****

Contenido

[1](#_Toc193386355)

[**1.1 Qué es el SSID** 2](#_Toc193386356)

[3](#_Toc193386357)

[3](#_Toc193386358)

[Cómo cambiar tu SSID 3](#_Toc193386359)

[1.2 MAC 5](#_Toc193386360)

[1.3 Clave WPA2 6](#_Toc193386361)

[1.4 PASSWORD 7](#_Toc193386362)

[1.5 IP 8](#_Toc193386363)

[1.6 DHCP 9](#_Toc193386364)

**1.1 Qué es el SSID**

Las siglas SSID vienen del término *Service Set Identifier*  y en cuanto a qué es, se trata del **nombre que tiene tu red Wi-Fi** para poder encontrarla e identificarla entre otras redes y conexiones. Su objetivo es ese, el de ayudarte a identificar tu red. El nombre del SSID puede tener **un máximo de 23 caracteres alfanuméricos**. Sin embargo, no es necesario que los uses todos, y podrás crear un SSID para tu Wi-Fi con menos caracteres. Por último, si el router que tienes en casa es de doble banda, es posible que las conexiones de 2.4GHz y 5GHz tengan una SSID. Con esto, vas a poder diferenciar una de la otra y elegir cuál de las dos quieres utilizar. El nombre de la SSID predeterminado de tu conexión Wi-Fi **suele venir pegado en una etiqueta en tu router**. Se trata de una pegatina de información que tendrás en un costado o en la parte inferior del router, donde vendrá tu SSID y contraseña predeterminadas. Si tienes un móvil o un ordenador conectado a la Wi-Fi, no importa el sistema operativo, porque en la configuración de Wi-Fi del dispositivo podrás ver el SSID de la red a la que te has conectado.

## What is an SSID?

## 

SSDI

## Cómo cambiar tu SSID

La SSID de tu conexión **la puedes cambiar desde la configuración de tu router**. La interfaz de esta configuración depende de cada operador, por lo que no hay unos pasos determinados ni una sección concreta donde tengas que ir, todo depende de cada operador. Lo primero que tienes que hacer es abrir el navegador de Internet en tu ordenador o móvil, y escribir la dirección 192.168.1.1 o 192.168.0.1. Normalmente es la primera. Esto te llevará a una pantalla donde **debes iniciar sesión** con el nombre de usuario y contraseña que te del operador, que normalmente también aparece en la pegatina del router. El usuario y contraseña suelen ser peligrosamente fáciles, como admin, o 1234 1234.

Y una vez aquí, tendrás que buscar dónde está en esta pantalla de configuración el apartado para personalizar tu red Wi-Fi. Una vez lo encuentres, entonces podrás **personalizar el SSID y la contraseña de tu Wi-Fi** para usar unas que sean propias y más difíciles de adivinar.



## 1.2 MAC

El MAC, o “Media Access Control” es el **identificador único** que las empresas fabricantes de hardware asignan a la tarjeta de red de cada uno de los dispositivos que producen con el fin de que sean inequívocamente identificables en sus accesos a cualquier red (lo que por supuesto incluye a Internet).

Las direcciones MAC están formadas por 48 bits, representados por dígitos hexadecimales. Traducido de una forma más entendible, esto quiere decir que las direcciones MAC constarán de **12 dígitos** (tanto letras como números) divididos en 6 parejas separadas habitualmente de las demás por dos puntos (aunque no siempre tendrán esta separación). Así, las direcciones MAC tendrán una estructura del tipo 00:xx:01:xy:x0:y1 (por ejemplo).

Y ahora te preguntarás… ¿cómo es posible que cada número sea diferente? ¿Cómo sabe una fabricante de software que el número MAC que está dando a un dispositivo no ha sido ya utilizado por otra fabricante? Pues es muy sencillo: una parte de la dirección MAC, de hecho, está formada por identificadores del fabricante. En concreto, los 6 primeros dígitos de la dirección nos cuentan cuál es el fabricante del dispositivo, mientras que los 6 últimos son los que el fabricante atribuye a ese dispositivo en concreto.



## 1.3 Clave WPA2

WPA2 (Acceso protegido Wi-Fi 2) es un protocolo cifrado de seguridad que protege el tráfico de Internet en redes inalámbricas. La segunda generación del protocolo de seguridad de Acceso protegido Wi-Fi (WPA2) aborda errores anteriores y ofrece un cifrado más potente. Desde su lanzamiento en 2004, se ha convertido en el estándar de seguridad de las redes Wi-Fi.

Su router de Internet crea redes y administra los datos enviados y recibidos por sus dispositivos conectados, y esto hace a su router vulnerable frente a las amenazas de seguridad, ya que los datos privados son valiosos para los hackers.

Al igual que sus predecesores WPA y WEP, WPA2 utiliza la tecnología de cifrado para codificar datos, con el fin de que resulten indescifrables para los hackers. Entre todos esos protocolos de seguridad, WPA2 ofrece los niveles de cifrado más sofisticados.



## 1.4 PASSWORD

**Password** es una palabra que no forma parte del diccionario de la **Real Academia Española (RAE)**. El término, sin embargo, es muy popular en nuestra **lengua**, aunque puede reemplazarse por **contraseña** o **clave**, nociones que sí son aceptadas por la **RAE**.

Un password es una **combinación de letras y/o números** que brinda, a quien lo conoce, la posibilidad de acceder a un recurso. El password sirve como protección y como mecanismo de seguridad: aquellas personas que no conocen la **clave**, no pueden acceder al recurso en cuestión.

Los passwords también protegen las cuentas de correo electrónico (email) y de otros servicios en Internet (como Facebook, Twitter, etc.). El usuario, al registrarse, escoge un password que sólo debe conocer él. De esta manera, nadie podrá utilizar su correo o su perfil en las redes sociales sin su consentimiento.

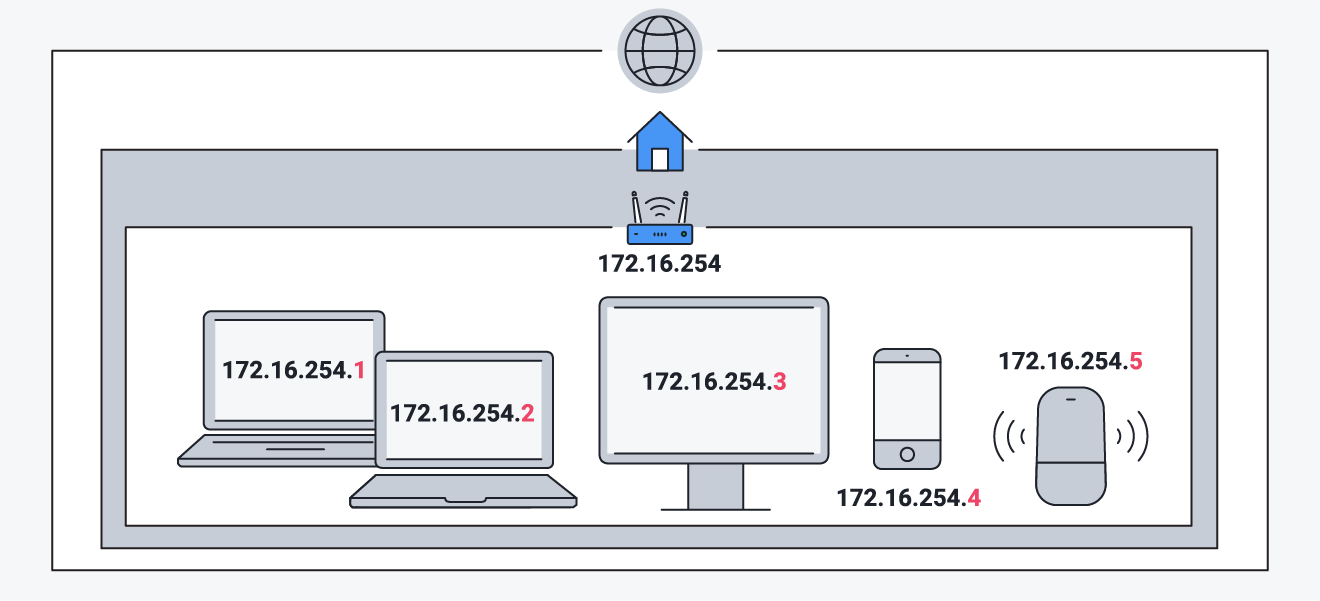


## 1.5 IP

Una dirección IP, abreviatura de **dirección de Protocolo de Internet**, es un identificador único de un dispositivo conectado a Internet o a una infraestructura de red. Es fundamental para facilitar la comunicación y la transferencia de datos entre dispositivos en línea.

En este artículo, daremos la definición de dirección IP y explicaremos cómo funciona una dirección IP. También exploraremos cómo contribuyen al flujo fluido de información a través de las redes.

Además, describiremos los diferentes tipos de direcciones de Protocolo de Internet, analizaremos las amenazas más comunes a las direcciones IP y ofreceremos consejos sobre cómo asegurar una dirección IP para proteger tu presencia en línea y tus datos confidenciales.



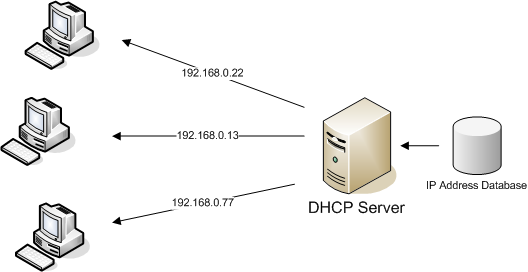
## 1.6 DHCP

El protocolo DHCP (Protocolo de configuración dinámica de host) es un protocolo de red que utiliza una arquitectura cliente-servidor. Por tanto, tendremos uno o varios servidores DHCP y también uno o varios clientes, que se deberán comunicar entre ellos correctamente para que el servidor DHCP brinde información a los diferentes clientes conectados.

Este protocolo se encarga de **asignar de manera dinámica** y automática una dirección IP, ya sea una dirección IP privada desde el router hacia los equipos de la red local, o también una IP pública por parte de un operador que utilice este tipo de protocolo para el establecimiento de la conexión.

**Cuando tenemos un servidor DHCP** en funcionamiento, todas las direcciones IP que ha proporcionado a diferentes clientes se guardan en un listado donde se relaciona la IP que se le ha proporcionado (dirección lógica) y la dirección MAC (dirección física de la tarjeta de red). Gracias a este listado, el servidor DHCP se asegura de no proporcionar a dos equipos diferentes la misma dirección IP, lo que ocasiona un caos en la red local.

A medida que el servidor **va asignando direcciones IP**, también tiene en cuenta cuándo pasa un determinado tiempo y caducan, quedando libres para que otro cliente pueda obtener esta misma dirección IP. El servidor DHCP sabrá en todo momento quién ha estado en posesión de una dirección IP, cuánto tiempo ha estado, y cuándo se ha asignado a otro cliente.



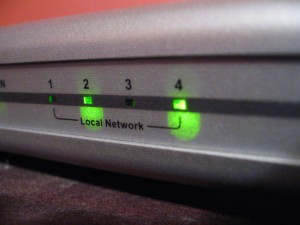
2.1 TIPOS DE REDES POR SU ALCANCE

### **1. Red de área personal (PAN)**

Hablamos de una **red informática de pocos metros**, algo parecido a la distancia que necesita el Bluetooth del móvil para intercambiar datos. Son las más básicas y sirven para espacios reducidos, por ejemplo si trabajas en un local de una sola planta con un par de ordenadores.

Las **redes PAN** pueden serte útiles si vas a conectar pocos dispositivos que no estén muy lejos entre sí. La opción más habitual, sin embargo, para aumentar el radio de cobertura y para evitar la instalación de cablea estructurado, suele ser la compra de un router y la instalación de una red de área local inalámbrica.

### **2. Red de área local (LAN).**

[](https://www.gadae.com/blog/wp-content/uploads/file00014075359811.jpg)

Es la que todos conocemos y la que suele instalarse en la mayoría de las empresas, tanto si se trata de un edificio completo como de un local. Permite conectar ordenadores, impresoras, escáneres, fotocopiadoras y otros muchos periféricos entre sí para que puedas intercambiar datos y órdenes desde los diferentes nodos de la oficina.

Las redes LAN pueden abarcar **desde los 200 metros hasta 1 kilómetro de cobertura**.

### **3. Red de área de campus (CAN).**

Vale, supongamos que tenemos varios edificios en los que queremos montar una [red inalámbrica](https://www.gadae.com/blog/redes-inalambricas-o-redes-por-cable/). ¿Qué pasa si el área de cobertura debe ser mayor a los 1000 metros cuadrados? Y no lo digo sólo por las universidades; las instalaciones de los parques tecnológicos, recintos feriales y naves comerciales pueden superar perfectamente esa superficie.

En tal caso, tenemos las **redes CAN**. Habría varias redes de área local instaladas en áreas específicas, pero a su vez todas ellas estarían interconectadas, para que se puedan intercambiar datos entre sí de manera rápida, o pueda haber conexión a Internet en todo el campus.

### **4. Red de área metropolitana (MAN)**

Mucho más amplias que las anteriores, abarcan espacios metropolitanos mucho más grandes. Son las que suelen utilizarse cuando las administraciones públicas deciden **crear zonas Wifi en grandes espacios**. También es toda la infraestructura de cables de un operador de telecomunicaciones para el despliegue de **redes de fibra óptica**. Una red MAN suele conectar las diversas LAN que hay en un espacio de unos 50 kilómetros.

### **5. Red de área amplia (WAN)**

[](https://www.gadae.com/blog/wp-content/uploads/file000261790595.jpg)

Son las que suelen desplegar las empresas **proveedoras de Internet** para cubrir las [tipos de casino](https://www.netbet.org/) necesidades de conexión de redes de una zona muy amplia, como una ciudad o país.

### **6. Red de área de almacenamiento (SAN)**

Es una red propia para las **empresas que trabajan con servidores y no quieren perder rendimiento** en el tráfico de usuario, ya que manejan una enorme cantidad de datos. Suelen utilizarlo mucho las empresas tecnológicas. En Cisco te cuentan las [ventajas de una red SAN](http://www.cisco.com/web/LA/soluciones/la/data_storage/index.html).

### **7. Red de área local virtual (VLAN)**

Las redes de las que hablamos normalmente se conectan de forma física. Las **redes VLAN** se encadenan de forma lógica (mediante protocolos, puertos, etc.), reduciendo el tráfico de red y mejorando la seguridad. Si una empresa tiene varios departamentos y quieres que funcionen con una red separada, la red VLAN.

Espero que con esto tengas una imagen un poco más clara de las diferentes **redes informáticas según su alcance**. Si quieres saber más, puedes ver el artículo [«Tipos de redes informáticas según su topología»](https://www.gadae.com/blog/tipos-de-redes-informaticas-topologia/). Lo más lógico en una PYME es que necesite simplemente una LAN, pero para casos de mayor envergadura o si se quiere que las redes funcionen de forma separada, es bueno conocer que hay otras posibilidades.