Acceso seguro a las redes sociales

Dentro de las redes sociales los usuarios comparten una cantidad significativa de información personal, por lo que es importante tomar en cuenta las siguientes recomendaciones de seguridad para evitar que la información personal esté en riesgo (SKYNET, 2021):

- **Contraseñas seguras:** evitar contraseñas que incluyan nombres propios o de familiares, fechas de nacimiento o sean demasiado predecibles. Se sugiere crear una contraseña diferente para cada red social y mezclar símbolos, mayúsculas y minúsculas.
- **Doble autenticación:** las redes sociales cuentan con la opción de solicitar tu contraseña y también un código generado en una app de autenticación instalada en el dispositivo móvil. Esto ayuda a que si alguien, a pesar de contar con la contraseña, no pueda ingresar. Algunas apps de autenticación son el autenticador de Google y Microsoft Authenticator.
- **Enlaces sospechosos:** en ocasiones se presentan como sorteos, ofertas o premios atractivos, pero al ingresar a las páginas pueden resultar virus o robo de identidad.
- **Solicitudes de amistad o follow de desconocidos:** se recomienda tener precaución, ya que no sabemos la intención que puedan tener otros usuarios y el uso que le puedan dar a la información privada que hay en la red social.

Referencias bibliográficas

- SKYNETSYSTEMS. (2021). 10 consejos para estar seguro en Redes Sociales. Recuperado de https://skynet-sys.es/10-consejos-para-estar-seguro-en-redes-sociales/