



INSTITUTO de ENSEÑANZAS a DISTANCIA de ANDALUCÍA

2º de Bachillerato
Tecnologías de la Información y Comunicación
Contenidos

**Diseño web funcional. Prevención y buenas prácticas:
Ciberseguridad, criptografía y cifrado**



Imagen en Pixabay de [Alexas_Fotos](#)

bajo licencia CC0 Public Domain

"El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él" (Eugene Spafford, Profesor de Informática en la Universidad de Purdue (Indiana, EEUU) Y experto en seguridad informática).

Hoy en día es prácticamente inconcebible el uso de un ordenador sin conexión a Internet o un smartphone sin conexión de datos.

Esta claro que el estar interconectados nos ofrece una infinidad de servicios y utilidades, pero también implica sus riesgos. Ya no estamos aislados, si no que nos conectamos a una red mundial a la que también pueden estar conectados otros individuos con no tan buenas intenciones.

Veremos en este tema, algunos de los posibles peligros que aparecen cuando nos conectamos a una red, y algunas herramientas para minimizarlos.

1. Cortafuegos o Firewalls

Desde el momento en que nos conectamos a Internet o a cualquier red externa, aparecen peligros potenciales.

Para filtrar y bloquear estos posibles ataques desde fuera de nuestra red (red local o corporativa de una empresa) aparecen los firewalls (o cortafuegos).

Internet se basa en el sistema TCP/IP en el que los mensajes de datos, para su transmisión por la red, se fragmentan en otros denominados paquetes (que además de los datos incorporan información necesaria para su transmisión por la red). La función de un cortafuegos es la de analizar estos paquetes y permitir su acceso a nuestra red o bloquearlos, en función de unas reglas que el administrador o usuario debe haber definido.

Nos podemos encontrar cortafuegos en dos niveles diferentes:

- Por un lado, tenemos cortafuegos personales, que se instalan en equipos de usuarios que se conectan a Internet desde casa o cualquier otro lugar, para proteger a ese equipo y a sus datos.
- Por otro lado, existen cortafuegos profesionales, que pueden ser servidores con un software específico o máquinas especialmente diseñadas para este fin. Se suelen instalar en empresas y su función es aislar la red corporativa de Internet. Suelen tener distintas tarjetas de red, de forma que aplican reglas distintas a las diferentes redes dentro de la empresa.

Los cortafuegos pueden funcionar de dos formas:

- Se deniega todo por defecto y se añaden reglas indicando lo que está permitido (es más restrictivo, pero mucho más seguro).
- Se permite todo por defecto y se van añadiendo distintas reglas indicando que tipo de tráfico o aplicaciones son las que no permitimos.

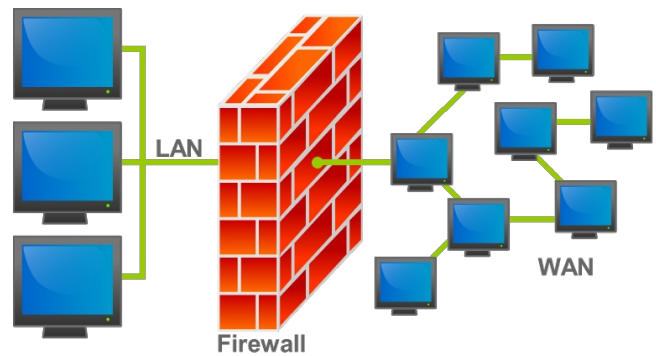


Imagen en Wikimediacommons de [Bruno Pedrozo](#) bajo licencia [Creative Commons Attribution-Share Alike](#)

Hoy en día es habitual tener conexión a Internet en los hogares, por lo que también surge la necesidad de proteger a estos equipos que se conectan por ADSL, fibra o cualquier otra tecnología a Internet.

Este tipo de cortafuegos de uso personal, sobre un equipo concreto (no a nivel de red), suele proporcionarse de distintas formas:

- Puede venir **incluido en el propio sistema operativo**, como hace Windows o Linux con [Iptables](#).

En el caso de Windows, para acceder a la configuración: **Inicio /Panel de Control /Sistema y seguridad/Firewall de Windows**.

En el menú izquierdo aparecerán las distintas posibilidades, entre las que caben destacar:

- **Activar o desactivar Firewall de Windows**: que permitirá parar o no el firewall, en caso de desactivación, dejará de analizar los paquetes y permitirá todo el tráfico.

- **Permitir un programa o una característica acceder a través de Firewall de Windows**: Nos permite determinar si programas locales en nuestro equipo, pueden o no acceder a Internet y cómo queremos que lo hagan. En caso de no estar permitido, el programa al ejecutarse, no podría salir a Internet ni conectarse con ninguna máquina exterior.

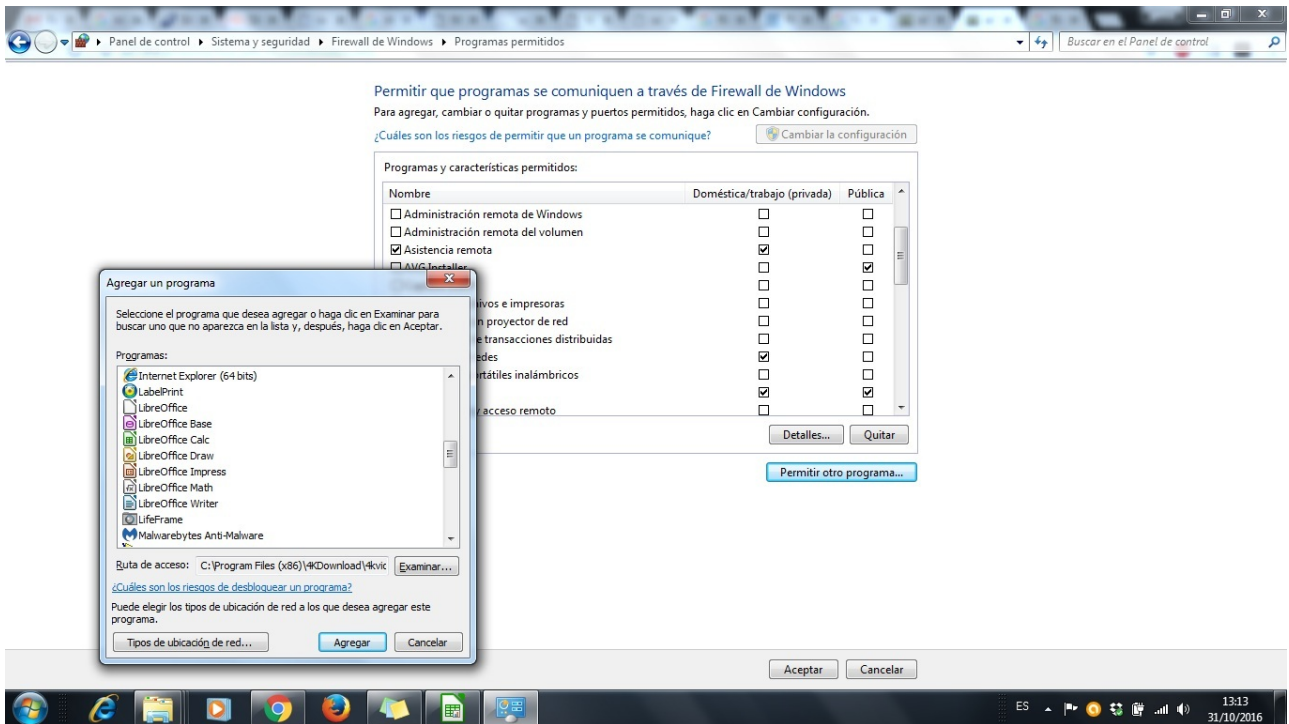


Imagen de creación propia bajo licencia CC

- **Configuración avanzada**: permite establecer reglas específicas, especificando puertos, protocolos e IPs permitidas o no.

- O instalarse como **aplicación específica**. Hoy en día generalmente viene ya integrado en paquetes de seguridad que incluyen además del firewall, antivirus, filtros anti-spam, etc. Algunos ejemplos serían [Avast](#) o [ZoneAlarm](#). Otros desarrolladores como Avira han decidido suprimir el firewall de sus suites de seguridad, entendiéndose que el incluido en los S.O. es suficiente.



Imagen en Wikimediacommons de [Cuda-mwolve](#) bajo licencia [Creative Commons Attribution-Share Alike 4.0 International](#)

los paquetes que pretenden ir o que salen, de una u otra red, a través de las distintas tarjetas o bien dos Firewalls, uno que ponga reglas al tráfico hacia o desde Internet y otro que proteja la red interna (LAN).

Sea cual sea la configuración física, el comportamiento y configuración es el mismo, se establecerán una serie de reglas atendiendo al protocolo, dirección IP o red de destino, dirección IP o red de origen origen, y se le atribuirá una acción en caso de que se cumplan los requisitos, esta acción será rechazar el paquete o permitirlo.

Se trata de servidores con software específico o máquinas diseñadas como firewalls. Su misión es proteger unos segmentos de red de otros y de Internet.

En una empresa grande, normalmente hay dos redes diferenciadas, una, los puestos de los trabajadores, y otra, la zona de servidores (correo, web, FTP, etc.) que no sólo deben acceder a Internet, si no que además deben poder ser accedidos desde el exterior (un servidor web sin acceso sería poco útil). Los servidores normalmente se encuentran en una subred aparte, denominada DMZ (o zona desmilitarizada).

Respecto a la configuración del firewall, puede ser uno, con varias tarjetas de red, de forma que separe la zona de puestos de trabajo, de la DMZ y de Internet, aplicando las reglas configuradas a

1.3. Reglas



Para definir reglas en un firewall deberemos tener en cuenta lo siguiente:

Configuración inicial	Si por defecto permitimos todo salvo aquello para lo que luego añadamos reglas, o si por el contrario, lo vamos a cortar todo, salvo aquello que luego permitamos.
Dirección	Si las reglas se aplican para el tráfico que entra desde Internet o para el que sale hacia Internet. En el caso de firewall con varias tarjetas de red, esto se complica, pues tendremos que decir si se aplica para el tráfico de salida o entrada por una tarjeta o para todas.
Protocolo y puerto	Para definir una aplicación, deberemos especificar el protocolo que utiliza (TCP/UDP) y el puerto.
Red o IP origen destino.	Dirección IP de la máquina que vamos a permitir o denegar o subred (para el caso de varias máquinas en la misma red).
Acción	Una vez establecida la aplicación y direcciones de origen y destino, deberemos decir si los paquetes (de tráfico) que verifiquen esa condición los vamos a dejar pasar a través del firewall (ACCEPT) o si los vamos a rechazar (DENY)



Imagen en Wikimedia Commons de [Wi-Fi Alliance](#) bajo licencia [Public Domain with non-copyright restrictions](#)

Hoy en día el auge de las redes inalámbricas es indiscutible.

Son mucho más flexibles que las redes cableadas, nos permiten movernos de un lado a otro, tienen bastante cobertura (depende de los obstáculos que encuentren las ondas que propagan las señales, pero en espacios abiertos puede ser de cientos de metros), son más cómodas y además más económicas que las cableadas, nos permiten conectar nuestro smartphone, nuestra tablet, nuestro portátil, etc. sin tener que permanecer anclados en un punto, como ocurría antes con los ordenadores de sobremesa conectados por un cable a una red ethernet.

Pero aunque en principio todo parecen ser ventajas no es así, presentan más vulnerabilidades que las redes cableadas, que comprometen la confidencialidad, integridad y disponibilidad de la información que viaja por ella.

Cualquiera en el área de alcance de la red puede intentar distintos ataques a ésta.

- **Ataques de denegación de servicio (DoS):** metiendo señales a la misma frecuencia que emite nuestro punto de acceso de forma que se impide la conexión de cualquier equipo a él.
- **Ataques con MAC falsa:** de forma que el equipo atacante cambia su MAC por la de nuestro punto de acceso, engañando a todos los equipos de nuestra red.
- **Escuchas de tráfico o sniffing:** puesto que la información viaja por el aire cualquiera en el área de cobertura podría interceptarla.
- **Captura de claves de acceso:** se podrían capturar las conversaciones entre una máquina y nuestro router o punto de acceso, obteniendo así las claves de acceso (este procedimiento es relativamente fácil en redes poco seguras como las WEP).
- **Conexión a la red a usuarios no autorizados:** si un equipo es capaz de capturar la clave de acceso a la red wifi, podrá conectarse a esta libremente.

Puesto que en las redes wifi la información viaja por el medio aéreo y puede ser capturada por cualquiera en la zona de cobertura, parece obvia la necesidad de encriptar la información con el fin de protegerla.

Antes de ver los protocolos de cifrado que se usan en este tipo de redes, recordemos algunas de las ideas fundamentales acerca de la criptografía.

Para saber más

Criptografía proviene del griego, *krypto* significa oculto y *graphos* escribir, es decir, sería algo como escritura oculta.

La criptografía engloba los mecanismo por los cuales un mensaje inicial (texto en claro) se convierte en otro inteligible (texto cifrado) del que se podrá de nuevo obtener el mensaje original, pero sólo en el caso en que se posea la clave.

Los distintos métodos para ocultar o cifrar la información de partida se conocen como **algoritmos de cifrado**.




Imagen en [WikimediaCommons](#)
bajo licencia [Dominio público](#)

TIPOS DE SISTEMAS DE CIFRADO

- **Criptografía simétrica:** en la que emisor y receptor comparten una misma clave para el cifrado y descifrado del mensaje.
- **Criptografía asimétrica:** emisor y receptor usan un par de claves, clave pública y clave privada, la clave pública es compartida, pero no así la privada. El emisor cifrará con la clave pública siendo sólo posible el descifrado con la clave privada del receptor.

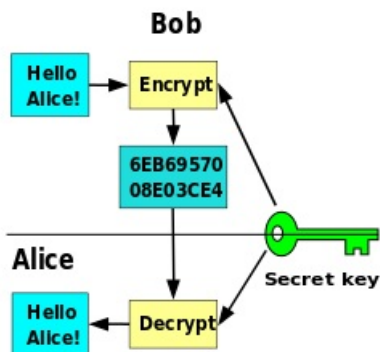


Imagen en [WikimediaCommons](#) de [Phayzfaustyn](#) bajo licencia [CC0 1.0 Universal Public Domain Dedication](#)

ENCRIPCIÓN CON CLAVE SIMÉTRICA

En este tipo de sistemas el mensaje es cifrado y descifrado con la misma clave privada, que debe ser conocida por el transmisor y por el receptor.

Esto representa un problema pues es necesario encontrar un modo seguro de comunicar la clave entre emisor y el receptor.

Si el mensaje cifrado es interceptado y no se dispone de la clave, este será inteligible, pero si por cualquier mecanismo el atacante descubre la clave, el sistema de criptografía se habrá roto.

Otro inconveniente es que el emisor debe compartir una clave privada distinta con cada receptor, por lo que si envía mensajes a muchos usuarios distintos será necesario el recordar muchas claves distintas.

VENTAJAS

Son rápidos y eficientes, por lo que resultan adecuados para cifrar grandes volúmenes de datos.

INCONVENIENTES

Requieren una clave por cada emisor-receptor.

Requieren un medio seguro de transmisión de la clave.

No son robustos. Pueden romperse por ataques como el de clave relacionada (como ocurre con el cifrado WEP de redes inalámbricas), aprovechando la naturaleza del algoritmo y relaciones entre texto original y claves o por mecanismos de fuerza bruta, que prueban todas las posibles claves (cuanto más larga sea la clave más tiempo se empleará en obtenerla)

ENCRIPCIÓN CON CLAVE ASIMÉTRICA

Los sistemas de cifrado por clave asimétrica usan un par de claves: una privada (que solo conoce el propietario) y otra pública (que es la que se intercambia).

En este caso no habrá problemas con el intercambio de la clave (tal y como ocurría en los sistemas de clave simétrica) pues el atacante no podrá hacer nada sólo con la clave pública, necesitaría también la privada (que sólo la tiene el propietario y no se ha intercambiado en ningún momento).

Estos sistemas nos serán de utilidad para dos fines principales:

- **Confidencialidad** (encriptación del mensaje de forma que solo el usuario con la clave privada adecuada lo podrá descodificar).
- **Autenticación** (garantizando que el mensaje ha sido emitido por quién dice ser)

Veamos estas dos posibilidades.

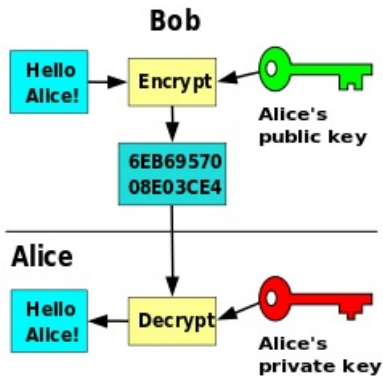


Imagen en WikimediaCommons de [Davidgothberg](#) bajo licencia [public domain](#)

revocación de certificados).

Bob desea mandar un mensaje a Alice, Bob usará su clave pública (que es de conocimiento general) para encriptar el mensaje. Pero sólo Alice, que posee la clave privada adecuada podrá descifrarlo.

VENTAJAS

La clave privada nunca se distribuye, por lo que no existe el problema de comunicación de la clave que existía en los sistemas con clave simétrica.

Solo he de conocer dos claves (la pública, de conocimiento general, y la privada, que conozco y exclusivamente), independientemente del número de receptores con los que vaya a intercambiar información (evitamos el problema de elevado número de claves cuando el número de receptores era grande que veíamos en los sistemas de clave simétrica).

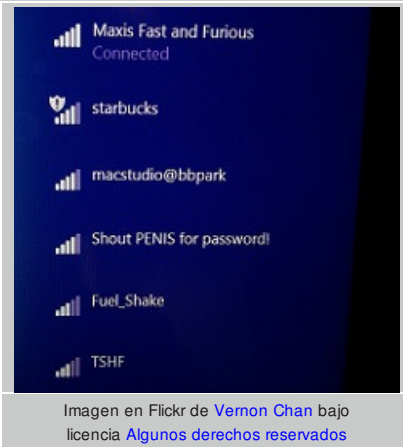
INCONVENIENTES

Requieren mayor tiempo de cifrado, los mensajes generados son más grandes, las claves empleadas también son de mayor tamaño para garantizar la seguridad. Por lo que en general requieren más tiempo y recursos que los sistemas de clave simétrica.

Es necesario algún sistema que garantice que la clave pública, que se distribuye libremente, es auténtica (p.ej. **PKI** (Infraestructuras de clave pública) que son las usadas en los DNle o con los certificados digitales emitidos por la Fábrica Nacional de Moneda y Timbre o las **listas de**

Para saber más

¿QUÉ ES EL SSID?



El **SSID (Service Set Identifier)** es el nombre de la red. Los puntos de acceso (generalmente routers inalámbricos) los anuncian constantemente, de forma que los usuarios podrán listar las redes accesibles.

Todos los dispositivos en la misma red wifi comparten el SSID.

RED ABIERTA

No usa autenticación en el control de acceso a la red, con lo que cualquiera en la zona de alcance se podría conectar, tampoco cifra las comunicaciones.

WEP(Wired Equivalent Privacy o Privacidad Equivalente a Cableado):

El objetivo de este sistema es proporcionar a la red inalámbrica la misma seguridad que tiene una red cableada (de ahí su nombre).

Para encriptar mensajes usan claves de 104 o 40 bits (WEP 128 o WEP 64).

Para autenticar existen dos posibilidades:

- **Sistema abierto u Open system:** el cliente no se autentica para asociarse con el punto de acceso, pero una vez asociado sí tendrá que tener la clave WEP correcta para poder comunicarse.
- **Clave precompartida, Pre-Shared Keys o PSK:** En este caso existe una clave precompartida, que se usa tanto para la autenticación como para el cifrado WEP.

Es aconsejable usar la autenticación de sistema abierto para la autenticación WEP (es decir, sin autenticación), ya que es posible averiguar la clave WEP (que se usará en el cifrado de datos en la red) interceptando los paquetes intercambiados entre equipo y punto de acceso en la fase de autenticación.

Curiosidad

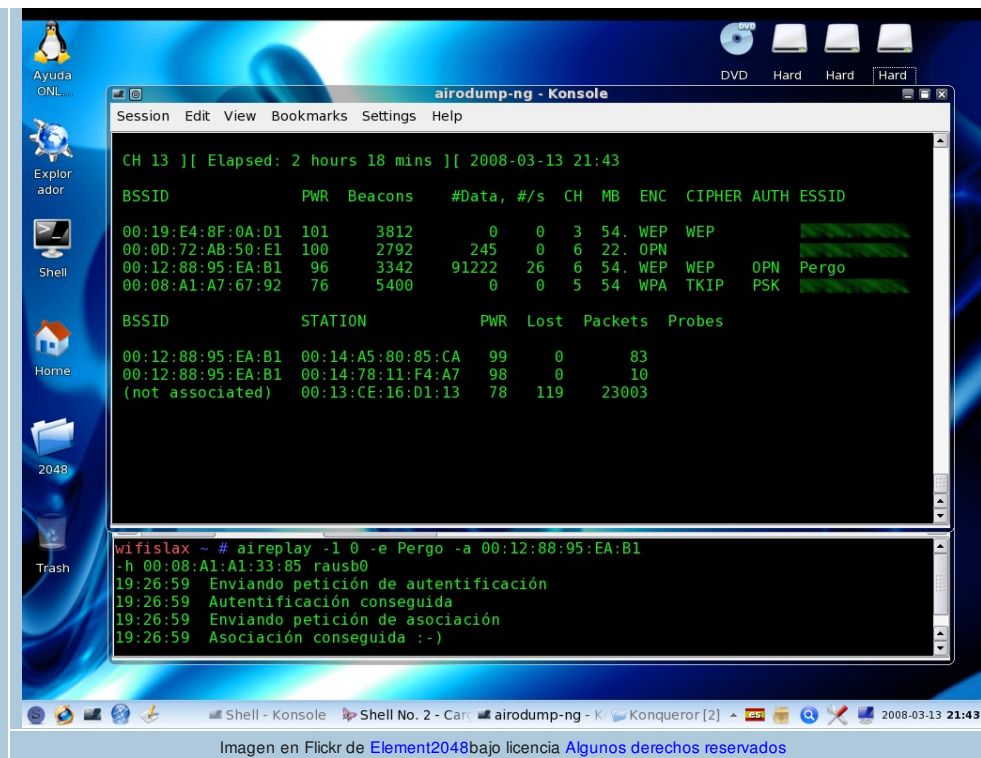


Imagen en Flickr de [Element2048](#) bajo licencia [Algunos derechos reservados](#)

AIRCRAK-NG

Esta es una suite de herramientas para estudiar y evaluar la seguridad de una red inalámbrica.

IMPORTANTE: Su uso debe quedar restringido a redes propias o a entornos de prueba y evaluación controlados. En cualquier otro caso se estarían sobrepasando los límites legales.

Hasta hace poco solo funcionaba para Linux, aunque ya hay versiones para Windows.

Se compone de varias aplicaciones:

- **Airon-ng:**
 - Nos permite poner nuestra tarjeta en modo monitor, es decir, podremos capturar paquetes de la red aunque no vayan dirigidos a nosotros.
- **Airodump-ng:**
 - Detecta puntos de acceso a nuestro alcance.
 - Para un SSID determinado (y a partir de la dirección MAC del punto de acceso) captura gran número de paquetes y los almacena en un fichero de salida.
- **Aircrack-ng:**
 - A partir de los ficheros de la fase anterior (deben tener más de 1000 paquetes útiles) intentará sacar la contraseña WEP.
 - Si no es capaz es porque el número de paquetes capturados es insuficiente, será cuestión de repetir y ser algo más pacientes.

Es por esto por lo que WEP se considera un protocolo muy débil e inseguro, ya que se puede obtener su clave con ataques sencillos y en poco tiempo.

[Página oficial \(para más información\)](#)

WPA y WPA2 (Wi-Fi Protected Access o Acceso Protegido Wi-Fi)

Creado para corregir las deficiencias del sistema WEP.

WPA fue un desarrollo intermedio y WPA2 la versión definitiva.

- **WPA Empresarial:** para grandes empresas, la autenticación usa de un servidor RADIUS donde se almacenan las contraseñas de los usuarios de la red.
- **WPA Personal:** donde la autenticación se realiza mediante clave precompartida, de un modo similar al WEP pero introduciendo como mejora, la implementación del protocolo de integridad de clave temporal (**TKIP - Temporal Key Integrity Protocol**), que cambia claves dinámicamente. También es posible usar el algoritmo de cifrado simétrico AES, más seguro que TKIP, aunque su implementación requiere de hardware más potente por lo que no se encuentra disponible en todos los dispositivos.

Existen otras medidas, que aunque las hemos oído muchas veces, realmente no aportan seguridad a la red o incluso la empeoran:

- **Filtrado por MAC**, puesto que la dirección MAC identifica de forma inequívoca a una interfaz de red, parece que el filtrar por MAC es una buena idea para limitar que equipos pueden conectarse a nuestra red, y así sería si no fuese porque existen programas para modificar la dirección MAC muy fácilmente. De forma que podríamos estar autorizando al atacante con MAC falsa.
- **Ocultar el SSID**, parece que si nuestro SSID no aparece en el listado de redes accesibles, nuestra red es ya segura. Pues bien, esto no es exactamente así, puesto que el punto de acceso no difunde su SSID, son los clientes los que continuamente preguntan al punto de acceso si esa red sigue operativa, con lo que un atacante podría hacerse pasar por el punto de acceso respondiendo a esas peticiones y suplantar la red.

Curiosidad

SIMULADORES DE ROUTERS DE LINKSYS

Esta herramienta te ofrece simuladores de equipos linksys, puntos de acceso y routers inalámbricos.

Con lo que podrás ver como son en realidad y como se configuran las distintas opciones:

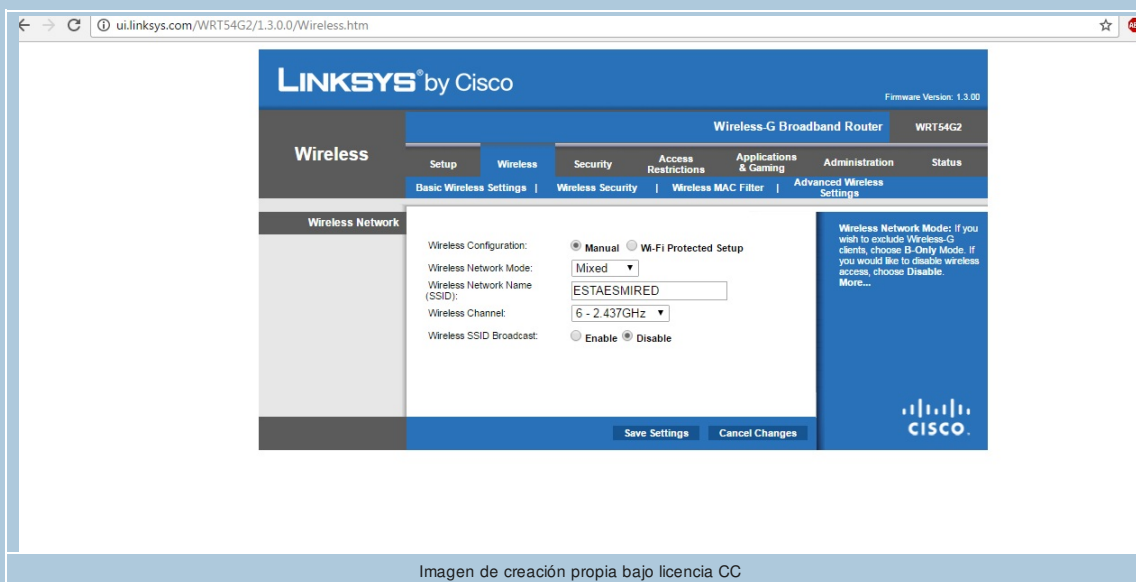
- Parámetros de la wifi
- DHCP (para que de direcciones a los equipos automáticamente).
- Opciones de seguridad
- Filtrado por MAC
- Filtrado por protocolo y puerto
- Etc

Todo ello sin miedo a equivocarte, porque se trata de simuladores y no de equipos reales.

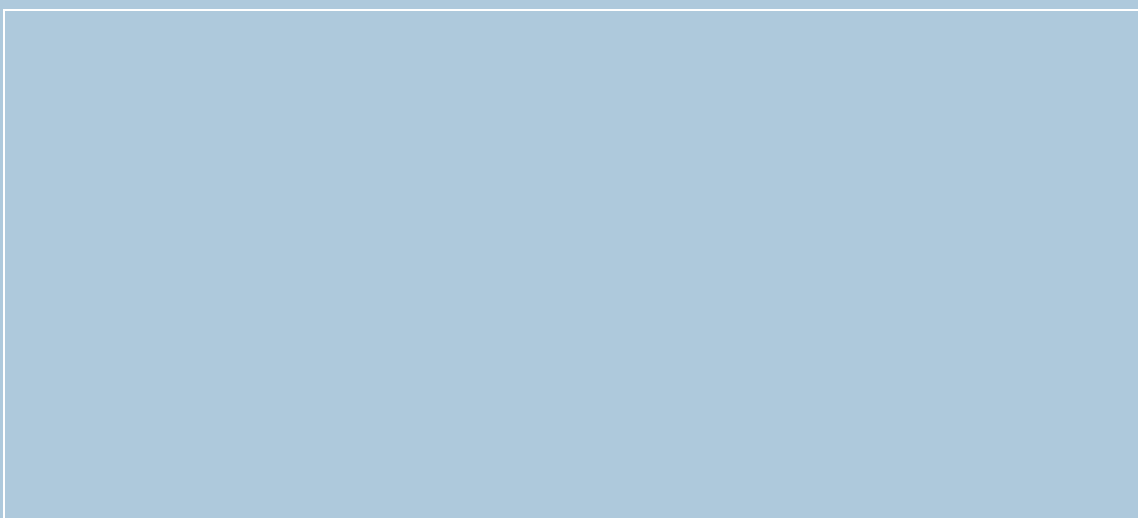
[Listado completo de equipos](#)

[Modelo de ejemplo WRT54GX4](#). Aquí puedes ver como serían algunas de las pantallas con configuraciones básicas de cualquier router inalámbrico:

Configuración básica red Wifi:



Filtrado MAC:



ui.linksys.com/WRT54G2/1.3.0.0/WFilter.htm

LINKSYS by Cisco Firmware Version: 1.3.0B

Wireless-G Broadband Router **WRT54G2**

Wireless | Setup | **Wireless** | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | **Wireless MAC Filter** | Advanced Wireless Settings

Wireless MAC Filter

Wireless MAC Filter: Enable Disable

Prevent: Prevent PCs listed from accessing the wireless

Permit only: Permit only PCs listed to access the wireless network

MAC Address Filter List - Google Chrome

ui.linksys.com/WRT54G2/1.3.0.0/WMList.htm

MAC Address Filter List

Enter MAC Address in this format: xx:xx:xx:xx:xx:xx

MAC 01:	<input type="text"/>	MAC 11:	<input type="text"/>
MAC 02:	<input type="text"/>	MAC 12:	<input type="text"/>
MAC 03:	<input type="text"/>	MAC 13:	<input type="text"/>
MAC 04:	<input type="text"/>	MAC 14:	<input type="text"/>
MAC 05:	<input type="text"/>	MAC 15:	<input type="text"/>
MAC 06:	<input type="text"/>	MAC 16:	<input type="text"/>
MAC 07:	<input type="text"/>	MAC 17:	<input type="text"/>
MAC:	<input type="text"/>	MAC:	<input type="text"/>

Wi-Fi_Logo.svg.png Wi-Fi_Logo.svg.png Wi-Fi_Logo.svg.png 16px-Wi-Fi_Logo....png

Imagen de creación propia bajo licencia CC



Imagen de creación propia bajo licencia CC

Aviso legal

El presente texto (en adelante, el "**Aviso Legal**") regula el acceso y el uso de los contenidos desde los que se enlaza. La utilización de estos contenidos atribuye la condición de usuario del mismo (en adelante, el "**Usuario**") e implica la aceptación plena y sin reservas de todas y cada una de las disposiciones incluidas en este Aviso Legal publicado en el momento de acceso al sitio web. Tal y como se explica más adelante, la autoría de estos materiales corresponde a un trabajo de la **Comunidad Autónoma Andaluza, Consejería de Educación, Cultura y Deporte (en adelante Consejería de Educación, Cultura y Deporte Andaluza)**).

Con el fin de mejorar las prestaciones de los contenidos ofrecidos, la Consejería de Educación, Cultura y Deporte Andaluza se reservan el derecho, en cualquier momento, de forma unilateral y sin previa notificación al usuario, a modificar, ampliar o suspender temporalmente la presentación, configuración, especificaciones técnicas y servicios del sitio web que da soporte a los contenidos educativos objeto del presente Aviso Legal. En consecuencia, se recomienda al Usuario que lea atentamente el presente Aviso Legal en el momento que acceda al referido sitio web, ya que dicho Aviso puede ser modificado en cualquier momento, de conformidad con lo expuesto anteriormente.

1. Régimen de Propiedad Intelectual e Industrial sobre los contenidos del sitio web

1.1. Imagen corporativa

Todas las marcas, logotipos o signos distintivos de cualquier clase, relacionados con la imagen corporativa de la Consejería de Educación, Cultura y Deporte Andaluza que ofrece el contenido, son propiedad de la misma y se distribuyen de forma particular según las especificaciones propias establecidas por la normativa existente al efecto.

1.2. Contenidos de producción propia

