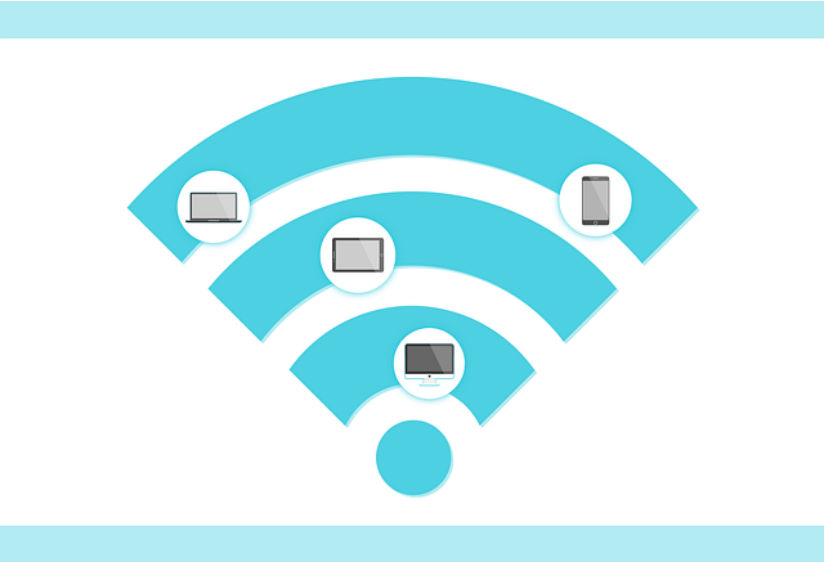
# Infraestructura de red y conectividad

Recomendaciones de seguridad en torno a conectividades y redes:

- Definir **distintas redes en el centro** en función de la sensibilidad de los datos con los que se trabaje y proteger cada una de ellas de de accesos no autorizados, lo mismo si se dispone de conexión wifi**.** Para ello es recomendable crear una **subred** para dirección / administración, otra para profesorado, y otra para alumnado.
- Las tomas que dan **acceso a la red por medio de cable Ethernet también se deberán proteger**, evitando que estas se encuentren en lugares públicos o con poco control.

Imagen de storyset en Freepik

- Definir pautas de uso y política de usuario/contraseña de la **red WIFI** del centro, por parte de todos los miembros de la comunidad educativa.



Pixabay License

- **Controlar el DHCP.** El Protocolo de Configuración Dinámica de Host (DHCP)  que es un protocolo de Internet que los equipos en red utilizan para obtener direcciones IP y otra información como la puerta de enlace predeterminada. Cuando el usuario se conecta a Internet, un equipo configurado como un servidor DHPC en el ISP le **asigna automáticamente una dirección IP**. Podría ser la misma dirección IP que tenía anteriormente o podría ser una nueva. Cuando se cierra una conexión a Internet que usa una dirección IP dinámica, el ISP puede asignar esa dirección IP a un usuario diferente. Por todos ello y con el fin de evitar vulnerabilidades, el centro educativo debe decidir sopesando la seguridad y las necesidades del centro, el tener habilitada / limitada la franja de IPs  / deshabilitada, está configuración dinámica.

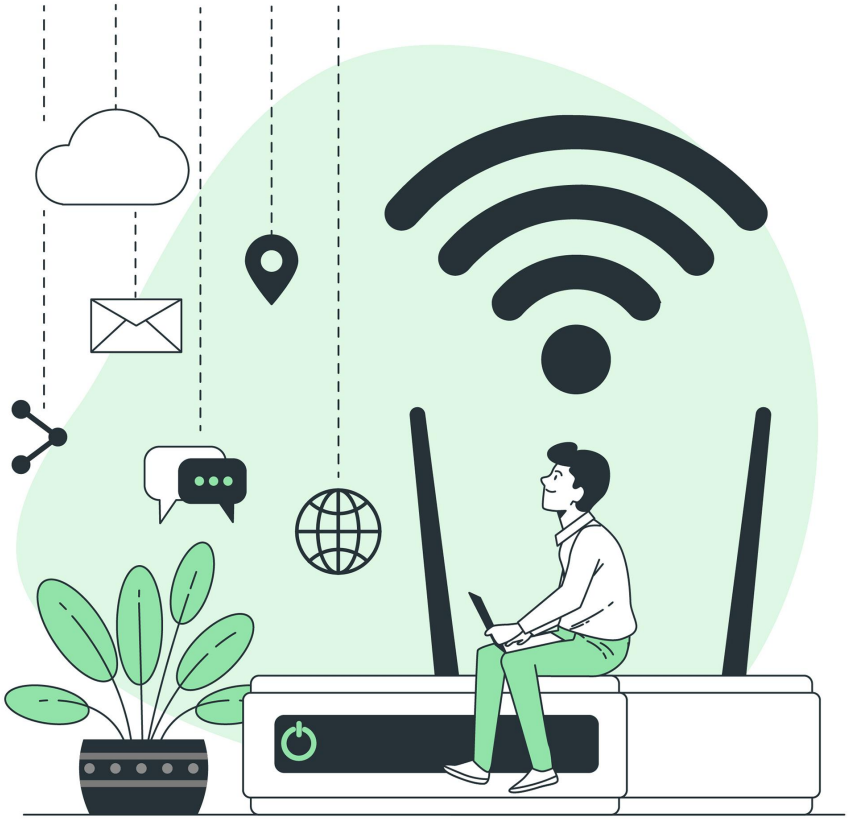


Imagen de storyset en Freepik

- Configuración del **Router** con criterios de seguridad (sino lo está, pueden espiar nuestras comunicaciones, utilizar la red para envío de spam, infectar los dispositivos conectados, reducir el ancho de banda,...), en los centros educativos sostenidos con fondos públicos, está **configuración viene por defecto definida por la administración educativa** y es la que realiza el soporte de los mismos, pero deberíamos de saber que aspectos de seguridad es conveniente conocer y si alguno podríamos personalizarlo para nuestro centro con la ayuda del servicio técnico que dispone la administración, por lo tanto tendremos en cuenta:
  - Asignar el mejor **protocolo de seguridad** posible en las conexiones Wifi, en estos momentos en los entornos educativos la mas segura y estable es el **WPA2**, pero ya se está hablando de la WPA3 aunque necesita ir adaptándose a la realidad educativa
  - **Cambiar u ocultar el nombre de la red o SSID**: Cuando modificamos las credenciales de acceso a nuestro router o a nuestra red wifi, estamos protegiéndolos de terceros evitando que puedan acceder a ellos. Para aumentar aún más la protección de nuestra red, es recomendable que cambiemos el nombre de nuestra red wifi (SSID)
  - **Filtrar las direcciones MAC**: Una práctica muy útil para mejorar la seguridad de nuestra conexión y protegerla de terceros es revisar eventualmente los dispositivos que están conectados a nuestra red y realizar un filtrado por dirección MAC, que es un identificador único que posee cada dispositivo. De esta forma, habilitaremos el acceso solo a aquellos dispositivos que conocemos y evitaremos que se conecten dispositivos desconocidos

- **Desactivar el acceso remoto.** Si queremos evitar que se pueda entrar a nuestro router desde el exterior, es decir, desde otra red, tendremos que asegurarnos de que esta funcionalidad está desactivada

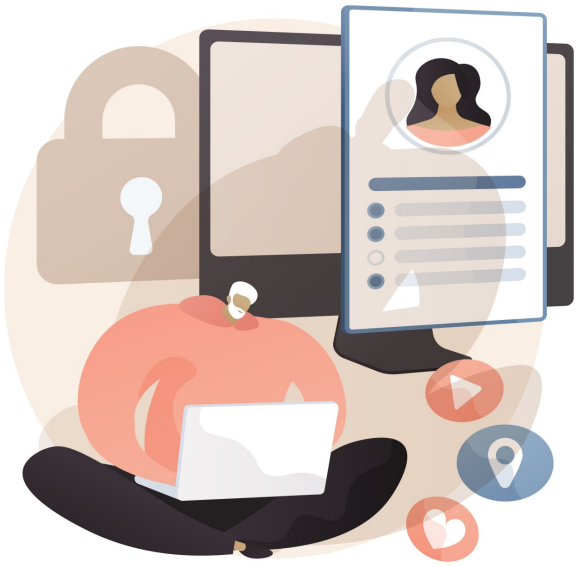


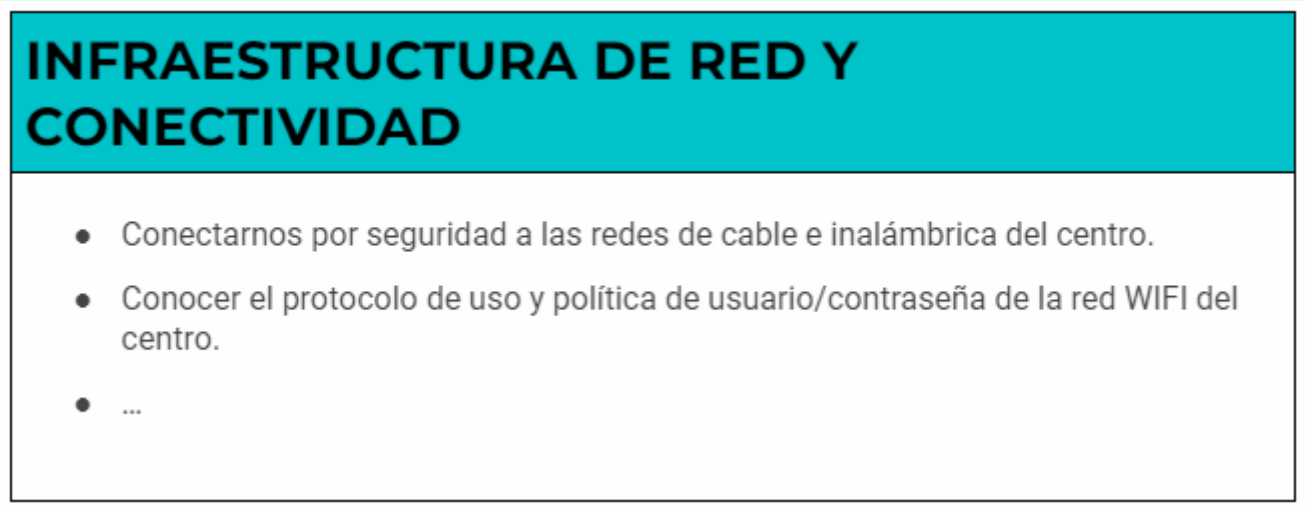
Imagen de vectorjuice en Freepik

- **Desactivar el WPS o conexión rápida**: Los router y sus configuraciones de seguridad han evolucionado mucho a lo largo de los años. La funcionalidad WPS, por ejemplo, es una funcionalidad que, si bien resultaba muy útil a la hora de conectar dispositivos a la red, a día de hoy puede suponer una gran amenaza contra nuestra seguridad y privacidad. El WPS es un mecanismo creado para facilitar la conexión de dispositivos a nuestra red wifi. Aunque existen diversas formas mediante las cuales un dispositivo puede conectarse a una red inalámbrica utilizando, para ello, dicha funcionalidad, la más extendida de todas sigue siendo mediante una clave PIN.
- **Puertos del router**. Los puertos del router se utilizan como un canal para establecer conexiones de diferentes aplicaciones con los correspondientes servidores remotos para poder funcionar. Nuestro router es el encargado de transmitir la información que entra o sale de los dispositivos conectados a la red y la encamina, a través de router intermedios hasta su destino.
- **Crear una red para invitados**. Una red de invitados tiene como objetivo el permitir que varios dispositivos se conecten a nuestra conexión a Internet, pero permitiéndoles navegar en una red distinta a la de nuestros dispositivos habituales. De este modo, podrán acceder a nuestra conexión a Internet sin comprometer la seguridad de nuestra red principal y, sin que perdamos el control de los accesos.

A modo de resumen os dejamos un pequeño vídeo donde la OSI nos indican como proteger nuestra red

https://www.youtube.com/embed/POeuXk1UXHo

Una posible plantilla donde ir escribiendo lo relacionado con infraestructura de red y conectividad comenzaría así.




Revision #18
Created 1 February 2023 19:46:26 by Javier
Updated 23 February 2023 23:16:27 by Javier Gerico