

# Seguridad de las redes WiFi suministradas por los proveedores de Internet



Bandaancha.eu, como titular de los derechos de autor de esta obra, licencia su contenido bajo los terminos de Creative Commons Reconocimiento 3.0 España. Se permite la copia, distribución y comunicación pública de esta obra bajo las condiciones siguientes:

**Reconocimiento:** Debe reconocer los créditos de la obra haciendo referencia expresa tanto a bandaancha.eu como a su sitio web: <http://bandaancha.eu>

Texto completo de la licencia: <http://creativecommons.org/licenses/by/3.0/es/legalcode.es>

## Introducción

El WiFi se ha convertido en una prestación básica incorporada en la mayoría de dispositivos de acceso a Internet. Gracias al WiFi es posible acceder a la red desde cualquier ubicación dentro del domicilio u oficina sin necesidad de utilizar un cable para establecer la conexión.

Como cualquier señal de radio, el WiFi se transporta mediante señales radioeléctricas y puede ser captado e interferido por otras señales procedentes del exterior de recinto donde se este utilizando.

Para proteger la privacidad de las comunicaciones WiFi, se desarrollo el sistema WEP (Wired Equivalent Privacy). Dos años después de su estreno ya eran conocidas varias vulnerabilidades que lo hacían inseguro, por lo que en el año 2003 fue sustituido por el sistema WPA. El organismo estandarizador IEEE recomendó que no se continuará utilizando WEP como una forma de proteger redes WiFi.

## WiFi en los dispositivos de acceso a Internet

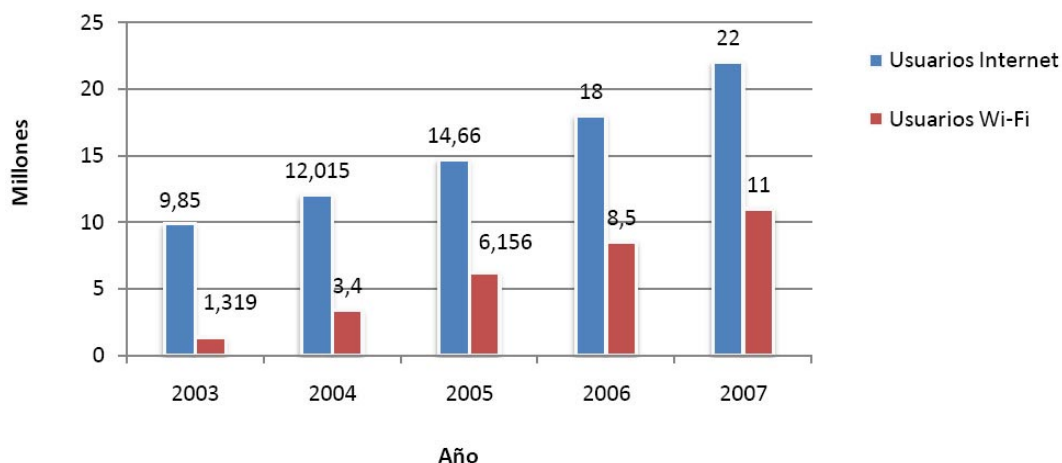
Los proveedores de Internet promocionan la contratación de sus productos de acceso a Internet subvencionando los dispositivos necesarios para conectar a su red. Si la red de acceso utiliza el par telefónico, se proporciona un router ADSL. En el caso de las redes de cable HFC el dispositivo es un cablemodem.

La amplia mayoría de los routers de acceso proporcionados en la actualidad incorporan conectividad WiFi. El proveedor de Internet entrega al cliente el router WiFi listo para su uso, preconfigurando sus parámetros para que funcione en la mayoría de escenarios posibles.

## Uso de WiFi

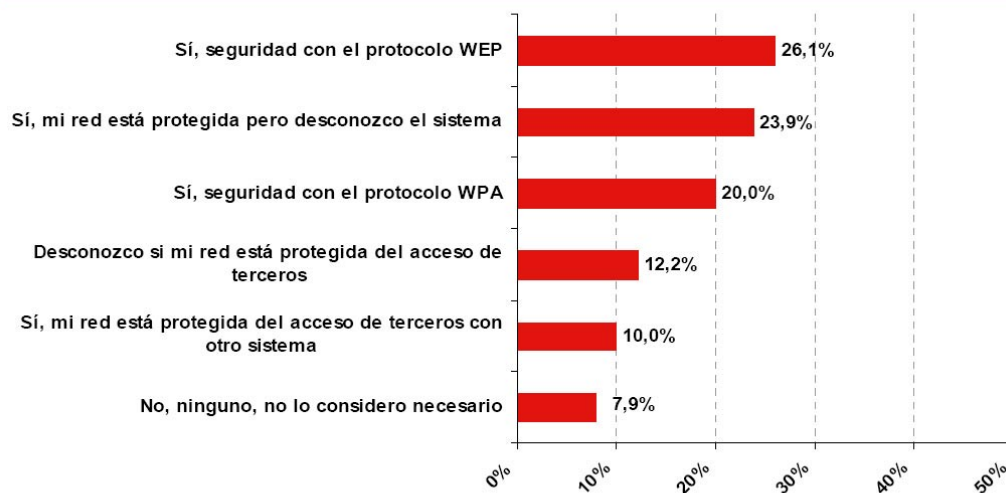
Según el Informe Wifi 2008 del Observatorio Wireless del Grupo Gowex, la mitad de los internautas españoles se conectan a Internet mediante WiFi.

**Usuarios de Internet y de Wi-Fi**



Según el “Estudio sobre la situación de seguridad y buenas prácticas en dispositivos móviles y redes inalámbricas” publicado por el Instituto Nacional de Tecnologías de la Comunicación (Inteco), solo el 30% de los usuarios han protegido su red WiFi con encriptación WPA u otro sistema, mientras que casi un 50% de los usuarios sigue utilizando WEP o desconoce la encriptación de su punto de acceso inalámbrico.

**Gráfico 13: Estado de la protección de accesos inalámbricos a Internet en el hogar**



Fuente: INTECO (Mayo 2008)

## WEP como encriptación por defecto

La configuración que los proveedores de Internet establecen en el router WiFi está diseñada para facilitar su uso y maximizar la compatibilidad con los dispositivos WiFi del cliente. El usuario medio desconoce los detalles técnicos de configuración de su router, de modo que en la mayoría de los casos esta configuración permanecerá inalterada durante toda la vida útil del router.

Aunque la inseguridad del protocolo WEP es conocida desde hace años, a día de hoy algunos proveedores de Internet siguen proporcionando routers WiFi configurados por defecto con encriptación WEP. La razón podría estar en que aún hay muchos usuarios que siguen utilizando dispositivos obsoletos cuya conectividad inalámbrica solo soporta WEP. Para evitar problemas que acaban convirtiéndose en incidencias abiertas en el Servicio de Atención al Cliente de la operadora, se opta por preconfigurar la encriptación más común, renunciando a la seguridad superior que ofrecería WPA.

El resultado es que durante los últimos años, coincidiendo con la explosión del uso del WiFi, se han estado creando continuamente redes WiFi vulnerables. Con la falsa seguridad de sentirse protegido por una clave, estas redes permiten el acceso de terceros a la información que por ellas circula.

## La debilidad de la encriptación WEP

Para enviar un mensaje a través de la red inalámbrica, el protocolo WEP sigue el siguiente proceso:

Calcula la redundancia cíclica (CRC32) del mensaje para que el destinatario pueda comprobar su integridad.

Genera el vector de inicialización, un número aleatorio entre 0 y 4094.

Genera una semilla concatenando la clave secreta y el vector de inicialización.

Encripta la semilla con el algoritmo RC4.

Se encriptan los datos realizando una operación binaria O exclusiva entre el mensaje concatenado al CRC32 y la semilla encriptada.

Se adjunta al mensaje encriptado el vector de inicialización para que el destinatario, conociendo la clave secreta, pueda realizar la operación inversa y obtener el mensaje original.

Los problemas de seguridad que plantea este proceso han sido ampliamente documentados y se pueden resumir en los siguientes:

El Vector de Inicialización (IV) solo permite 4095 valores distintos, por lo que acabará repitiéndose con frecuencia. Aunque debería ser aleatorio, en muchos casos simplemente es incremental y por tanto predecible.

Se utiliza RC4, un sistema de cifrado de datos diseñado en 1987 y que desde 2001 está descartado su uso como encriptación segura por ser vulnerable a varios ataques.

Existen varias aplicaciones públicamente disponibles en Internet que automatizan el proceso de obtención de la clave secreta a partir de los mensajes encriptados capturados.

## La claves establecidas por los ISP son predecibles

Si por sí solo el protocolo WEP es inseguro, el problema se agrava debido a las claves con las que los ISP preconfiguran los equipos. Supuestamente, el ISP establece en cada uno de los equipos que entrega, una clave aleatoria singular. Solo conociendo esta clave única por equipo se puede autenticar un usuario ante el router para acceder a la red.

En realidad, la estructura de la clave responde a un patrón predefinido. Si lo conocemos, podemos averiguar varios caracteres de la clave, reduciendo drásticamente el número de combinaciones posibles. Aunque en este estudio solo se describe el patrón de claves utilizado por el principal operador español, el problema se repite en la mayoría de proveedores de Internet.

Telefónica preconfigura claves WEP de 104 bits en sus equipos. Sus 13 caracteres nos permitirían 1.048.575 variaciones. Sin embargo, el patrón utilizado por la operadora nos permite deducir 9 de los 13 caracteres. Solo 4 caracteres de la clave son aleatorios, lo que reduce las combinaciones a 65.535, que acabarán siendo bastantes menos puesto que solo se utilizan letras mayúsculas y números.

El primer carácter de la clave de acceso corresponde a el fabricante del router, que podemos averiguar cotejando los tres primeros dígitos de la MAC del punto de acceso (dato público emitido por el router) con el listado de fabricantes que mantiene el organismo estandarizador IEEE.

Los seis siguientes caracteres de la clave corresponden con los seis primeros caracteres de la MAC del punto de acceso.

El nombre de la red WiFi que el usuario ve en el listado de redes disponibles de sus sistema operativo, tiene el patrón WLAN\_XX, donde XX son dos caracteres alfanuméricos que corresponden con los dos últimos caracteres de la clave secreta.

## Ejemplo

Estando bajo la cobertura de una red WiFi queremos averiguar su clave de 13 caracteres:

xxxxxxxxxxxxx

La red se identifica como WLAN\_45, por lo que los dos últimos caracteres de la clave serán 45.

xxxxxxxxxx45

La dirección MAC del punto de router es 00:01:38:45:23:10. Con sus primeros 3 valores obtenemos 6 caracteres más de la clave.

x000138xxxx45

Según el IEEE las MACs iniciadas por 00:01:38 son utilizadas por el fabricante Xavi. Su inicial, X, será el primer carácter de la clave.

X000138xxxx45

Ya tenemos 9 de los 13 caracteres, el 70% de la clave. Para averiguar el resto solo hará falta capturar varios paquetes y probar a desencriptarlos recorriendo todas las combinaciones posibles de los 4 caracteres que faltan. Con el poder de computación de un procesador actual resulta prácticamente instantánea la obtención de los 4 caracteres que faltan mediante fuerza bruta.

## Popularización de las herramientas de explotación

Este proceso, que por su complejidad solo podría ser llevado a cabo por usuarios expertos, resulta muy sencillo de reproducir por cualquier persona sin grandes conocimientos técnicos gracias a la popularización de herramientas que automatizan la explotación de las vulnerabilidades. Estas son algunas de ellas:

### Aircrack-ng

Conjunto de herramientas de referencia para auditar la seguridad de redes inalámbricas. Incluye programas para capturar paquetes y realizar varios ataques sobre ellos para obtener la clave secreta.

<http://www.aircrack-ng.org/>

## Wifiway y Wifislax

Distribuciones GNU/Linux para la auditoría de seguridad de redes inalámbricas. Reúnen las principales herramientas necesarias y pueden ser ejecutadas sin necesidad de instalar en el equipo, arrancando desde el CD.

<http://www.wifiway.org/>

<http://www.wifislax.com/>

## Estudio de Redes Wireless

Interfaz gráfico para diversas herramientas de auditoría wireless sobre Windows. Contiene aplicaciones específicas para obtener la clave de redes de Telefónica y Orange.

[http://lampiweb.com/erw\\_estudio\\_de\\_redes\\_wireless.html](http://lampiweb.com/erw_estudio_de_redes_wireless.html)

## WLAN Decripter

Generador de diccionario de claves específico para routers de Telefónica.

Con estas herramientas, la obtención de la clave a partir de un paquete capturado de un cliente autenticado es cuestión de segundos. Destaca especialmente el hecho de que existan programas específicos creados a medida para determinados proveedores de Internet.

## Implicaciones

En el ámbito doméstico, el principal problema puede surgir por el mal uso de la conexión a Internet que realice el atacante. Una vez obtenido el acceso, sus actividades en la red dejaran como rastro la IP del titular de la línea de banda ancha, por lo que cualquier acto ilegal, como la intromisión en sistemas informáticos o la descarga de pornografía infantil, señalará a la IP del abonado.

En el ámbito empresarial, una red vulnerable representa un talón de Aquiles a través del que un tercero puede obtener acceso a la red corporativa, permitiendo el espionaje industrial, la obtención de claves mediante la captura de tráfico, etc.

## Configuración WiFi en los routers de Telefónica

Este estudio se centra en la configuración por defecto con la que Telefónica de España S.A. entrega los routers a los clientes que contratan una conexión de banda ancha fija, como puede ser ADSL o FTTH (fibra óptica hasta el hogar). La elección de este proveedor de Internet queda justificada por su posición de dominio con la mayor cuota de mercado de accesos de banda ancha.

Producto comercializado	Router inalámbrico	Encriptación	Longitud de clave	Clave
Dúo y Trío ADSL	Zyxel P660HW-D1	WEP	104 bits	Patrón alfanumérico
Trío Futura	Zyxel P2302 HWUDL-P1	WEP	104 bits	Patrón alfanumérico

En ambos casos se entrega al cliente el router configurado con encriptación WEP con clave de 104 bits que sigue un patrón alfanumérico parcialmente predecible. Bajo el dispositivo se adhiere una etiqueta con la configuración de la red inalámbrica suministrada.



En la siguiente imagen puede verse la configuración con la que se entrega el router Zyxel P2302 HWUDL-P1 a los clientes que contratan el producto Trío Futura. De nuevo, la configuración por defecto es encriptación WEP con clave de 104 bits que sigue un patrón alfanumérico parcialmente predecible. En este caso la opción WPA aparece destacada como recomendable.



El "Manual de Usuario del Router Inalámbrico" dedica la sección "Implicaciones de acceso público" a informar sobre el riesgo de intrusiones externas desde Internet y recomienda el uso de un firewall. Sin embargo no se informa sobre el riesgo de intrusiones a través de la red inalámbrica. Únicamente se hace alusión a este problema en la sección "Red inalámbrica" recomendando la encriptación WPA si todos los clientes son compatibles, así como modificar la clave suministrada por defecto.

# Informe

## Metodología

Durante la tarde del lunes 8 de diciembre de 2008, se realizó un recorrido de 15 km. por algunas de las principales calles de la ciudad de Alicante con el objetivo de recoger una muestra lo suficientemente representativa de las redes WiFi activas en un núcleo urbano. Aunque se ha seleccionado esta ciudad por la proximidad al lugar de residencia del autor del estudio, cualquier otra capital de provincia del estado español hubiese resultado igualmente útil para el propósito de este estudio, ya que los operadores proporcionan el mismo equipamiento a sus clientes independientemente de su ubicación.



## Equipo utilizado

Fonera con firmware Legend 4.5

Antena omnidireccional 9 dBi Zaapa ZW-UL895-02

Ordenador portátil Macbook ejecutando Windows XP

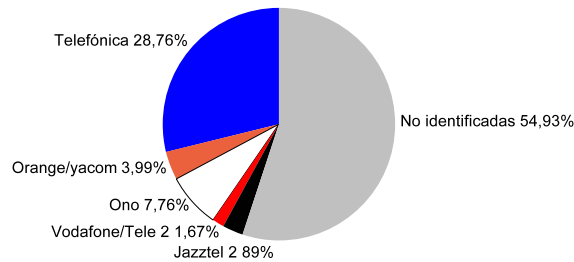
Se ha utilizado una Fonera ya que su chip Atheros tiene una excelente sensibilidad para la captura de señales de radio a gran distancia. El firmware original fue sustituido por el Legend, que incluye todos los paquetes necesarios para auditar redes wireless. Mediante el detector de redes Kismet, se capturaron datos sobre las redes disponibles en bloques de 300 hasta alcanzar un total de 3.326 ESSID válidas. El listado obtenido se filtró para descartar clientes y MACS repetidas debido al efecto de ida y vuelta sobre una misma calle.

La sesión se realizó en coche y duró aproximadamente 1 hora. La velocidad media fue de 15 km/h. En algunos tramos se llegaron a capturar más de 200 redes en solo 100 metros de recorrido. Los datos recogidos automáticamente quedaban almacenados en la carpeta compartida en el ordenador portátil, debidamente montada en la Fonera mediante CIFS.

# Resultados

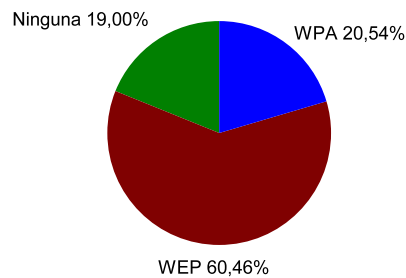
## ISPs detectados

A partir del nombre de la red (SSID) se ha deducido el proveedor de Internet que da servicio al punto de acceso. Se han descartado del estudio los puntos de acceso en los que el SSID ha sido modificado por el usuario.



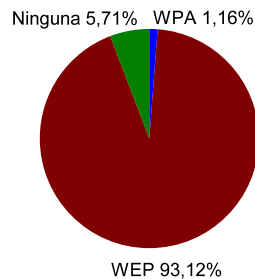
## Todas las redes

De las 3.326 redes detectadas, 2.011 utilizan WEP, mientras que 632 permanecen desprotegidas. Solo 683 están protegidas con WPA.



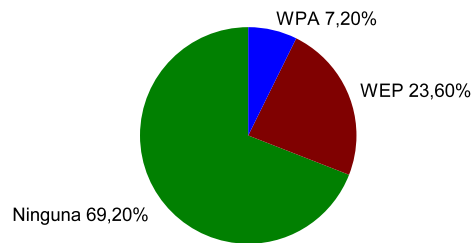
## Telefónica

Se han detectado 923 redes de Telefónica, de las que 880 permanecían con la configuración original establecida por la operadora: identificador WLAN\_XX, encriptación WEP y patrón de clave alfanumérico.

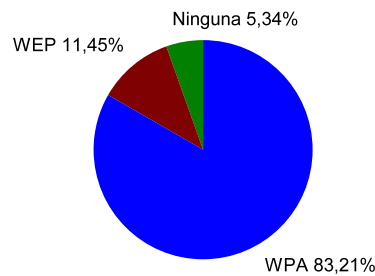


## Ono

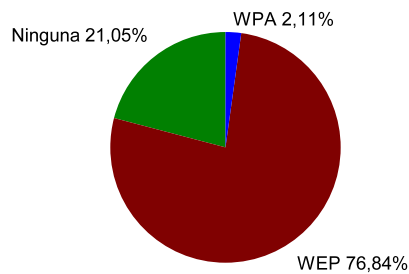
Ono tiene el mayor porcentaje de redes abiertas. Esto puede ser debido a que hasta hace poco suministraba equipos con la encriptación desactivada.



## Orange/Yacom

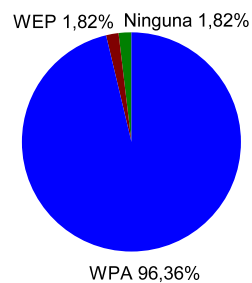


## Jazztel



## Vodafone/Tele 2

Vodafone/Tele2 es la operadora con mayor porcentaje de puntos de acceso protegidos por WPA.



## Conclusiones

Más de la mitad de las redes WiFi siguen utilizando en la actualidad la encriptación WEP y por tanto su seguridad puede ser fácilmente vulnerada.

La situación es especialmente grave en las redes del principal ISP, donde un 93% de los routers WiFi de Telefónica continúan con la configuración original establecida por la operadora. En este caso, además de ser vulnerables debido a el uso de WEP, las claves son parcialmente predecibles debido a el uso de patrones.

El uso de WEP en las redes de Jazztel es muy similar a la de Telefónica.

Ono ha dejado en manos de sus clientes la decisión de proteger su red, lo que ha provocado que gran parte de las redes del operador ellas estén completamente abiertas.

Orange con el 88% y Vodafone con 96% son los que mejor protegen las redes WiFi de sus clientes.

## Recomendaciones

Establecer un configuración WiFi segura en el punto de acceso inalámbrico:

- Cambiar el identificador SSID predefinido para evitar que se identifique el ISP y configuración original

- Activar la encriptación WPA

- Utilizar una longitud de clave de 160 o 504 bits.

- Establecer una clave formada por una combinación aleatoria de mayúsculas, minúsculas, números y símbolos.





B A N D A A N C H A . E U