

Seguridad en redes Wi-Fi inalámbricas

Consideraciones previas.

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio –en principio- pueden viajar más allá de las paredes y filtrarse en habitaciones/casas/oficinas contiguas o llegar hasta la calle.

Si nuestra instalación está **abierta**, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino también acceder a nuestra red interna o a nuestro equipo –donde podríamos tener carpetas compartidas- o analizar toda la información que viaja por nuestra red –mediante *sniffers*- y obtener así contraseñas de nuestras cuentas de correo, el contenido de nuestras conversaciones por MSN, etc.



Si la infiltración no autorizada en redes inalámbricas de por sí ya es grave en una instalación residencial (en casa), mucho más peligroso es en una instalación corporativa. Y desgraciadamente, cuando analizamos el entorno corporativo nos damos cuenta de que las redes cerradas son más bien escasas.

Nuestro objetivo: conseguir una red Wi-Fi más segura.

Más que hablar de **la gran regla de la seguridad** podemos hablar de una serie de estrategias que, aunque no definitivas de forma individual, en su conjunto pueden mantener nuestra red oculta o protegida de ojos ajenos.

Acción	Dificultad
Cambia la contraseña por defecto	Baja
Usa encriptación WEB/WPA	Alta
Cambia el SSID por defecto	Baja
Desactiva el broadcasting SSID	Media
Activa el filtrado de direcciones MAC	Alta
Establece el nº máximo de dispositivos que pueden conectarse	Media
Desactiva DHCP	Alta
Desconecta el AP cuando no lo uses	Baja
Cambia las claves WEP regularmente	Media

Nota: En los manuales de los dispositivos, como Puntos de Accesos o Routers tendrás la información detallada sobre cómo hacerlo.

Analizamos a continuación los diferentes puntos o acciones reseñadas:

Objetivo: Asegurar el Punto de Acceso.

Cambia la contraseña por defecto.

- Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso. Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible acceder al dispositivo. *No utilices contraseñas como nombres, fechas, etc, intenta intercalar letras con números, ejemplo cpt24mej8a.*

Objetivo: Aumentar la seguridad de los datos transmitidos.
Usa encriptación WEP/WPA

- Activa en el Punto de Acceso la encriptación WEP. Mejor de 128 bits que de 64 bits... cuanto mayor sea el número de bits mejor.
- Los Puntos de Acceso y Routers más recientes permiten escribir una **frase** a partir de la cual se generan automáticamente las claves. Es importante que en esta frase intercales mayúsculas o minúsculas y números, evites utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado como "qwerty", "fghjk" o "12345").
- También tendrás que establecer en la configuración WEP la clave que se utilizará de las cuatro generadas (*Key 1, Key 2, Key 3, o Key 4*).
- Después de configurar el AP tendrás que configurar los accesorios o dispositivos Wi-Fi de tu red. En éstos tendrás que marcar la misma clave WEP (posiblemente puedas utilizar la **frase** anterior) que has establecido para el AP y la misma clave a utilizar (*Key 1, Key 2, Key 3, o Key 4*).
- Algunos Puntos de Acceso más recientes soportan también encriptación WPA (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP. Si activas WPA en el Punto de Acceso, tanto los accesorios y dispositivos WLAN de tu red como tu sistema operativo deben soportarlo. Windows XP requiere instalar una actualización.

Objetivo: Ocultar tu red Wi-Fi
Cambia el SSID por defecto.

- Suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID". En vez de "MIAP", "APManolo" o el nombre de la empresa es preferible escoger algo menos atractivo para *posibles atacantes*, como puede ser "Broken", "Down" o "Desconectado". Si no llamamos la atención de nuestros *"enemigos"* hay menos posibilidades de que intenten entrar en nuestra red.

Desactiva el broadcasting SSID.

- El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual. Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.

Objetivo: Evitar que se conecten:
Activa el filtrado de direcciones MAC.

- Activa en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengas funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a tu red Wi-Fi.

Establece el número máximo de dispositivos que pueden conectarse.

- Si el AP lo permite, establece el número máximo de dispositivos que pueden conectarse al mismo tiempo al Punto de Acceso.

Desactiva DHCP.

- Desactiva DHCP en el router ADSL y en el AP. En la configuración de los dispositivos/accesorios Wi-Fi tendrás que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario. *Si un posible atacante conoce el formato y el rango de IPs que usamos en nuestra red, no habremos conseguido nada con este punto.*

Objetivo: Para los más cautelosos: Desconecta el AP cuando no lo uses.

- Desconecta el Punto de Acceso de la alimentación cuando no lo estés usando o no vayas a hacerlo durante una temporada. El AP almacena la configuración y no necesitarás introducirla de nuevo cada vez que lo conectes.

Cambia las claves WEP regularmente.

- Por ejemplo semanalmente, o cada 2 o 3 semanas.
- Existen aplicaciones capaces de obtener la clave WEP de nuestra red Wi-Fi analizando los datos transmitidos por la misma. Pueden ser necesarios entre 1 y 4 GB de datos para romper una clave WEP, dependiendo de la complejidad de las claves.
- Cuando lleguemos a este caudal de información transmitida es recomendable cambiar las claves.
- Recuerda que tendrás que poner la misma clave WEP en el Punto de Acceso y en los dispositivos que se vayan a conectar a éste.

