



# Uso seguro y responsable de las TIC

# ¿Qué vamos a aprender hoy?

- Identificar los **principales riesgos** relacionados con el uso de las TIC.
- **Identificar pautas** para saber actuar ante ellos.
- **Adquirir buenos hábitos** en el uso de las TIC.

# Acceso a contenido inapropiado



Acceso a contenidos inapropiados



# Riesgos de acceso a contenidos inapropiados



Acceso a información,  
conductas y consejos no  
adecuados a su edad



'Amistades' poco  
recomendables



Víctima de ciberacoso y  
ciberbullying



Víctimas de potenciales engaños y  
estafas (anuncios publicitarios)



Virus y programas espía (acceso no  
consentido a información personal)

# Recomendaciones para su prevención



Accede sólo a aquellos **contenidos recomendados** y **adaptados** a tu **edad**.



**No ofrezcas información personal**, que permita rastrear tus datos, ni tuya ni de familiares, amigos y conocidos.



Evita publicar fotos o conectar la webcam con **desconocidos**. **Sé cauto** y piensa antes de hacer clic.



Debes ser consciente de **infracciones legales** asociadas al uso de Internet y sus consecuencias.



**Déjate ayudar** cuando tengas un problema. **Dialoga con tus padres y educadores**.

# Verificación de la información



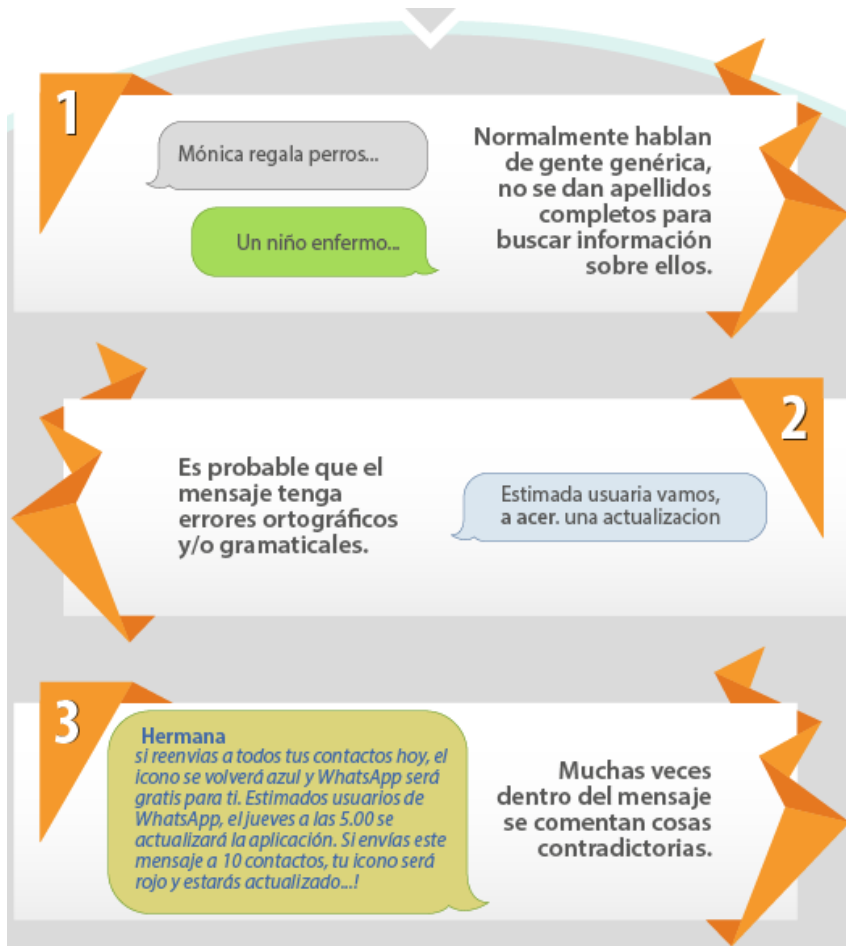
**¡Ojo!** no toda la información publicada en Internet es siempre veraz, completa e imparcial.

**¡Verifica SIEMPRE la información  
ANTES de creértela!**

# Bulos, mitos y fraudes



# Mentiras en la red



Hablan de  
forma  
genérica

Errores  
ortográficos  
y  
gramaticales

Sin dar datos

Contradicciones



# Mentiras en la red

Regalos caros,  
desorbitados, sin  
siquiera concurso

Petición  
de  
reenvío  
(viralidad)

Referencias a  
compañías e  
instituciones  
conocidas

Falsa  
credibilidad



# Mentiras en la red

Molestias y  
miedos

Evita daños  
directos y a  
terceros

Ante la duda  
busca e  
infórmate en  
fuentes de  
confianza: OSI,  
Policía, Guardia  
Civil, etc.



**Y NUNCA**  
reenvíes  
estos  
mensajes



## ¿Qué conoces de los virus? ¿Cuál es tu estrategia frente a ellos?

Reflexiona. ¿Qué conoces sobre los virus? ¿Cuál es tu estrategia frente a ellos?



# ¿Qué es un virus?

**Es un programa malicioso capaz de colarse en el ordenador con distintos fines:**

- **Robar datos**
- **Hacer que el dispositivo deje de funcionar**
- **Tomar el control para hacer un uso malicioso**

# Principales vías de infección

**CORREO  
ELECTRÓNICO**

**FALLOS DE  
SEGURIDAD**

**PÁGINAS  
WEB  
MALICIOSAS**

**DISPOSITIVOS DE  
ALMACENAMIENTO**

**DESCARGA  
DE  
FICHEROS  
DE  
INTERNET**

**REDES  
SOCIALES**

**APPS  
MALICIOSAS**

# Ejemplo

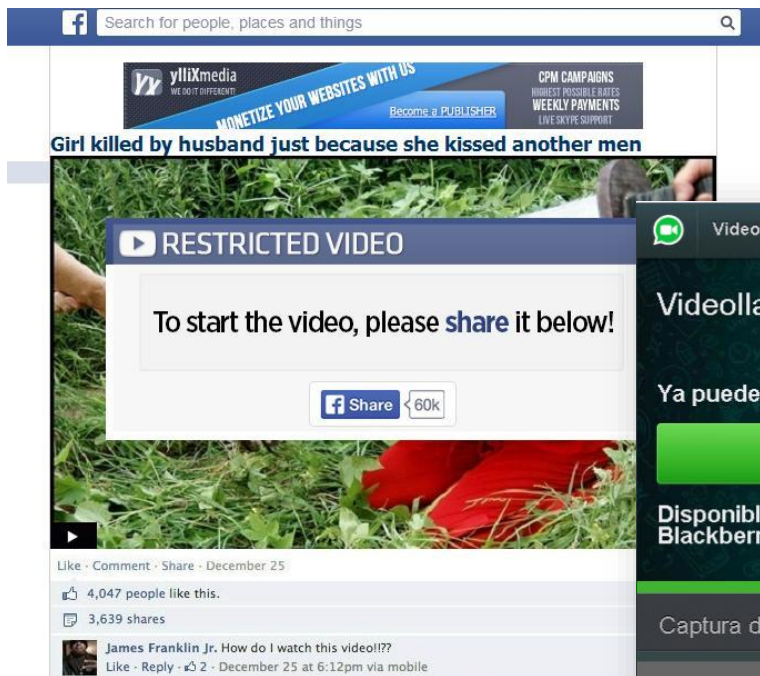
RANSOMWARE. BLOQUEO DE FICHEROS. CIFRADO DATOS

## Virus de la Policía

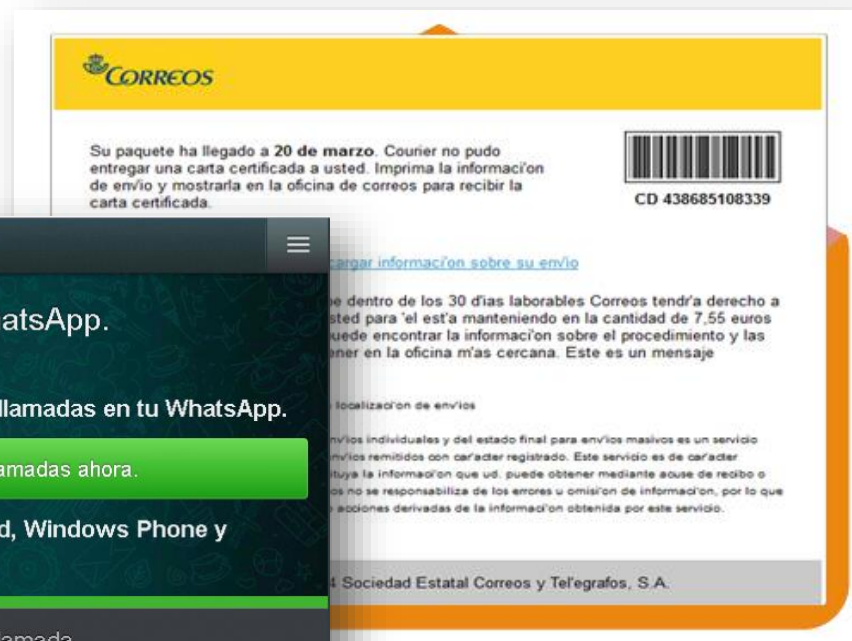




# Ejemplos de fraudes



**Vídeos virales en redes sociales**



**Phishing**



**Falsas aplicaciones**

Conociendo algunos fraudes



# El adivino Dave



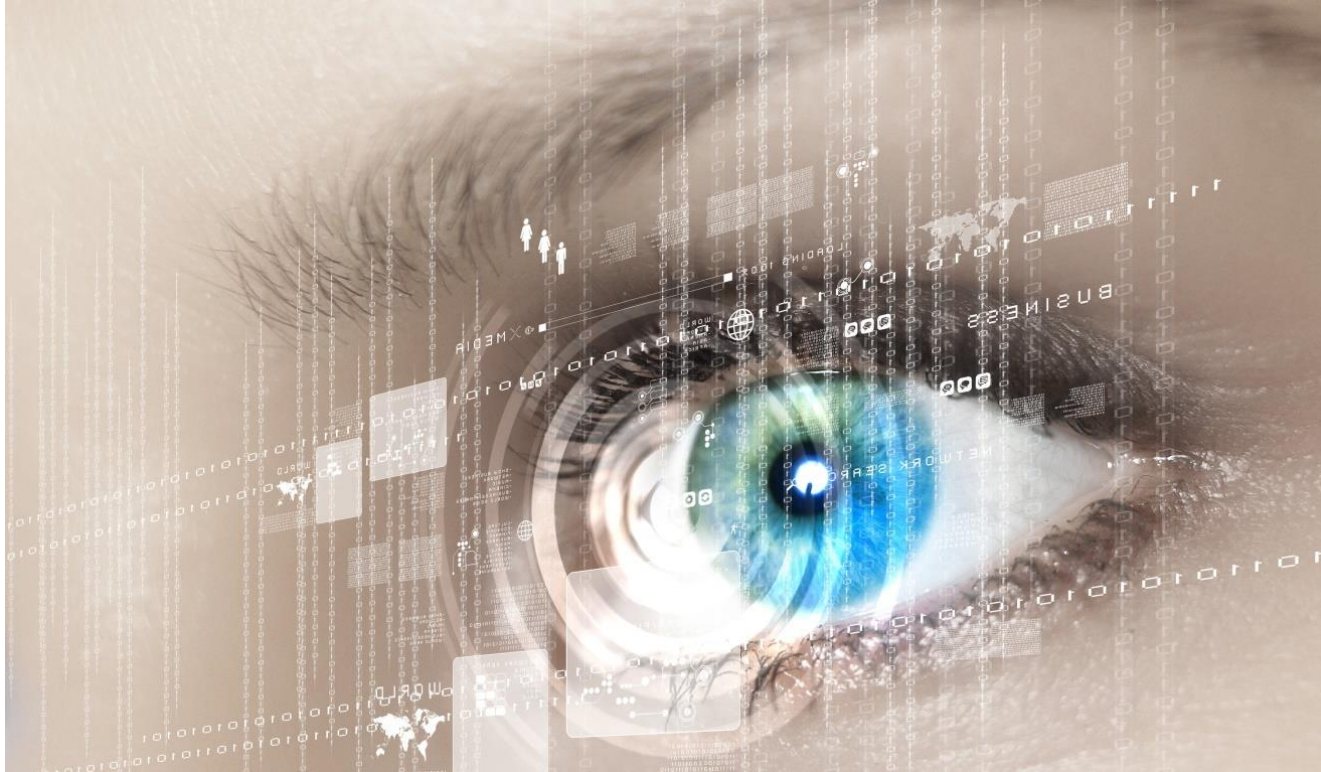


# Qué información voy dejando sobre mí en la red

- Lo que **pienso, digo, publico**.
- Lo que **comparto**: mis aficiones, gustos, intereses, etc.
- Lo que **compro**.
- **Con quién me relaciono**: contactos.
- **Fotos y vídeos** que subo.



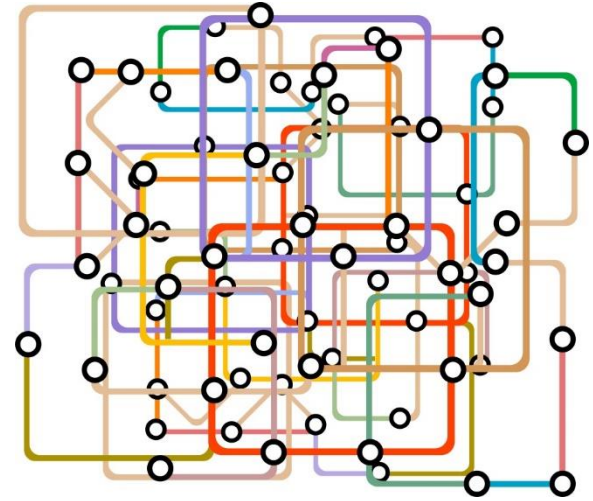
# Privacidad en Internet



“Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión”

## Identidad digital

Información sobre una persona publicada en Internet que le caracteriza y le diferencia de los demás.



## Reputación online

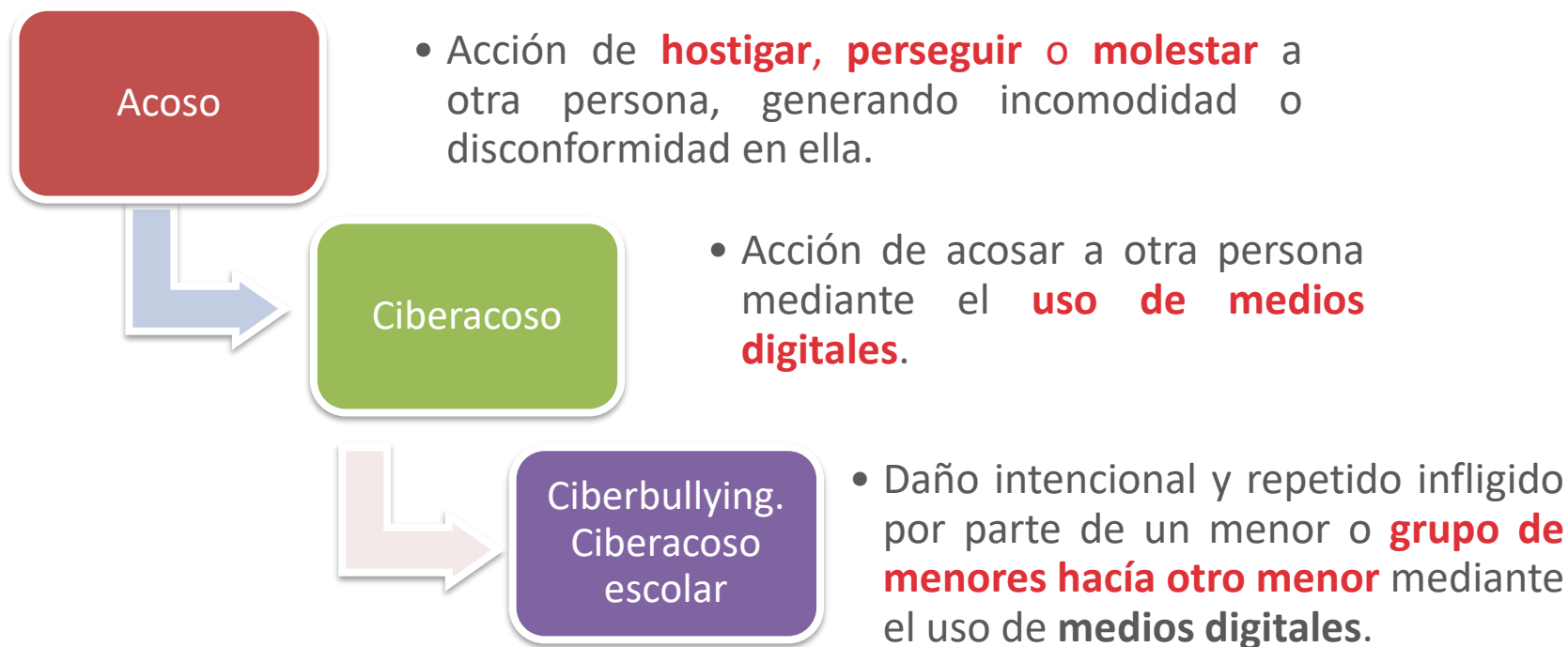
Imagen de nosotros en Internet (identidad digital) que provoca en los demás una valoración.

# ¿Qué pasa si alguien vulnera nuestra privacidad?, ¿puede ser un delito?

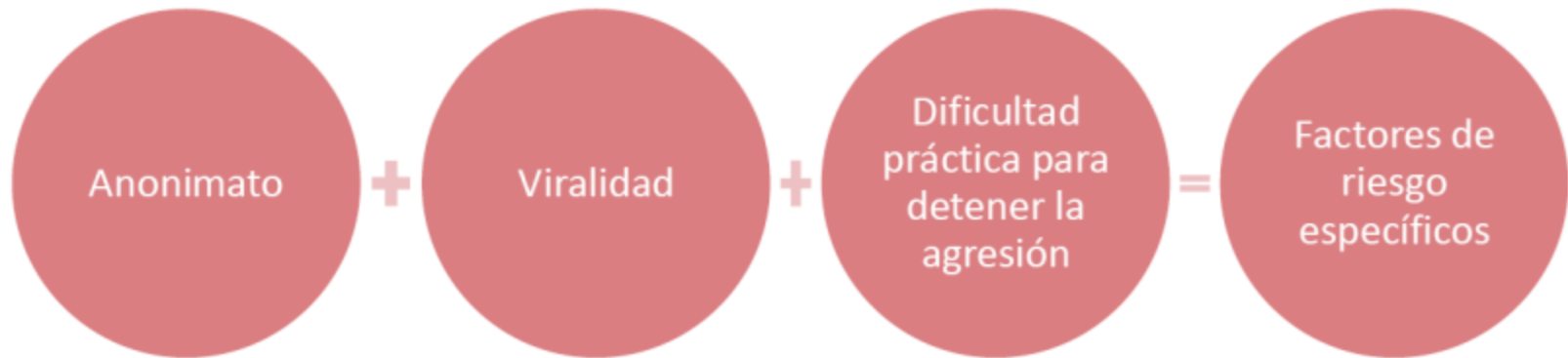
- **Reenviar** por WhatsApp una **foto o vídeo** de un compañero que alguien te ha enviado **sin su consentimiento**.
- **Acceder a la cuenta** de Twitter de un **compañero** que se ha dejado la **sesión abierta**.



# Definiendo qué es el ciberacoso. Cyberbullying



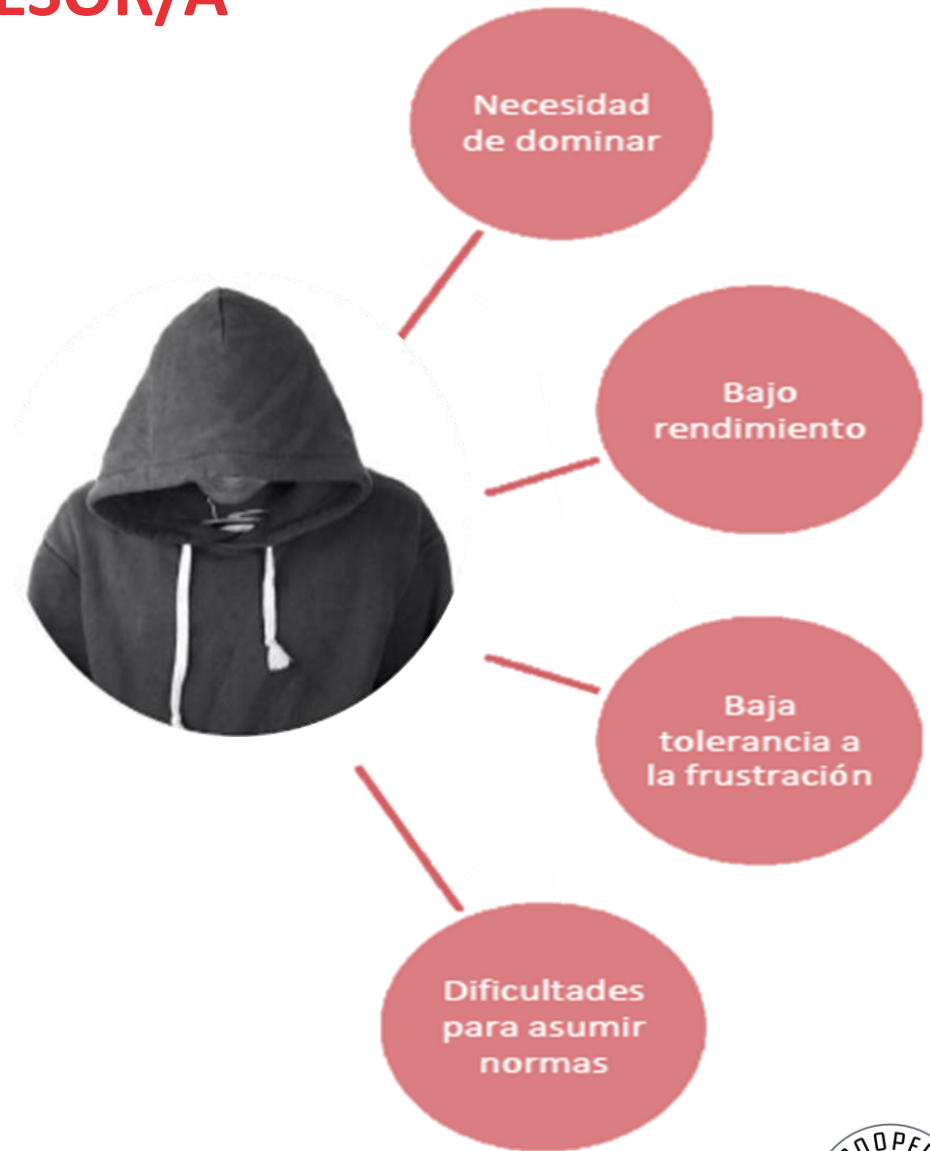
# Características del ciberacoso



- **Efecto desinhibidor:** se actúa de manera impulsiva sin pensar en las consecuencias.
- **Supuesto anonimato:** capacidad para ocultar la identidad
- **Viralidad:** extender un mensaje masivamente a una gran velocidad.
- **Conexión permanente:** 24 horas, 7 días de la semana.

# AGRESOR/A

Rol de las personas  
implicadas en el  
ciberacoso





# VÍCTIMA

Rol de las personas  
implicadas en el  
ciberacoso



Pocos  
amigos

Bajo  
conceptos  
de sí  
mismos

Dificultades  
de  
interacción  
social

Víctima de  
acoso off-  
line



# OBSERVADORES/ESPECTADORES/TESTIGOS

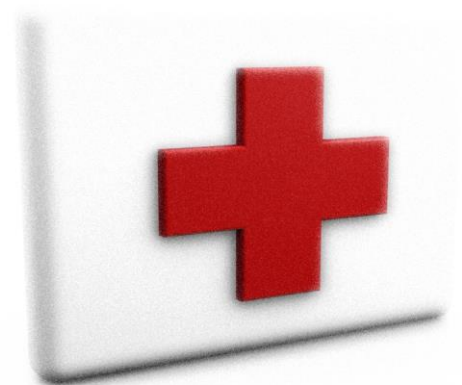
## Rol de las personas implicadas en el ciberacoso

- Miedo a convertirse en víctimas
- Necesidad de integrarse en el grupo
- Indiferencia, falta de empatía
- Falta de valor y responsabilidad...



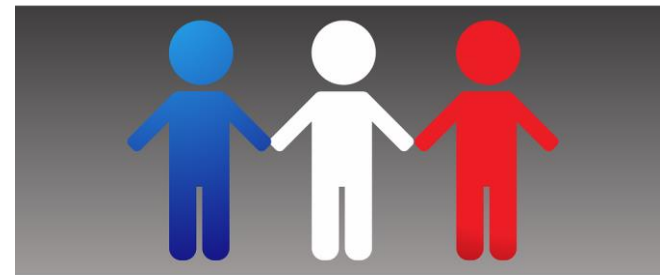
# Cómo actuar ante un caso de ciberacoso

- **No contestes** a las provocaciones.
- Si te molestan **abandona la Red**.
- Si te acosan, **guarda las pruebas**.
- **Informa o denuncia la situación** de acoso ante el administrador del servicio Web (Twitter, Facebook, Instagram).
- No te sientas culpable. Es quien te acosa, quien está cometiendo un delito. **Tú no tienes la culpa**.
- **Pide ayuda** siempre a un adulto de referencia y confianza para ti. Si la amenaza es grave, pide ayuda con urgencia.



# Otras consideraciones sobre el ciberacoso (I)

- **Comunica lo que piensas, de forma asertiva:** hablando clara y honestamente sobre tus necesidades, emociones, intereses y opiniones.
- Trata a los demás con **amabilidad y respeto.**
- **Fomenta la empatía,** siendo capaz de ponerte en la piel del otro.
- **No hagas en la Red lo que no harías en persona.** Desarrolla tu pensamiento crítico: analiza y cuestiona la realidad, tomando tus propias decisiones.



## Otras consideraciones sobre el ciberacoso (II)

- No seas partícipe del **sexting**, ni creándolo, ni reenviándolo, ni fomentándolo.
- **No calles ni ocultes el ciberacoso.** Confía en familia, profesorado, mediadores. Si detectas o sospechas de una situación de posible acoso a tu alrededor, **no dudes en ofrecer ayuda.**



# Recomendaciones

Sistema operativo, antivirus y programas siempre actualizados.

Gestiona bien tus contraseñas. ¡No las compartas con nadie!

TUS CONTRASEÑAS DEBEN SER...



SECRETAS



ROBUSTAS



NO REPETIDAS



CAMBIADAS PERIÓDICAMENTE



Utiliza patrones de seguridad en smartphones y tabletas

Ten precaución al usar dispositivos y wifi públicos.

Evita navegar por webs sospechosas y analiza los enlaces cortos.

Revisa los permisos que solicitan las apps para instalarse

Descargas siempre desde sitios oficiales.



# Recomendaciones



Siempre que puedas, conéctate a través de páginas seguras.

Configura las opciones de privacidad de tus redes sociales y revísalas periódicamente.

No publiques excesiva información personal. Piensa en las consecuencias.



Valora cuando tener activados los servicios de geolocalización.

Haz copias de seguridad de la información que te interesa.



# Dónde localizar más información



<https://www.osi.es>



<https://www.is4k.es>

Más información





# Cibercooperantes

contacto@is4k.es

## Gracias por su atención

<https://www.is4k.es/programas/cibercooperantes>



Internet Segura for Kids



@is4kids





# Licencia de contenidos



La presente publicación pertenece a **INCIBE (Instituto Nacional de Ciberseguridad)** y está bajo una licencia **Reconocimiento-No Comercial-Compartir Igual 4.0 Internacional de Creative Commons**. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a **INCIBE** y la iniciativa **Internet Segura for Kids (IS4K)** como a sus sitios web: <https://www.incibe.es> y <https://www.is4k.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es> **ES**