

- [Noticias](#)
- [Foros](#)
- [Descargas](#)
- [Drivers](#)
- [Manuales](#)




Publicidad

Qué comentan tus amigos

**Regístrate**

Crea una cuenta o [inicia sesión](#) para ver qué están haciendo tus amigos.

---



**Cómo conceder permisos de acceso a archivos y carpetas en Windows 7**  
Una persona recommended esto.

---

Plug-in social de Facebook

Publicidad



### Especiales Windows 7

- [Trucos para Windows 7](#)
- [de Windows XP a Windows 7](#)
- [Antivirus para Windows 7](#)
- [Programas de descargas Windows 7](#)
- [Salvapantallas de Windows 7](#)

### Especial Sistemas Operativos

- [de Windows XP a Windows 7](#)
- [Moblin 2.0 beta](#)
- [Android en Windows 7](#)
- [Lanzamiento de Snow Leopard](#)

### Webs amigas

- [iPad 2](#)
- [OJO Internet](#)
- [OJO Buscador](#)

## 10 secretos de seguridad para tu router

La mayoría de gente que instala una red casera nunca investiga ni ahonda en las opciones de seguridad de su router. ¿Quién puede culparlos? Lo que sigue son 10 ajustes de router que puedes usar para hacer tu red más segura. Para el propósito de este artículo, se utilizó un router muy popular, el DLink DI-524. Para jugar con las opciones del router, es necesario acceder a su panel de control, y esto se hace escribiendo la dirección IP interna del router en el navegador web de cualquier PC de la red local. Para routers DLink esta dirección será <http://192.168.0.1> Para routers Linksys es <http://192.168.1.1>, y <http://192.168.1.2> para otros routers. Revisa el manual del router si ninguna de las anteriores funcionó, o mira la dirección IP del gateway por defecto con el comando `ipconfig /all` (ifconfig en GNU/Linux).

### 1. Deshabilitar UPnP

UPnP, o Universal Plug and Play, es una función práctica que permite a los dispositivos en una red autoconfigurarse solos, pero también es un riesgo de seguridad. Un troyano o un virus en una máquina de tu red podría usar UPnP para abrir un agujero en el firewall de tu router y permitir la entrada a foráneos. Así pues, es buena idea deshabilitar UPnP cuando no se utilice. Para hacer esto, pulsa en la pestaña Tools seguido del botón Misc, y en Disabled próximo al listado UPnP. Asegúrate de pulsar Apply para aplicar los cambios .

## 2. Cambiar la contraseña del administrador

Los routers vienen de fábrica con un ID de usuario y una contraseña para salvaguardar un panel de configuración del router. En un router DLink el ID de usuario es admin y la contraseña queda en blanco. Por lo tanto se debería cambiar (o crear) la contraseña lo antes posible para evitar que intrusos modifiquen la configuración del router. Para cambiar la contraseña, pulsar la pestaña Tools seguido del botón Admin y escribir la nueva en el campo Administrator .

## 3. Desactivar broadcast SSID

SSID es la abreviación de Service Set Identifier y es el nombre de tu red wireless que es difundida por un router en el espectro de radiofrecuencia. Puede ser vista por sistemas con el Wi-Fi activado que buscan conectarse a una red. Puedes deshabilitar esta función de difusión (broadcast) y así hacer invisible el router ante las intromisiones casuales de los fisgones. Pulsa la pestaña Home seguido del botón Wireless, y selecciona Disable en el campo SSID Broadcast .

Nota: hoy día existe software especializado disponible en Internet que permite encontrar redes vulnerables, así desactivar el broadcast SSID no es una medida de seguridad muy efectiva.

## 4. Activar el DMZ

Abreviatura de Demilitarized Zone, esta función te permite designar un dispositivo interno en tu red para aparentar que está fuera del firewall de tu router. Es útil y cómodo si tienes una webcam o una estación de juegos que no serán bloqueados por el firewall del router. Para configurar un DMZ, simplemente asigna a la estación (o webcam) una dirección IP interna fija, y luego activa el DMZ en el router y añade la dirección IP de la estación. Los ajustes DMZ se pueden encontrar en un router DLink pulsando la pestaña Advanced seguido del botón DMZ .

## 5. Filtrar direcciones MAC

Una dirección MAC (Media Access Control) es un identificador único -como una huella digital humana- que se asigna durante la fabricación de un dispositivo de red, tales como tarjetas de red o adaptadores Wifi. La dirección MAC de un dispositivo puede ser hallada generalmente en la base del mismo. En un PC se puede encontrar en las preferencias de la red.

En un sistema Windows, ejecutar `ipconfig /all` (o `ifconfig` en GNU/Linux) en una ventana DOS y buscar la entrada Physical Address o Dirección Física (o HWaddr en GNU/Linux). Es una serie de seis números hexadecimales semejante a este:

00-13-CE-32-E3-58

El filtrado MAC se puede usar para mantener a los fisgones fuera de nuestra red. Para activar el filtrado en un router DLink haz lo siguiente: Pulsa en la pestaña Advanced seguido del botón Filters, y después en el botón MAC Filters. Esto tiene que hacerse para cada dispositivo wireless permitido en la red. (Si tienes una caja TiVo wireless, necesitas añadir esta, también). Nota que los dispositivos conectados por un cable de red físico al router están exentos de filtrado MAC.

## 6. Personalizar el SSID

Cambia el nombre SSID en tu router borrando el de fábrica. En un router Linksys, es linksys. En un router DLink, es default. Cambia estos por otros más familiares pero originales y únicos que no faciliten ningún tipo de información personal, como tu nombre o dirección. Esto demuestra al supuesto cracker que has cambiado los ajustes de fábrica del router y que sabes cómo funciona tu router. No modificar el SSID de fábrica equivale a dar una invitación de acceso a cualquiera que se lo proponga.

## 7. Actualizar el firmware

El Firmware es el software que opera dentro de un router. Y precisamente como el software de una computadora, necesita actualizarse de vez en cuando porque los errores en el software necesitan ser parcheados. Periódicamente el fabricante de tu router publicará actualizaciones del firmware en su web, por tanto es importante comprobar a menudo si hay nuevas versiones del firmware. En un DLink DI-524, pulsa el enlace en la pestaña **Tools** y después en el botón **Firmware** para enlazar con el site de DLink donde podrás descargar el fichero del nuevo firmware. Después navega desde la pagina **Firmware Settings** en el router hasta el fichero del firmware en tu HD, y pulsa **Apply** para instalarlo en tu router. Es buena idea hacer esto sobre una conexión cableada. Una instalación fallida provocará que el router no pueda arrancar, y tendrás que reiniciar los valores de fábrica.

## 8. Reset a los valores de fábrica

Si enredas con los parámetros de configuración y no consigues devolverlos a su estado anterior, entonces puedes restaurar los valores al día en que lo compraste. Pulsa la pestaña **Tools** seguido del botón **system**. Ahora pulsa el botón **Restore** en esa página. Si tú mismo has bloqueado el router, puedes hacer un **reset hardware**. Suele haber un pequeño agujero (a veces un botón) en la parte posterior de la mayoría de routers con la palabra **RESET** a su lado. Con la ayuda de un clip u otro objeto similar, presiona el **RESET** durante 10 o 20 segundos. Cuando lo liberes, el router se reiniciará y se reseteará a los valores de fábrica. No olvides volver de nuevo a la configuración y reajustar todos los parámetros a tu antojo, incluido el update del firmware .

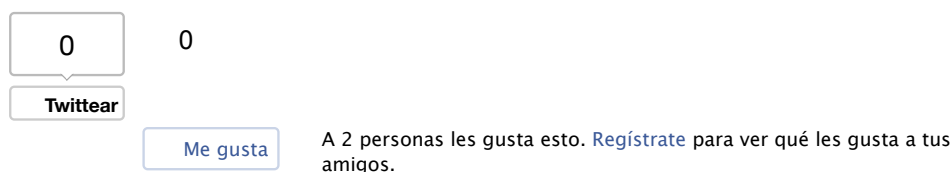
## 9. Activar cifrado WEP

WEP es la abreviación de Wired equivalent Privacy. Es sistema de cifrado incluido en el estándar 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Para habilitar el WEP, pulsa en botón **Home**, seguido del botón **wireless**. Desde el desplegable, elige **WEP**. Introduce ahora una serie de números (0 a 9) y letras (A a F). Para una clave de 64 bits, introduce 10 caracteres. Para una clave de 128 bits, introduce 26 caracteres. Así, cada vez que se intente conectar una computadora vía Wireless a tu router, se le requerirá introducir esa clave para autenticarse en tu sistema.

## 10. Activar cifrado WPA

Abreviatura de Wi-Fi Protected Access, WPA es el método preferido para encriptar tu red. Es un sistema para asegurar redes inalámbricas, creado para corregir las debilidades de WEP, como ataques estadísticos que permiten recuperar claves WEP. WPA implementa la mayoría del estándar IEEE 802.11i. Puede usarse en lugar de WEP porque es un protocolo más nuevo y seguro. Para activar el cifrado WEP, pulsa el botón **Home**, seguido del botón **wireless**. Desde el desplegable **Security**, elige **WPA-PSK** (PSK también es conocido como personal mode, abreviatura de pre-shared key). Introduce ahora frase-contraseña como “Mi carro me lo robaron”. Puedes introducir de 8 a 64 caracteres, incluyendo espacios en blanco. Pulsa **Apply** para aplicar los cambios. Ahora, cada vez que se intente conectar una computadora u otro sistema Wi-Fi a tu sistema via Wireless, se le requerirá introducir la frase-contraseña para autenticarse.

Por [Nixom](#)



© 1995 - 2013 [Ethek](#)

[Media S.L.](#) ([datos legales](#)) - [sitemap](#)  
loading