

Seguridad de la red inalámbrica.

A diferencia de las redes cableadas, donde es más complicado conectarse de forma ilegítima, en las redes inalámbricas, donde la comunicación se realiza mediante ondas de radio, la posibilidad que un intruso acceda a nuestra red puede llegar a ser muy sencilla. Debido a esto hay que poner especial cuidado en asegurar las redes Wi-Fi.

Las señales de radio en las que se basan las redes inalámbricas atraviesan las paredes y obstáculos de habitaciones, casas, oficinas, etc., y se propagan por las calles. Si la red no tiene la seguridad habilitada, es decir, es una red *abierta*, cualquiera podría no sólo utilizar la conexión a Internet, sino también acceder a la red y a la información compartida de la misma, colocar gusanos, troyanos, *sniffer*, etc., y obtener así contraseñas de cuentas de correo, archivos privados, vídeos, fotos, conversaciones, etc.

¿Cómo conseguir una red inalámbrica Wi-Fi más segura?

Como en casi todo, no existe una regla de oro, sino una serie de reglas o estrategias que en su conjunto pueden mantener la red más protegida.

Dependiendo del nivel de seguridad a implementar se debe valorar qué puntos o reglas se pondrán en práctica.

Algunas de esas reglas son las siguientes:

-Cambiar la contraseña de administración o de acceso al Punto de Acceso: Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso, estas claves son las mismas en todos los equipos del mismo fabricante y por tanto públicas, por ello se hace necesario cambiarla por algo más privado. Se aconseja evitar emplear como contraseñas la fecha de nacimiento, el nombre de la pareja, de la madre, del perro, etc. Además, es una buena práctica intercalar letras con números y hacer uso de las mayúsculas y minúsculas.

-Usar encriptación (WEP/WPA): Activar el cifrado de la transferencia de datos en la red estableciendo un algoritmo de encriptación y la correspondiente clave de red en el Punto de Acceso. El algoritmo más extendido es la encriptación WEP que permite claves de 64 a 128 bits. Tener en cuenta que cuanto mayor sea la clave mejor seguridad ofrece, pero las comunicaciones pueden verse ralentizadas. El método WPA es más seguro pero no todos los dispositivos lo soportan.

Los Puntos de Acceso más recientes permiten escribir una *frase* a partir de la cual se generan automáticamente las claves numéricas. Se aconseja evitar emplear como contraseñas la fecha de nacimiento, el nombre de la pareja, de la madre, del perro etc. Además, es una buena práctica intercalar letras con números y hacer uso de las mayúsculas y minúsculas.

-Cambiar el SSID por defecto: Cambie el ID o nombre de la red inalámbrica que se suele establecer por defecto por algo más privado y menos atractivo para los intrusos. Si no se llama la atención de los intrusos habrá menos probabilidad de sufrir un ataque.

-Desactivar la difusión o broadcasting SSID: La difusión de las SSID permite que los equipos puedan escanear o rastrear las redes que se encuentran disponibles en un radio de acción, facilitando así la configuración de las redes. Pero esta facilidad es contraproducente en cuanto a la seguridad ya que conocer el SSID es el primer paso para acceder a una red y una forma más de tentar a los intrusos a acceder a nuestra red. Se recomienda desactivar esta característica que por defecto viene activada e introducir manualmente el SSID en la configuración de cada nuevo equipo que se quiera conectar.

-Activar el filtrado de direcciones MAC: De forma predeterminada cualquier equipo que solicite conectarse y conozca los parámetros de conexión a la red podría tener acceso a la misma. Para evitar esto y asegurarse que solo se conectarán los equipos y dispositivos autorizados, se puede activar el filtrado de las direcciones MAC (dirección única e invariable de cada interfaz de red) que permite especificar qué equipos están autorizados a conectarse a la red inalámbrica.

-Establecer 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.

-Desactivar el servicio de DHCP: Este servicio asigna de forma automática los parámetros de conexión a un equipo que desea conectarse a la red. Para hacer más seguras las redes, desactivar esta característica en el router o en el AP. De esta forma, la configuración de los dispositivos/accesorios Wi-Fi tendrá que realizarse a mano por lo que se complica el mantenimiento de las configuraciones de los equipos.

-Desconectar el AP cuando no se use: Apague el Punto de Acceso cuando no se esté usando. El AP almacena la configuración y no será necesario introducirla de nuevo cada vez que se conecte.

-Cambiar las claves WEP regularmente: Esto permite que alguien que se ha hecho con su clave vuelva a estar descolgado una vez que se cambie la clave. Aunque es difícil, existen aplicaciones capaces de obtener la clave WEP de una red Wi-Fi analizando los datos transmitidos por la misma. Se recomienda cambiar las claves periódicamente dependiendo del volumen de datos que se transfiera por la misma y de la complejidad de las claves.

-Activar el Firewall o cortafuegos del router y de los equipos de la red: Cerrar todas las puertas que innecesariamente están abiertas y así evitar el acceso de los intrusos, para ello, activar el firewall y especificar las reglas necesarias para los puertos, servicios y aplicaciones autorizados y no autorizados.