

# Wifi

(Redirigido desde «Wi-Fi»)



Logotipo de la marca Wi-Fi

El **wifi** (sustantivo común en español, incluido en el *Diccionario* de las Academias,<sup>1</sup>proveniente de la marca Wi-Fi)<sup>2</sup> es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con wifi (como una computadora personal, un televisor inteligente, una videoconsola, un teléfono inteligente o un reproductor de música) pueden conectarse a internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso tiene un alcance de unos veinte metros en interiores, distancia que es mayor al aire libre.

Wi-Fi es una marca de la Alianza Wi-Fi, la organización comercial que adopta, prueba y certifica que los equipos cumplen con los estándares 802.11 relacionados a redes inalámbricas de área local.

## Etimología

El término *wifi*, sustantivo común escrito normalmente en redonda (sin comillas ni cursiva),<sup>2</sup> proviene de la marca comercial Wi-Fi. La WECA, el consorcio que desarrolló esta tecnología, contrató a una empresa de publicidad para que le diera un nombre a su estándar, de tal manera que fuera fácil de entender y recordar. Phil Belanger, miembro fundador de WECA, actualmente llamada Alianza Wi-Fi, apoyó el nombre *Wi-Fi*:<sup>[*cita requerida*]</sup>

"Wi-Fi" y el "Style logo" del Yin Yang fueron inventados por la agencia Interbrand. Nosotros (Wi-Fi Alliance) contratamos a Interbrand para que nos hiciera un logotipo y un nombre que fuera corto, tuviera mercado y fuera fácil de recordar. Necesitábamos algo que fuera algo más llamativo que "IEEE 802.11b de Secuencia Directa". Interbrand creó nombres como "Prozac", "Compaq", "OneWorld", "Imation", por mencionar algunos. Incluso inventaron un nombre para la compañía: VIATO."

Phil Belanger

La similitud con la marca Hi-Fi (del inglés *high fidelity*; usado frecuentemente en la grabación de sonido) ha hecho creer, erróneamente, que el término *Wi-Fi* es una abreviación de *wireless fidelity* (traducido al español, *fidelidad inalámbrica*).

## Historia

Esta nueva tecnología surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuese compatible entre distintos dispositivos. Buscando esa compatibilidad, en 1999 las empresas 3Com, Airones, Intersil, Lucent Technologies, Nokia y Symbol Technologies se unieron para crear la *Wireless Ethernet Compatibility Alliance*, o WECA, actualmente llamada Alianza Wi-Fi. El objetivo de la misma fue designar una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

De esta forma, en abril de 2000 WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b, bajo la marca Wi-Fi. Esto quiere decir que el usuario tiene la

garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos.

En el año 2002 la asociación WECA estaba formada ya por casi 150 miembros en su totalidad<sup>[*cita requerida*]</sup>. La familia de estándares 802.11 ha ido naturalmente evolucionando desde su creación, mejorando el rango y velocidad de la transferencia de información, su seguridad, entre otras cosas.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red wifi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de CABLE 802.3 (Ethernet).

## Estándares que certifica la Alianza Wi-Fi

---

*Artículo principal:* IEEE 802.11

Existen diversos tipos de wifi, basado cada uno de ellos en una estándar IEEE 802.11 aprobado. Son los siguientes:

- Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que la banda de 2,4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbit/s, 54 Mbit/s y 300 Mbit/s, respectivamente.
- En la actualidad ya se maneja también el estándar IEEE 802.11ac, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, además, no existen otras tecnologías (Bluetooth, microondas, ZigBee, WUSB) que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2,4 GHz (aproximadamente un 10 %), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

Existen otras tecnologías inalámbricas como Bluetooth que también funcionan a una frecuencia de 2,4 GHz, por lo que puede presentar interferencias con la tecnología wifi. Debido a esto, en la versión 1.2 del estándar Bluetooth por ejemplo se actualizó su especificación para que no existieran interferencias con la utilización simultánea de ambas tecnologías, además se necesita tener 40 000 kbit/s.

## Seguridad y fiabilidad

---

Uno de los problemas a los cuales se enfrenta actualmente la tecnología wifi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad el estándar wifi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instalados sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables ante el intento de acceder a ellas por terceras personas), sin proteger la información que por ellas circulan. De hecho, la configuración por defecto de muchos dispositivos wifi es muy insegura (*routers*, por ejemplo) dado que a partir del identificador del dispositivo se puede conocer la clave de éste; y por tanto acceder y controlar el dispositivo se puede conseguir en solo unos segundos.

El acceso no autorizado a un dispositivo wifi es muy peligroso para el propietario por varios motivos. El más obvio es que pueden utilizar la conexión. Pero, además, accediendo al wifi se puede supervisar y registrar toda la información que se transmite a través de él

(incluyendo información personal, contraseñas...). La forma de hacerlo seguro es seguir algunos consejos:<sup>3 4</sup>

- Cambios frecuentes de la contraseña de acceso, utilizando diversos caracteres, minúsculas, mayúsculas y números.
- Se debe modificar el SSID que viene predeterminado.
- Desactivar la difusión de SSID y DHCP.
- Configurar los dispositivos conectados con su IP (indicar específicamente qué dispositivos están autorizados para conectarse).
- Utilización de cifrado: WPA2.
- Filtrar los dispositivos conectados mediante la dirección MAC.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares wifi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire. Este tipo de cifrado no está recomendado debido a las grandes vulnerabilidades que presenta ya que cualquier *cracker* puede conseguir sacar la clave, incluso aunque esté bien configurado y la clave utilizada sea compleja.
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.
- Filtrado de MAC, de manera que solo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- Ocultación del punto de acceso: se puede ocultar el punto de acceso (*router*) de manera que sea invisible a otros usuarios.
- El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren *hardware* y *software* compatibles, ya que los antiguos no lo son.

La seguridad de una red wifi puede ser puesta a prueba mediante una auditoría de wifi. Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

## Dispositivos


---



Router wifi

Existen varios dispositivos wifi, los cuales se pueden dividir en dos grupos: **dispositivos de distribución o de red**, entre los que destacan los enrutadores, puntos de acceso y repetidores; y **dispositivos terminales** que en general son las tarjetas receptoras para conectar a la COMPUTADORA personal, ya sean internas (tarjetas PCI) o bien USB.

- Dispositivos de distribución o de red:
  - Los puntos de acceso son dispositivos que generan un *set de servicio*, que podría definirse como una *red wifi* a la que se pueden conectar otros dispositivos. Los puntos de acceso permiten, en resumen, conectar dispositivos de forma inalámbrica a una red existente. Pueden agregarse más puntos de acceso a una red para generar redes de cobertura más amplia, o conectar antenas más grandes que amplifiquen la señal.
  - Los repetidores inalámbricos son equipos que se utilizan para extender la cobertura de una red inalámbrica, éstos se conectan a una red existente que tiene señal más débil y crean una señal limpia a la que se pueden conectar los equipos dentro de su alcance. Algunos de ellos funcionan también como punto de acceso.
  - Los enrutadores inalámbricos son dispositivos compuestos, especialmente diseñados para redes pequeñas (hogar o pequeña oficina). Estos dispositivos incluyen, un enrutador (encargado de interconectar redes, por ejemplo, nuestra red del hogar con Internet), un punto de acceso (explicado más arriba) y generalmente un conmutador que permite conectar algunos equipos vía CABLE (Ethernet y USB). Su tarea es tomar la conexión a Internet, y brindar a través de ella acceso a todos los equipos que conectemos, sea por cable o en forma inalámbrica.
- Los dispositivos terminales abarcan tres tipos mayoritarios: tarjetas PCI, tarjetas PCMCIA y tarjetas USB:
  - El wifi puede ser desactivado por un terminal del dispositivo.
  - Las tarjetas PCI para wifi se agregan (o vienen de fábrica) a los ordenadores de sobremesa. Hoy en día están perdiendo terreno debido a las tarjetas USB. Dentro de este grupo también pueden agregarse las tarjetas MiniPCI que vienen integradas en casi cualquier computador portátil disponible hoy en el mercado.
  - Las tarjetas PCMCIA son un modelo que se utilizó mucho en los primeros ordenadores portátiles, aunque están cayendo en desuso, debido a la integración de tarjeta inalámbricas internas en estos ordenadores. La mayor parte de estas tarjetas solo son capaces de llegar hasta la tecnología B de wifi, no permitiendo por tanto disfrutar de una velocidad de transmisión demasiado elevada
  - Las tarjetas USB para wifi son el tipo de tarjeta más común que existe en las tiendas y más sencillo de conectar a un pc, ya sea de sobremesa o portátil, haciendo uso de todas las ventajas que tiene la tecnología USB. Hoy en día puede encontrarse incluso tarjetas USB con el estándar 802.11N (Wireless-N) que es el último estándar liberado para redes inalámbricas.

- También existen impresoras, CÁMARAS  Web y otros periféricos que funcionan con la tecnología wifi, permitiendo un ahorro de mucho cableado en las instalaciones de redes y especialmente, gran movilidad.

En relación con los manejadores de dispositivo, existen directorios de circuito integrado auxiliar de adaptadores inalámbricos.<sup>5</sup>


## Ventajas y desventajas

---

Las redes wifi poseen una serie de ventajas, entre las cuales podemos destacar:

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un espacio lo bastante amplio.
- Una vez configuradas, las redes wifi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, ni gran cantidad de cables.
- La Alianza Wi-Fi asegura que la compatibilidad entre dispositivos con la marca Wi-Fi es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología wifi con una compatibilidad absoluta.

Pero como red inalámbrica, la tecnología wifi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. Algunos de ellos son:

- Una de las desventajas que tiene el sistema wifi es una menor velocidad en comparación a una conexión CABLEADA , debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.
- La desventaja fundamental de estas redes reside en el campo de la seguridad. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta wifi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente *fáciles de conseguir* con este sistema. La Alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. De todos modos, muchas compañías no permiten a sus empleados utilizar una red inalámbrica <sup>[cita requerida]</sup>. Este problema se agrava si consideramos que no se puede controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista (por ejemplo: desde fuera de una oficina, desde una vivienda colindante).
- Esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.
- La potencia de la conexión del wifi se verá afectada por los agentes físicos que se encuentran a nuestro alrededor, tales como: árboles, paredes, arroyos, una montaña, etc. Dichos factores afectan la potencia de compartimiento de la conexión wifi con otros dispositivos.