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.

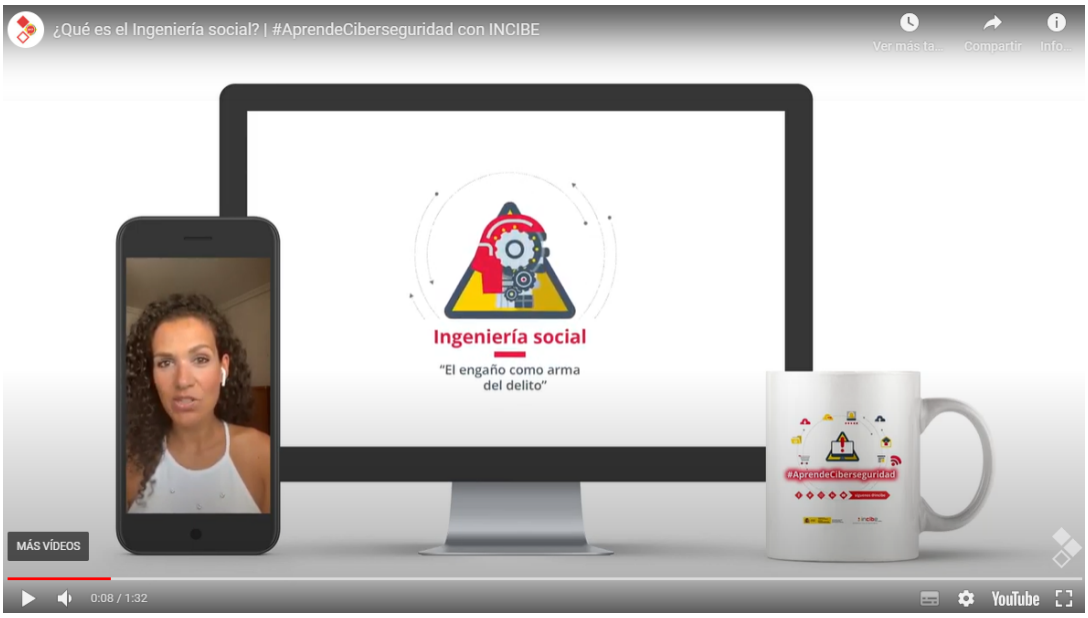
Copyright 2026



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.**

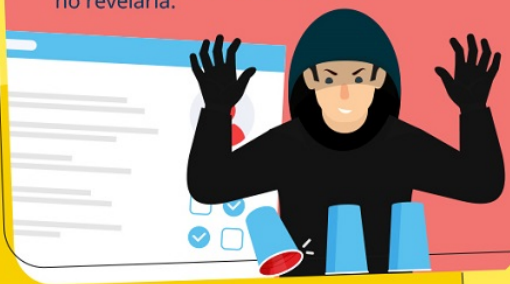
Existen diferentes técnicas de ingeniería social:

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

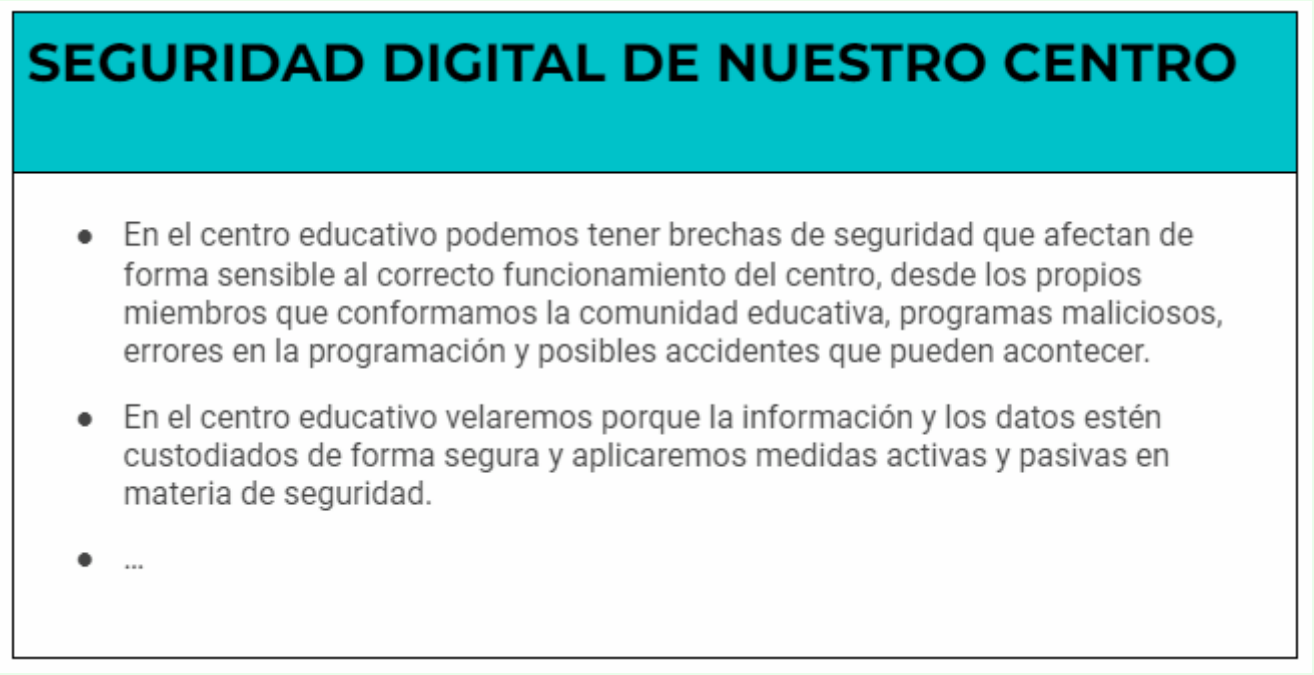
Consiste en mirar por "encima del hombro". Al atacante le basta con observar lo que escribe o tiene en pantalla otro usuario para obtener información muy útil.



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

Revision #14
Created 2023-02-03 10:33:03 CET by Javier Gerico
Updated 2023-03-20 10:14:50 CET by Alejandro Folch

Copyright 2026