Privacidad y seguridad van de la mano

- Riesgos de Internet
- El factor humano

Copyright 2026

Riesgos de Internet



Internet es una herramienta poderosa que nos brinda una amplia gama de posibilidades, pero también conlleva ciertos riesgos que deben ser considerados por los centros educativos y las familias para proteger a los menores. Sobre todo desde la aparición y acceso a las redes sociales, entornos que les permiten abrir un perfil con datos personales para comunicarse y compartir información con otras personas, ya sea de forma pública o restringida.

Un ejemplo concreto en el ámbito educativo sería el de los **festivales de fin de curso, u otras actividades,** donde las familias toman fotos o graban vídeos. El centro educativo informará a los asistentes que esas fotos y vídeos son para uso exclusivo en el ámbito personal y doméstico y no

Copyright 2026

deben de publicarse abiertamente en las redes sociales, puesto que se vulnera la protección de datos de los menores.



Fuente AEPD

Los riesgos más graves son aquellos que afectan a la integridad, tanto física como emocional, de los menores. No es fácil evitarlos, no son infrecuentes y, aunque no se produzca agresión física por parte de los acosadores, los efectos sobre la víctima pueden ser devastadores.

Dichos riesgos están relacionados con:

- La **publicación de datos personales:**

- **Suplantación de identidad**: cuando alguien se hace pasar por otra persona generalmente para cometer algún delito u obtener algún beneficio en nombre de otra persona de forma ilícita.

- **Engaño pederasta o *grooming***: Situación en la que un adulto se hace pasar por un menor para ponerse en contacto con un niño o niña, para luego ganarse su confianza y finalmente cometer algún tipo de abuso o chantaje sexual.

- Un **uso incorrecto de las redes sociales:**

Copyright 2026

- **Ciberacoso**: la realización de comentarios y publicaciones negativas o humillantes en redes sociales supone una forma de acoso en el entorno digital. Dar *me gusta*, compartir las burlas o no denunciarlas también implica ser cómplice.

- **Uso excesivo**: el no establecer límites de tiempo, descuidando otras actividades tan importantes como la comida, la actividad física o el descanso, puede generar en muchos casos síntomas de dependencia o adicción.

- El acceso a **contenidos inadecuados** puede exponer a los menores a bulos y fraudes, discursos de odio y publicaciones de comunidades peligrosas en las que se fomentan malos hábitos relacionados con desórdenes de alimentación, autolesión, consumo de drogas, etc.

A pesar de todo lo anterior, es posible usar internet y las redes sociales de manera positiva y segura, todo ello dependerá de cómo se utilicen y cómo sea la actitud del menor frente a ellas. Por ello nuestra labor, ya sea como docentes o como familiares, implica el ejercer de guías y acompañantes durante todo ese proceso.

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU



Copyright 2026

El factor humano

La seguridad y, por tanto, también la ciberseguridad en nuestro ámbito tienen como fin último la protección de los centros educativos y las personas que conforman la comunidad educativa a través de la protección de sus dispositivos y redes utilizando medidas organizativas, jurídicas y técnicas. Las medidas de ciberseguridad protegen los sistemas, redes y servicios de las administraciones públicas, las entidades privadas o, incluso, a nuestro entorno doméstico de ataques tecnológicos. Sin embargo, **la ciberseguridad no es un fin en sí mismo, sino un medio** para proteger a las organizaciones y a las personas.

El **factor humano** es el elemento clave que hay detrás de la cadena de garantías de la seguridad y, a la vez, el activo final a proteger. Sin embargo, si la información personal de cada individuo está expuesta, éste será vulnerable a ataques de ingeniería social específicamente dirigidos a sus debilidades. De esta forma, el atacante podrá alcanzar tanto a la organización como a los individuos, sorteando las protecciones tecnológicas.

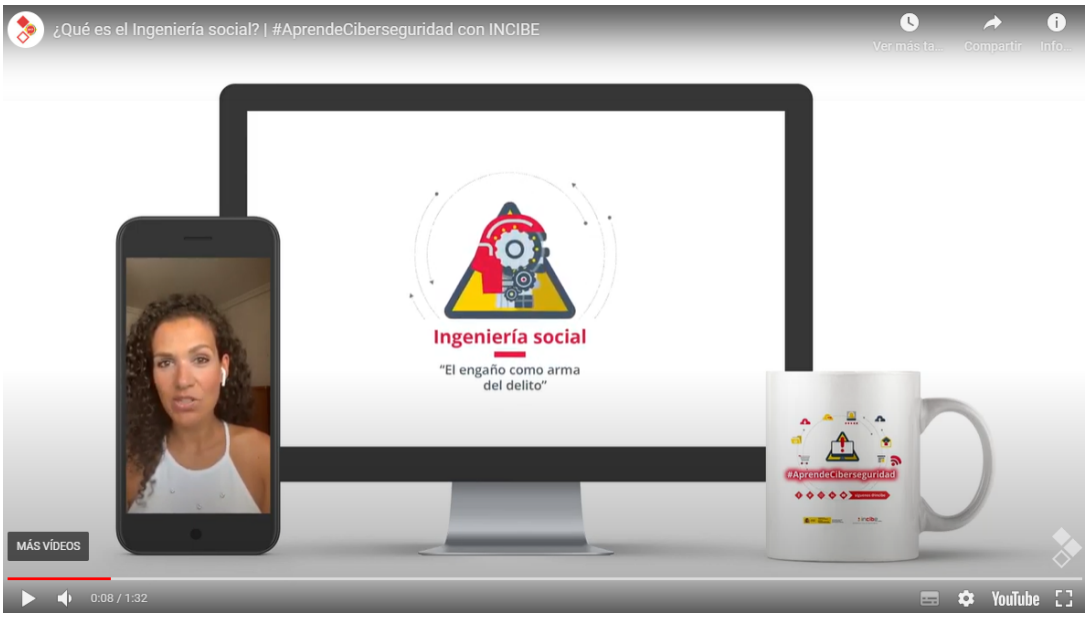
Copyright 2026



Fuente Incibe

Durante el año 2020, el 85% de las brechas tecnológicas involucraron el factor humano. La realidad pone de manifiesto que el camino más fácil para comprometer una organización es conseguir que, desde dentro, se abran las puertas a los intrusos, o incluso que ejecute directamente las acciones que el intruso desea. Para conseguirlo se han desarrollado las técnicas de ingeniería social.

Copyright 2026



¿Qué es la ingeniería social?

Es la acción de **engañar o chantajear** a una persona para que revele información o emprenda una acción que pueda usarse para comprometer o afectar negativamente un sistema o una organización, en nuestro caso sería el entorno educativo. Se aprovechan de la forma de ser las personas, ya que ofrecemos facilidades a la ingeniería social con nuestras actitudes:

- **Todos queremos ayudar.**
- El primer movimiento es siempre de **confianza hacia el otro.**
- **No nos gusta decir NO.**
- A todos nos **gusta que nos alaben.**

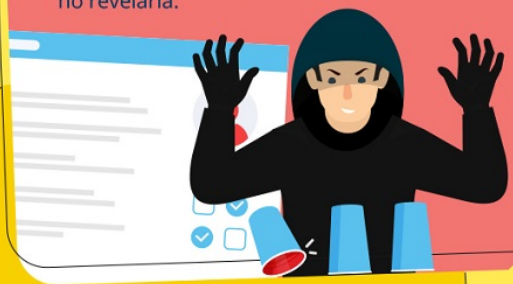
Existen diferentes técnicas de ingeniería social:

Copyright 2026

Técnicas de ingeniería social ¿Cómo consiguen engañarnos?

Pretexting

Base de cualquier ataque de ingeniería social.
Consiste en elaborar un escenario/historia ficticia, donde el atacante tratará de que la víctima comparta información que, en circunstancias normales, no revelaría.



Sextorsión

Chantaje donde amenazarán a la víctima con distribuir supuestamente contenido comprometido de ella a sus contactos (aunque no exista dicho contenido), si no accede a las peticiones del ciberdelincuente, generalmente a realizar un pago.





Phishing

Busca "pescar" víctimas.
Generalmente se emplean correos electrónicos con archivos adjuntos infectados o links a páginas fraudulentas con el objetivo de tomar el control de sus equipos y robarles información confidencial.



Baiting

Emplea un cebo con software malicioso a la vista de sus víctimas para que ellos mismos infecten sus dispositivos.





Smishing

Se trata de una variante del "phishing" pero que se difunde a través de SMS.
Se pide al usuario que llame a un número de tarificación especial o que acceda a un enlace de una web falsa.



Vishing

Llamadas telefónicas donde el atacante se hace pasar por una organización/persona de confianza para que la víctima revele información privada.



Shoulder Surfing

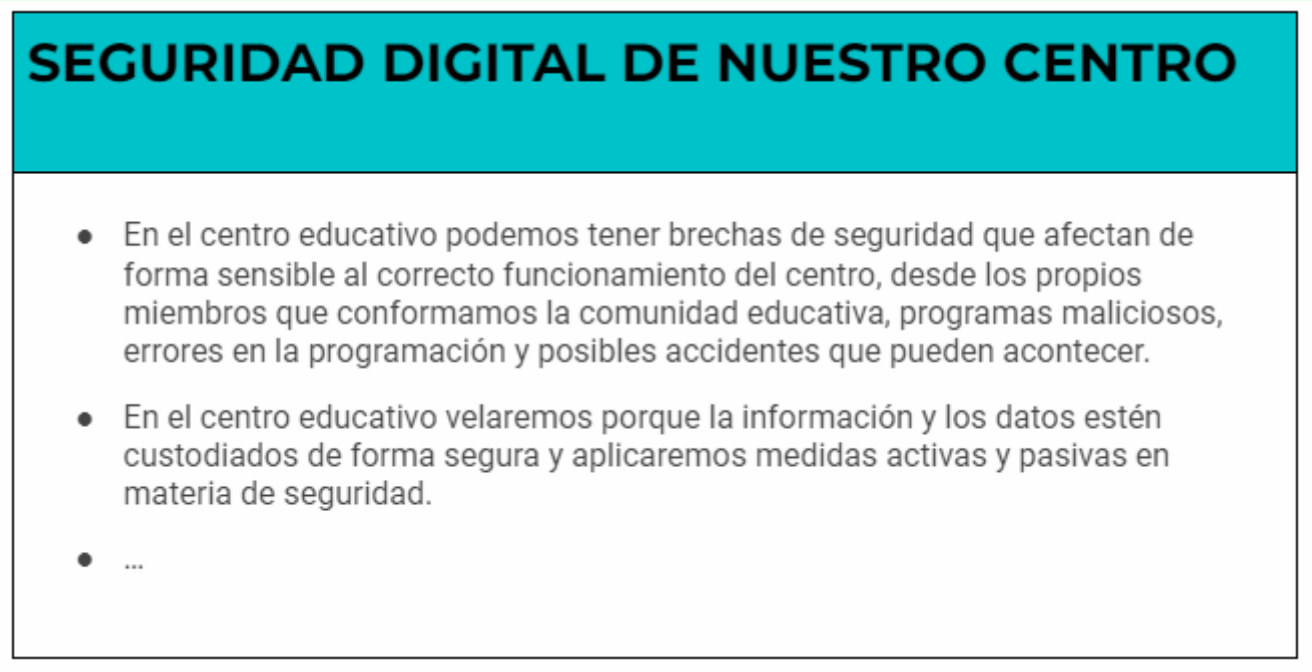
Consiste en mirar por "encima del hombro". Al atacante le basta con observar lo que escribe o tiene en pantalla otro usuario para obtener información muy útil.



Quid pro quo

Infografía del Incibe

Una ejemplo de plantilla donde plasmar acuerdos y compromisos en materia de seguridad en el centro puede ser esta.



Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
GOBIERNO DE ARAGON