

Actividad 06. Seguridad en redes sociales

La seguridad en las redes sociales se refiere a estrategias que las empresas y los individuos pueden usar para proteger sus cuentas sociales de amenazas como hackeos, phishing y malware.

Los riesgos de seguridad más comunes en redes sociales son:

- Ataques de phishing y estafas
- Cuentas impostoras
- Ataques y hacks de malware
- Aplicaciones vulnerables de terceros
- Robo de contraseña
- Configuración de privacidad y seguridad de datos
- Dispositivos móviles no seguros

En los siguientes artículos se muestra información sobre la seguridad en redes sociales:

- [Seguridad en redes sociales: ventajas y desventajas](#)
- [Así puedes aumentar la seguridad y privacidad en tus redes sociales](#)
- [Herramientas y consejos de seguridad en redes sociales para reducir los riesgos](#)
- [Configuración de privacidad en redes sociales](#)

Actividad 06. Seguridad en redes sociales



Se pide:

1. Busca información en Internet sobre las amenazas y vulnerabilidades existentes en el uso de las redes sociales y elabora un documento explicándolo, así como las estrategias a seguir para protegerlas.
2. Muestra también las opciones de seguridad de una red social que utilices (Instagram, TikTok, Facebook, LinkedIn, etc.).
3. El docente planteará en clase un debate sobre el uso seguro de las redes sociales, explica tus conclusiones.