

is4k
INTERNET
SEGURA
FOR KIDS

Internet Segura for Kids: uso seguro en el contexto educativo



¿QUÉ USOS DE INTERNET IDENTIFICAMOS EN EL CENTRO?

Participar en desafíos

Experimentar cambios en el carácter

Hacerse pasar por mi hermana en su cuenta de Instagram

Utilizar apps de ligues
(sin ningún filtro)

No limitar la información pública

Comprar «chollos» a través de Wallapop

patri_guardo_2001@hotmail.com

Meterse con Ángel a través del chat de clase

Probar a entrar en los
ordenadores sin
autorización

Enviar fotos provocativas para demostrar mi amor

Pinchar en enlaces sin precaución

Hacer amigos online

(y resultar ser adultos que se hacen pasar por chavales... con distintas intenciones)

Reutilizar contenidos sin precaución alguna

ÍNDICE

- Identidad digital positiva
 - Suplantación de identidad
 - Sexting
- Relaciones positivas en línea
 - Grooming
 - Ciberacoso

IDENTIDAD DIGITAL POSITIVA

PRIVACIDAD -> IDENTIDAD DIGITAL -> REPUTACIÓN



La **huella** que dejamos en **Internet** da forma a nuestra **identidad digital** y condiciona como nos ven los demás (**reputación**)

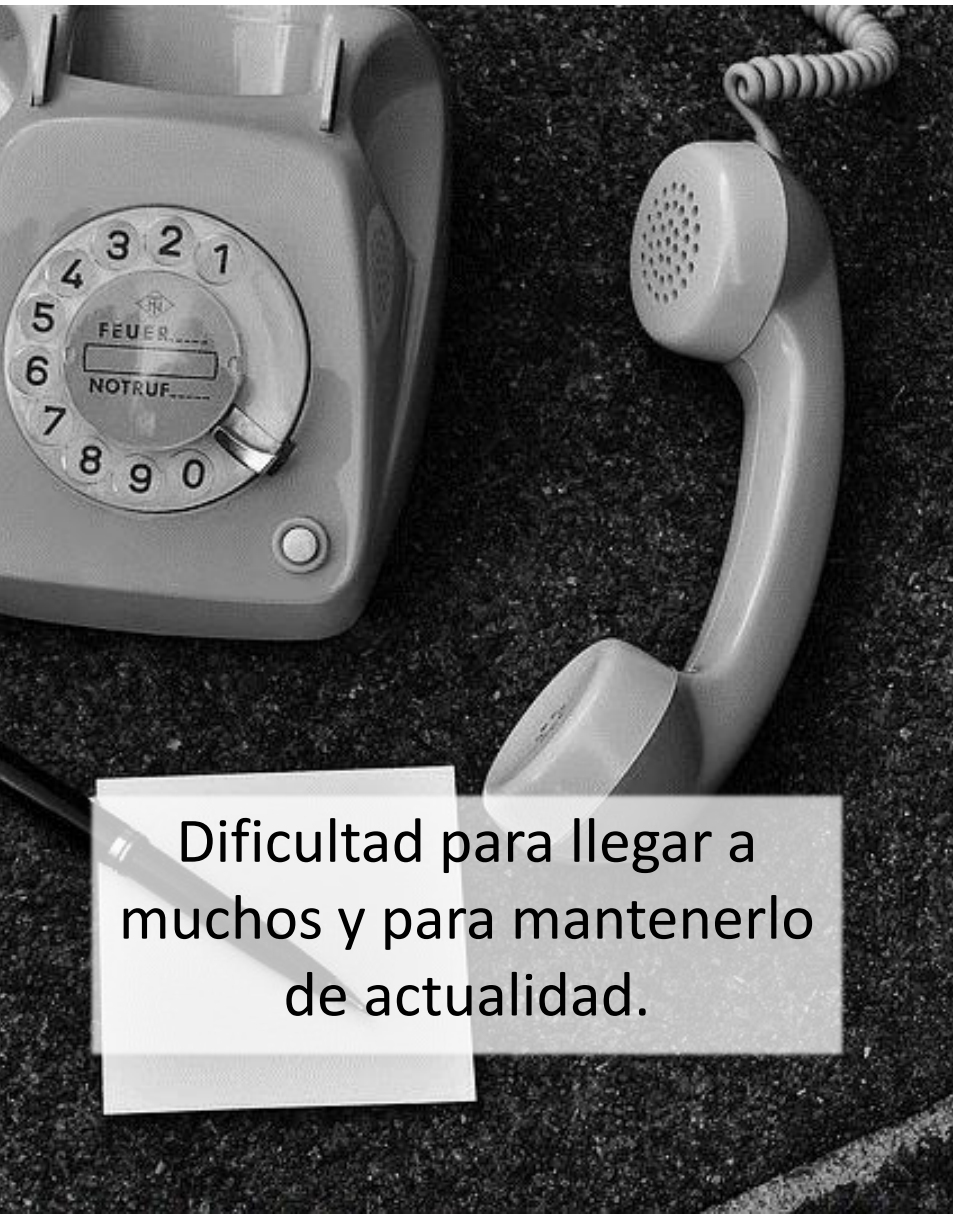
¿POR QUÉ SE EXPONEN LOS MENORES?

- Perciben beneficios > riesgos
- Influidos por el contexto social
- Cuantifican la popularidad



«búsqueda de reconocimiento social y aceptación del grupo para desarrollar el autoconcepto y la autoestima»

VIRALIDAD Y PERMANENCIA

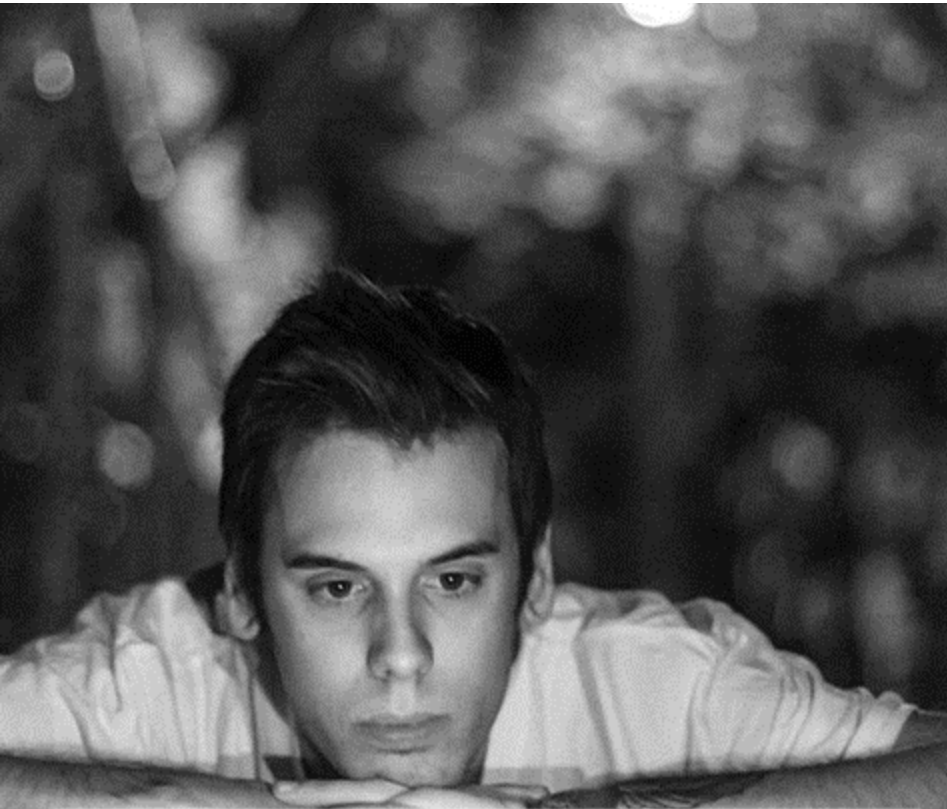


Dificultad para llegar a muchos y para mantenerlo de actualidad.



Puede compartirse muy fácilmente y puede reaparecer en cualquier momento.

INMEDIATEZ DE LAS COMUNICACIONES



Si entraban muchas ganas de ver a la novia...tocaba esperar o hablar por teléfono.



Se envían fotos y videos subidos de tono...¿Dónde acaban luego?

PRO
JUVEN
TUTE

PRIVACIDAD

- ¿Qué publicamos...?
- ¿Qué publican...?
- ¿Qué datos generamos...?
- ¿Quién puede acceder a ella...?



«capacidad que tiene un usuario de controlar qué información personal sube y genera, y quién puede acceder a ella»

¿HABLAN DE NOSOTROS?

- Menciones
- Etiquetas
- Fotos
- Comentarios



¿QUÉ DICE EL CONTEXTO?

- ¿Quiénes son nuestros amigos?
- ¿Qué “me gusta”?
- ¿Qué apps utilizamos?



Música



Radio León -
Cadena SER



Anda Ya!



LOS 40
PRINCIPALE

Televisión



El
Hormiguero



Mundo
Hacker TV

Otros

CyberCamp, Oficina de Seguridad del Internauta, P
Guardia Civil, McDonalds - Guardia Civil, Universid
Universidad de Deusto, Universidad de Salamanca
Sevilla, Universidad de Murcia, Universidad de Cue
Cantabria, Acceso Global, Grupo de Delitos Telem
26 más



IDEAS PARA GESTIONAR LA PRIVACIDAD



- >14 años en Redes Sociales
- Condiciones de uso
- Opciones de privacidad
- ¿Son gratis las redes sociales?
- Controlar lista de amigos
- Publicar datos de 3º
- Aplicaciones de 3º

«deben conocer lo que es Internet, su funcionamiento y el alcance de las actividades realizadas»

TÉRMINOS DE USO / POLÍTICAS DE PRIVACIDAD



- ¿que información recopila?
- ¿propósito de recopilarla?
- ¿que harán con ella? ¿cesión a 3º?
- ¿medidas adopta el sitio para asegurar mi información?
- ¿derechos ARCO?



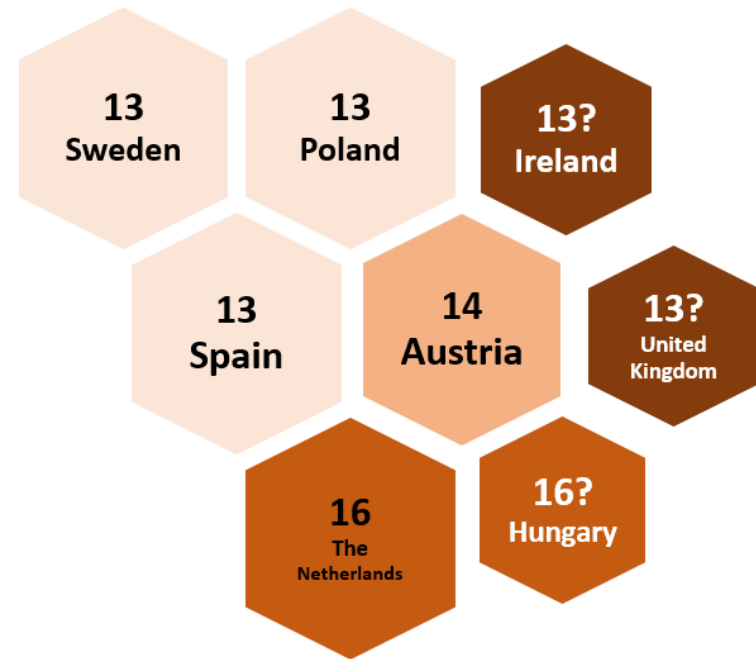
Nuestros sistemas automatizados analizan tu contenido (incluidos los correos electrónicos) para ofrecerte funciones de productos que sean relevantes para ti, como resultados de búsqueda y anuncios personalizados, así como detección de software malicioso y spam.

La información de tu cuenta. Proporcionas tu número de teléfono móvil para crear una cuenta de WhatsApp. Nos proporcionas los números de teléfono de la libreta de direcciones de tu teléfono móvil regularmente, incluidos los de los usuarios de nuestros Servicios y los de los demás contactos de la libreta de direcciones de tu teléfono móvil. Confirmas que estás autorizado a proporcionarnos dichos números. También puedes



NUEVO REGLAMENTO EUROPEO PROTECCIÓN DATOS (EU RGDP)

- Aplicable en mayo 2018
- Adaptación LOPD (anteproyecto de Ley Orgánica)
- Art 8. Consentimiento de los menores de edad.
 - Tratamiento lícito ≥ 13 años
- Art 21. Transparencia e información al afectado.
- Existen dudas de interpretación.



¿SON REALMENTE GRATIS LAS REDES SOCIALES?



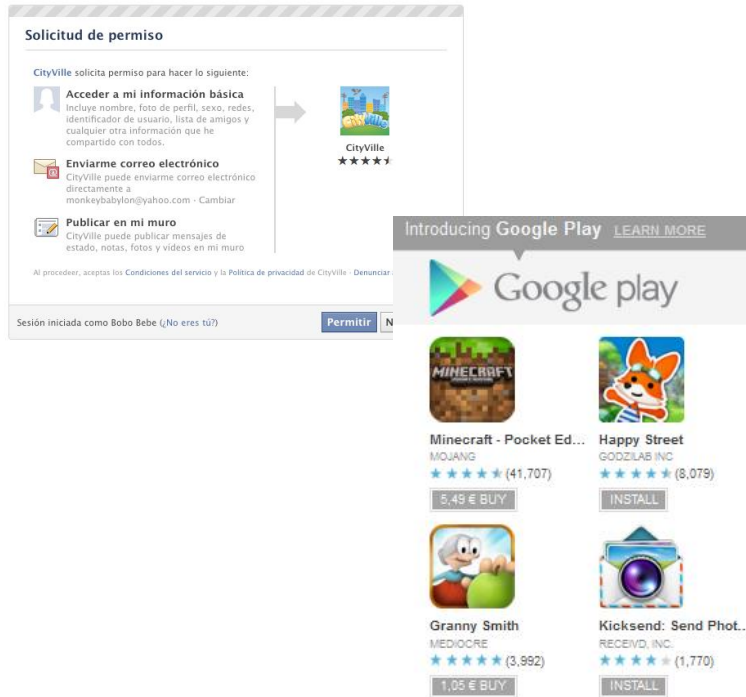
«si no estas pagando por algo, no eres el cliente, eres el producto»

CONTROLAR LA LISTA DE CONTACTOS



«entre 300 amigos es posible que alguno no lo sea tanto»

RIESGOS DE APLICACIONES DE 3º



- Acceso a datos básicos (legítimo)
- Captura de contraseñas
- Escuchar y grabar llamadas
- Grabar con la webcam
- Obtener geoposicionamiento

«los controles de seguridad de las redes sociales y plataformas móviles son limitados»

INTIMIDAD DE 3º



**¿Has pensado en lo
que cuentas de otras
personas en tu red social?**

PREVENCIÓN REPUTACIÓN EN LÍNEA

- Qué están creando una identidad digital que les acompañara el resto de su vida.
- Minimizar la difusión de datos personales.
- Pensar antes de publicar.
- Configurar adecuadamente las opciones de privacidad.
- Ser selectivos a la hora de aceptar a sus contactos online.
- Respetar los derechos de los demás.

SUPLANTACIÓN DE IDENTIDAD

SUPLANTACIÓN DE IDENTIDAD

“Hacerse pasar por otra persona a través de perfiles o cuentas falsas en cualquier tipo de servicio, utilización de cuentas y perfiles reales por otras personas e incluso el mero acceso a las mismas”



CÓMO SE PRODUCE

- Creación de cuentas falsas
 - Información e imágenes públicas
 - Opciones de privacidad en RRSS



CÓMO SE PRODUCE

- Acceso a cuentas legítimas
 - Sesiones abiertas
 - Dispositivos desprotegidos
 - Contraseñas y preguntas secretas débiles
 - Ingeniería social
 - Phishing
 - Malware



Correo electrónico o teléfono

☒ No cerrar sesión



PREVENCIÓN SUPLANTACIÓN DE IDENTIDAD

- Importancia de la seguridad en dispositivos
 - Bloqueo de terminales
 - Usuario limitado
 - Actualización de S.O. y programas
- Minimizar la difusión de datos personales.
- Pensar antes de publicar.
- Configurar adecuadamente las opciones de privacidad.
- Ser selectivos a la hora de aceptar a sus contactos online.

PARODIAS / FAKES



«entre la suplantación y la parodia»

SUPLANTACIÓN DE IDENTIDAD, CASO PRÁCTICO

CONTEXTO

- En el centro se habla de un perfil en redes sociales que parodia a un alumno.
- Se desconoce quién es el autor.
- Las publicaciones de ese perfil exageran un problema de dicción del alumno y ridiculizan sus gustos, aficiones...

¿Cómo actuar?

SUPLANTACIÓN DE IDENTIDAD, CASO PRÁCTICO

ANÁLISIS

- Investigación
 - El alumno suplantado no sabe nada, pero hay un grupo de alumnos que se burla de él indirectamente
 - Estos alumnos están entre los contactos del perfil falso, sin excepción
 - Preguntando por separado uno dice que “*él ya dijo que no había que hacerlo*” y otro confesó quién creó el perfil falso

SUPLANTACIÓN DE IDENTIDAD, CASO PRÁCTICO

SOLUCIÓN

- Se insta al creador a eliminar el perfil escribiendo a todos sus contactos para mostrar sus disculpas públicas.
- Disculpas del creador y el grupo de instigadores hacia el afectado.
- Trabajo de sensibilización con el colectivo de alumnos sobre usos TIC y acoso.

SEXTING

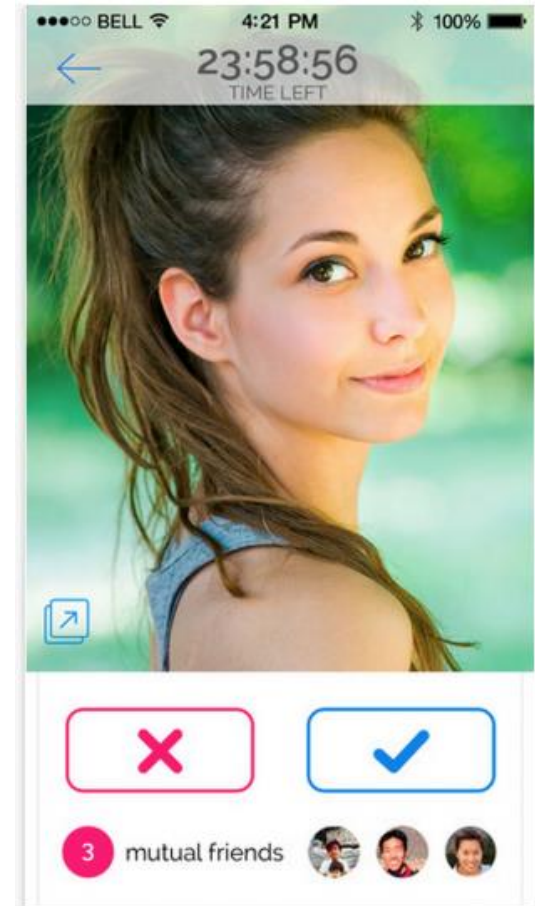
SEXTING, ¿QUÉ ES?



«Envío de contenido de tipo sexual (principalmente fotografía o vídeo), producido por el propio remitente, a través del móvil u otros medios digitales»

SEXTING, ¿POR QUÉ SE PRODUCE?

- Adolescentes en plena revolución hormonal y psicológica.
- Contexto cultural y sexualización precoz de la infancia.
- Inmediatez de las comunicaciones / generalización de los móviles.



«las motivaciones son las mismas de siempre, sólo que viven en un mundo digital»

Filtración del contenido:

- Intencionada:

- Venganza (revenge porn)
- Presumir
- Diversión

- Accidental:

- Dejarle el móvil a alguien
- Pérdida o robo del teléfono
- Venta, cambio, reparación del teléfono
- Virus o fraudes
- Filtraciones de bbdd de servicios
- Destinatario equivocado
- Sincronización automática de servicios



¿CÓMO DE COMÚN ES?

- 7% menores entre 9 y 16 años han recibido o visto mensajes de contenido sexual.
- Crece su uso con la edad.
 - 3% entre los 11 y 12 años.
 - 10% entre los 15 y 16 años.
- Diferencias por sexo: chicos reciben + / chicas envían +
- Los padres subestiman la incidencia del riesgo.
- 81% de las menores no se sintieron cómodas con la petición, el 35% accedió.

SEXTING, ¿CONSECUENCIAS?

Para quien aparece en la fotografía:

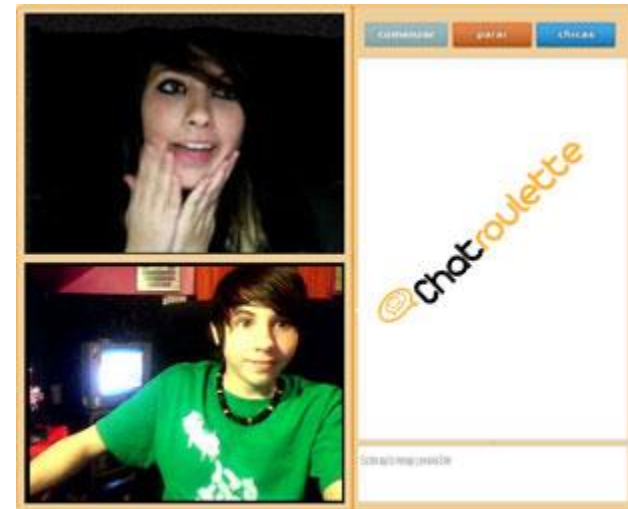
- Perdida de privacidad y daño a su reputación:
 - Imposibilidad de eliminar el contenido
 - Reutilización en otras web (ej. pornográficas)
- Humillación pública y linchamiento social.
- Sentimiento de traición y desconfianza futura.
- Riesgos psicológicos (ej. estrés emocional, ansiedad, depresión).



Y puede derivar en...

- Extorsión y chantaje.
- *Ciberbullying*.
- *Grooming* (ej. riesgo por geolocalización).
- Autolesión y suicidio.





«Snapchat: la autodestrucción del mensaje genera una falsa sensación de seguridad»



REPERCUSIONES



Para quien lo difunde:

- Pérdida de confianza y rechazo social.
- Repercusiones legales
 - Reforma CP: Difundir y revelar secretos ([art. 197](#)) introduce figura delictiva del sexting (art. 197.7)

"7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

Para quien lo recibe:

- Repercusiones legales
 - Poseer pornografía infantil ([art. 189.5](#))

«la mera tenencia de material pornográfico en el que aparezcan menores ya es un delito»

- Paradojas legales
 - ¿Es delito el sexting entre adolescentes?
 - ¿Y si la foto de una menor llega a un joven de 18 años (adulto)? ¿Y si es su pareja?
 - ¿Y si enviamos la foto a las FFCCSE para denunciar?



PREVENCIÓN SEXTING

1. No producirlo

- ¿Donde puede acabar esa foto? ¿Consciente de las dimensiones de Inet?
- Hoy confías en esa persona, pero ¿y mañana?
- Respeta tu propia intimidad y pide respeto. No ceder ante la presión y el chantaje.
- El sexting siempre implica riesgos.

2. No compartirlo. Por respeto y porque es un delito.

3. No promoverlo. Cuida de su intimidad.

4. Al menos...sin rasgos personales y detalles del entorno.

¿CÓMO PREVENIRLO? ÁMBITO ESCOLAR

- Fomentar una solida cultura de la privacidad.
- Adaptar procedimientos a la nueva realidad digital:
 - Plan de convivencia
 - Normas de régimen interno
 - Protocolos de respuesta a incidentes
- Formación del personal.
- Sensibilización del alumnado.
- Estructuras de ayuda entre alumnado.



¿CÓMO RESPONDER ANTE UN INCIDENTE?

ÁMBITO ESCOLAR

1. La detección y obtención de información preliminar.
2. Evaluar la situación y trazar un plan de actuación.
3. El plan de actuación.
4. Evaluación y seguimiento del plan.



1. La detección y obtención de información preliminar

- ¿Quién se encarga de la investigación?
- ¿Obligación de ponerlo en conocimiento de profesores, Tutor, Orientador, Dirección?
- Cuidar la confidencialidad y discreción en los procesos de comunicación.
 - Mínimas personas posibles involucradas.
 - Interlocutor víctima una persona de su mismo sexo.
 - No visualizar las imágenes del incidente.
- Analizar información a la mayor brevedad (ED, Tutor, Orientador, Inspector)
- No guardar evidencias salvo causa justificada.



- ¿Qué información debe obtener de los implicados/as?
 - Tipo de contenido
 - ¿Generado voluntariamente o con coacción?
 - ¿Filtrado intencionalmente?, ¿con que propósito?
 - ¿Otros jóvenes o adultos implicados?, ¿en el centro o fuera?
 - Grado de difusión y ubicación actual
(ej. páginas de Internet, dispositivos de los alumnos)

2. Evaluar la situación y trazar un plan de actuación

- Trabajar en línea con los protocolos de convivencia existentes.
- Registrar el incidente.
- Analizar las implicaciones:
 - Contexto de los menores implicados.
 - Evaluar el riesgo:
 - Tipo de incidente
 - Gravedad
 - Difusión
 - Intencionalidad
 - Victimización
 - Alcance temporal
 - Personas fuera del centro
- Valorar pedir ayuda



- Tipología del incidente:

- Agravados:

- Participación de adultos.
 - Intención de dañar (a raíz de conflictos interpersonales, existencia de amenazas y abusos).
 - Imágenes tomadas sin el consentimiento del afectado.

- Experimentales:

- Relación de pareja.
 - Búsqueda de atención.
 - Otros...

- Valorar pedir ayuda:
 - Convivencia (Dpto. Educación)
 - Sanidad (Pediatría) y Servicios Sociales.
 - Denuncia a la Policía / Fiscalía:
 - No siempre es conveniente denunciar, puede aumentar victimización.
 - Denunciar siempre que haya adultos implicados.
 - Considerar para tipologías agravantes.
 - Línea de emergencia (*helpline*)
- www.is4k.es/ayuda**
- Línea de denuncia (*hotline*)



3. El plan de actuación

- Medidas para detener la difusión de la imagen y apoyar a las víctimas.
- Acciones punitivas (RRI).
- Medidas restaurativas de la convivencia (para el filtrador).
- Activar mecanismos de mediación.
- Solicitar la retirada de los contenidos.

4. Evaluación y seguimiento del plan.

- Todas las actuaciones registradas.
- Copia del informe a la Comisión de Convivencia (Consejo Escolar).
- Identificar e implementar mejoras.



RELACIONES POSITIVAS EN LÍNEA

NETIQUETA: EDUCACIÓN EN LÍNEA

- Empatizar.
- Respetar la privacidad de los demás.
- Respetar el espacio y tiempo ajenos.
- Mantener un ambiente sano y agradable.
- No abusar de la superioridad.
- Comprender los errores de los demás.
- Respeto por lo ajeno.



EFFECTO DESINHIBIDOR

- Sentimiento de invencibilidad en línea
 - Supuesto anonimato
 - Desconocimiento de los delitos
- Reducción de las restricciones sociales
- Dificultad para percibir el daño causado



CIBERBULLYING, ¿QUÉ ES?



«daño intencional y repetido infligido por parte de un menor o grupo de menores hacía otro menor a través de medios digitales»

¿CÓMO SE PRODUCE? MÉTODOS Y MEDIOS

- Ataques directos
- Publicaciones y ataques en público
- Ciberbullying mediante terceros

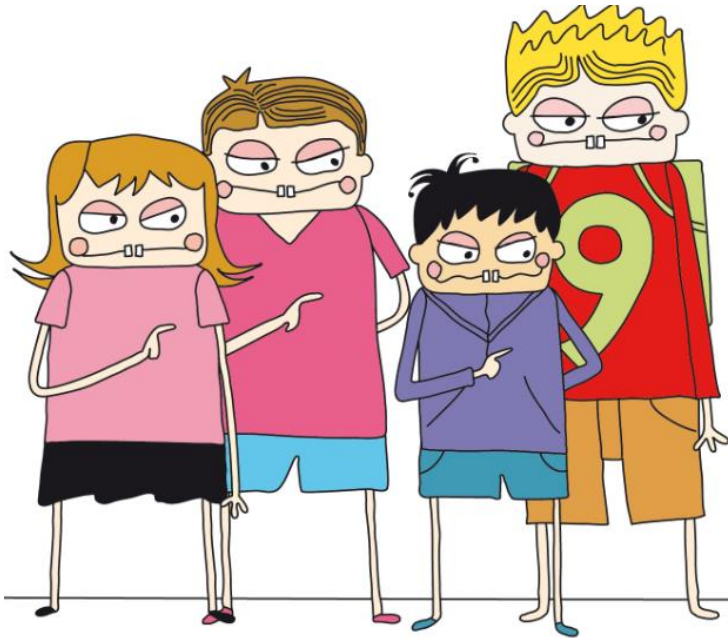


CARACTERÍSTICAS ÚNICAS DEL CIBERBULLYING

- Efecto desinhibidor
- Aumento del alcance de la victimización
 - Acceso 24x7 a la víctima
 - Viralidad y audiencia ampliada
 - Desconocimiento del acosador/res

«el ciberbullying se lleva a efecto de forma más sistemática y estable, provocando un mayor impacto sobre la víctima al aumentar su indefensión ante la situación»

¿ROLES IMPLICADOS?



- **No presentan perfil único.**
- Internet favorece la aparición de perfiles agresores indirectos.
- Escasa red social, baja autoestima y limitadas habilidades sociales.
- Otros perfiles: empollón, LGTB, alumno descolocado, etc.
- Víctimas que canalizan la frustración repitiendo el patrón.

ESPECTADORES



«el rol de los espectadores es clave, con su actitud pueden legitimar el acoso por lo que se hace necesaria su implicación»

SÍNTOMAS ASOCIADOS AL CIBERACOSO ESCOLAR

- Cambios de conducta y sociales / académicos / físicos y emocionales.



¿CÓMO PREVENIRLO? A TRASLADAR AL MENOR

- Cuida tu privacidad / Piensa antes de publicar.
- Internet nunca olvida.
- Chequea tu identidad digital (Googleate, alertas).
- Acuérdate de cerrar la sesión.
- Protege tus contraseñas.
- Vigila tus pertenencias.
- ¡Peligro geolocalización!
- Piensa ante de aceptar amistades.
- En Internet no todo el mundo es quien dice ser.

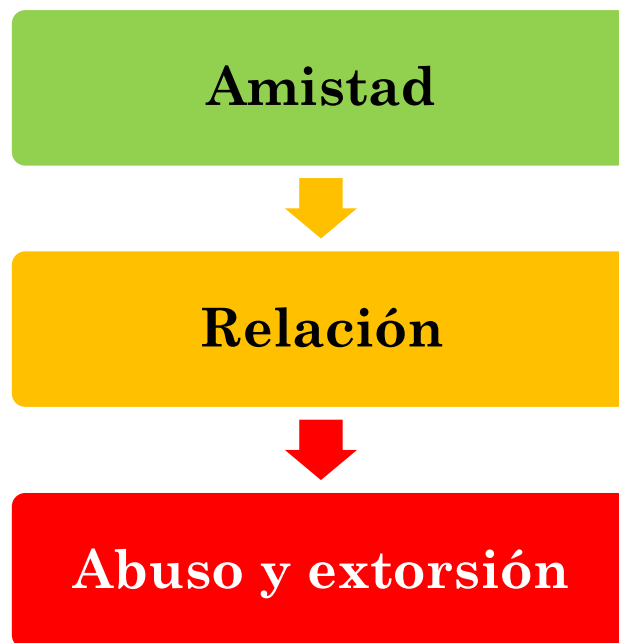


¿CÓMO PREVENIRLO? ÁMBITO ESCOLAR

- Fomentar una solida cultura de la privacidad:
 - Autoafirmación en la comunidad educativa (asertividad ante el abuso, «Declaración Antibullying»).
- Adaptar procedimientos a la nueva realidad digital
 - Plan de Convivencia, políticas de uso, normas de régimen interno.
 - Protocolos de respuesta a incidentes.
- Formación de la comunidad educativa
 - Sensibilización del alumnado (metodologías facilitadoras).
 - Capacitación a educadores.
 - Escuelas de familias.
- Estructuras de apoyo
 - Grupos de trabajo estable contra el ciberacoso.
 - Equipos de alumnos ayudantes.



GROOMING, ¿QUÉ ES Y CÓMO SE DESARROLLA?



«Acercamiento a menores por un adulto con finalidad sexual»

GROOMING, FASE DE AMISTAD



- Crean perfiles falsos “interesantes”
(ej. guapos/as, edad y gustos similares)



«¿seguro que la otra persona es quien dice ser?»

GROOMING, FASE DE AMISTAD → RELACIÓN



- Conectan con ellos

- “Coinciden”  en sus gustos e intereses.

- Les adulan, lanzan mensajes positivos.

- **Se ganan su confianza**

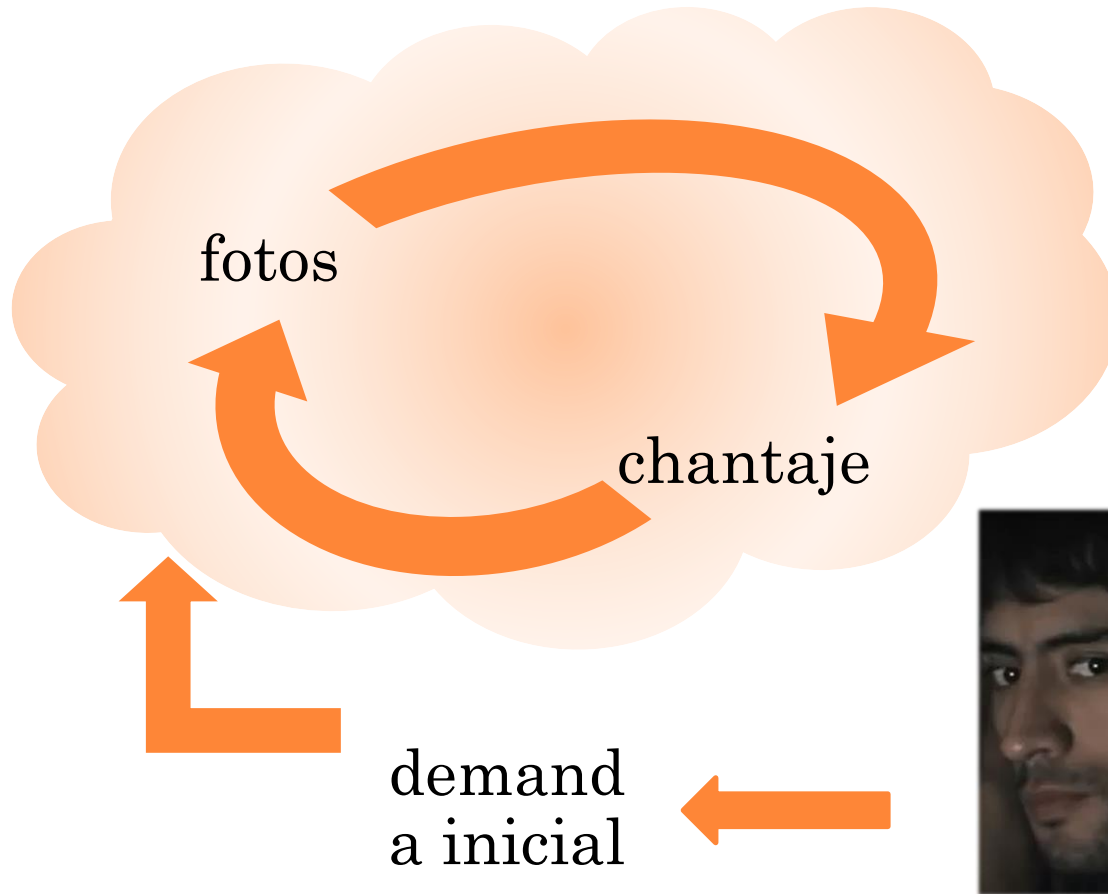
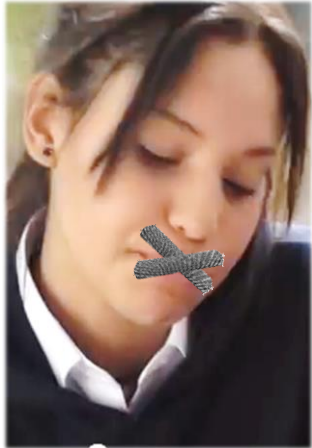
- Afinidad, sentirse especiales, queridos.

- Confesiones íntimas, más información personal.

- Regalos (posición social).

- Constancia y perseverancia (semanas... o meses).

GROOMING, FASE DE ABUSO Y EXTORSIÓN



«en cuanto logran la primera foto o confianza, el chantaje está servido, quieren más y más»

GROOMING, CONSIDERACIONES LEGALES

- Delitos contra la libertad e indemnidad sexuales, CP
 - Abuso y agresión sexual [art. 183](#), [183 bis](#), espec. [183 ter](#)
 - Acoso sexual [art. 184](#)
 - Exhibicionismo y provocación sexual [art. 185](#) y [art. 186](#)
 - Corrupción de menores [art. 188](#)
 - Pornografía infantil [art. 189](#)



GROOMING, ¿CÓMO PREVENIRLO?

- Configuración segura de dispositivos y servicios



- Contraseñas robustas, opciones de privacidad, webcam tapada, geolocalización desactivada, sistemas actualizados, cuentas limitadas.

- Extremas precauciones al conversar en línea

- No todo es lo que parece, cuidado al aceptar “amigos”, no quedar con desconocidos.

- Trabajar la autoestima y la asertividad

- No ceder a la presión y al chantaje.

- Pensar antes de compartir

- Consecuencias, ¿podrán utilizarlo en mi contra?



RESUMEN RIESGOS

- **Publicaciones propias que dañan la reputación**
(ej. imágenes inapropiadas, *sexting*, comentarios desafortunados)
- **Uso comercial de información personal**
(hábitos de navegación, motivaciones, preocupaciones)
- **Uso malintencionado de su información por 3º**
 - Ciberacoso escolar (*ciberbullying*)
 - *Grooming* / sextorsión
 - Suplantación de identidad

PENSAR ANTES DE PUBLICAR



«Tengan cuidado con lo que suben a Internet, porque permanecerá allí el resto de sus vidas»

¡Participa en IS4K!

is4k INTERNET
SEGURA
FOR KIDS



www.is4k.es



contacto@is4k.es



Internet Segura for Kids



@is4k