

---

# **Almacenar, compartir y procesar datos a través de las redes de computadores**

---

PID\_00279841

Lorenza Giupponi  
Toni Adame



---

Universitat  
Oberta  
de Catalunya

---

**Lorenza Giupponi**

Ingeniera de Telecomunicaciones por la Universidad de Roma La Sapienza y doctora por el departamento de Teoría de la Señal y Comunicaciones de la Universidad Politécnica de Cataluña. Se unió en el año 2003 al grupo de comunicaciones móviles de la UPC con una beca del programa Formación Profesorado Universitario. Durante 2006 y 2007 fue profesora ayudante en la UPC. En 2007 se unió al Centro Tecnológico de Telecomunicaciones de Cataluña (CTTC), donde actualmente es investigadora sénior en el departamento de Redes Móviles. Además, desde 2007 es directora de relaciones institucionales del comité de dirección del CTTC. Ha recibido premios al mejor artículo de la conferencia en tres ocasiones, entre ellas IEEE CCNC 2010, IEEE WCNC 2018. Dos de sus *transactions* han sido listados por IEEE Comsoc entre las mejores lecturas en el área de la gestión de recursos radio y de la radio cognitiva. Desde 2015 es miembro del comité ejecutivo de ns-3, responsable del área Long Term Evolution (LTE) y del área New Radio (NR). Ha liderado y participado en múltiples proyectos nacionales, europeos o financiados por empresas internacionales.

**Toni Adame**

Ingeniero superior de telecomunicaciones por la Universidad Politécnica de Cataluña (UPC). Ha trabajado durante varios años en el sector privado como consultor preventa en el ámbito de la integración de sistemas y tecnologías. Desde 2013 pertenece al grupo de investigación Network Technologies and Strategies (NeTS) de la Universidad Pompeu Fabra (UPF), donde ejerce como investigador sénior en proyectos europeos y nacionales que promueven el uso de tecnologías de comunicación inalámbricas (WSN, Wi-Fi, LPWAN, redes celulares y RFID) como habilitadoras del internet de las cosas (IoT). Sus áreas de investigación se focalizan en las comunicaciones de acceso múltiple, los protocolos de acceso al medio y los mecanismos de ahorro energético. Desde 2017 también es profesor asociado en la UPF, donde ha impartido clases en los diferentes grados del ámbito de la ingeniería.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por la profesora: Cristina Cano Bastidas

Primera edición: febrero 2021

© de esta edición, Fundació Universitat Oberta de Catalunya (FUOC)

Av. Tibidabo, 39-43, 08035 Barcelona

Autoría: Lorenza Giupponi, Toni Adame

Producción: FUOC

Todos los derechos reservados

*Ninguna parte de esta publicación, incluyendo el diseño general y la cubierta, puede ser copiada, reproducida, almacenada o transmitida de ninguna forma ni por ningún medio, sea este eléctrico, químico, mecánico, óptico, grabación, fotocopia, o cualquier otro, sin la previa autorización escrita de los titulares de los derechos.*

# Índice

<b>Introducción</b>	5
<b>1. ¿Qué es el <i>cloud computing</i>?</b>	6
1.1. Las tecnologías habilitadoras del <i>cloud computing</i>	6
1.2. Los servicios del <i>cloud computing</i>	8
1.3. La geografía del <i>cloud</i> : <i>cloud</i> , <i>fog</i> y <i>edge computing</i>	9
1.4. El <i>cloud computing</i> y la gestión de los datos.	11
<b>2. <i>Cloud computing</i> y las redes de computadores</b>	13
2.1. Los requisitos de las redes para habilitar el <i>cloud computing</i>	14
2.2. La virtualización de la red y su nueva gestión elástica.	15
2.2.1. La virtualización de las funciones de red o NFV	16
2.2.2. Las redes definidas por <i>software</i> o SDN.	16
<b>3. Otros retos: gasto energético y seguridad</b>	18
3.1. La seguridad en el <i>cloud</i>	18
3.2. El gasto energético	19
<b>4. <i>Cloud computing</i> para aplicaciones IoT</b>	20
<b>5. Ejemplo de aplicación IoT: cerrando el círculo del ciclo de vida de los datos</b>	22
<b>Ejercicios de autoevaluación</b>	24
<b>Solucionario</b>	25
<b>Glosario</b>	26
<b>Bibliografía</b>	27

## Introducción

En esta asignatura recorreremos todo el ciclo de vida de los datos desde el punto de vista de las redes de computadores.

En el «**Reto 1. ¿Cuál es el papel de las redes de computadores en el ciclo de vida de los datos?**» se ha presentado una introducción a las funciones que desempeñan las redes en las diferentes fases de cualquier aplicación o servicio basado en la transmisión y el procesamiento de datos.

A continuación, en el «**Reto 2. Las redes de computadores como generadoras de datos**», se han presentado las tecnologías que permiten la generación de datos. Se ha introducido el paradigma de Internet de las cosas (IoT), hemos hablado de las redes de sensores, fundamentales para la generación de datos, así como de los drones, que también pueden actuar como sensores remotos. En el mismo reto hemos introducido las diferentes opciones que existen respecto a las tecnologías de acceso inalámbrico, que facilitan una infinidad de casos de uso de recogida de datos, y hemos visto que las redes mismas pueden generar datos a partir sus propios protocolos de funcionamiento o de sus usuarios.

En el «**Reto 3. Las redes como medio para obtener datos**», hemos presentado las redes de computadores como una herramienta para extraer datos de redes externas, ya sea a través de APIs (*application programming interface*) o protocolos específicamente diseñados para tal fin.

En este documento, cerramos el círculo, y nos centramos en el paradigma que permite que los datos se puedan almacenar, compartir y luego procesar, remotamente. Complementaremos la información presentada en el resto de los recursos de este reto, introduciendo conceptos básicos del *cloud computing*, qué servicios puede ofrecer, qué retos presentan las redes para ofrecer dichos servicios, y discutiremos sobre las diferentes opciones de despliegue, con énfasis en las arquitecturas descentralizadas y novedosas basadas en el *fog* y el *edge computing*. Descubriremos la importancia de las redes de computadores para poder hacer realidad el concepto de *cloud computing* y los cambios revolucionarios que se están llevando a cabo en el ámbito de la gestión de red para aprovechar al máximo sus beneficios potenciales en entornos heterogéneos. Discutiremos sobre los principales retos funcionales actuales asociados a esta tecnología, como la seguridad y el gasto energético. Finalmente, estudiaremos los retos adicionales que la implementación del paradigma del IoT impone sobre la arquitectura del *cloud*.

## 1. ¿Qué es el *cloud computing*?

El *cloud computing* (computación en la nube) es un nuevo modelo de gestión de los datos y de la información, que permite el almacenamiento, el acceso y el procesamiento de los datos bajo demanda. Los usuarios usan los servicios ofrecidos por el *cloud* (la nube), según sus necesidades específicas, y pagan por el servicio que reciben y el uso que le dan, sin necesidad de desplegar o mantener una infraestructura de forma permanente. En este caso, el modelo económico prevé que las inversiones de capital en infraestructura y en mantenimiento sean asumidas por un proveedor de servicios, que las reparte entre los diferentes usuarios que subscriben el servicio. El usuario usa el servicio que contrata y no tiene que preocuparse de cómo se implementa la prestación del servicio que recibe.

El *cloud computing* ofrece a sus usuarios recursos a diferentes niveles: computacionales, de almacenamiento, de red, etc. Estos recursos se ofrecen sobre Internet, mediante mecanismos de abstracción y gestión dinámica, que hacen que el usuario reciba un servicio que proporciona una experiencia similar a la que tendría si estos recursos se encontrasen en máquinas físicas locales. El nombre *cloud* se utiliza para indicar que el complejo sistema que opera detrás de los servicios recibidos por el usuario, interconectando servidores a través de redes y soportando movimientos de datos, se abstrae de la infraestructura tecnológica mediante varias técnicas de virtualización, como si estuviera en una *nube*. Siempre que consultas tu correo web, entras en Facebook o miras una película en Netflix, en realidad, te estás conectando al servidor en el *cloud* que ofrece este servicio y que realiza por ti las operaciones necesarias para que tú puedas acceder al contenido y usar el servicio de manera transparente.

En el resto de esta sección conoceremos las diferentes tecnologías que han hecho posible desarrollar la tecnología del *cloud computing*, los servicios que puede ofrecer el *cloud computing* así como las arquitecturas de *fog* y *edge computing* y finalmente el rol del *cloud computing* en la gestión de los datos.

### 1.1. Las tecnologías habilitadoras del *cloud computing*

La tecnología del *cloud computing* se ha hecho viable gracias a los avances en múltiples áreas de conocimiento, y en particular es el resultado de la convergencia de tres tecnologías:

- la **gestión de la red**,
- la **computación distribuida**,
- la **virtualización del hardware**.

La **gestión de red** es el conjunto de operaciones que se encargan de hacer un uso eficiente de una red y de sus recursos, en función de ciertos objetivos de diseño o de prestaciones.

La **computación distribuida** es un área de conocimiento en el ámbito de la informática que se dedica a estudiar el modo en el que sistemas distribuidos, formados por muchos ordenadores independientes y autónomos, operan para alcanzar un objetivo común, y lo hacen interactuando a través de una red.

La **virtualización del hardware** es uno de los grandes avances informáticos que permite hoy en día ahorrar muchos recursos de *hardware*. En particular, la virtualización, mediante un *software* llamado *hipervisor*, permite generar entornos simulados y recursos dedicados, como CPU (*central processing unit*), RAM (*Random Access Memory*), disco duro, etc., a partir de un único *hardware* físico. Vamos a ver un sencillo ejemplo: imagina que tienes un disco duro de 1000 GB en el que gracias a la virtualización puede crearse un disco duro virtual de unos 100 GB. Dicho disco duro virtual podría usar un sistema operativo diferente, por ejemplo Linux. Además, una porción de RAM del *hardware* original podría también dedicarse al nuevo sistema operativo.

El hipervisor permite dividir el sistema físico en entornos separados, independientes y seguros, que se llaman máquinas virtuales. El hipervisor opera por encima del *hardware* físico, extrae y separa los recursos de la máquina. Esto permite que, con un solo servidor, podamos generar muchas máquinas, lo que representa un ahorro en *hardware* físico y diseños de sistemas escalables.

El *cloud computing* no existiría sin la virtualización del *hardware*, aun así, el concepto de *cloud* es más complejo, y requiere que los recursos virtuales se coordinen con un *software* de gestión y automatización. En particular, los usuarios acceden a los recursos a través de servidores virtuales distribuidos. Estos recursos virtuales pueden moverse entre múltiples servidores físicos, de manera que los recursos disponibles, en términos de CPU, memoria y capacidad de almacenamiento, se ajusten dinámicamente para satisfacer la demanda de los usuarios y los requisitos del tráfico. Por lo tanto, los usuarios se ven incentivados a externalizar servicios y aplicaciones a proveedores *cloud*, ya que supone un abaratamiento de los costes debido a la eficiencia que proporciona el *cloud* al adaptarse dinámicamente a las necesidades. Es decir, si muy puntualmente necesitamos procesar datos en un disco duro de 1000 GB pero la mayor parte del tiempo solo necesitamos uno de 1 GB, no es necesario pagar por uno de 1000 GB, sino que resulta más económico usar el *cloud* y que nos

#### Hipervisor de red

Un hipervisor es el *software* que genera y ejecuta máquinas virtuales. Gestiona los recursos (CPU, memoria, almacenamiento, etc.) como un conjunto para asignarlos a las máquinas virtuales.

Más detalles sobre las bases del *cloud computing*, los hipervisores y los servicios que puede ofrecer el *cloud* se presentan en el primer capítulo del documento *Fundamentos y plataformas de cloud computing*.

proporcione esa capacidad de procesamiento únicamente durante el tiempo que la necesitamos

## 1.2. Los servicios del *cloud computing*

Como hemos visto, los servicios *cloud* consisten en utilizar remotamente componentes de *software* y *hardware* de terceros, de manera segura y fiable, y a bajo coste. Estos servicios normalmente se despliegan en los *data centers*, constituidos por numerosos servidores. Los *data centers* tienen que ser escalables respecto a la velocidad de datos y los tiempos de procesamiento que ofrecen, manteniendo al mismo tiempo limitado el coste de despliegue y el gasto energético.

Según el nivel de control requerido por el usuario, o el nivel que el proveedor de servicios *cloud* quiera ofrecer a sus clientes, se definen tres tipos principales de servicios *cloud*:

- El **software como servicio** (*software as a service* - SaaS): Un sistema SaaS ofrece a los clientes el acceso a aplicaciones que han sido desplegadas por el proveedor de servicios *cloud*. Los clientes acceden al servicio a través de Internet, con un simple navegador web. El *software* está controlado por el proveedor, y el cliente solo tiene acceso a la aplicación que no se ejecuta localmente. Un ejemplo son los proveedores de correo electrónico. Este modelo permite una rápida puesta en marcha y un mantenimiento a cargo del gestor del *cloud*. Entre los inconvenientes de este modelo hay la cesión total de los datos, la constante necesidad de una conexión a Internet segura, la posibilidad de rescisión del servicio, etc.
- La **plataforma como servicio** (*platform as a service* - PaaS): El sistema PaaS ofrece el servicio de la infraestructura (servidores, almacenamiento, redes) y de las herramientas de desarrollo. En este caso, a diferencia del servicio SaaS, el cliente tiene acceso a la aplicación y a la configuración del sistema según sus necesidades. A través de una API puede, por ejemplo, ajustar dinámicamente los recursos de computación (la memoria o el espacio de almacenamiento) de acuerdo con sus requisitos. El PaaS permite ahorrar en el coste de compra de la infraestructura y de la administración de las licencias de *software*.
- La **infraestructura como servicio** (*infrastructure as a service* - IaaS): Finalmente, el sistema IaaS ofrece a los usuarios el control de las máquinas virtuales, de modo que es el cliente quien las administra y puede llegar a elegir, por ejemplo, el sistema operativo de cada máquina virtual. El servicio IaaS escala según las necesidades del cliente, lo que permite pagar solo para lo que se use.

### 1.3. La geografía del *cloud*: *cloud*, *fog* y *edge computing*


En general, el *cloud computing* prevé una arquitectura centralizada. No obstante, dicha arquitectura no siempre es la más adecuada para todas las aplicaciones, como por ejemplo para aquellas que requieran baja latencia y cercanía en la gestión de los datos, las que necesiten una arquitectura escalable ante un crecimiento inesperado del número de usuarios, o aquellas en las que los datos requieran especial privacidad. Para dar respuesta a estas circunstancias, se han introducido dos paradigmas diferentes, basados en arquitecturas más distribuidas, el *fog* y el *edge computing*. El *fog* y el *edge computing* se encargan de extender la arquitectura y los servicios del *cloud* a los extremos de la red, más cerca del usuario final.

En el *edge computing* el procesamiento de los datos se realiza en el dispositivo mismo, o en un nodo cercano a los dispositivos. Por otro lado, el *fog computing* representa una solución intermedia entre *cloud* y *edge*, y presta servicio a grupos de usuarios finales de forma colaborativa, moviendo el procesamiento a nodos conectados a una red de área local, y que por eso resultan más lejanos de los dispositivos.

Gracias a esta proximidad al usuario final, el *fog/edge computing* tiene la potencialidad de ofrecer servicios caracterizados por una baja latencia. En particular, en aplicaciones en tiempo real centradas en el *cloud*, por ejemplo en entornos IoT, el retardo introducido por el envío de los datos de los sensores/dispositivos al *cloud*, más el retardo introducido por el *cloud* al procesar los datos de manera centralizada y devolverlos a los extremos de la red, puede llegar a ser de muchos minutos, lo que puede resultar inaceptable para ciertas aplicaciones. Imaginaros, por ejemplo, tener que esperar ese tiempo en una aplicación de coches inteligentes para prevenir un accidente.

Las razones que justifican el diseño de una arquitectura más descentralizada, además de reducir el retardo de red y ofrecer mejores servicios en tiempo real, también se deben a la necesidad de protección de los datos, que no deja de presentarse como un reto durante el envío de los datos al *cloud* y en el *cloud* mismo. En el *fog computing*, los datos quedan distribuidos entre diferentes nodos, lo que reduce el riesgo de manipulación en comparación con las arquitecturas centralizadas. En el caso del *edge*, los datos quedan en el mismo dispositivo o en un nodo próximo, que según las circunstancias puede considerarse un valor añadido en términos de seguridad. Finalmente, el *cloud* requiere una conexión a Internet constante, mientras que el *fog* y el *edge* pueden funcionar incluso sin Internet, de manera que resultan más adecuados para aplicaciones en las que los dispositivos no tienen acceso a Internet de forma continua.

Respecto al *fog* y al *edge*, el *cloud* ofrece en general mayores capacidades computacionales, de almacenamiento y de comunicación, por lo que resulta más



El concepto de IoT se introduce en el documento *Las redes de computadores como generadoras de datos*, asociado al reto 2.



adecuado para análisis de mayores volúmenes de datos. Por otro lado, el *edge* y el *fog* son más apropiados cuando se necesita un análisis más rápido. En particular, para el caso de aplicaciones IoT, *fog* y *edge computing* se posicionan como las mejores arquitecturas de red debido a las siguientes características:

- **Localización:** Los recursos de *fog* o *edge computing* se ubican entre los objetos inteligentes que generan datos y el *data center* ubicado en el *cloud*, proporcionando mejores prestaciones en términos de retardo.
- **Distribución:** Los *data centers* usados en los esquemas de *fog* y *edge computing* suelen tener menores capacidades de almacenamiento, procesamiento y comunicación que los del *cloud computing*. Dichos *data centers* pueden desplegarse más cerca del usuario final y con mayor densidad, ya que su coste es típicamente una pequeña fracción en comparación con los *data centers* ubicados en el *cloud*.
- **Escalabilidad:** *Fog* y *edge computing* permiten a la red ser más escalable. En escenarios IoT, donde el número de usuarios finales puede crecer exponencialmente, también lo hace el número de *data centers fog* o *edge* que es necesario desplegar. Este incremento de capacidad es más complicado de gestionar en un *cloud*, debido a su alto coste.
- **Movilidad:** Los recursos *fog* y *edge* actúan como recursos móviles, porque pueden desplegarse bajo demanda y más cerca del usuario final.
- **Análisis de datos en tiempo real:** El *fog* y el *edge computing* tienen la potencialidad de proporcionar mejores prestaciones en servicios interactivos y en tiempo real.
- **Procesamiento de datos:** Los recursos *fog* y *edge* pueden realizar agregación de datos y enviar al *cloud* datos parcialmente procesados, en vez de datos en bruto extraídos directamente de los dispositivos.

A veces, para proporcionar servicios *cloud* adecuados a un tipo de aplicación y usuarios concretos, incluyendo aplicaciones IoT, puede diseñarse una arquitectura jerárquica basada en *cloud*, *fog* y *edge computing*.

Vamos a ver algunos ejemplos de casos de uso para cada arquitectura.

El *edge computing* es la arquitectura de referencia para aplicaciones que requieren muy baja latencia, como es el caso de los vehículos autónomos o de aplicaciones en el ámbito de las finanzas, donde se requiere procesamiento de datos en tiempo real. Las granjas eólicas son otra posible aplicación que podría beneficiarse del *edge computing*, porque al encontrarse en áreas remotas, no tienen fácil conexión con un *cloud*. Otra aplicación son las fábricas inteligentes. En estos escenarios, se utilizan líneas de producción que realizan un producto pieza por pieza. En estas líneas de producción, el control de calidad es fundamental y requiere de un procesamiento de los datos local.

Los oleoductos y gaseoductos generan terabytes de datos cada año, y pueden ser un área de aplicación del *fog computing*. Puede diseñarse un sistema de comunicación entre nodos de *fog computing* que compartan datos entre ellos, de manera que al *cloud* solo llegue la información relevante y se ahorre mucho ancho de banda. La vigilancia inteligente en áreas de la ciudad es otra aplicación del *fog computing*. Podemos imaginar una red de muchas videocámaras conectadas a través de un enlace óptico, con el procesamiento de los datos distribuido en los nodos del *fog*. La clave en esta arquitectura es la agregación de datos de diferentes nodos para realizar un procesamiento colaborativo.


Finalmente, si hay que hacer un seguimiento del transporte de bienes comerciales, desde los vehículos hasta las mercancías que se han de transportar, el *cloud* es la arquitectura adecuada, porque los datos crecen de manera exponencial, y no se podrían gestionar mediante arquitecturas descentralizadas con menor capacidad de almacenamiento y computacional. Además, las áreas que se han de cubrir en esta aplicación son extensas y no es posible entonces un procesamiento de datos local.

#### 1.4. El *cloud computing* y la gestión de los datos

El uso del paradigma del *cloud computing* está ya ampliamente consolidado, dado que múltiples operadores móviles (como ATT, British Telecom, etc.) y empresas tecnológicas (por ejemplo, Google, Salesforce, Microsoft, Dropbox, Amazon, etc.) ya ofrecen servicios de *cloud*. En el ETSI (*European telecommunication standard institute*) o el ANSI (*American national standard institute*) en EE.UU., hay también en curso diferentes actividades de estandarización.

Una de las aplicaciones importantes del *cloud computing* es su rol fundamental en la gestión de los datos. En el Reto 2 introdujimos el concepto de IoT. La conexión a Internet de un gran número de dispositivos, como sensores, smartphones, ordenadores, etc., genera, como hemos visto en otros retos, la oportunidad de crear una gran cantidad de datos que pueden aportar mucho conocimiento. Es lo que se denomina *big data*.

El *big data* es una tendencia reciente orientada a extraer información y conocimiento a partir de grandes cantidades de datos no estructurados y complejos. La visión e implantación del *big data* requiere la tecnología habilitadora del *cloud computing* para muchos aspectos diferentes: para soportar el almacenamiento de enormes cantidades de datos que sería difícil gestionar localmente, para proporcionar capacidad computacional distribuida y paralela que sería muy costosa desplegar localmente, y para garantizar el acceso privado, eficiente y seguro de una ingente cantidad de dispositivos móviles a datos y servicios heterogéneos, que además requieren sofisticados mecanismos de seguridad y privacidad.



El concepto de IoT se introduce en el documento *Las redes de computadores como generadoras de datos*, asociado al reto 2.

Por todas estas razones, el *cloud computing* es la tecnología clave que proporciona la capacidad computacional, de almacenamiento, las aplicaciones y la capacidad de red necesarias para implementar el *big data*. Existen diferentes plataformas que permiten el procesamiento analítico de grandes cantidades de datos (*big data analytics*), como por ejemplo **Hadoop** y **SciDB**. Estas plataformas, además, evolucionan para habilitar la capacidad de procesamiento en tiempo real que el IoT puede necesitar. A modo de ejemplo, Facebook ha producido una versión avanzada de Hadoop para analizar billones de mensajes cada día y así ofrecer estadísticas en tiempo real de las acciones de sus usuarios.

Por otro lado, las prestaciones del *cloud computing* dependen de las redes de computadores existentes dentro y entre diferentes *data centers*. Las limitaciones o fallos en la infraestructura de red pueden poner en serio peligro las prestaciones de los servicios ofrecidos por el *cloud*. Por esta razón, en el siguiente capítulo estudiaremos la relación que existe entre el *cloud* y las redes de computadores. En particular, el desafío de la gestión de soluciones *cloud* en *data centers* distribuidos. La alta demanda generada por IoT incentiva la definición de nuevos paradigmas de gestión de las redes, para así fomentar una gestión dinámica de la carga de tráfico, promover la movilidad de los datos y favorecer un diseño eficiente desde el punto de vista energético.

## 2. *Cloud computing* y las redes de computadores

En la era del *cloud computing*, el IoT, el *big data* y la movilidad extrema a la que nos estamos acostumbrando, las redes adquieren un papel cada vez más fundamental como tecnología habilitadora. La enorme cantidad de datos que generamos a diario a través de la multitud de redes sociales que usamos, los tuits, los sensores o drones para una infinidad de aplicaciones, el IoT, las transacciones económicas o las compras en línea necesitan transmitirse de un punto a otro o a muchos otros, de manera fiable y a menudo con requisitos de tiempo real.

Todos los datos que manejamos hoy en día viajan a través de las redes de comunicaciones, incluso datos que son sensibles para empresas. Los datos atraviesan redes de Internet públicas y privadas. Las empresas, para garantizar la privacidad, tienden a privilegiar las redes privadas, aunque sean más costosas de desplegar y mantener. Precisamente, en este tipo de redes suele ser más fácil garantizar niveles de seguridad de extremo a extremo y prestaciones acordadas entre las partes mediante contratos entre cliente y proveedor de servicio, los denominados acuerdos de nivel de servicio, en inglés *service level agreements* (SLA).

Aspectos como la calidad del servicio en la red y el SLA son de gran importancia, porque acaban afectando a la calidad de la experiencia percibida por el usuario en el *cloud*. Por ejemplo, imaginemos que unos usuarios están disfrutando de un servicio de audio o vídeo en tiempo real. En este caso, la red de extremo a extremo tiene que configurarse de manera automática teniendo en cuenta la calidad del servicio que hay que proporcionar a nivel de red, para asegurar la calidad de la experiencia percibida por el usuario. Una experiencia decepcionante para los usuarios, un incumplimiento del SLA o una degradación del soporte técnico constituyen algunas de las razones que podrían causar la migración de los usuarios a otro proveedor capaz de ofrecer una mayor calidad de servicio.

Teniendo en cuenta todos estos factores, parece evidente que la gestión de la red es un factor determinante para el éxito en el despliegue de un *cloud*, cuyo diseño requiere un enfoque integral que tenga en cuenta no solo las características del *cloud*, sino también la infraestructura de red que le da apoyo. En particular, esta última tiene que ser capaz de soportar las diferentes características de un tráfico dinámico, mientras se garantizan no solo prestaciones en términos de capacidad o latencia, sino también aspectos de disponibilidad, seguridad y privacidad.

### Service level agreement

Un SLA es un contrato que se establece entre un cliente y un proveedor de servicio y que describe el nivel de servicio que se acuerda entre las dos partes. En español, también se llama acuerdo de nivel de servicio (ANS). Su objetivo es establecer unos indicadores de prestaciones que puedan medirse para valorar y regular el servicio que se presta.

## 2.1. Los requisitos de las redes para habilitar el *cloud computing*

Los principales requisitos que las redes tienen que garantizar para poder facilitar las operaciones del *cloud* son los siguientes:

- **Comunicaciones fiables:** Las comunicaciones dentro de la infraestructura del *cloud*, ya sea dentro del *data center* o entre diferentes *data centers*, tienen que ser completamente fiables para entregar mensajes de datos a su receptor de forma correcta y en tiempo real. Los organismos de estandarización están discutiendo estos aspectos para mejorar las comunicaciones en las infraestructuras presentes y futuras del *cloud*.
- **Comunicaciones eficientes:** Los organismos de estandarización también están estudiando cómo las comunicaciones dentro de la infraestructura del *cloud* pueden ser lo más eficientes posible, en cuanto a la gestión de los recursos, con el objetivo de no malgastar recursos.
- **Interoperabilidad:** La interoperabilidad es la capacidad de mover de manera dinámica y automática las cargas de trabajo y los datos entre diferentes *clouds*. La interoperabilidad es fundamental para permitir el intercambio de recursos entre proveedores de servicios en el *cloud* de una manera transparente. Este ámbito requiere esfuerzos de estandarización, para que los proveedores puedan desplegar infraestructuras compatibles. En 2019, por ejemplo, Oracle y Microsoft firmaron el primer acuerdo de interoperabilidad de sus *clouds*, que permitirá a los clientes migrar y ejecutar cargas de trabajo empresariales entre Microsoft Azure y Oracle Cloud.
- **Seguridad:** Los proveedores de servicios *cloud* tienen que ofrecer servicios seguros a sus clientes, protegiendo datos y operaciones. La fiabilidad es un requisito fundamental y crítico para todos los clientes.
- **Resiliencia:** La resiliencia se define como la capacidad del servicio de *cloud computing* de seguir proporcionando la calidad del servicio de acuerdo con los SLA contratados, en aquellos casos en los que la infraestructura se enfrenta a amenazas de seguridad u otros retos funcionales como, por ejemplo, un corte de energía.
- **Virtualización de la red:** Por último, otro requisito que se ha convertido en un aspecto crítico es la extensión del concepto de virtualización del *hardware*, que hemos visto en el capítulo precedente, al concepto de red. La virtualización de la red, que veremos más en detalle en la siguiente sección, es una forma eficiente de gestión de la red, que tiene el objetivo de hacerla más flexible, reconfigurable y ágil ante la demanda de servicios. Por ejemplo, la gestión de amplias bases de datos requiere el uso de la virtualización de la red para poder hacer frente a picos de tráfico.

## 2.2. La virtualización de la red y su nueva gestión elástica

Hemos visto que la virtualización de la red es un requisito importante de las redes de comunicaciones para habilitar el *cloud computing*.

Como hemos dicho anteriormente, se prevé que el tráfico en Internet, así como la generación de datos, aumente durante los próximos años, y esto requiere que las redes planteen nuevos enfoques de gestión para adaptarse a cargas dinámicas de tráfico. Las redes necesitan ser hoy más reactivas frente a cambios y su actualización tiene que ser flexible, automática, y no puede necesitar costosas actualizaciones de *hardware*, que tiende a quedarse rápidamente obsoleto.

Para hacer frente a las limitaciones de los equipos de *hardware* tradicionales, se ha consolidado la idea de la *softwarización* de las funciones de red. Es decir, si podemos traducir a *software* las funciones ejecutadas por los equipos de *hardware* especializados, podemos simplemente instalar y ejecutar dicho *software* en dispositivos de propósito general. Las funcionalidades de red vienen dadas entonces por el *software* y no por el *hardware*, y acaban desplegándose a través de máquinas virtuales en *hardware* de propósito general. Esto permite un abaratamiento de los costes de despliegue y mantenimiento de la infraestructura de red, y una total flexibilidad a la hora de gestionarla. Apostar por la gestión basada en *software* permite invertir en equipos de muy alta calidad y configurables.

Imaginemos, como ejemplo práctico, una red que tenga que ejecutar una funcionalidad A y otra funcionalidad B. En una red tradicional, un equipo *hardware* especializado se encargaría de la funcionalidad A, y otro equipo diferente de la funcionalidad B. Si de repente no necesitamos ejecutar más la funcionalidad A, y la funcionalidad B resulta la predominante, los equipos específicos que se encargan de la funcionalidad A ya no nos sirven y no pueden ser reutilizados para otros propósitos. Por otro lado necesitamos adquirir y desplegar más equipos específicos para ejecutar la funcionalidad B. Esta manera de diseñar la red es poco flexible con respecto a la realidad cambiante en la que vivimos. La virtualización de red permite tener unos equipos de propósito general y configurarlos para ejecutar las funcionalidades A y B mientras se necesitan. Cuando la funcionalidad A resulte obsoleta, el *software* puede actualizarse de manera ágil, para ejecutar solo la funcionalidad B, y así con nuevas funcionalidades. Los picos de tráfico en determinadas áreas, por ejemplo los causados por un evento (un concierto o un partido de fútbol) o los que supongan un acceso masivo a vídeos en *streaming*, se pueden gestionar más ágilmente en una red virtualizada, igual que

vimos con el *cloud computing*. De la misma manera, si un equipo se estropea, o necesita mantenimiento, cualquier otro con una simple actualización de *software* y reorganización de la carga de trabajo, puede absorber sus tareas.

### 2.2.1. La virtualización de las funciones de red o NFV

La **virtualización de funciones de red o NFV (*network function virtualization*)** nos permite separar las funcionalidades de red de sus dispositivos específicos. En particular, el NFV es un nuevo paradigma de gestión de la red que permite disociar las funciones de red de dispositivos de *hardware* dedicados y virtualizarlas, de modo que los servicios de red que ahora son ejecutados por *routers*, *firewalls*, balanceadores de carga, conmutadores y otros dispositivos de *hardware* dedicados sean hospedados en máquinas virtuales.

Para virtualizar las funciones de red, se usa el *software* hipervisor, que ya hemos citado, y que permite que los servicios que solían desplegarse a través de *hardware* dedicado puedan ejecutarse vía *software* en servidores estándar. Esta capacidad permite a los administradores de red prescindir de dispositivos de *hardware* dedicado para prestar un conjunto de servicios. Será suficiente gestionar dispositivos de propósito general más simples, con la consecuente reducción de gastos de capital (CAPEX) y gastos operativos (OPEX).

#### Network function virtualization

La virtualización de las funciones de red, o NFV, tiene como objetivo virtualizar funciones de red que, tradicionalmente, se han llevado a cabo mediante *hardware* propietario y dedicado. El concepto está siendo desarrollado por el ETSI.

Como ejemplo práctico, imaginemos que una aplicación que se ejecuta sobre una máquina virtual requiere más ancho de banda. En este caso, el administrador podría simplemente mover la máquina virtual a otro servidor físico de mayor capacidad o aprovisionar otra máquina virtual en el servidor original para redistribuir la carga entre las dos máquinas virtuales. La flexibilidad ofrecida por el nuevo concepto de NFV permitirá a los departamentos informáticos responder de manera más ágil a los objetivos cambiantes del negocio y a las demandas de servicios de red.

#### Software defined networking

Las redes definidas por *software* (SDN), como su mismo nombre indica, nos ayudan a gestionar las redes virtualizadas. Se trata de un conjunto de técnicas para crear redes donde el plano de control (*software*) se separa del plano de datos (*hardware*). Representan un nuevo paradigma de arquitectura de red que usa aplicaciones de *software* para controlar y programar de manera centralizada e inteligente la red.

### 2.2.2. Las redes definidas por *software* o SDN

Para gestionar las redes virtualizadas, es necesario coordinar un gran número de equipos multipropósito entre sí, determinando los procesos que van a realizarse en los diferentes equipos en cada instante de tiempo. Las **redes definidas por *software* o SDN (*software defined networking*)** permiten que esta distribución y organización de procesos se gestione en un punto centralizado, mediante la centralización del plano de control.

Volviendo a nuestro caso de uso del *cloud*, para un proveedor de servicios *cloud* es definitivamente deseable asegurar que sus clientes puedan mover sus cargas virtuales sin la necesidad de planear la red de manera estricta, de modo que esta pueda reconfigurarse según las necesidades que aparezcan. La solución tecnológica para gestionar la red de manera flexible es que sea configurable por *software*.

Las técnicas SDN también se han consolidado gracias a los enormes avances tecnológicos alcanzados por diferentes proyectos de *software* de código abierto que han estado evolucionando muy rápidamente en los últimos años, y que proporcionan el *software* que habilita el SDN. Por ejemplo, **OpenFlow** se ha establecido como el principal protocolo de comunicación y **OpenDaylight** como el principal proyecto de código abierto para habilitar y proporcionar SDN.

Vamos a ver a continuación un ejemplo práctico sobre el impacto de la virtualización de la función de los conmutadores en una red convencional, respecto a una red gestionada por *software*.

En la práctica, en una red tradicional, cuando un conmutador recibe un paquete, ejecuta unas reglas predefinidas e implementadas en su *firmware* que le indican dónde transferir el paquete. Existen conmutadores más inteligentes, diseñados con circuitos integrados de aplicación específica (ASIC, por su sigla en inglés), que son capaces de reconocer si hay paquetes de diferente tipo, que pueden necesitar un tratamiento diferenciado.

Por otro lado, en una red definida por *software*, el tráfico puede administrarse desde un punto de control centralizado, sin tener que configurar individualmente cada conmutador. Las reglas de los conmutadores de red pueden ser modificadas de manera flexible, alterando la prioridad de los paquetes, modificando las rutas, o hasta bloqueando ciertos tipos de paquetes, según se estime necesario. Habilitar estas capacidades es especialmente interesante en una arquitectura con múltiples *tenants* o usuarios (*multi-tenant architecture*) en el *cloud*, porque esta flexibilidad permite al administrador gestionar cargas de tráfico de manera diferenciada, flexible y eficiente. Se pueden implementar diferentes algoritmos de gestión dinámica e inteligente, para así garantizar en todas las circunstancias los SLA contratados.

#### Redes multi-tenant

La arquitectura *multi-tenant* permite a una red física dividirse en redes lógicas más pequeñas y aisladas, a través de técnicas de virtualización. Las redes *multi-tenant* comparten las redes físicas, pero funcionan de manera independiente, cada una con su propia política de gestión, seguridad, etc.



### 3. Otros retos: gasto energético y seguridad

El paradigma del *cloud computing* presenta no solamente ventajas y oportunidades, sino también problemas de despliegue e implementación, así como retos por resolver e investigar. Entre ellos, los más remarcables son los retos de seguridad y de gasto energético que representan el mantenimiento y la oferta de servicios del *cloud*. En este apartado vamos a discutir brevemente estos aspectos.

#### 3.1. La seguridad en el *cloud*

El problema de la seguridad ha sido durante mucho tiempo obviado por los proveedores de servicios *cloud*, pero últimamente se está reconociendo como un punto clave que se ha de tener en cuenta, ya que es un aspecto muy sensible para los clientes que desean tener garantías respecto a la seguridad de sus datos y sus operaciones.

La seguridad no es una característica que tiene que proporcionar solamente el proveedor. Los proveedores de servicios y los usuarios comparten la responsabilidad de proporcionar una protección adecuada a los servicios basados en el *cloud*, tal como reconocen los organismos de normalización líderes, como el National Institute of Standards and Technology (NIST) y la Cloud Security Alliance, así como los principales proveedores de *cloud* privado y público. En general, se considera que la seguridad del servicio de *cloud computing* no debería ser inferior a la que un cliente experimentaría en su red de infraestructura local. Específicamente, existen cuatro pilares clave en la seguridad *cloud*:

**1) Defensa del host:** tanto si los servicios se están ejecutando en las instalaciones o en el *cloud*, una organización necesita reforzar las máquinas virtuales mediante el uso de protección basada en *host*, como por ejemplo, antivirus, *antispywares* y sistemas de prevención de intrusiones en el *host*.

**2) Control de accesos:** proporciona una capa adicional de protección para asegurar la infraestructura de red y las cargas de trabajo que ayuda a administrar las cuentas de usuario y proporciona autenticación y autorización.

**3) Encriptación:** la encriptación permite ocultar los mensajes asociados a los activos de la empresa, mediante un algoritmo asociado a una o varias contraseñas.

**4) Simplificación operativa:** la seguridad tiene que ser coherente, transparente y sencilla de gestionar, tanto si las cargas de trabajo se están ejecutando en el *data center*, en un *cloud* privado o en una infraestructura de *cloud* pública.

Finalmente, cabe destacar que las amenazas de seguridad también dependen del tipo de servicio al que acceda el cliente. Por ejemplo, un servicio SaaS es muy similar a un simple servicio web sobre HTTP, heredando así las vulnerabilidades de los servicios web. Por otro lado, en el caso de un sistema PaaS, los recursos ofrecidos por estas plataformas son compartidos entre diferentes clientes (*tenants*). En consecuencia, es necesario que el proveedor proporcione el aislamiento apropiado para que un usuario no pueda acceder a recursos de otro usuario. Para lograr este objetivo, existe un claro compromiso, que se ha de formalizar en el SLA, entre el nivel de aislamiento de los activos de los usuarios y los recursos consumidos.

### 3.2. El gasto energético

Detrás del *cloud computing* existen centros físicos encargados del almacenamiento y la gestión de los datos. Se trata de edificios que consumen una gran cantidad de electricidad, generada principalmente a partir de combustibles fósiles. En el pasado se han publicado informes alarmantes de Greenpeace, como el famoso *How clean is your cloud?*, del año 2012, donde se analizaron los servicios ofrecidos por catorce empresas proveedoras de servicios *cloud*. Entre ellas, Facebook se llevó los mejores elogios por haber centralizado un importante *data center* en Suecia, donde las temperaturas ayudan al mantenimiento de la infraestructura y cuya principal fuente de energía es la hidroeléctrica.

Por otro lado, estudios recientes del Laboratorio Nacional del Departamento de Energía de Lawrence Berkeley, en EE.UU., han puesto de relieve que, a pesar del aumento de la demanda de servicios *cloud*, el aumento de consumo energético de los *data centers* va a crecer de forma más sostenible que en el pasado, debido a la virtualización y a la mejora de la eficiencia en la gestión de los *data centers*. En este sentido, no hay que olvidar además que el *cloud computing* representa un indudable ahorro en términos de gasto energético para las empresas.

## 4. *Cloud computing* para aplicaciones IoT

En el Reto 2 introducimos el paradigma de IoT. Los sistemas IoT se caracterizan por infraestructuras de red dinámicas y autoconfigurables donde «cosas», «objetos», dispositivos inteligentes, etc. interactúan y se comunican con el entorno a través de Internet, intercambiando datos extraídos por sensores, o reaccionando de manera autónoma a eventos, normalmente sin la necesidad de interacción humana. Dado que estos sistemas pueden utilizarlos una infinidad de aplicaciones, pueden estar caracterizados por múltiples propiedades. Hablamos de sensores, electrodomésticos, pasando por coches, relojes, gafas, ropa... ¡La lista es prácticamente infinita!

Las redes IoT y los datos que estas generan son la base de muchas de las revoluciones tecnológicas que están por venir. Los ejemplos de aplicaciones para la sociedad son muchos. El ámbito de las ciudades inteligentes es una de estas infraestructuras; la seguridad pública basada en el análisis de vídeo y la visión artificial (*video analytics computer vision*), el transporte inteligente mediante el uso de datos geolocalizados, las redes de energía inteligentes (*smart grids*) o las comunicaciones vehiculares, así como la conducción autónoma, generan una enorme cantidad de datos de forma localizada y requieren de infraestructuras de redes capaces de proporcionar prestaciones de baja latencia y seguras.

Las ventajas de conectar objetos a la red son numerosas. Por una parte, podemos gestionarlos a distancia, lo que por ejemplo permite automatizar el funcionamiento de toda una fábrica como parte de la denominada industria 4.0, o IoT industrial. Además, los objetos conectados recogen información de su entorno que luego podemos procesar para obtener estadísticas y tendencias. Imaginemos, por ejemplo, cuántas vidas podrían haberse salvado si un análisis proactivo de los datos recogidos del puente Morandi de Génova hubiera podido evitar su derrumbe. Finalmente, los objetos conectados pueden interactuar con otros sistemas en línea; un ejemplo podría ser el de una nevera capaz de detectar la falta de leche. La nevera misma se podría encargar de conectarse a los servidores de vuestro supermercado en línea y hacer un pedido de manera automática.

Sin embargo, esta visión no podría convertirse en realidad sin el soporte fundamental de las redes. El IoT añade una presión y una carga significativa a las redes y a los *data centers*, que deben transmitir, almacenar y procesar cada vez más datos generados por un número creciente de objetos conectados. Nos enfrentamos en el diseño de la red a un problema de escalabilidad. Si incrementamos la conexión a Internet de millones de objetos nuevos que vuelcan

a la red ingentes cantidades de datos, la capacidad de los servicios de *cloud computing* podría llegar a su límite y requerir la ampliación o la construcción de nuevos *data centers*. Ya hemos discutido este problema en el apartado 1.3 dedicado a la geografía del *cloud*. Este problema puede verse aliviado recurriendo al uso del *edge/fog computing*. A diferencia del *cloud computing*, con el *edge/fog computing* el procesamiento informático no se realiza en *data centers* centralizados, sino que se reparte a lo largo de la red. Como ya hemos visto, esto permite que la computación se realice más cerca de los objetos conectados, lo que tiene dos grandes ventajas: evita la sobrecarga de los *data centers* y hace que la información recorra menos distancia entre el objeto conectado y el servidor que analiza los datos y proporciona la información o el servicio solicitado.

El futuro del *cloud*, para dar respuesta a las diferentes necesidades de plataformas de IoT, pasa entonces por un enfoque híbrido: la combinación de *data centers* de alta densidad, encargados de realizar las tareas más exigentes, con numerosos *data centers* más pequeños repartidos a lo largo de toda la red, y que proporcionan servicios de *edge/fog computing* más rápidos y cercanos para las aplicaciones que lo requieran.

El *cloud computing* proporciona al IoT muchas propiedades interesantes, como la gestión eficiente de los recursos, la escalabilidad, la capacidad de gestionar grandes cantidades de datos y la posibilidad de acceder al *cloud* desde cualquier sitio. En la actualidad, ya existen proveedores de servicios *cloud* para IoT que permiten conectar los dispositivos al *cloud* y almacenar los datos generados por ellos. Algunos ejemplos de productos han sido diseñados e implementados por los mayores actores del mercado:

- IBM Bluemix Platform, que es la plataforma propuesta por IBM.
- Parse, que es una plataforma para soporte IoT ofrecida por Facebook.
- Google IoT, es la plataforma Google que es parte de Google Cloud.
- Amazon Web Service.
- Azure es la plataforma ofertada por Microsoft.

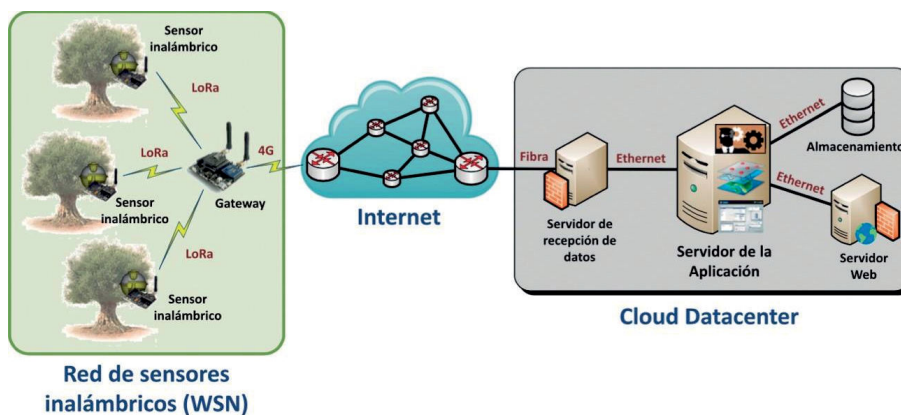
## 5. Ejemplo de aplicación IoT: cerrando el círculo del ciclo de vida de los datos

En este apartado se presenta un ejemplo ilustrativo de una aplicación IoT alojada en un *cloud data center* que necesita extraer datos de una red externa y, a su vez, publicar dichos datos en una web para que un usuario final pueda visualizarlos.

La aplicación seleccionada se trata de un sistema de monitorización de cultivos mediante sensores. Dichos sensores están colocados en árboles frutales y miden de forma periódica magnitudes físicas como la temperatura y la humedad, de forma que un agricultor puede tener información en tiempo real de las condiciones climáticas de sus cultivos.

En primer lugar, se necesita que la información extraída por los sensores sea transmitida hasta el *cloud* donde se aloja la aplicación que procesa y publica los datos (véase figura 1). Para ello, los datos se transmiten primero por una red de acceso, que en este caso se trata de una red de sensores (*wireless sensor network*, WSN), y después a través de una red troncal, Internet.

Figura 1. Publicación de datos en un *data center*



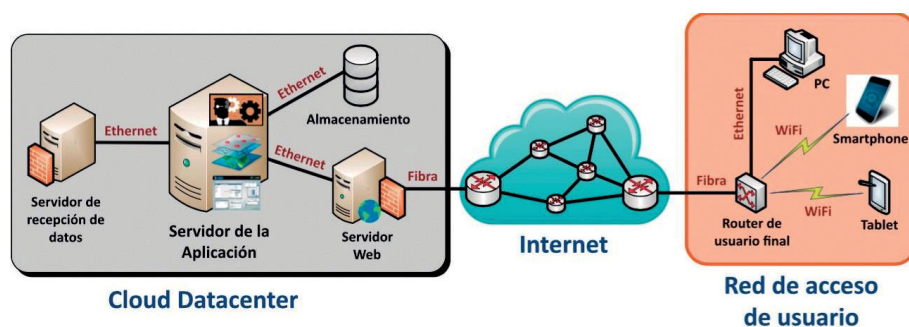
Debido a la distancia existente entre los árboles frutales y el primer dispositivo agregador de datos (*gateway*), se ha elegido una tecnología low-power wide area network (LPWAN) como LoRa para realizar las transmisiones de ese primer enlace. A continuación, el *gateway* establece un enlace celular 4G para hacer llegar toda la información a través de Internet al servidor de recepción de datos ubicado en el *cloud*.

El protocolo de aplicación utilizado para transmitir la información de los sensores es CoAP, debido a su sencillez y a su compatibilidad con dispositivos de recursos limitados. En particular, se establece un esquema de comunicación cliente/servidor entre cada nodo sensor y el servidor de recepción de datos, siendo este último el responsable de emitir las peticiones de información de forma periódica.

La información se guarda en un dispositivo de almacenamiento, procesada en el servidor correspondiente de la aplicación y publicada en Internet mediante un servidor web. Nótese que las comunicaciones en el interior del *cloud data center* se basan en ethernet, mientras que la salida a Internet se realiza mediante fibra óptica.

En segundo lugar, los datos publicados en el *cloud* deben ser accesibles para el agricultor, que será el principal usuario de dicha aplicación. Para ello, se ha diseñado la arquitectura que se muestra en la figura 2, con una red de acceso de usuario y, de nuevo, usando Internet como red troncal.

Figura 2. Extracción de datos desde un *data center*



Las tecnologías utilizadas en el interior de la red de acceso de usuario dependen del dispositivo final usado por el agricultor para acceder a los datos recopilados: por ejemplo, su PC utiliza ethernet para conectarse a su *router* local, mientras que su smartphone o su tablet utilizan Wi-Fi. En cuanto al *router* proporcionado por su *Internet service provider* (ISP), dispone de una salida a Internet mediante fibra óptica.

Sea cual sea el dispositivo final elegido (PC, smartphone o tablet), el agricultor podrá acceder a la información recogida por los sensores de sus árboles frutales mediante una web API RESTful basada en el protocolo HTTP, ejecutada desde un navegador web y que usa JSON como formato de intercambio de datos.

## Ejercicios de autoevaluación

1. ¿Cuál de las siguientes opciones puede considerarse una de las principales ventajas del *cloud computing*?

- a) Acceso a servicios IT bajo demanda.
- b) Ahorro energético para el proveedor de servicio.
- c) Gestión eficiente de la red.
- d) Incremento de la seguridad en las redes.

2. ¿Cuál de las siguientes opciones puede considerarse una de las principales ventajas del *edge* respecto al *cloud computing*?

- a) Mayor capacidad computacional para procesar datos de usuarios.
- b) Mejores prestaciones de retardo y de coste de despliegue.
- c) Mayor capacidad de almacenaje.
- d) Ahorro energético.

3. ¿Cuál de las siguientes afirmaciones es cierta?

- a) El *cloud computing* es un sinónimo de virtualización de los recursos de *hardware*.
- b) El SDN y el NFV son tecnologías habilitadoras del *cloud computing*.
- c) La seguridad en el *cloud* es un reto aún abierto en el que hay que trabajar.
- d) Todos los servicios *cloud* presentan los mismos retos de seguridad.

4. ¿Cuál de las siguientes afirmaciones es cierta?

- a) El *cloud computing* ofrece servicios *best effort* sobre Internet.
- b) Los proveedores de *cloud computing* acuerdan un SLA con sus clientes donde se especifica el servicio que se va a proporcionar.
- c) El diseño eficiente de las redes no tiene mayor impacto en el servicio proporcionado a los clientes.
- d) La seguridad en el *cloud* es una responsabilidad del proveedor de servicios del *cloud*.

5. ¿Cuál de las siguientes afirmaciones es cierta?

- a) El *cloud computing* no presenta problemas de escalabilidad para aplicaciones IoT.
- b) El *edge computing* es una respuesta a los problemas de escalabilidad en caso de aplicaciones IoT.
- c) Los proveedores no necesitan diseñar servicios específicos para IoT.

## Solucionario

1. a
2. b
3. c
4. b
5. b



## Glosario

**ANSI** American national standard institute

**API** application programming interface

**CoAP** constrained application protocol

**CPU** central processing unit

**ETSI** European telecommunication standard institute

**HTTP** hypertext transfer protocol

**IaaS** infrastructure as a service

**IoT** Internet of things

**ISP** Internet service provider

**IT** information technology

**JSON** JavaScript object notation

**LPWAN** low-power wide area network

**NFV** network function virtualization

**OPEX** operating expenses

**PaaS** platform as a service

**SaaS** software as a service

**SDN** software defined networking

**SLA** service level agreement

**VM** virtual machine

**WSN** wireless sensor network

## Bibliografía

**Das, P.; Mitra, R.** (2016). «A survey on cloud computing and networking in the next generation». En: *Foundations and Frontiers in Computer, Communication and Electrical Engineering* (págs. 275-280). Londres: Taylor Francis Group.

**Greenpeace.** (2012). *How clean is your cloud?* White Paper.

**Lawrence Livermore National Lab. (LLNL)** (2012). <<https://www.llnl.gov/news/energy-and-cost-savings-llnl-data-center-consolidation-earn-doe-award>>

**Moura, J.; Hutchison, D.** (2016). «Review and Analysis of Networking Challenges in Cloud Computing». *Journal of Network and Computer Applications* (vol. 60, n.º 1). Elsevier.

**Wardley, S.** (2009). *Cloud Computing - Why IT Matters?* Open Source Convention (OSCON).

**Xavier, G.; Kantarci, B.** (2018). «A survey on the communication and network enablers for cloud-based services: state of the art, challenges, and opportunities». *Annals of Telecommunications*. Springer Verlag.