaaS**, **PaaS** y **SaaS**. Mira el siguiente vídeo, accesible mediante el código QR, para conocer estos modelos en profundidad.

A continuación, se explicarán este tipo de servicios y otros intermedios. Ninguno es mejor que otro; la elección dependerá de las necesidades de la empresa y de sus objetivos a la hora de implementar el **cloud computing**.

2.1. Tipos de servicios en la nube y su aplicación práctica

Existen cuatro tipos principales de servicios en la **nube**, en función de las necesidades de las empresas, que se decantarán por uno u otro dependiendo del grado de descentralización informática que precisen (figura 3.1).

A) IaaS (infrastructure as a service)

La infraestructura como servicio es el sistema que proporciona mayor flexibilidad, dado que da acceso a las características de la red, los equipos —ya sean virtuales o dedicados— y las bases de datos.

Ejemplo: Netflix, la empresa líder mundial en streaming de contenido audiovisual, utiliza servicios **IaaS** a través de **Amazon Web Services (AWS)** para mantener y escalar su infraestructura tecnológica. Aunque los servidores físicos, el almacenamiento y las redes son propiedad del proveedor, es el personal técnico de Netflix quien **administra los sistemas operativos, las aplicaciones y las bases de datos**, ajustando la capacidad según la demanda de los usuarios. Este modelo le permite disponer de una infraestructura global altamente flexible y fiable sin necesidad de poseer centros de datos propios.



B) PaaS (platform as a service)

En el caso de la plataforma como servicio, el usuario no tiene que administrar el sistema operativo o el hardware. Es el cliente quien se encarga de instalar aplicaciones, administrarlas y usarlas a su antojo. Si usamos el símil del coche, el usuario solamente echa gasolina y conduce.

Ejemplo: Coca-Cola utiliza servicios **PaaS** mediante **Google App Engine** para ejecutar aplicaciones y campañas interactivas sin tener que gestionar servidores ni sistemas operativos. En este modelo, el proveedor se encarga de toda la infraestructura y del entorno de ejecución, mientras que Coca-Cola se centra en desarrollar y administrar las aplicaciones. Gracias a esta solución, la empresa puede desplegar nuevas herramientas digitales con rapidez y fiabilidad en todo el mundo.



C) SaaS (software as a service)

Con esta opción, es el proveedor el que se encarga de instalar y mantener las aplicaciones, y el usuario simplemente las utiliza. Este último no necesita administrar el servicio, dado que el proveedor ya lo hace por él. Son ejemplos de este servicio un webmail para la empresa o un sistema de contabilidad online. Muchos usuarios que contratan servicios en la **nube** lo hacen bajo este sistema, puesto que resulta más cómodo y económico, al no tener que conseguir personal especializado; simplemente utilizan el software y disponen del soporte de la compañía que proporciona el servicio. Según Exploding Topics, actualmente el sistema **SaaS** supone un tercio del gasto total en los servicios en la **nube**.

Ejemplo: Toyota emplea la plataforma **Salesforce**, un servicio **SaaS** especializado en la gestión de relaciones con clientes. En este modelo, el proveedor se encarga de instalar, mantener y actualizar el software, mientras que Toyota solo necesita acceder a la aplicación a través de internet para gestionar información de ventas y atención al cliente. Este sistema les permite reducir costes de mantenimiento y aumentar la eficiencia de sus operaciones comerciales.



D) CaaS (container as a service)

En relación con los contenedores como servicio, se desarrollan y despliegan aplicaciones mediante contenedores. El entorno para crear aplicaciones es gestionado por el proveedor de servicios en la **nube**, y los desarrolladores pueden utilizar los **CaaS** para desarrollar y ejecutar aplicaciones sin preocuparse por la infraestructura o la plataforma.

Ejemplo: Spotify utiliza servicios **CaaS**

a través de **Google Kubernetes Engine (GKE)**, lo que le permite desplegar y administrar aplicaciones en contenedores de forma ágil y escalable. En este modelo, **Google Cloud** proporciona la infraestructura y las herramientas necesarias, mientras que los ingenieros de Spotify gestionan los contenedores y las aplicaciones que ejecuta la empresa. Gracias a esta arquitectura, Spotify puede ofrecer un servicio continuo, estable y adaptado a millones de usuarios en todo el mundo.



Hay tantos tipos de implementación en la **nube** como necesidades pueda tener una empresa. Por ejemplo: si la **nube** es pública, la empresa tendrá todas las aplicaciones alojadas en ella, ya sean creadas desde cero o migradas desde su infraestructura local; si la **nube** es híbrida, la empresa tendrá aplicaciones tanto de forma local como en la **nube**. Existe otro modelo, llamado **on-premise** —o **nube** privada—, en el que la **nube** se asemeja más a una infraestructura local, porque no es compartida con otros clientes u otras compañías.

Sabías que...

AWS (Amazon Web Services) es la **nube** más grande que existe actualmente, y ofrece más de doscientos tipos de servicios a sus clientes. Los países que más utilizan la **nube**, según BSA Global **Cloud Computing** Scorecard, son Alemania, Japón y Estados Unidos, mientras que los que menos lo hacen son Rusia, China, Vietnam e Indonesia.

Para las empresas menos pudientes o tecnológicamente menos avanzadas, existe la **nube** comunitaria, que es una infraestructura compartida por organizaciones del mismo sector, la cual permite reducir los costes individuales y aumentar la **seguridad**, al proteger datos conjuntos.

3. Trabajo en la nube y nuevos perfiles profesionales

El trabajo móvil es ya una realidad en prácticamente la mayoría de las empresas. En muchas compañías, no es necesaria la presencialidad para realizar el trabajo del día a día. Una consecuencia de ello es la pérdida de ciertos puestos de trabajo clásicos para dar cabida a otro tipo de perfiles profesionales.

En cuanto a la informática, muchos de los problemas de los sistemas **on-premise** antiguos, como los relativos a la **seguridad**, la rigidez de uso o el rendimiento remoto, son solventados mediante las nuevas aplicaciones **SaaS**. Con ellas, técnicos de empresas especializadas velan tanto por la **seguridad** como por el rendimiento. Además, se añaden funcionalidades que proporcionan a los clientes una experiencia de usuario más gratificante.



Te proporcionamos una lista con los nuevos empleos relacionados con el trabajo en la nube:

- **Arquitecto cloud:** Tiene experiencia en migración de servicios **on-premise** a la **nube**, y es capaz de proponer y poner en funcionamiento una infraestructura cloud para cualquier empresa.
- **Ingeniero cloud:** Conoce los principales servicios cloud, como **Amazon Web Services (AWS)**, **Microsoft Azure**, **Oracle Cloud** o **Google Cloud Platform (GCP)**. Entre sus tareas está diseñar aplicaciones en la **nube**.
- **Desarrollador cloud:** Crea aplicaciones cloud para los clientes, siguiendo los pliegos de condiciones y especificaciones que estos imponen. Trabaja de forma coordinada con los demás profesionales de la **nube**.



• **Arquitecto de datos cloud:** Es el responsable de la gestión de datos en las bases de datos cloud —como MongoDB, por ejemplo— y de su procesamiento. Parte de su trabajo consiste en realizar analíticas e informes para luego tomar decisiones.

• **Ingenieros DevOps:** Tienen conocimientos de Docker, Kubernetes, Jenkins, etc. Se encargan de gestionar los servidores y contenedores cloud de la empresa, integrando y automatizando

procesos de desarrollo y operaciones. Realizan la supervisión y la optimización de los sistemas cloud de la empresa.

- **Data scientist:** Elabora modelos predictivos mediante machine learning y otras técnicas, lo que permite a la empresa obtener ventajas competitivas. Maneja herramientas como TensorFlow y PyTorch, y lenguajes como R y Python.

4. Edge computing

El **edge computing**, o computación en el borde, es un tipo de arquitectura que complementa al **cloud computing**. Mientras que en el cloud los datos se procesan en grandes **centros de datos** alejados de donde se generan, el **edge computing** acerca el procesamiento al origen de los datos, es decir, al propio dispositivo o a un servidor cercano.

Este tipo de computación se está volviendo cada vez más importante debido a la expansión de los dispositivos del Internet of Things (IoT), los cuales generan grandes cantidades de información que necesitan ser procesadas casi en tiempo real.

Ejemplo: Un coche autónomo no puede depender exclusivamente del **cloud computing**, ya que la **latencia** sería demasiado alta. Necesita procesar los datos que recibe de sus sensores al instante, por lo que utiliza **edge computing** para tomar decisiones inmediatas, como frenar ante un obstáculo o mantener la distancia de **seguridad**.



Ventajas del edge computing

- Menor **latencia**: al procesar los datos cerca de su origen, las respuestas son mucho más rápidas.
- Ahorro de ancho de banda: no es necesario enviar toda la información a la **nube**, solo los datos relevantes.
- Mayor fiabilidad: si la conexión a internet falla, los dispositivos pueden seguir funcionando de manera autónoma.



- **Seguridad y privacidad**: los datos sensibles pueden procesarse localmente, reduciendo el riesgo de exposición.

Sabías que...

El **edge computing** se considera el complemento ideal del **cloud computing**. Según la consultora Gartner, para 2025 el 75 % de los datos generados por las empresas se procesará fuera de los **centros de datos** tradicionales o de la **nube**.

5. Cloud híbrido y multicloud

El **cloud híbrido** es una solución que combina **nubes** públicas y privadas, con el objetivo de aprovechar lo mejor de cada una. En este modelo, algunas aplicaciones o servicios se ejecutan en la **nube** pública, mientras que otros, más sensibles o críticos, permanecen en una **nube** privada o en la infraestructura local de la empresa.

Este sistema ofrece flexibilidad, **escalabilidad** y control, ya que las organizaciones pueden decidir qué cargas de trabajo colocar en cada entorno. Por ejemplo, una empresa puede mantener sus bases de datos confidenciales en una **nube** privada, y al mismo tiempo utilizar la **nube** pública para ejecutar aplicaciones de menor riesgo o para aumentar temporalmente su capacidad en momentos de alta demanda.



Ventajas del cloud híbrido

- **Flexibilidad:** permite mover aplicaciones y datos entre distintos entornos según las necesidades del momento.
- **Escalabilidad:** las empresas pueden ampliar o reducir sus recursos fácilmente, sin grandes inversiones.
- Optimización de **costes:** se paga solo por lo que se usa en la **nube** pública, y se aprovecha la infraestructura existente.
- Mayor **seguridad:** los datos más sensibles se mantienen en entornos privados o controlados.
- **Continuidad** del negocio: en caso de fallo de una parte del sistema, otra puede seguir funcionando.

Multicloud

El término **multicloud** hace referencia al uso de varios proveedores de servicios en la **nube** de manera simultánea. En este caso, no se trata de combinar **nubes** públicas y privadas, sino de utilizar diferentes plataformas, como **Amazon Web Services (AWS)**, **Microsoft Azure**, **Google Cloud Platform (GCP)** o **IBM Cloud**, para distintos fines.



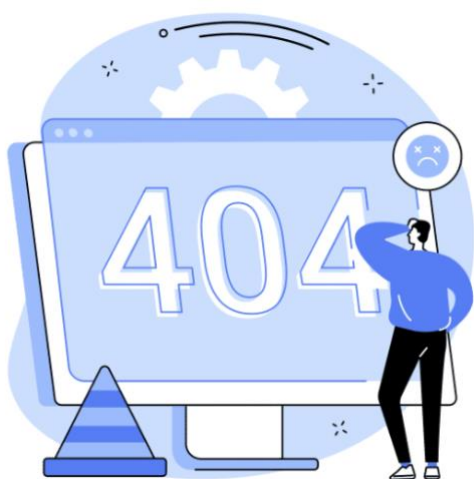
Por ejemplo, una empresa puede usar **AWS** para alojar sus aplicaciones, **Azure** para su base de datos y **GCP** para sus servicios de inteligencia artificial. Esto le permite evitar la dependencia de un único proveedor (**vendor lock-in**), además de optimizar costes y aprovechar las fortalezas específicas de cada plataforma.

Ejemplo: Imaginemos una empresa de comercio electrónico que utiliza una infraestructura híbrida: su página web y su sistema de ventas están alojados en la **nube** pública, pero los datos de los clientes y las operaciones financieras se guardan en una **nube** privada por motivos de **seguridad**. Además, la empresa emplea un entorno **multicloud**: utiliza **AWS** para el alojamiento de la página web, Azure para la gestión de la base de datos y Google Cloud para análisis de comportamiento de usuarios mediante machine learning.

Sabías que...

Según Flexera 2024 State of the Cloud Report, el 89 % de las empresas utiliza actualmente una estrategia de **multicloud**. Esta tendencia demuestra que las organizaciones buscan equilibrio entre **seguridad**, rendimiento y flexibilidad.

5. Seguridad en la nube



Uno de los temas que más preocupa a las empresas cuando adoptan soluciones cloud es la **seguridad** de los datos. A diferencia de los sistemas locales, donde todo se almacena y gestiona internamente, en la **nube** los datos se guardan en servidores de terceros, por lo que resulta fundamental confiar en proveedores que garanticen medidas sólidas de protección.

La **seguridad** en la **nube** implica un conjunto de tecnologías, políticas y procedimientos destinados a proteger los datos, las aplicaciones y la infraestructura frente a amenazas. Los proveedores de servicios cloud invierten enormes recursos en mantener la **seguridad** de sus sistemas, ya que es la base de la confianza de sus clientes.

Principales amenazas en la nube

- Accesos no autorizados: los ciberdelincuentes pueden intentar entrar en los sistemas mediante contraseñas débiles o vulnerabilidades.
- Pérdida o robo de datos: un error humano, un fallo técnico o un ataque informático puede provocar la pérdida de información sensible.
- Fugas de información: compartir recursos en entornos multicliente puede generar riesgos si la segmentación no está correctamente implementada.
- Malware y ransomware: estos ataques pueden cifrar los datos del usuario y exigir un rescate por su recuperación.
- Configuraciones incorrectas: muchas brechas de **seguridad** provienen de errores en la configuración inicial de los servicios cloud.

Medidas de seguridad esenciales

- **Autenticación multifactor (MFA)**: añade una capa adicional de **seguridad** más allá de la contraseña.

- **Cifrado** de datos: tanto en tránsito como en reposo, garantiza que la información solo pueda ser leída por quienes tienen autorización.
- **Copias de seguridad** automáticas: permiten recuperar los datos en caso de incidente.
- **Gestión de identidades y accesos (IAM)**: controla quién puede acceder a qué recursos y en qué condiciones.
- **Monitoreo y auditoría continua**: los proveedores suelen ofrecer herramientas para detectar comportamientos anómalos o accesos sospechosos.
- **Cumplimiento normativo**: las empresas deben asegurarse de que su proveedor cumple el **RGPD** en Europa.

Ejemplo práctico

Philips, la multinacional neerlandesa de tecnología médica, utiliza la plataforma **HealthSuite Digital Platform**, basada en **Amazon Web Services (AWS)**, para gestionar millones de historiales médicos digitales y datos clínicos procedentes de hospitales de todo el mundo.



El sistema aplica **cifrado de extremo a extremo**, **autenticación multifactor** y cumple con estándares internacionales como **ISO/IEC 27001**, **HIPAA** (en EE. UU.) y **RGPD** (en Europa). Gracias al uso de la nube, Philips puede ofrecer servicios de telemedicina, análisis de imágenes médicas y monitorización remota de pacientes con un alto nivel de **seguridad y cumplimiento normativo**.

Responsabilidad compartida

La **seguridad** en la **nube** se basa en un modelo de **responsabilidad compartida**: el proveedor

Sabías que...

Según el *IBM Cost of a Data Breach Report 2024*, el coste promedio de una brecha de datos a nivel global es de **USD 4,88 millones**. Las organizaciones que aplican medidas preventivas como cifrado, automatización de seguridad e inteligencia artificial logran **reducir significativamente** el coste de las brechas.

se encarga de proteger la infraestructura (hardware, red, **centros de datos**, etc.); el cliente debe proteger sus datos, controlar el acceso de los usuarios y configurar adecuadamente los servicios. En otras palabras, el proveedor ofrece las herramientas, pero depende del cliente utilizarlas correctamente.

7. Ventajas y desventajas del cloud computing

La adopción del **cloud computing** ofrece numerosos beneficios para empresas, instituciones y usuarios particulares. Sin embargo, también presenta ciertos inconvenientes que deben considerarse antes de su implementación. A continuación, se detallan las principales ventajas y desventajas de este modelo tecnológico.

Ventajas

- **Ahorro de costes:** no es necesario realizar grandes inversiones iniciales en hardware, mantenimiento o licencias de software.
- **Escalabilidad:** los recursos pueden ampliarse o reducirse fácilmente según la demanda del momento.
- **Accesibilidad:** los datos y aplicaciones pueden consultarse desde cualquier lugar y dispositivo con conexión a internet.
- **Actualizaciones automáticas:** los proveedores se encargan de mantener los sistemas actualizados y seguros sin intervención del usuario.
- **Colaboración y trabajo remoto:** las herramientas en la **nube** permiten trabajar en equipo en tiempo real.
- **Seguridad y respaldo:** la mayoría de los servicios ofrecen **copias de seguridad** automáticas y recuperación ante desastres.
- **Sostenibilidad:** al optimizar los recursos y reducir equipos físicos, disminuye el consumo energético y la huella de carbono.



Desventajas

- **Dependencia** de internet: sin conexión, no se puede acceder a los servicios ni a los datos almacenados.
- **Costes** a largo plazo: aunque la inversión inicial es baja, los pagos por suscripción pueden acumularse.
- **Seguridad** y privacidad: al almacenarse en servidores externos, pueden surgir problemas si no se elige bien al proveedor.
- **Menor control:** el usuario depende de las políticas, disponibilidad y actualizaciones del proveedor.
- **Latencia:** en algunos casos, el acceso puede ser más lento que en sistemas locales.
- **Migración compleja:** trasladar datos o aplicaciones a la **nube** o entre **nubes** puede requerir tiempo y personal especializado.

Ejemplo: Una empresa de marketing digital que decide migrar sus sistemas a la **nube** reduce significativamente sus gastos en servidores y mantenimiento. Además, su equipo puede trabajar desde cualquier lugar y colaborar en tiempo real. No obstante, durante la transición deben reforzar la **seguridad** de los datos de sus clientes y garantizar el cumplimiento del **RGPD**.

8. Principales proveedores de Cloud

El mercado de la computación en la **nube** está dominado por un grupo de grandes empresas tecnológicas que ofrecen una amplia gama de servicios, desde infraestructura hasta aplicaciones especializadas. A continuación, se presentan los principales proveedores y sus características más destacadas.

1) Amazon Web Services (AWS)

Es el líder mundial en servicios de **cloud computing**. Ofrece más de doscientos servicios diferentes que incluyen almacenamiento, bases de datos, análisis, inteligencia artificial y herramientas de desarrollo. **AWS** destaca por su fiabilidad, **seguridad** y amplia red global de **centros de datos**, además de su modelo de precios pay-as-you-go.

Ejemplo de uso: Netflix utiliza **AWS** para gestionar su infraestructura global, transmitir contenido a millones de usuarios y analizar grandes volúmenes de datos en tiempo real.

2) Microsoft Azure

Es el segundo proveedor más importante a nivel mundial. Integra de forma nativa los productos de Microsoft, como Windows Server, Office 365 o Dynamics. Azure ofrece soluciones tanto para entornos **híbridos** como **multicloud**, lo que la convierte en una opción muy atractiva para empresas que ya trabajan con tecnología Microsoft.

Ejemplo de uso: Volkswagen emplea Azure para conectar y analizar datos de sus vehículos, optimizando la **seguridad** y el mantenimiento predictivo.

3) Google Cloud Platform (GCP)

Google Cloud se especializa en análisis de datos, machine learning e inteligencia artificial. Su infraestructura se basa en la misma tecnología que utiliza Google para sus propios servicios, lo que garantiza alta disponibilidad y rendimiento.

Ejemplo de uso: Spotify usa Google Cloud para gestionar el análisis de comportamiento de los usuarios y ofrecer recomendaciones personalizadas.

4) IBM Cloud

Combina servicios públicos y privados con una fuerte orientación hacia el sector empresarial. Es conocida por su integración con sistemas de inteligencia artificial a través de IBM Watson y su soporte para tecnologías de blockchain y **edge computing**.

Ejemplo de uso: American Airlines utiliza **IBM Cloud** para mejorar la experiencia del cliente mediante chatbots inteligentes y análisis de datos en tiempo real.

5) Oracle Cloud

Ofrece una plataforma completa de servicios empresariales, con especial enfoque en bases de datos, aplicaciones ERP y soluciones de inteligencia empresarial. Su fortaleza está en la gestión avanzada de datos y la integración con entornos corporativos complejos.

Ejemplo de uso: Zoom confía en **Oracle Cloud** para manejar picos de tráfico durante videoconferencias masivas, garantizando estabilidad y rendimiento.

6) Alibaba Cloud

Es el principal proveedor en Asia y uno de los cinco mayores del mundo. Ofrece servicios de big data, inteligencia artificial y almacenamiento masivo, y ha experimentado un rápido crecimiento gracias al comercio electrónico y a su expansión internacional.

Ejemplo de uso: Las plataformas de compras del grupo Alibaba, como Taobao y Tmall, funcionan sobre su propia infraestructura en la **nube**, lo que permite manejar millones de transacciones simultáneamente.

Sabías que...

Según el informe Synergy Research Group (2024), **AWS** mantiene cerca del **31 %** del mercado global, seguido de **Microsoft Azure** (**25 %**), Google Cloud (**12 %**), e IBM, Oracle y Alibaba completan el resto.

9. Tendencias actuales y futuro del cloud computing

La computación en la **nube** sigue evolucionando a gran velocidad y adaptándose a las nuevas demandas tecnológicas, sociales y empresariales. Las tendencias actuales muestran un futuro en el que la **nube** será aún más inteligente, sostenible y descentralizada.

1) Inteligencia artificial y machine learning integrados

Los servicios cloud están incorporando de forma creciente herramientas de inteligencia artificial (IA) y aprendizaje automático (machine learning) para automatizar procesos, analizar grandes volúmenes de datos y ofrecer predicciones en tiempo real. Las empresas ya pueden entrenar modelos de IA directamente desde la **nube**, sin necesidad de contar con potentes servidores locales.



2) Sostenibilidad y eficiencia energética

La conciencia medioambiental ha llevado a los grandes proveedores cloud a invertir en **centros de datos** sostenibles. El objetivo es reducir el consumo energético y las emisiones de carbono mediante el uso de energías renovables y sistemas de refrigeración eficientes.

3) Computación cuántica en la nube

Aunque todavía se encuentra en fase experimental, la computación cuántica promete revolucionar la forma de procesar información. A través del **cloud computing**, los usuarios podrán acceder a ordenadores cuánticos de forma remota sin necesidad de disponer de ellos físicamente. Esto permitirá resolver problemas complejos en criptografía, simulaciones químicas o desarrollo farmacéutico.

4) Expansión del edge computing

El crecimiento del Internet of Things (IoT) y de los dispositivos conectados impulsa la combinación de **edge computing** y **cloud computing**. Esta integración busca ofrecer una infraestructura más distribuida, en la que los datos se procesen tanto en el borde como en la **nube**, reduciendo la **latencia** y mejorando la velocidad de respuesta.

5) Serverless computing o computación sin servidor

El modelo **serverless** está ganando popularidad porque permite ejecutar código sin necesidad de gestionar servidores. El proveedor se encarga de toda la infraestructura y el usuario solo paga por el tiempo de ejecución de su aplicación. Esto facilita la creación de aplicaciones escalables, ágiles y rentables.

6) Mayor enfoque en seguridad y soberanía de datos

Con el aumento del uso del cloud, también crece la preocupación por la protección de la información. Por ello, los proveedores están creando **nubes** soberanas, donde los datos se almacenan y procesan dentro de un territorio concreto para cumplir las regulaciones nacionales o regionales (como el **RGPD** europeo).

7) Multicloud inteligente

Cada vez más empresas combinan varios proveedores de servicios para aprovechar las ventajas de cada uno. El futuro apunta hacia plataformas que gestionen automáticamente diferentes **nubes** desde una sola interfaz, optimizando costes, rendimiento y **seguridad**.

Repasa lo aprendido

- La nube: servicios informáticos ofrecidos a través de internet.
- Ventajas: menor inversión, seguridad gestionada, ahorro energético, teletrabajo.
- 80 % de las empresas valoran positivamente la nube tras su implantación.

2. Niveles y funciones

- IaaS: infraestructura virtual (Netflix – AWS).
- PaaS: entorno para desarrollar apps (Coca-Cola – Google App Engine).
- SaaS: software online (Toyota – Salesforce).
- CaaS: contenedores gestionados (Spotify – Google Kubernetes Engine).
- Tipos de nube: pública, privada, híbrida, comunitaria.

3. Trabajo en la nube

- Favorece el trabajo remoto y nuevos perfiles: arquitecto e ingeniero cloud, DevOps, data scientist.
- Ventajas: reducción de costes, sostenibilidad, retención del talento.

4. Edge computing

- Procesamiento cerca del origen de los datos → menor latencia y mayor seguridad.
- Clave para IoT, coches autónomos y fábricas inteligentes.

5. Cloud híbrido y multicloud

- Híbrido: mezcla nube pública/privada (flexible y segura).
- Multicloud: varios proveedores para evitar dependencia.
- 89 % de las empresas usa multicloud (Flexera 2024).

6. Seguridad en la nube

- Amenazas: accesos no autorizados, pérdida de datos, malware.
- Medidas: MFA, cifrado, copias de seguridad, IAM, cumplimiento RGPD.
- Modelo de responsabilidad compartida (proveedor + cliente).
- Ejemplo: Philips HealthSuite (AWS).

7. Ventajas y desventajas

- Ventajas: ahorro, escalabilidad, accesibilidad, sostenibilidad.
- Desventajas: dependencia de internet, costes acumulativos, privacidad.

8. Principales proveedores

- AWS (Netflix), Azure (Volkswagen), GCP (Spotify), IBM Cloud (American Airlines), Oracle Cloud (Zoom), Alibaba Cloud.

9. Tendencias futuras

- IA y *machine learning* integrados.
- Sostenibilidad y energía renovable (2030).
- Computación cuántica y *serverless*.
- Nubes soberanas y multicloud inteligente.

