

11.2 Wifi

Las redes wifi utilizan una tecnología inalámbrica que realiza la conexión entre dispositivos situados en un área relativamente pequeña, como una habitación, una oficina, una casa o un edificio, a través de ondas electromagnéticas.

Algunas de las medidas de seguridad básicas que se pueden configurar en el router para mantener una red wifi segura son las siguientes:

- **Personalizar la contraseña de acceso:** las contraseñas por defecto de algunos routers suelen ser muy vulnerables o se pueden averiguar rápidamente en Internet.
- **Cambiar el SSID:** el nombre de la red es el identificador con el que se etiqueta la red inalámbrica para que cada usuario pueda localizarla.
- **Revisar el cifrado:** la señal inalámbrica puede ser interceptada más fácilmente por una red cableada, por lo que es necesario utilizar estándares de cifrado como WPA2.
- **Desactivar el acceso por WPS:** el estándar WPS facilita la configuración de una red segura con WPA2 a sus usuarios.
- **Filtrar las MAC:** las direcciones MAC son establecidas por el fabricante y únicas para cada dispositivo de la red.
- **Actualizar el firmware:** el firmware es el software que controla los circuitos de los dispositivos electrónicos.
- **Comprobar el historial de actividad:** la actividad del router puede desvelar información sobre posibles intrusiones, ya que muestra los datos de los equipos conectados, los horarios, la duración de la sesión, etc...
- **Utilizar software de auditoría:** en el mercado existen herramientas diseñadas para evaluar la seguridad de una red y detectar sus posibles vulnerabilidades. Una de las más populares es Nmap.