Convivencia Segura En La Red:Ciberayudantes

- Una red segura para menores
- 1. Privacidad e identidad digital
  - 1.1 Definición y conceptos
  - 1.2 Pautas y recomendaciones
  - 1.3 Datos y ejemplos
  - 1.4 Estrategias de prevención
  - 1.5 Normativa
- 2. Suplantación de identidad
  - 2.1 Definición y conceptos
  - 2.2 Datos y ejemplos
  - 2.3 Pautas y recomendaciones
- 3 Prevención de virus y fraudes
  - 3.1 Definición y conceptos
  - 3.2 Datos y ejemplos

Copyright 2026

- 3.3 Pautas y recomendaciones
- 3.4 Estrategias de prevención

- 4. Acceso a contenidos inapropiados
  - 4.1 Definición y conceptos
  - 4.2 Datos y ejemplos
  - 4.3 Pautas y recomendaciones

- 5. Tecnoadicciones
  - 5.1 Definición y conceptos
  - 5.2 Datos y ejemplos
  - 5.3 Pautas y recomendaciones

- 6. Ciberbullying, sexting y grooming
  - 6.1 Definición y conceptos
  - 6.2 Datos y ejemplos
  - 6.3 Pautas y recomendaciones

- 7. Ciberayudantes: Un programa de centro
  - 7.1 Contexto del proyecto y del centro
  - 7.2 Marco teórico
  - 7.3 Justificación
  - 7.4 Objetivos
  - 7.5 Metodología
  - 7.6 Actividades realizadas
  - 7.7 Criterios y herramientas de evaluación.
  - 7.8 Resultados y conclusiones
  - 7.9 Repercusión en medios de comunicación.

- Glosario
  - Glosario y recursos
  - Créditos

Copyright 2026

Copyright 2026

Una red segura para menores

El uso de Internet y las nuevas tecnologías nos brinda múltiples beneficios pero también nos expone a un conjunto de riesgos. El acceso a este nuevo escenario es una experiencia distinta y requiere que la familia y los centros educativos estén preparados para conducir a los menores hacia un uso seguro, responsable y respetuoso de Internet.

Resulta vital, entonces, **conocer los impactos negativos a los cuales se exponen los menores** con el objeto de tomar conciencia, estar prevenidos, protegerlos de cualquier posible daño y enseñarles el uso adecuado de las tecnologías. Queremos mejorar el clima de convivencia en los centros docentes tanto en el entorno real como virtual, favoreciendo valores prosociales de dialogo, respeto y tolerancia que contribuyan a prevenir la violencia y el maltrato, y que permitan asimilar los valores propios de la cultura de paz. **La mejora de la convivencia es**, por tanto, **un factor general de la calidad educativa.**

Este curso de formación online responde a la necesidad de desarrollar una formación entre el profesorado de primaria y secundaria en el uso seguro y responsable de las TIC por parte de los menores.

El **objetivo genera**l del curso consistirá en adquirir las destrezas oportunas para **identificar los principales riesgos a los que puede enfrentarse su alumnado y para darles las pautas necesarias para poder abordarlos**. Pero además pretende hacerlo con la participación y colaboración del propio alumnado a partir de la experiencia llevada a cabo en el IES Parque Goya con su programa Ciberayudantes.

Se trata de un curso eminentemente práctico que pretende dar una visión general de algunos aspectos relacionados con la gestión de la privacidad y los principales riesgos a los que se pueden enfrentar los menores en su uso cotidiano de las TIC y facilitar pautas y recursos para desarrollar su uso seguro y responsable en el aula.

Los temas que vamos a tratar estarán relacionados con la identidad digital, la gestión de la privacidad en la red, los impactos negativos del uso de internet como son: fraudes y virus que acechan en las redes sociales, el acceso a contenidos inapropiados, el ciberbullying, el sexting , el grooming y las tecnoadicciones. Pero también queremos proponer iniciativas que permitan un uso

Copyright 2026

adecuado de las redes sociales por parte de nuestros y que sirvan de base para una reflexión seria sobre estos temas.

OBJETIVOS Y CONTENIDOS

OBJETIVOS:

Como objetivo transversal vinculado a la formación docente, nos proponemos mejorar la competencia digital profesional del docente. Además nos planteamos los siguientes objetivos específicos en este curso: 1. Promover el uso seguro y responsable de las TIC entre los menores. 2. Introducir en la práctica educativa el buen uso y saludable de internet. 3. Conocer los riesgos e impactos negativos del uso de internet. 4. Fomentar actuaciones centradas en la protección de menores de edad mediante material pedagógico dirigido al alumnado de primaria y secundaria. 5. Dar respuesta a situaciones que dañan la convivencia en el centro. 6. Fomentar una cultura de diálogo, la escucha activa, el interés por el compañero basado en valores prosociales de respeto, ayuda y solidaridad. 7. Prevenir la aparición de comportamientos de riesgo social, tales como: ciberbullying, sexting, grooming etc. 8. Iniciar una estrategia de participación y protagonismo de los adolescentes, apoyada en las buenas prácticas para hacer de Internet un entorno saludable.

CONTENIDOS:

La estructura del curso es modular y secuencial. El curso consta de 4 módulos. Cada uno de ellos comprende dos unidades didácticas. El último de ellos se centrará sobre el programa Ciberayudantes, una experiencia llevada a cabo en el IES Parque Goya.

MÓDULO I: IDENTIDAD DIGITAL 1. Privacidad e identidad digital. 2. Suplantación de identidad.

MÓDULO II: Riesgos en la red I 3. Prevención de virus y fraudes 4. Acceso a contenidos inapropiados.

MÓDULO III: Riesgos en la red II 5. Tecnoadiciones. 6. Ciberbullying, sexting y grooming.

MÓDULO IV: CIBERAYUDANTES un programa de centro 7. Justificación, objetivos y contenidos. 8. Iniciativas

Observamos. Observatorio sobre el uso de redes sociales en la ESO. Visionamos cortos y reflexionamos Tuiteamos. Jugamos. Kahoot y Quiziz Creamos Cibercortos, Animaciones y

videojuegos Colaboramos con la Familias Creamos equipo de Ciberayudantes. Formación de los futuros ciberayudantes. Netiqueta. Otras actividades.

ANEXOS: Glosario de términos Recursos y Material complementario Bibliografía y webgrafía

Copyright 2026

1. Privacidad e identidad digital

Copyright 2026

1. Privacidad e identidad digital

1.1 Definición y conceptos

DEFINICIÓN Y CONCEPTOS

Cuando hablamos de **privacidad en Internet** nos estamos refiriendo al control que tenemos sobre los datos personales que posee un determinado usuario cuando se conecta a Internet, interactúa e intercambia datos durante la navegación.

Para evitar problemas es necesario saber gestionar nuestra privacidad, ya que nuestros datos personales informan sobre nuestro nombre, domicilio o correo, pero también nuestras aficiones, gustos o creencias. Por tanto debemos poner los medios para proteger nuestra información y mantener el equilibrio entre seguridad y privacidad.

Resulta importante hacer referencia a algunos aspectos relacionados con la seguridad en la red:

- **Confidencialidad.** Hace referencia a la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. Resulta de vital importancia en el entorno virtual porque un mal uso de la información podría traer graves consecuencias en la vida de las personas.
- **Autenticación.** Es proceso de confirmar y verificar la identidad digital de las personas para comprobar que algo (o alguien) es quien dice ser.
- **Huella o Identidad digital**. Es el rastro que cada usuario de Internet deja en la red como resultado de su interacción con otros usuarios o con la generación de contenidos. Y los límites entre identidad analógica y digital cada vez son menos claros.

Hoy en día los menores van construyendo su propia identidad digital, incluso antes de haber utilizado Internet, como consecuencia de la información que otros han subido a la red, y de forma muy especial los propios padres, que comparten con sus amigos pero también con desconocidos.

Es muy fácil subir imágenes, vídeos o comentarios a la red, pero resulta difícil borrarlos. Es preciso ser muy selectivos a la hora de compartir cualquier contenido en Internet ya que una foto graciosa ahora, puede no serlo en el futuro. Tengamos en cuenta que la foto más graciosa o el comentario más perspicaz puede no serlo dentro de unos años. Por tanto, es fundamental explicar a los menores la importancia de esta huella digital así como la perdurabilidad de dicha información en la red.

Copyright 2026

- **Reputación Online**. Es el reflejo del prestigio o estima de una persona en Internet. Cuando un menor sube un contenido a su red social lo que busca es la aceptación y aprobación de sus iguales. Esto genera una falta de control sobre los comentarios que se vierten y las consecuencias por incrementar la popularidad pueden ser impredecibles. Pero, ¿cuáles son las **motivaciones** que le impulsan a publicarlo?
- En primer lugar está el afán de ser más popular, que se mide en función del número de amigos o contactos registrados en su perfil.
- En segundo lugar tenemos la validación social que recibe por parte de sus iguales y que determinan el desarrollo de su autoconcepto y la autoestima. Cuando un adolescente publica algo en su muro, pretende provocar una respuesta y el silencio se interpreta como un rechazo.
- Finalmente, en la red tienen una oportunidad para exponerse y mostrar su vida, para autoafirmarse y buscar nuevas experiencias.
- **Problemas y riesgos asociados a la privacidad.** Una de las preocupaciones de familias y educadores es el tema de la publicidad en internet**.**
- Como es sabido, una de las formas en que la publicidad se lleva a cabo es a través de las **cookies.** Se trata de herramientas que facilitan la navegación del usuario, con la finalidad de almacenar y recuperar datos que se encuentran en nuestro equipo. Esto tiene una implicación importante en relación con la privacidad, ya que dicha información permite ofrecer publicidad atendiendo a nuestros intereses.
- Otro de los riesgos que podemos destacar es la **geolocalización** cuya finalidad se orienta a la utilización de información vinculada a una localización geográfica del mundo real. Y citamos como ejemplo la aplicación de Facebook Places, en la que podemos compartir la posición con los amigos.

Es importante gestionar adecuadamente nuestra privacidad, y no podemos olvidarnos de la privacidad de los demás a partir de nuestro propio comportamiento en la red. Tenemos que salvaguardar el derecho al honor, a la intimidad y a la imagen de terceras personas. Tanto adultos como menores debemos siempre pensar antes de publicar alguna información no solo de nosotros, sino también de otras personas.

Videos sobre la privacidad e identidad digital de **EDUCAINTERNET:**

- Datos de carácter personal:

https://www.youtube.com/embed/LqD2OBeeaNE?rel=0

- Privacidad:

https://www.youtube.com/embed/OdZCGKlwmrk?rel=0

Copyright 2026

- Identidad digital y reputación:

https://www.youtube.com/embed/pq8RgKNylmo?rel=0

1.2 Pautas y recomendaciones

PAUTAS Y RECOMENDACIONES PARA FAMILIAS Y EDUCADORES

En caso de detectar algún tipo de vulneración de intimidad o privacidad de nuestros menores (por ejemplo, una foto/vídeo privado o dato de carácter personal en Internet que se ha publicado sin nuestro consentimiento -en caso de menores de 14 años- o sin el consentimiento del menor -si es mayor de 14-, y no es por un error de algún conocido), en primer lugar deberíamos comunicárselo a la persona implicada y pedirle la retirada de la imagen. De no ser esto posible, el camino que se debemos seguir como padre, madre y/o tutor sería:

- Guardar pruebas de los hechos o de las evidencias electrónicas imprimiendo pantallazos, grabando la información, tomando imagen de la pantalla mediante un móvil.
- Ponerse en contacto con los administradores del portal o red social para solicitar su retirada junto con los comentarios ocasionados. Buena parte de las redes sociales cuentan con mecanismos para que los soliciten la supresión de fotos o vídeos que violan su intimidad.
- Denunciar ante la Agencia Española de Protección de Datos. www.aepd.es
- Presentar una denuncia ante la Policía o la Guardia Civil. En las webs: www.policia.es y www.guardiacivil.org podemos poner la denuncia.
- También debemos recordar a los menores es que cuando publiquen un contenido en la red deben comprobar que no violan la política de privacidad y que lo que deseen que sea privado no lo pongan público utilizando la configuración de la red social.

Copyright 2026

1. Privacidad e identidad digital

1.3 Datos y ejemplos

ALGUNOS DATOS Y EJEMPLOS QUE EVIDENCIAN RIESGOS CONTRA LA PRIVACIDAD

En España, los menores de 14 años no pueden acceder a las redes sociales, excepto si lo hacen con consentimiento paterno. A pesar de esto, en España, un 37% de los niños menores de 11 años participa en mundos virtuales.

La sección española del **proyecto EU Kids online** ha dado a conocer los resultados de sus estudios sobre la privacidad de los menores en Internet y según sus datos, sólo el 55% de los menores sabe cómo cambiar su configuración de privacidad en las redes sociales. Además, un 9% de los menores españoles que usan este tipo de redes sociales publican en ellos información privada como el número de teléfono o la dirección de su domicilio. Además, el 71% de los padres y madres han publicado imágenes de sus hijos e hijas menores de 2 años, el 24% de sus hijos recién nacidos y el 24% las ecografías prenatales. Así, estos niños y niñas reciben en herencia una identidad digital que otros han construido para ellos y tienen una huella digital en Internet antes de llegar a la vida.

A continuación os presentamos algunos ejemplos reales de privacidad de datos en la red, publicados en los medios de comunicación. Para acceder a ellos sólo tienes que hacer clic en cada ejemplo:

Ejemplo 1: Carrefour multado por exponer la imagen de un cliente con un hijo menor de edad

El Tribunal Supremo condenó a Carrefour a indemnizar con 12.000 euros a un padre de familia cuya fotografía, acompañado de uno de sus hijos menores, fue exhibida por error en un ordenador que la compañía puso a la venta después de que el afectado lo devolviera por el mal funcionamiento del dispositivo.

Copyright 2026

Juan R. C. compró un ordenador portátil en un centro comercial de la citada entidad en Cádiz, pero tras un breve período de uso hubo de devolverlo porque su funcionamiento no era el correcto. Cuando lo hizo, el ordenador contenía fotografías suyas, su esposa e hijos menores, pero la entidad comercial le aseguró que borraría las fotografías al formatear el disco duro, cosa que no hizo. «Días más tarde, la entidad demandada expuso el ordenador en un muestrario de informática, enseñando como salvapantallas una foto de dicho cliente con un hijo menor en la casa familiar», relata la sentencia.

http://www.abc.es/economia/20141130/abci-supremo-condena-carrefour-foto-201411301222.html

Ejemplo 2: Disturbios en un pueblo holandés en una fiesta convocada por error en Facebook

Merthe, una adolescente holandesa que quería celebrar este viernes a lo grande su 16 cumpleaños, se ha pillado los dedos en Facebook. Olvidó mencionar que la fiesta nocturna sería privada, y la invitación remitida a través de la red social ha llegado a 25.000 personas. El Ayuntamiento de su pueblo, Haren, al norte del país, declaró el estado de alerta. La policía confirmó la asistencia de cerca de 4.000 de personas. La situación desbordó las previsiones y los jóvenes lanzaron petardos y botellas a los agentes en un ambiente muy tenso. También han tumbado farolas y arrancado señales de tráfico, además de pisotear jardines y dañar coches. Los disturbios se han saldado con al menos seis heridos, tres de ellos graves, y 20 detenidos..

http://internacional.elpais.com/internacional/2012/09/21/actualidad/1348236645_311482.html

Ejemplo 3: La lección de privacidad de una profesora se hace viral

¿Hasta dónde puede llegar una foto vuestra en Internet? Esa era el título de la lección que Julie Ann Culp quería impartir a sus alumnos de quinto. La profesora de Tennessee (EEUU) quería aleccionar a su clase sobre los peligros de Internet y sobre cómo viaja la información en la Red.

Para ello, se fotografío con un cartel en el que se leía: "Estoy hablando a mis alumnos de quinto sobre la seguridad en Internet y cómo de rápido una foto puede ser vista por montones de personas. Si estás leyendo esto, por favor, pincha en "me gusta". ¡Gracias!"

Seguro que la profe no fue consciente del tsunami que se iba a desatar por culpa de su acción. En apenas seis días, la foto lleva más de 4.200.000 ‘me gusta‘ y 100.000 compartidos en Facebook. En otro muro en el que fue publicada lleva más de 900.000 ‘me gusta’ y más de 24.000 compartidos.

https://es.finance.yahoo.com/blogs/fintechnologiayredeses/lecci-n-privacidad-profesora-viral-002051461.html

Copyright 2026

1. Privacidad e identidad digital

1.4 Estrategias de prevención

ESTRATEGIAS DE PREVENCIÓN EN CENTROS EDUCATIVOS

Algunas de las pautas y recomendaciones preventivas que hemos de conocer han de venir determinadas en primer lugar por la formación de los menores, y en segundo lugar por un seguimiento continuado en el tiempo. Algunas de ellas son las siguientes:

- Es importante facilitar tanto desde la familia como desde el centro pautas de comportamiento y reiterar al menor que siempre debe dialogar con sus padres o un adulto de confianza sobre las dudas que tenga sobre su privacidad.
- Los educadores deben reflexionar junto a los menores sobre los riesgos que conlleva divulgar los datos personales en Internet y deben educar en las buenas prácticas de la privacidad.
- Se deben promover charlas con las familias y tutores para informar de los peligros que corren sus hijos si no gestionan bien la intimidad de éstos.
- Revisar los ajustes de configuración de los perfiles en las redes sociales para comprobar que no alteran la política de privacidad y que lo que quieren que sea privado no lo pongan público.
- Examinar lo que otros publican explicando el peligro de los etiquetados de terceras personas sin su consentimiento, siendo un acto denunciable, y enseñar que derechos tiene cada niño o niña respecto a su privacidad.
- Desde el centro escolar, se tiene que comunicar al alumnado las responsabilidades civiles, administrativas o penales cuando se vulneran los derechos, como el del honor, la intimidad personal y familiar y la propia imagen, tanto propios como de terceros en Internet.
- Proteger la información delicada, enseñando a los menores cuáles son sus derechos frente a sus datos personales y cómo pueden ejercer los mismos. Es preciso hacerles conscientes de la peligrosidad de revelar los datos a desconocidos, como no lo harían en la vida real.

Copyright 2026

- Participar en el **Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos**, que pretende potenciar actuaciones preventivas en relación con los riesgos a los que se ven sometidos los menores y los jóvenes, en temas tan importantes como el uso de Internet y las nuevas tecnologías, entre otros.
- Instalar un antivirus y actualizarlo periódicamente, poner un anti espía o antispyware que ayude a eliminar los programas espías o troyanos que puedan entrar a través de distintas páginas, actualizar el sistema operativo y las aplicaciones instaladas activando para ello las actualizaciones automáticas para evitar que a través de un fallo de seguridad del mismo alguien se pueda apoderar de datos del ordenador...

Además los adultos podemos darles una serie de consejos como:

- No entrar en páginas Web sospechosas.
- No facilitar nuestras contraseñas a nadie y modificarlas periódicamente.
- En el uso del correo electrónico, cuando se mande una misma información a varios contactos se debe usar el CCO (correo con copia oculta) para no mostrar los contactos a los demás destinatarios.
- Controlar el uso de la webcam y cuando no estén en uso, taparlas o quitarlas pues pueden ser encendidas por control remoto sin darnos cuenta.
- No compartir libremente los datos de geolocalización pues todos sabrán dónde estás y dónde no.

La creencia de que los niños y adolescentes son nativos digitales, no garantiza un mayor control sobre las herramientas que utilizan, por lo que la falta de privacidad se convierte en un problema. Además su menor conciencia del riesgo, el exceso de confianza tecnológica y la necesidad de pertenencia e identificación grupal, puede aumentar los peligros que entrañan las prácticas de publicación de datos personales, imágenes y vídeos.

Copyright 2026

1.5 Normativa

NORMATIVA APLICABLE A LOS MENORES EN TEMAS DE PRIVACIDAD

La imagen de los menores en Internet es algo a lo que la legislación presta una especial atención. Y con razón. A poco que naveguemos por las redes sociales, encontraremos familias que publican continuamente y sin ningún pudor fotografías de sus hijos e hijas.

La imagen de una persona, sea adulto o menor, se considera un dato de carácter personal, puesto que permite identificar a una persona. Esto viene recogido en el **artículo 3 de la LOPD**, y por lo tanto se trata de un dato protegido por esta Ley y por las regulaciones que la desarrollan.

En el caso de los menores, corresponde a sus padres o tutores legales la función de velar por este derecho. Lo cual no quiere decir que el padre o la madre puedan autorizar indiscriminadamente el uso de la imagen del menor para cualquier cosa. Se trata de velar por este derecho, no de jugar con él. Recordemos que la Ley dice que es un derecho irrenunciable.

A modo de ejemplo, las fotos que publicas en **Facebook** de tus hijos siguen siendo tuyas pero has concedido a la red social el derecho a utilizarlas mientras no las elimines de la red. Pero **incluso si tú las eliminas pero las has compartido con otra persona en Facebook, y ésta no lo hace, pueden seguir usándolas.**

Además, la **Ley Orgánica 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen** también establece que el derecho al honor, a la intimidad personal y familiar y a la propia imagen es irrenunciable, inalienable e imprescriptible.

La protección de menores se encuentra muy visible en la normativa española, de modo que siempre que pueda afectarles, se incluye una referencia a la protección de los mismos.

La Constitución Española de 1978 al enumerar, en el capítulo III del Título I, los principios rectores de la política social y económica, hace mención en primer lugar a la obligación de los Poderes Públicos de asegurar la protección social, económica y jurídica de la familia y dentro de ésta, con carácter singular, la de los menores. Además, La Constitución, **en su artículo 18.4** dispone que "La Ley limitará el uso de la informática para garantizar el honor y la intimidad

Copyright 2026

personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Se incluye aquí también a los menores.

Otras leyes españolas, que protegen la difusión de las imágenes de los menores son la **Ley Orgánica 1/1982, de 5 de mayo**, **de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen**, la **Ley Orgánica 1/1996, de protección jurídica del menor** y la última **instrucción 2/2006 sobre el Fiscal y la Protección del Derecho al Honor, Intimidad y propia imagen de los menores**, que prohíben la difusión de datos o imágenes referidos a menores de edad cuando sea contrario a su interés, incluso cuando conste el consentimiento del menor.

Otras normativas más relevantes sobre este tema son **La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD**), la Ley 34/2002 de servicios de la sociedad de la información y comercio electrónico, la Ley 7/2010 General de comunicación audiovisual, y la Ley 26/ 2015 de modificación del sistema de protección a la infancia y a la adolescencia.

A modo de conclusión podemos decir que la imagen de los menores en la Red no nos pertenece, y ser su padre, su madre o su tutor legal no nos autoriza a jugar con este derecho, sino al contrario: debemos velar por él. Se trata de reflexionar sobre el escaso control que podemos tener en las redes sociales. A partir de ahí, utilizar el sentido común y conocer la legislación.

> Legislación estatal de la Agencia Española de Protección de datos.

2. Suplantación de identidad

Copyright 2026

2. Suplantación de identidad

2.1 Definición y conceptos

DEFINICIÓN Y CONCEPTOS

La “**Suplantación de Identidad**” en general consiste en el uso de información personal para hacerse pasar por otra persona con el fin de obtener un beneficio propio. Normalmente este beneficio genera un perjuicio a la persona que sufre dicha suplantación de identidad. En el caso de menores, es un riesgo cada vez más frecuente que se produce cuando una persona malintencionada actúa en nombre del menor haciéndose pasar por él mediante la utilización de diversas técnicas.

Hay que diferenciar entre dos conceptos:

- **Suplantación de identidad**. La suplantación de identidad consiste en la apropiación de derechos y facultades propias de la persona suplantada (por ejemplo, acceder a la cuenta de una red social).
- **Usurpación de la identidad**. La usurpación de identidad consiste en que una vez suplantada la identidad se empiece a interactuar como si realmente fuera propietario de esos derechos y facultades (por ejemplo, realizar comentarios o subir fotografías).

Ejemplos de suplantación de identidad:

- Registrar un perfil en una red social con el nombre de otra persona sin su consentimiento y utilizando datos o imágenes de la víctima, sería una suplantación de identidad y en principio se consideraría delito.
- Si únicamente se registra un perfil falso por medio del nombre/alias y no se utiliza información o imágenes personales de la persona suplantada, no se consideraría delito. Para considerarse delito la apropiación no se debe limitar al nombre, sino a todas las características o datos que integran la identidad de la persona.
- Acceder sin consentimiento a una cuenta ajena para tener acceso a la información allí almacenada. Sería una suplantación de identidad y en principio se consideraría delito (al menos un delito de descubrimiento y revelación de secretos).
- Acceder sin consentimiento a una cuenta ajena utilizando los datos personales y haciéndose pasar por el suplantado (por ejemplo, realizando comentarios o subiendo fotografías). Sería una usurpación de identidad y se consideraría delito

- Publicación sin consentimiento de anuncios o comentarios utilizando el nombre de un tercero o incluso utilizando sus datos personales para identificarse con terceras personas a través, por ejemplo, de correo o mensajería instantánea (Whatsapp). Sería una usurpación de identidad y se consideraría delito.

Ejemplos de suplantación de identidad entre menores.

- Entrar sin consentimiento.
- Acceder a información sensible como puede ser el caso de una foto o un vídeo.
- Acosar o desprestigiar a la otra persona (casos de ciberbullying), por ejemplo, publicando comentarios polémicos o denigrantes que serán vistos por terceros.
- Ganarse la amistad de un menor con el fin de cometer un abuso sexual (casos de grooming donde el acosador utiliza la usurpación de identidad para acceder a cuentas que sirvan de “puente” para facilitar el contacto con la víctima).
- ***Hacerse pasar por otra persona.*** Crear una cuenta para hacerse pasar por otra persona. Aunque esta forma se suele dar en menores, es uno de los casos más frecuentemente utilizados para suplantar a gente famosa.

Técnicas más utilizadas para la suplantación de identidad

Las técnicas utilizadas para la suplantación de identidad tienen que ver con el concepto de **ingeniería social**, que se refiere al uso que hacen los ciberdelicuentes de la manipulación psicológica sobre las personas para conseguir sus fines, teniendo en cuenta la tendencia general de éstas a la confianza. Método basado en la persuasión y muy eficaz en el caso de los menores de edad que, debido tanto a su falta de experiencia y conocimientos relacionados con este tema como con su confianza e inocencia, son considerados especialmente vulnerables. Normalmente el motivo que impulsa a los adolescentes para la realización de suplantación de identidad es, habitualmente, la mera diversión. Las más utilizadas son el **Phishing , el Pharming y el SMiShing**.

Phishing. Es un término informático utilizado para denominar el fraude por suplantación de identidad, una técnica de ingeniería social. El término phishing procede de la palabra inglesa fishing (pesca) haciendo alusión a “picar el anzuelo”. Lo que significa que no aprovecha una vulnerabilidad en los ordenadores sino un "fallo humano" al engañar a los usuarios de Internet con un correo electrónico que aparentemente proviene de una empresa fiable, comúnmente de una página Web bancaria o corporativa.

Dado el cada vez más creciente número de denuncias de incidentes relacionados con el phishing en el contexto de los menores de edad, se hace necesaria la creación y utilización de métodos adicionales de protección dirigidos a los menores.

En menores de edad, uno de los servicios más utilizados por los hackers suplantar la identidad de los mismos son las redes sociales. Suelen emplear una serie de excusas para engañar al usuario

tales como enviar un mensaje privado en el que le recomiendan cambiar la contraseña. En otras ocasiones crean sitios web falsos para que cuando se introduzca el correo electrónico y la contraseña se grabe y conserve esta información.

Ejemplo de Phishing en Facebook.



Finalmente, encontramos casos de phishing a menores a través de juegos online. El objetivo sigue siendo apropiarse de cuentas, datos privados, bancarios y suplantar la identidad de los usuarios. Normalmente, la excusa que suelen emplear para engañar a los menores se encuentra relacionada con fallos de seguridad en la plataforma del juego o en la cuenta de los usuarios.

Pharming. Es una modalidad más peligrosa de phishing, por medio de la cual el ciberdelincuente infecta el ordenador del usuario de forma que se acaba redireccionando el tráfico web de una página legítima, utilizada habitualmente por el usuario, hacia otra página falsa creada por el ciberatacante.

La diferencia principal con phishing es que en el caso de pharming la redirección a la página falsa es automática, sin que sea necesario que el usuario necesite pulsar ningún enlace. Así, los estafadores pueden entrar en nuestro ordenador para modificar nuestros ficheros a través de virus de forma que, cuando escribamos en nuestro navegador una dirección determinada, entremos directamente en otra sin saberlo.



Resultado de imagen de pharming informatico

Fuente. https://es.slideshare.net/joycesalas/delitos-informaticos-15846183

SMiShing. Es una estafa en la que por medio de mensajes SMS, se solicitan datos o se pide que se llame a un número de teléfono o que se entre a una web. El objetivo del fraude puede ser suscribir al usuario a un servicio SMS Premium, ofreciéndole por ejemplo una oferta o premio especial, que llame a un número con coste adicional o estafarle con algún producto o servicio inexistente.

En este caso, al jugar en muchas ocasiones con premios y grandes oportunidades, los menores pueden caer fácilmente en la trampa accediendo a las solicitudes de los estafadores sin dudar de la autenticidad de dichos mensajes.



Resultado de imagen de smishing ejemplos

Hacking o intrusismo informático, consistente en el acceso no autorizado, por lo general violando los mecanismos de seguridad allí donde los haya, a los archivos y bases de datos contenidos en los sistemas informáticos ajenos, normalmente de grandes empresas o instituciones. “Las conductas de mero hacking acceso a los a los sistemas informáticos perpetrados con la única finalidad de acceder al password o puerta lógica no son actualmente constitutivos de delito pues carecen del elemento subjetivo del injusto”. (Manuel Marchena).

Cracking, también conocido como sabotaje informático. No debemos confundirlo con el password cracking o rompimiento o desciframiento de claves (passwords) que se asimila al hacking. En el primer sentido, Manuel Marchena en “El sabotaje informático: entre los delitos de daños y los desórdenes públicos” los define como conducta consistente en la destrucción o en la producción generalizada de daños en su sistema, datos, programas informáticos o telemáticos.

Indicios de suplantación de identidad

Los menores deben conocer la existencia de ciertos indicios para detectar la posibilidad de que hayan sufrido suplantación de identidad. Algunos de los más importantes son:

- Accesos o usos anómalos de las cuentas. En este caso, por ejemplo, el indicio de suplantación lo tendríamos si nuestros contactos reciben mensajes de nuestra cuenta sin que nosotros los hubiéramos enviado.
- Inminente desactivación de algún servicio que tuviéramos activado sin que hayamos procedido a ello.
- Cambios en el estado de los juegos online sin que los haya realizado por sí mismo.

Las redes sociales suelen tener mecanismos de denuncia a través de los cuales ellos mismo eliminan perfiles que se consideran falsos. Si ninguna de estas dos acciones tienen el final esperado, se debe acudir a las Fuerzas y Cuerpos de Seguridad del Estado o autonómicas para interponer una denuncia.

La suplantación de personalidad es un delito, pero hay que saber cuándo se ha cometido realmente para tipificarlo como tal, pues en ocasiones produce confusión. Según el artículo 401 del Código Penal, sólo se considera delito si lo que se usurpa es el estado civil de otro (es decir, hacerse pasar por otro), y puede conllevar una pena de prisión entre seis meses y tres años.

Ateniéndonos al Código Penal si se crea un perfil falso, entonces no se puede considerar un delito de suplantación de personalidad, porque participar en una red social con datos falsos no implica un

delito de usurpación de estado civil.

Otra cosa es que un individuo entre en una cuenta o perfil de otra persona, ya que se estaría cometiendo un delito contra el derecho a la privacidad debido a que se considera como una forma de revelación de secretos (caso que se recoge a partir del artículo 197 de Código Penal y se contempla como hacking). Y al mismo tiempo. Si para el acceso a la cuenta privada de un ajeno se ha tenido que cometer algún otro delito como el conseguir claves y contraseñas o provocar algún daño en el sistema informático del propietario, el delito se recoge en el artículo 264 del Código Penal y se considera cracking.

Copyright 2026

2. Suplantación de identidad

2.2 Datos y ejemplos

ALGUNOS DATOS Y EJEMPLOS DE SUPLANTACIÓN DE IDENTIDAD

Según datos obtenidos por el estudio “Risk and safety on the internet: the perspective of european children”, el 12% de los menores europeos entre 9 y 16 años han sido víctimas de estos riesgos a través de Internet.

Los resultados de estos estudios resaltan la importancia y la necesidad del diseño de programas de prevención y de campañas de concienciación y sensibilización para garantizar una navegación segura por la Red y evitar en la medida de lo posible la exposición ante estas amenazas de los menores.

Veamos algunos ejemplos de casos reales de suplantación de identidad publicados en los medios de comunicación.

Ejemplo 1. Detenida una joven de 17 años por usurpar el perfil de otra persona en una red social.

Una joven de 17 años ha sido arrestada en Tudela (Navarra), junto con un menor de edad que ha sido puesto a disposición del correspondiente tribunal, acusada de usurpar el perfil de una persona en una red social, publicar fotos íntimas suyas y extorsionarle.

Ambos fueron interceptados por la Policía Foral cuando recogían el dinero exigido a la víctima para devolver las claves de acceso y acusados de los delitos de usurpación de estado civil, contra la intimidad, extorsión y amenazas, según ha informado este jueves el Gobierno de Navarra en un comunicado. La víctima descubrió los hechos cuando, al intentar acceder a una red social de Internet, vio que no podía hacerlo utilizando sus claves habituales, y al entrar desde otra cuenta constató que alguien había usurpado su perfil, colgando además fotos íntimas suyas acompañadas de comentarios desagradables, por lo que presentó una denuncia.

http://cadenaser.com/ser/2010/11/18/ciencia/1290050665_850215.html

Ejemplo 2. Dos jóvenes detenidos por robar fotos de una menor y crearle un perfil falso en Internet.

La Guardia Civil ha detenido en Motril a dos jóvenes de 18 y 17 años de edad, como presuntos autores de los delitos de usurpación de identidad y de descubrimiento y revelación de secretos a través de Internet, por usurpar la identidad de una menor a la que crearon un perfil falso en internet a través del que engañaban a terceras personas. El mayor ha pasado a disposición del Juzgado de Guardia y el menor a Fiscalía de Menores.

En concreto, los dos jóvenes detenidos se apoderaron de las fotografías de una menor granadina y con ellas crearon un perfil falso en la red social “Tuenti”. Este perfil lo utilizaban para engañar a compañeros de clase. La madre de la menor, residente en la localidad granadina de Maracena, denuncio que su hija había descubierto un perfil en la red social “Tuenti” con su fotografía.

http://www.elmundo.es/elmundo/2012/11/23/andalucia/1353676945.html

Ejemplo 3. Imputado un menor por usurpación de identidad en una red social.

Aunque actualmente el aún presunto autor de este delito ya se encuentra dentro de la mayoría de edad, contaba con 16 años en el momento en que decidió abrir un nuevo perfil en una conocida red social. Hasta aquí, nada que nos deba extrañar sin embargo este chico utilizó para crear dicho perfil tanto la fotografía como los datos personales de una tercera persona que, una vez se percató de los hechos, lo denunció a la Guardia Civil.

http://www.delitosinformaticos.com/05/2015/delitos/usurpacion-de-identidad/imputado-menor-usurpacion-identidad-una-red-social

Ejemplo 4. Desarticulada una banda que estafaba en internet con suplantación de identidad.

Agentes de la Guardia Civil han desarticulado en Zaragoza una banda criminal formada por siete adultos y un menor que robaban documentos para suplantar la identidad sus víctimas y crear cuentas bancarias a su nombre con las que extraer dinero y adquirir productos de lujo a través de internet.

http://cadenaser.com/emisora/2017/01/31/radio_zaragoza/1485861767_855722.html

2. Suplantación de identidad

2.3 Pautas y recomendaciones

PAUTAS Y RECOMENDACIONES PARA FAMILIAS Y EDUCADORES (OSI)

A continuación presentamos una serie de medidas que podemos realizar en caso de detectar una suplantación de identidad en nuestros menores.

- En caso de detectar que alguien se hace pasar por un menor, creando una cuenta similar a la suya, tenemos derecho a denunciarlo ante la misma web del servicio, notificando esta situación a la red social o sistema implicado para solicitarles que tomen las medidas necesarias para restaurar el nivel de seguridad anterior a la suplantación de identidad.
- Es importante saber que si nos encontramos ante un caso de usurpación de identidad, si el incidente no se considera muy grave se recomienda proceder a su denuncia en el correspondiente servicio contactando con los responsables y/o administradores de las redes sociales o sitios web. La mayoría de ellos ponen a nuestra disposición mecanismos de denuncia de este tipo de situaciones. El segundo paso, si tras denunciar los hechos al servicio la problemática no se soluciona, sería interponer una denuncia ante las propias las autoridades, como son las Fuerzas y Cuerpos de Seguridad del Estado.
- En caso de denuncia, es necesario recopilar todas las pruebas y evidencias relacionadas con la suplantación de identidad producida en el menor, como capturas de pantalla, copias de correos, copias de ficheros, etc.
- Denunciar el caso a la agencia de protección de datos.
- Como medida de seguridad, sería conveniente cambiar todas las contraseñas que piense le hayan podido interceptar.

En caso de requerir denunciar un caso de suplantación de identidad en menores ante los cuerpos de seguridad del estado, debemos conocer los siguientes grupos especializados:

- **Policía Nacional (Brigada de Investigación Tecnológica)** http://www.policia.es/bit. delitos.tecnologicos@policia.es

- **Guardia Civil (Grupo de Delitos Telemáticos)**
  https://www.gdt.guardiacivil.es/webgdt/home_alerta.php. Teléfono: 900.101.062

Desde el ámbito familiar tenemos que concienciar a los menores sobre la importancia de limitar la difusión voluntaria de datos personales y privados en redes sociales configurando de forma correcta las opciones de privacidad de las diferentes redes sociales que utilicen, pero también manteniendo los equipos seguros con las actualizaciones de software oportunas. Además la familia debe fomentar entre sus hijos la discreción a la hora de publicar fotografías o comentarios en la red.

De acuerdo con la **Oficina de Seguridad del Internauta (OSI)** para usar el ordenador de una manera organizada y segura se recomienda crear una cuenta por cada usuario que vaya a utilizar el ordenador. De esta forma, cada usuario podrá tener su propio escritorio, con una configuración y preferencias personalizadas. Se recomienda además:

- Bloquear las ventanas emergentes.
- Hacer uso de filtros antispam ya que filtran el correo electrónico que consideran basura a una carpeta donde lo almacenan.
- Es importante no utilizar la misma contraseña para varios servicios, deben ser secretas, robustas y modificadas periódicamente.
- Debemos tener precaución frente a enlaces sospechosos, las descargas que realizamos, desconfiar de correos de desconocidos, sobre todo con ficheros sospechosos.
- Tener precauciones al utilizar ordenadores públicos y conectarse a redes WiFi públicas, como tener instalado y habilitado un cortafuego, así como personalizar la configuración de red de nuestro equipo.
- Establecer una contraseña para el bloqueo de la pantalla del teléfono además de los propios números de seguridad PIN y PUK para el acceso a la tarjeta SIM del mismo como medida de prevención ante un posible robo o pérdida de dispositivos móviles.

> El país: Han suplantado mi identidad en Internet o en redes sociales ¿qué hago?
>
> http://economia.elpais.com/economia/2016/04/29/actualidad/1461949659_081309.html

3 Prevención de virus y fraudes

Copyright 2026

3 Prevención de virus y fraudes

3.1 Definición y conceptos

DEFINICIÓN Y CONCEPTOS

El término “virus” se utiliza comúnmente para referirse a las aplicaciones informáticas que buscan alterar el funcionamiento de los dispositivos (PC, tabletas, smartphones, etc.) y en muchos casos, robar información del usuario. Existen numerosos tipos de programas maliciosos que se han vuelto más sofisticados y más peligrosos, y más difíciles de detectar.

Al principio los virus solían centrar su actividad en causar molestias al usuario, borrando información, impidiendo el uso de determinados programas o ralentizar el arranque del ordenador.

Por desgracia, **la mayoría de los virus actuales tienen como objetivo el obtener información de los usuarios infectados**, tales como datos bancarios fotos, contraseñas o uso de la webcam.

Hoy en día existen muchos **programas maliciosos** que permiten tomar el control absoluto del ordenador y realizar cualquier tipo de acción sin nuestro conocimiento, como por ejemplo:

- Suplantar nuestra identidad y enviar correos electrónicos en nuestro nombre.
- Utilizar nuestro ordenador para realizar ataques a otros ordenadores.
- Realizar estafas en las que figurará nuestro ordenador (y nuestra IP) como origen del delito.
- Enviar publicidad.
- Secuestrar y cifrar nuestros archivos, y exigir un pago para recuperarlos.

Los ciberdelincuentes utilizan diversas **técnicas para infectar los sistemas con virus**, como por ejemplo:

- La infección puede llevarse a cabo al instalar un archivo o un programa supuestamente legítimo pero que contiene código malicioso porque haya sido pirateado.
- La infección puede producirse simplemente conectándote a una web infectada, aprovechando una vulnerabilidad (fallo de seguridad) en el sistema operativo, en el navegador, en plugins y aplicaciones que los usuarios utilizan habitualmente
- Otra forma de infección se produce cuando se pulsa sobre un enlace malicioso recibido a través de alguna aplicación de mensajería (por ejemplo, WhatsApp, Twitter, o Facebook).

Copyright 2026

En el momento de pulsar el enlace se redirige al usuario a una web en la que se produce la infección. El gancho para pulsar sobre el enlace suele consistir en una invitación para ver una noticia llamativa.
- Los dispositivos externos como pen drives también pueden incluir virus que infecten los ordenadores.
- Algunas estrategias de engaño pueden infectar tu equipo, por ejemplo cuando recibes un mensaje indicándote que proporciones tus datos de clave de usuario y contraseña para activar tu cuenta, alegando un falso mantenimiento del servicio.

En la actualidad **existen virus para todas las plataformas y dispositivos**, por lo que cualquier ordenador conectado a Internet es susceptible de ser infectado por un virus, independientemente de la plataforma (Windows, Apple, Linux) o el dispositivo (ordenador, tabletas, teléfono móvil).

A estos riesgos, hay que añadir que los menores poseen ciertas características tales como inocencia, curiosidad, inexperiencia o impaciencia, que los pueden hacer especialmente débiles al potenciar los riesgos de infección y fraude.

Tipos de fraude online

Los fraudes electrónicos pueden ser muy variados. En algunos casos, se estudian los hábitos de la víctima (especialmente a través de la redes sociales), y se busca ganar su confianza para eliminar protecciones (por ejemplo, se suele aconsejar desactivar el antivirus para que el ordenador vaya más rápido).

En otros casos, se recurre a incluir condiciones en unos términos ambiguos antes de instalar un juego o programa, confiando en que el usuario aceptará las condiciones de instalación sin leerlas, especialmente, si se trata de un menor.

Algunos **tipos de fraude online** que te puedes encontrar en tu actividad diaria en la red son:

- **Rogue software o fakeav**: Se le denomina Rogue Software (o también Rogue Rogueware, FakeAVs, Badware, Scareware) a los “Falsos programas de seguridad” que no son realmente lo que dicen ser, sino que todo lo contrario. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado. Estos falsos Antivirus y Antispyware están diseñados para mostrar un resultado predeterminado (siempre de infección) y no hacen ningún tipo de escaneo real en el sistema al igual que no eliminaran ninguna infección que podamos tener. La estafa consiste en invitarnos a descargar la versión completa del programa de protección solicitando para ello el pago, por medios “poco seguros”, de cierta cantidad de dinero
- **Phishing**: Es una actividad delictiva encaminada al robo de contraseñas personales y credenciales bancarias, es decir a la “pesca de contraseñas” que ya explicamos en el tema anterior.

- **Suscripción a servicios Premium o de pago**: Existen aplicaciones fraudulentas para dispositivos móviles que envían mensajes SMS Premium desde nuestro teléfono sin que seamos conscientes de ello hasta que recibimos la factura. A veces la información suele hallarse camuflada en el listado de condiciones que debemos aceptar antes de instalar una aplicación. Cuando pulsamos el botón y aceptamos la instalación, estamos dando nuestro consentimiento para que la aplicación envíe mensajes SMS Premium en nuestro nombre, cuyo coste será cargado en nuestra factura. Este tipo de fraudes se produce muy a menudo en la descarga de juegos, aprovechando la ingenuidad de nuestros menores.
- **Fraudes vinculados al mundo del videojuego.** Otro de los aspectos que aprovechan los ciberdelincuentes es el hecho de que muchos menores utilizan la misma clave de acceso y contraseña para distintos servicios lo que aumenta aún más el riesgo de robo de información personal cuando se es víctima de una estafa. Entre los más importantes tenemos la suscripción oculta y con coste y el robo de tatos. En el primer caso se produce al hacer clic en la publicidad de aplicaciones para móviles. En el segundo caso se produce en algunos juegos muy populares que te ofrecen algunos trucos o vidas infinitas ofreciendo a cambio sus datos de acceso a sus redes sociales.

Copyright 2026

3 Prevención de virus y fraudes

3.2 Datos y ejemplos

ALGUNOS DATOS Y EJEMPLOS QUE EVIDENCIAN FRAUDES Y VIRUS

La última encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España revela algunos datos en relación a este tema que hemos de tener en cuenta:

- **Uso de antivirus** El 82% de los equipos informáticos están protegidos con software antivirus.
- ***Configuración de perfil en redes sociales.*** El 53,1% de los usuarios de redes sociales tienen costumbre de configurar sus cuentas para que sólo sus contactos puedan acceder a sus perfiles.
- ***Uso de contraseñas.*** El 58,2% de los usuarios hace uso de las contraseñas para proteger sus equipos.
- ***Existencia de virus.*** El 22 % manifiesta haber sido infectado por un virus.
- ***Spam.*** El spam sigue siendo la incidencia más común que sufren los internautas (85%)
- ***Malware.*** Se ha detectado que alrededor de un 60% de los ordenadores están infectados de malware.
- ***Información a desconocidos***. Un 14,3% de las principales incidencias relacionadas con los menores se basan en haber facilitado información personal a desconocidos.
- ***Fraude electrónico***. El 48% de los usuarios ha sufrido alguna vez un intento de fraude electrónico.
- ***Datos personales.*** Existe un alto porcentaje de usuarios (44%) que tiene poca o ninguna confianza a la hora de facilitar sus datos personales mediante un e-mail o un servicio de mensajería instantánea.

A continuación vamos a ver algunos **ejemplos reales de infecciones de virus y fraudes o estafas**:

- La linterna molona

Se trataba de una aplicación que oficialmente ofrecía a los clientes de Android una linterna led para el teléfono, pero que una vez descargada permitía al desarrollador meterse en el terminal ajeno y enviar mensajes a números de tarificación elevada. En concreto, al aceptar las condiciones

Copyright 2026

de uso –que se presentaban en una ilegible letra gris sobre fondo negro–, el usuario autorizaba al fabricante a entrar en el dispositivo y enviar y borrar mensajes, tanto los que llegan como los que se mandan.

El programa publicaba automáticamente un post en la cuenta de Facebook de los usuarios que se lo descargaban. El post contaba las supuestas bondades de la app, un texto que todos los amigos del escritor inconsciente leían con gran entusiasmo creyendo que el autor había sido quien suscribía las líneas.

La aplicación fraudulenta se anunciaba como un programa que "hace brillar el led más que ninguna otra app de linternas y es totalmente gratuita", promesa que atrajo a miles de personas y que, por otro lado, en ningún caso se cumplía.

http://www.elconfidencial.com/espana/2015-03-05/medio-millon-de-estafados-por-una-app-linterna-que-se-suscribia-a-mensajes-premium-sin-autorizacion-del-usuario_722330/

- Vidas infinitas. Panda security descubre un estafa para el juego ‘Top Eleven Be a Football Manager’

PandaLabs han descubierto un malware en Windows que actúa disfrazado de aplicación. En teoría, si la descargamos podremos ganar tokens para el Football Manager con los que comprar jugadores.

Evidentemente, esto no sucede y, si lo que hacemos es seguir las instrucciones que nos dan, no solo no vamos a conseguir tokens gratis para Top Eleven sino que podremos perder el acceso a nuestra cuenta de correo electrónico o de Facebook.

La estafa para conseguir tokens gratis para el Top Eleven se hacía de la siguiente manera: 1º Te descargas esta app desde diferentes foros sobre juegos. 2º Para conseguir el número de tokens que selecciones tienes que insertar tu cuenta de correo electrónico o de Facebook, así como las contraseñas con las que accedes. Finalmente esos datos son enviados a los ciberdelincuentes que los utilizan para hacerse con el control de tu cuenta, impidiéndote el acceso a la misma.

http://www.pandasecurity.com/spain/mediacenter/noticias/estafa-para-top-eleven-football-manager/

- Estafas de falsos “amigos” en Facebook

Usted recibe una solicitud de amigo, pero no tiene tiempo de revisar esta nueva persona y pulsa ” aceptar ” de todos modos. O puede ser que la configuración de privacidad de su página está tan abierta y cualquiera puede verla. De cualquier manera, el estafador utiliza el acceso a su cuenta

para ver las imágenes y otros datos de su perfil. Luego crea una nueva cuenta bajo su mismo nombre y la llena de sus fotos, intereses y actualizaciones de estado. Con 500 millones de personas en Facebook en todo el mundo, es poco probable de detectar al impostor.

Después de crear una cuenta duplicada, el estafador envía solicitudes de amistad a sus amigos de Facebook. La gente reconoce su nombre y pulsa ” aceptar “, sin darse cuenta de que la cuenta es una falsificación. No se dan cuenta que algo anda mal hasta que su impostura comienza el envío de solicitudes de dinero y enlaces que son spam.

Los mensajes y los enlaces pueden ser estafas obvias cuando provenga de una dirección de correo electrónico desconocido, pero son mucho más creíbles cuando se comparte por un “amigo” de Facebook. ¡Siempre tenga cuidado con lo que haga clic, sin importar quién la comparte!

http://www.lafamiliadebroward.com/cuidado-con-las-estafas-de-falsos-amigos-en-facebook/

- El virus de la Policía ataca de nuevo al sistema Android

El virus de la policía es uno de los ransomwares más extendidos en los últimos años. Este virus, que está activo desde 2011, “secuestra” todos los archivos del ordenador, argumentando que el usuario ha estado navegando por páginas web pornográficas con contenido infantil, y pide “como multa” 100 € para liberar la información.

Hace varios días apareció una nueva familia de malware para Android, Android/Koler.A. Los medios se hicieron eco del mismo ya que era un ataque del tipo del “Virus de la Policía” / ransomware, parecido a los que hemos visto en ordenadores Windows, aunque en esta ocasión estaba dirigido a teléfonos móviles.

En este caso, el malware no es capaz de cifrar los datos del teléfono, pero aún así es bastante molesto y difícil de eliminar (si no cuentas con antivirus para Android) ya que el mensaje que muestra en pantalla está encima de todo lo demás y el usuario sólo dispone de unos pocos segundos para intentar desinstalarlo.

http://www.pandasecurity.com/spain/mediacenter/noticias/virus-policia-android/

3 Prevención de virus y fraudes

3.3 Pautas y recomendaciones

PAUTAS Y RECOMENDACIONES PARA FAMILIAS Y EDUCADORES

Virus en Android: ¿cómo detectar si mi dispositivo está infectado?

Como bien sabemos, en Internet circulan infinidad de virus y malware que pueden poner nuestros equipos informáticos en riesgo, y precisamente en el caso de Android, en los últimos años han comenzado a proliferar notablemente este tipo de amenazas.

- Se abren anuncios y publicidad extraña
- El dispositivo funciona más lento de lo normal, deja de responder o se bloquea con frecuencia.
- Comportamiento extraño del dispositivo (se apaga solo aun teniendo batería).
- Las aplicaciones no funcionan correctamente.
- El antivirus se desactiva solo.
- Los programas se inician de forma espontánea.
- Creación de accesos directos a páginas no deseadas, es decir a servidores DNS falso.
- Aumento en el uso de datos

¿Qué podemos hacer si nuestro dispositivo está infectado?

Ante la sospecha de que nuestro ordenador o teléfono ha sido infectado por un virus, debemos reaccionar rápidamente y llevar a cabo las siguientes medidas siguiendo el consejo de especialistas como la que se encuentra en la revista Computer:

1º Controla los permisos de las aplicaciones

| Permisos | Concede | Niega | | --- | --- | --- | | Acceso a los ajustes | Sólo las apps de Google deberían pedirte este permiso, para asegurarse de que el dispositivo puede ejecutar todos los

procesos que cada aplicación requiere. | Sólo las aplicaciones primarias de Google necesitan utilizar este permiso, así que si cualquier aplicación que requiera este permiso, desinstálala enseguida. | | Modificación | La mayoría de las apps basadas en medios sociales usa esta función para guardar archivos en la tarjeta SD. Y sobre todo es muy común en las apps que usan vídeo. | Cualquier app con acceso a los contenidos de la tarjeta SD puede instalar un virus en ella. También pueden robar archivos o borrarlos de la tarjeta. | | Uso de la ubicación | Sólo suele ser importante para las apps de navegación tipo Google Maps. Otras aplicaciones quieren acceder a estos permisos para mostrar sitios de interés cercanos. | Las apps maliciosas pueden reunir información sobre tu ubicación y los lugares a los que vas, para enviarte anuncios basados en tu localización. | | ID del dispositivo e información de las llamadas | El principal uso de este permiso es leer el ID del teléfono y su estado, esto está bien cuando se accede a diferentes redes sociales o cuentas de correo electrónico. | Este permiso da acceso a tu número de teléfono, que podría ser utilizado por una aplicación maliciosa para enviarte spam constantemente. | | Hacer llamadas | Se trata de un permiso muy común para aplicaciones que permitan realizar llamadas de voz dentro de ellas, y que son independientes de la app Teléfono del dispositivo. | Hay aplicaciones que usan este permiso para marcar números de tarificación especial. Estas pueden ser de hasta 2 €/minuto. Así que cuidado. |

2. Tipo de infección. La mayoría de las infecciones en smartphones vendrán en forma de pop-ups, o un simple malware. Aunque no son muy perjudiciales para tu dispositivo, pueden ralentizar el rendimiento del teléfono o la tableta. Acude al cajón de aplicaciones para intentar encontrar cuál es la aplicación problemática.

3. Análisis antivirus. Incluso cuando creas que ya has identificado la aplicación problemática, haz un análisis antivirus completo del dispositivo. Descarga la aplicación Avast y selecciona la opción “Ejecutar análisis” disponible en la pantalla principal de la aplicación. Puedes escanear el dispositivo con un antivirus online. Aquí se muestran algunos:

- http://www.pandasecurity.com/spain/
- http://www.bitdefender.es/scanner/online/free.html
- http://www.zonavirus.com/antivirus-on-line/
- **Escanear el dispositivo con herramientas Anti Malware y AntiSpyWare**.
- **Desinstala aplicaciones problemáticas**.

Existen métodos avanzados de desinfección de virus que pueden realizarse sin llevar el dispositivo a un servicio técnico, pero requieren conocimientos avanzados de Informática, y pueden suponer un riesgo de pérdida de información si no se tiene claro lo que se está haciendo.

En la Oficina de Seguridad del Internauta se ofrecen instrucciones detalladas para llevar a cabo la desinfección, siempre bajo la responsabilidad del usuario.

Copyright 2026

http://www.osi.es/es/desinfecta-tu-ordenador

Copyright 2026

3 Prevención de virus y fraudes

3.4 Estrategias de prevención

ESTRATEGIAS DE PREVENCIÓN EN EL HOGAR Y LOS CENTROS

Lo primero que debemos hacer las familias y tutores es informar a nuestros menores sobre cómo evitar este tipo infecciones de virus y fraudes. La buena comunicación es una de las claves fundamentales para la seguridad online..

Todas las precauciones son pocas para evitar infecciones de virus y para no ser víctima de un fraude electrónico.

A continuación se describen algunas recomendaciones técnicas a modo de prevención:

- ***Mantener actualizado todo el software instalado***, el sistema operativo, el navegador de Internet y antivirus: es fundamental contar con un antivirus actualizado en todos los dispositivos (ordenadores, tabletas y teléfonos móviles).
- ***Utilizar cuentas de usuario limitadas***: es aconsejable utilizar un usuario con permisos restringidos que no pueda instalar programas. De ese modo, si se cuela un virus, será más difícil que pueda instalarse.
- ***Realizar copias de seguridad***: las copias de seguridad permiten recuperar la información en caso de que un virus infecte un dispositivo, y deben realizarse en dispositivos externos (unidades de almacenamiento, discos duros, etc.).
- ***Realizar copias de seguridad en la nube*** (Cloud Computing): hacer copias de seguridad en la nube es una buena práctica que permite recuperar datos en caso de pérdida, pero no se deben hacer copias en la nube de información privada o confidencial, pues existe el riesgo de que esta información sea comprometida, ya que la información no suele estar cifrada (por ejemplo, Dropbox) y cualquier ciberdelincuente con acceso remoto al dispositivo puede acceder a la copia de seguridad.
- ***Gestión de contraseñas***: las contraseñas deben ser secretas, robustas y no repetidas. En este sentido, la Oficina de Seguridad del internauta ofrece varias técnicas para crear

contraseñas robustas y seguras en el siguiente enlace: http://www.osi.es/es/contrasenas

- ***Verificar los enlaces cortos antes de acceder a ellos***: los enlaces cortos, empleados especialmente en pantallas móviles para ahorrar en caracteres, se configuran como un caldo de cultivo perfecto para ataques de phishing, ya que el usuario no sabe hacia dónde apunta el enlace. A modo de ejemplo, recomendamos el siguiente servicio para verificar enlaces desconocidos : www.unshort.me
- ***Evitar la navegación por páginas webs sospechosas*** (programas gratis, juegos gratis, fotos de famosas, etc.).
- ***Configurar adecuadamente la privacidad en las redes sociales***.
- ***Utilizar herramientas de Control Parental***. Pueden suponer una gran ayuda para los padres a la hora de evitar que los menores puedan verse involucrados en fraudes electrónicos e infecciones de virus.

Consejos sobre la instalación de aplicaciones en dispositivos móviles

- Descargar aplicaciones sólo desde fuentes confiables: Play Store para Android. Apple Store para IOS. Marketplace para Windows Phone.
- Sospechar ante un número bajo de descargas.
- Desconfiar si los comentarios son excesivamente halagadores, pues pueden estar escritos por el propio desarrollador o personas de su entorno.
- Comprobar los permisos de acceso al teléfono que se solicitan antes de iniciar la instalación. Por ejemplo, una aplicación de linterna no tiene sentido que requiera permisos para acceder al registro de llamadas.
- Desactivar en los dispositivos móviles la opción Permitir Orígenes Desconocidos ubicada en Ajustes > Seguridad > Orígenes desconocidos.
- Instalar un antivirus para dispositivos móviles.
- No utilizar navegadores extraños, ya que pueden contener vulnerabilidades que permitan “a los malos” robar las contraseñas.

Copyright 2026

4. Acceso a contenidos inapropiados

Copyright 2026

4. Acceso a contenidos inapropiados

4.1 Definición y conceptos

DEFINICIÓN Y CONCEPTOS

En esta unidad vamos a describir algunos de los riesgos relacionados con el acceso a contenidos inapropiados en internet. No por ello vamos a prohibir el acceso de menores a la Red, sino que vamos a intentar proporcionarles las herramientas necesarias para estar protegidos ante determinados contenidos nocivos o ilícitos a los que pueden acceder de forma voluntaria o involuntaria.

A lo largo de esta unidad te daremos criterios y pautas de navegación segura, para que familias y educadores puedan ofrecer recomendaciones para su prevención o cómo actuar en caso de haber accedidos a dichos contenidos.

¿Qué consideramos contenidos inapropiados?

Por **contenido inapropiado** entendemos todo material en forma de imágenes o textos que provocan un perjuicio en el menor, estos son, aquellos peligros que circulan por la Red, y las características de la información que contienen.

A través de Internet los menores pueden acceder a páginas inapropiadas para su edad, hacer “amistades” poco recomendables. Además, Internet se ha convertido en uno de los canales preferidos de la publicidad y los menores son un público especialmente vulnerable, lo que les convierte en víctimas potenciales de engaños y estafas.

Para comprender mejor el concepto debemos diferenciar entre contenidos ilícitos y contenidos nocivos.

Los **contenidos ilícitos** son aquellos que no están legalmente permitidos y son considerados como actividades delictivas. Son contenidos relativos a pornografía con menores y contenidos pedófilos, racistas o xenófobos, la apología de terrorismo, fabricación de artefactos explosivos, drogas, armas, asociaciones ilícitas, etc.

Los **contenidos nocivos**, aunque sí están permitidos por Ley, se consideran dañinos en el desarrollo personal y social de los menores. Además de todos los anteriores incluiríamos juegos online de adultos.

Copyright 2026

Muchas páginas web se sirven de anuncios online o banners que, con el pretexto de publicitar cualquier cosa, pretenden introducir al niño en alguna sala de chat o foro, cuando lo que en realidad están haciendo es conducirlos a alguna página pornográfica que además contiene virus y programas espías que recopila información facilitada por el menor.

Cada vez se ponen más de moda páginas web, blogs, o redes sociales en las que se potencian actividades que pueden poner en peligro la vida de los menores con páginas de anorexia y bulimia (llamadas páginas de Ana y Mia), o las llamadas páginas de muerte, que incitan al suicidio a niños y adolescentes. (conocidas como páginas de Self Injury).

Vamos a revisar algunos de los ejemplos más comunes de contenidos inapropiados. De acuerdo a la Información recabada de Red.es “Monográfico Acceso a contenidos inapropiados. Secundaria (13-17 años)”. En Chaval.es [documento en línea: http://www.chaval.es/chavales/] Los principales tipos de contenidos inapropiados son los siguientes:

- **La pornografía**, información e imágenes sexuales explícitas con el fin de provocar la excitación del receptor. Estos materiales no son adecuados para menores de edad ya que ofrecen una visión distorsionada de las relaciones sexuales, categorizando a hombres y mujeres como meros objetos de deseo.
- **La violencia**, empleo intencional de la fuerza o poder físico, de hecho o como amenaza, contra uno mismo u otro/s que pueda causar daños físicos o psicológicos, trastornos del desarrollo o privaciones (física, psicológica, sexual, patrimonial).
- **Los contenidos falsos**, informaciones erróneas o visiblemente falsas que circulan por Internet y llegan fácilmente a un gran número de receptores debido a la naturaleza del contenido y la tendencia a propagarse rápidamente (leyendas urbanas, mensajes en cadena, videos virales).
- **El fomento del consumo de drogas**, sustancias introducida en el organismo que produce una alteración del natural funcionamiento del sistema nervioso central, siendo susceptible de crear dependencia física y/o psicológica, y provocar daños y enfermedades físicas graves.
- **El fomento de acciones que dañan la salud física y psicológica**, consecuencia de los ideales de belleza y el aspecto corporal dominante, cánones cultural, social y mediáticamente establecidos (Trastornos de la Conducta Alimentaria, cirugía estética, blanqueamiento dental etc.).
- **Los juegos de azar y apuestas,** donde la búsqueda de beneficio económico trae consigo el riesgo de ser engañado, o perder cantidades considerables de dinero.
- **La afición a los videojuegos y juegos online**, que puede convertirse en un riesgo grave cuando se convierten en adicción (aislamiento familiar y social, trastornos actitudinales, de personalidad y de conducta).
- La **publicidad online**, medio carente de filtros para que las empresas se publiciten, llegando fácilmente a un gran número de personas en todo el mundo.

- La **ingeniería social**, práctica informática delictiva para conseguir información sensible, personal y confidencial, manipulando y engañando a los usuarios legítimos.

Hábitos y actitudes que pueden propiciar el acceso a contenidos inapropiados

De acuerdo a la Información recabada de Red.es. “Monográfico Acceso a contenidos inapropiados. Secundaria (13-17 años)”. En Chaval.es [documento en línea: http://www.chaval.es/chavales/]

Algunas características en los hábitos de uso de Internet que pueden propiciar el acceso a contenidos inapropiados son:

- **Pérdida de control**. Hace alusión al tiempo invertido y a la pérdida de los objetivos de conexión inicial.
- **Evasión.** El uso TIC puede proporcionar sensación de evasión de la realidad y bienestar, de modo que la funcionalidad práctica y objetiva de las herramientas pasa a un segundo plano, con el fin de buscar un mayor grado de estimulación y satisfacción, con el consiguiente riesgo de acceder a temáticas no recomendadas para su edad (sexo, violencia, juego, o drogas).
- **Ocultación.** Ocultación por parte del menor tanto del tiempo empleado en Internet y demás tecnologías, como de los objetivos de conexión y las actividades realizadas durante las diferentes sesiones.
- **Abandono de actividades.** Para poder dedicar más tiempo al uso de las tecnologías, donde buscarán nuevos contextos de relación y/o actividades de ocio.
- **Chatear y quedar con desconocidos a través de Internet.** Es muy común sobre todo en las fases iniciales del proceso madurativo, donde pueden tener lugar los comportamientos más inconscientes y de mayor riesgo para la socialización del menor.

Algunas de las **principales motivaciones** que mueven a los menores a relacionarse con este tipo de material, pueden ser: individuales o sociales. Entre las primeras están las motivaciones basadas en las emociones, valores, creencias, sentimientos, actitudes y conductas de los menores de edad: Buscar formas de evasión e independencia. El acceso a Internet sin filtro y sin supervisión. Participar en páginas y redes sociales no recomendadas para menores de edad, representando identidades virtuales ficticias.

Entre las motivaciones sociales destacamos algunas de ellas: Integrarse, formar parte de un grupo con el que poder identificarse. Experimentar la sensación de anonimato, y la sensación de impunidad. Interés en experimentar con el sexo o con su sexualidad, presionados por una cultura sexualizada en exceso. Estar al tanto de aquello que es tendencia (trending topic), a fin de integrarse en los usos y costumbres sociales imperantes.

Entre las principales **consecuencias** del acceso a contenidos inapropiados con impacto emocional en el uso tecnológico destacamos:

- El descuido de la vida personal y actividades de ocio de los menores.
- El aislamiento social.
- El desarrollo o empeoramiento de la soledad o depresión.
- La adicción a contenidos violentos y perversos (permanentemente asociados a los videojuegos trasgresores y realistas indicados para adultos).
- La pérdida de la privacidad, y el fomento del consumo inadecuado (drogas, juegos de azar, apuestas).
- La población adolescente y su entorno pueden verse afectados a causa de la posibilidad que ofrecen las TIC de obtener gran cantidad de información sobre sus usuarios, muchas veces sin que sean conscientes de ello (campañas de publicidad implícita o persuasiva).
- Desarrollo de vidas paralelas, una online y otra offline, al construir distintas identidades.
- El éxito personal y social (sentido positivo de pertenencia a un grupo y una cultura), queda ligado a la imagen corporal de los individuos.
- Condicionamiento o distorsión de la visión de la realidad de los menores.

Copyright 2026

4. Acceso a contenidos inapropiados

4.2 Datos y ejemplos

ALGUNOS DATOS Y EJEMPLOS REALES DE SITUACIONES DE RIESGO

En la actualidad, los menores disponen de mucha más información y conocimiento sobre manejo de TIC, y aun así, un porcentaje elevado sigue accediendo a contenidos no apropiados para su edad.

Una reciente investigación en la que participaron una veintena de países europeos estudió la manera en que los más jóvenes utilizaban Internet, con el fin de identificar los factores de riesgo relativos a la seguridad en la Red. En ese estudio se puso de manifiesto la preocupación de los padres por el tipo de contenidos a los que tenían acceso sus hijos: imágenes explícitas de sexo o violencia (un 48%), o que pudiesen acceder a información dañina para su salud (25%).

La actividad de riesgo más común entre los menores es **relacionarse vía online con gente desconocida** siendo el segundo riesgo más común la exposición a peligros potenciales al acceder a contenidos inapropiados (violencia, sexo, conductas dañinas para la salud).



Fuente: Catalina García, MC López de Ayala López, A García Jiménez (2014): “Los riesgos de los adolescentes en Internet: los menores como actores y víctimas de los peligros de Internet”. Revista Latina de Comunicación Social, 69, pp. 462 a 485.

Veamos algunos ejemplos de casos reales.

1. Tampodka, eyeballing y oxy-shots: las prácticas con alcohol más arriesgadas.

http://www.abc.es/sociedad/20130617/abci-tampodka-eyeballing-alcohol-adolescentes-201306111114.html

Beber alcohol con celeridad para que suba cuanto antes y coger un colocón instantáneamente se ha convertido en la prioridad para algunos adolescentes cuando salen de fiesta. Las prácticas son cada vez más peligrosas y dañinas (…). Las modas y tendencias importadas de países extranjeros en las que los grados etílicos tienen su preponderancia parecen alcanzar un nuevo cenit en las últimas semanas con varias experiencias irreflexivas que ponen a prueba la propia vida de los adolescentes. (…) El «tampodka» resulta de la fusión de los términos «tampón» y «vodka» y no es otra cosa que la introducción vía vaginal de un tampón impregnado en alcohol de alta graduación, normalmente whisky o vodka. Desde esta zona, muy irrigada, el alcohol pasa directamente a la sangre y los síntomas de la borrachera se producen con mayor intensidad y celeridad. (…)En el caso del «eyeballing», aún va más allá, puesto que introducen el alcohol en la córnea como si fuese un colirio, cogen una botella y se lo echan directamente en el ojo, lo que ocasiona no solo conjuntivitis en el menor de los casos, sino lesiones de córnea, en la mucosa (…). El «oxy-shots», que consiste en inhalar chupitos de alcohol a través de un sistema de inhalación como los asmáticos, para absorber el alcohol más velozmente por vía aérea. Esta práctica de ingerir alcohol en dispositivos de nebulización junto con oxígeno al igual que en los tratamientos broncodilatadores, como las anteriores, «daña el sistema nervioso» y esquiva el filtro hepático de la sustancia tóxica, además de que «podría acarrear patologías pulmonares graves.

2. El reto de la canela: los peligros de un chiste de adolescentes.

http://www.bbc.co.uk/mundo/noticias/2013/05/130424_salud_cinnamon_challenge_canela_gtg

El "reto de la canela" (Cinnamonchallenge, en inglés), ha sido el tema de muchos videos que circulan en las redes sociales, en los que se ve a adolescentes intentando tragar una cucharada de canela en polvo en 60 segundos sin la ayuda de agua. Las imágenes muestran que, poco después, la gente expulsa parte del polvo por la nariz, en lo que se conoce como "aliento de dragón". Puede parecer apenas una broma tonta, pero expertos médicos aseguran que puede causar problemas de respiración, inflamación, sarpullido, irritación, ataques de asma y cicatrices en el pulmón que pueden durar años, si no para siempre. (…) Sólo en 2012, en Estados Unidos se registraron más de 220 llamadas al centro de envenenamiento de jóvenes afectados tras ingerir canela en polvo sin agua. A más de 30 se les recomendó atención médica inmediata.

3. El 21% de los adolescentes españoles están en riesgo de ser adictos a Internet

http://sociedad.elpais.com/sociedad/2013/01/15/actualidad/1358257857_400678.ht

El 21,3 % de los adolescentes españoles presentan indicios de desarrollar una conducta adictiva a Internet por el elevado tiempo que pasan conectados a la Red. Es decir, presentan indicios de aislamiento, irascibilidad y dejan de hacer cosas que antes hacían por estar en las redes sociales. Esta es la conclusión a la que ha llegado un estudio realizado sobre conductas adictivas en Internet, hecho en siete países europeos por la asociación Protégeles (…). El 58% de los jóvenes

europeos ha accedido a imágenes pornográficas en la Red, aunque para un 33% esta ha sido una experiencia "desagradable". España se sitúa entre los porcentajes más bajos de exposición a este tipo de imágenes.

Copyright 2026

4. Acceso a contenidos inapropiados

4.3 Pautas y recomendaciones

PAUTAS Y RECOMENDACIONES PARA FAMILIAS Y EDUCADORES

El papel de las familias y educadores en la educación de los menores en relación al uso responsable de las TIC es necesaria y primordial, de cara a prevenir riesgos para la salud y el bienestar por el acceso a contenidos inapropiados. Es importante **evitar posiciones alarmistas promoviendo la integración de actitudes positivas hacia el uso de las TIC**.

En España la mayoría de políticas de protección de la infancia en el entorno audiovisual se basan en medidas de carácter restrictivo sobre el acceso determinados contenidos establecidos por el **Instituto de Cinematografía y de las Artes Audiovisuales (ICAA).**

Por otro lado disponemos de la **Clasificación PEGI y PEGI online.** El primero se utiliza en la mayor parte de Europa, respaldado por los principales fabricantes de videoconsolas así como por editores y desarrolladores de juegos interactivos, indicando el grupo edad aconsejable para cada juego. El segundo sistema es un complemento del sistema PEGI, cuyo objetivo es ofrecer a los menores de edad una mejor protección frente a contenidos inapropiados de juegos en el entorno virtual.

Para prevenir el acceso de los menores a contenidos inapropiados, existen algunos sistemas de filtrado de contenidos para ayudar al control parental, como son los buscadores diseñados para filtrar determinados contenidos y direcciones inapropiadas tales como Yahoo! Kids, Ask Kids , KidsClick o YouTube Kids

Recomendaciones generales para familias y educadores. * Favorecer una actitud positiva y el diálogo con los menores sobre el uso de las TIC para así conocer sus preocupaciones y poder ofrecerles la confianza para hablar de cualquier tema, resolver sus dudas o problemas relacionados con algún contenido.

Copyright 2026

- Fomentar un uso responsable de las tecnologías.
- No utilizar la amenaza como estrategia educativa, pues asumimos el riesgo de que pueda encontrar otro sistema para acceder a esos contenidos sin el consentimiento de sus padres-
- Compartir el tiempo de navegación, enseñarles a controlar y manejar Internet de forma responsable.
- Es conveniente que los dispositivos estén en un sitio visible de la casa, para facilitar su supervisión.
- Las familiar deber fijar horarios y límites de uso de internet.
- Es necesario que familias y educadores cuente con la formación oportuna sobre los riesgos de los contenidos inapropiados.
- El control parental es oportuno realizarlo tanto en el entorno familiar como en el escolar.
- Promover entre los menores una adecuada gestión de privacidad desde edades tempranas.
- Ayudarles a seleccionar previamente los contenidos de blogs, foros, páginas etc. a los que va a acceder y a evita publicar fotos o conectar la webcam con desconocidos.
- Hacerles consciente de la existencia de infracciones legales asociadas al uso de Internet así como de sus consecuencias, como por ejemplo delitos contra la propiedad intelectual, amenazas, intimidación sexual, o piratería.

Estrategias para prevenir el acceso a pornografía

- Dialogar de forma abierta sobre sexo y relaciones sexuales saludables desde muy pequeños adaptándonos al nivel de desarrollo del menor.
- Reflexionar sobre los estereotipos sexuales representados por juguetes, ropa, o publicidad.
- Usar algún para controlar y bloquear contenidos sexuales explícitos.
- Actuar con tranquilidad si aparecen accidentalmente contenidos de carácter sexual.
- Explorar con los menores otras formas más saludables de una expresión sexual normal.
- Evitar que alguien pueda rastrear sus datos a través de la información facilitada.

Recomendaciones sobre el acceso a juegos y apuestas

- Reflexionar con los menores sobre los principales riesgos de los juegos de azar (adicción, pérdida de dinero,…)
- Explicarles que las casas de apuestas online generan más dinero del que inicialmente regalan.
- Educar las probabilidades de ganar dinero en los juegos de azar y apuestas.
- Cuidar los propios hábitos que tenemos los adultos y que pueden influir en los hábitos del menor.

Recomendaciones sobre el acceso a contenidos dañinos para la salud

- Promover modelos realistas de la imagen corporal.
- Promover estilos de vida y hábitos alimentarios saludables.
- Desarrollar positivamente la autoestima, en la autonomía y en la toma de decisiones.
- Abordar de forma constructiva los temas relacionados con los trastornos de la alimentación o el consumo de sustancias nocivas para la salud.
- Mostrarles las consecuencias derivadas del seguimiento de dietas milagrosas, de productos de adelgazamiento o el consumo de alcohol y drogas.

Copyright 2026

5. Tecnoadicciones

Copyright 2026

5. Tecnoadicciones

5.1 Definición y conceptos

DEFINICIÓN Y CONCEPTOS

“Ahora creo que muchos de mis amigos también están enganchados, aunque no lo saben” Beatriz Valera.

Esta afirmación de una adolescente y *tecnoadicta* en tratamiento es la mejor clave para entender lo que conlleva la adicción.

Se conoce como tecnoadicción aquella patología motivada por la dependencia de un determinado dispositivo o servicio tecnológico y en especial se habla de adicción a Internet (Internet Addiction Disorder) a la telefonía móvil o a los videojuegos. Se trata de adicciones comportamentales, como puede ser la ludopatía, la adicción al juego, al trabajo, a las compras… y va en función del espectro de edad.

Aunque no es taxativo pero se suelen generar los riegos por rango de edad. En los chicos las dificultades parten de los juegos y el cyberbullying, en la adolescencia se asocia a la dependencia de redes sociales, y en la edad adulta se suman la pornografía y el juego virtual.

Muy a menudo la detección y la solución no es muy diferente a la de otras patologías, por este motivo las familias y los profesores tienen que ser los primeros en estar formados, porque como muy bien leíamos al inicio de este capítulo, el niño o el adolescente no es consciente de su problema.

Vivimos a golpe de un clic, y nuestros jóvenes no son ajenos. Los niños y adolescentes hacen de las tecnologías su forma de vida, son verdaderos nativos digitales o milenial. Estos son algunos de los síndromes que pueden sufrir, y no son graves siempre y cuando no seas un adicto. (1,5% de los jóvenes españoles son adictos a las tecnologías):

a- ‘Fomo’ | Miedo a perderse algo (Fear of missing out)

Cuando se tiene la sensación de que te estás perdiendo cosas y eso te inquieta y te hace sentir incómodo. Estos síntomas de ansiedad son el *FOMO —miedo a perderse algo—*. Lo produce ver a través de las redes sociales cómo tus amigos se lo pasan bien sin ti. Tres de cada 10 jóvenes han experimentado esta sensación, según un estudio de la agencia J. Walter Thompson.

b-**Nomofobia | No sin mi 'smartphone'**

Te quedas sin batería y aún faltan horas para llegar a casa. Estás inquieto: notas un nudo en el estómago y no dej****as de preguntarte si alguien te estará escribiendo o llamando. Esta sensación de ansiedad cuando no puedes disponer del teléfono es la nomofobia. Afecta a más de la mitad de los usuarios aunque la mayoría ni siquiera sabe que la sufre.

c- **'Phubbing' | Ignoro y me ignoran por un móvil**

Estás en en la calle con tus amigos. Llevas el teléfono en la mano y una luz parpadeando te indica que tienes una notificación. La consultas, contestas y te entretienes mirando alguna otra aplicación. Estás haciendo *phubbing* a las personas que están contigo. Es decir, estás menospreciando a tus acompañantes mirando el teléfono en lugar de prestarles atención.

d- **Ciberadicción | No puedo vivir sin Internet**

Si a la actividad a la que más tiempo dedicas es estar en Internet o te pones nervioso si va lento o no funciona, es muy probable que seas *ciberadicto*. Los adolescentes deben aprender a aburrirse, a recomponer su tiempo libre. Muy a menudo esta situación afecta al rendimiento escolar y a las relaciones personales.

e- **Efecto Google | El buscador es mi oráculo**

Lo consultas todo en Google. El buscador se ha convertido para ti en un baúl donde siempre puedes volver a buscar ese dato que no recuerdas. Esta facilidad de acceso a la información y sus repercusiones en la memoria es el *Efecto Google*

f- **Ludopatía 'online' | El casino a un clic de distancia**

Un día inviertes tu dinero en una web de apuestas_,_ por probar. Haces pequeñas transferencias a la página y no te das cuenta del dinero que gastas. Perder solo te motiva a seguir jugando para recuperarlo. La ludopatía de casino ha evolucionado:ahora se lleva el juego *online.* El 40% de los jóvenes adictos al juego apuesta por Internet, según la Federación Española de Jugadores de Azar Rehabilitados.

g- **Juegos 'freemium' | Pagar para recuperar vidas**

Vas por la calle y no tienes cobertura. Recurres a los juegos que te has descargado en el móvil. En ellos, jugar es gratis, pero para pasar de nivel o recuperar vidas hay que pagar. La otra opción es esperar. Si te pone nervioso aguardar 30 minutos para recargar cada vida y pagas, es posible que

seas adicto a estos juegos, llamados *freemium*.

h- **Cibercondría | Internet es mi médico 'online'**

Cuando te duele algo buscas tus síntomas en Internet para saber qué te está pasando. Te pones tenso y piensas que te relajará encontrar una solución en la web. Si este es tu caso, sufres de *cibercondría*, la hipocondría de Internet. El acceso a la información fácil e inmediato ha hecho que la web se convierta en un médico.

i-**Vibranxiety' | El síndrome de la vibración fantasma**

Vas caminando y notas cómo vibra tu móvil en el bolsillo. Cuando lo consultas te das cuenta de que no tienes ninguna notificación. Pero realmente has sentido que alguien te llamaba. Has sufrido el síndrome de la vibración fantasma.

Fuente: https://elpais.com/elpais/2015/06/25/masterdeperiodismo/1435222559_337110.html

Visiona el siguiente vídeo y observarás alguno de estos "síndromes" o incluso crearás alguno nuevo.

https://www.youtube.com/embed/OINa46HeWg8?rel=0

Al hilo de estos "síndromes" o dificultades que plantean los expertos está el hecho de vivir hiperconectados.

Vivimos en un mundo conectado a través de las redes sociales que muchas veces nos lleva al exceso de información, ese estar ciberconectado o infoxicado (sensación de angustia que nos produce la imposibilidad de manejar tanta información) es el origen de la mayoría de esas afecciones. Es inaceptable que haya niños que declaren estar conectados más de 20 horas a la semana. Se debe ejercer el control parental, las familias tienen que establecer normas de uso, tanto de tiempo como de servicios. Los últimos estudios han detectado dos nuevos retos entre niños y adolescentes que habrá que trabajar sobre ellos porque son preocupantes. Por un lado la falta de descanso y el emergente consumismo a través de internet. Dos nuevas dificultades que habrá que ir solucionando a través de la educación de toda la Comunidad Educativa.

En un país del que ya no se habla de analfabetos, sino más bien de la Alfabetización Digital por la necesidad de ser conocedor de internet, redes sociales… porque van a acompañar a nuestro alumnado tanto en su vida de estudiante, en el mundo laboral y es su tiempo de ocio, sólo nos queda educar y no prohibir.

5.2 Datos y ejemplos

ALGUNOS DATOS Y EJEMPLOS QUE EVIDENCIAN LAS TECNOADICCIONES

El Inteco junto a Orange realizó en el año 2011 el ***Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles*** arroja una serie de datos que pueden poner algo de luz sobre el tema del que hablamos. El estudio íntegro lo puedes encontrar en este enlace:

http://www.pantallasamigas.net/pdf/estudio_sobre_seguridad_y_privacidad_en_el_uso_de_los_servicios_moviles_por_los_menores_espanoles.pdf

A continuación extraemos unos datos:

- La **edad media de inicio** en la telefonía móvil por parte de los menores españoles se sitúa entre los 10 y los 12 años.
- España es uno de los países donde los menores (de 10 a 16 años) afirman ver menos imágenes sexuales online: 11% frente a media europea del 14%
- También es uno de los países con menor incidencia del ciberbullying: 4%.
- El 17,8% de los menores dice haber sido objeto de perjuicio económico (estafas, fraudes, etc.) con su smartphone.
- El acceso a redes sociales: del 7,1% en 2010 se ha pasado al 54,3% en 2011
- Mensajería instantánea: del 12,4% al 48,3%
- Juegos: del 51,6% al 65%

A veces transformar este extenso informe al lenguaje de tus alumnos es lo realmente difícil. Hay muchas aplicaciones para adaptar cualquier información. Te pasamos un ejemplo sobre buenas prácticas de internet realizado con la aplicación Powtoon :

https://www.youtube.com/embed/MIdhs2unQfI?rel=0

Para acabar este apartado te ofrecemos un enlace a otro estudio en este caso sobre ***hábitos seguros en el uso de smartphones por los niños y adolescentes españoles***

Copyright 2026

http://www.observatoriodelainfancia.es/oia/esp/documentos_ficha.aspx?id=3379

Te ofrecemos a continuación algunas **noticias** aparecidas en los medios de comunicación en los que aparece el **riesgo de ser adicto**.

- “El 21% de los jóvenes está en riesgo de ser adicto a las nuevas tecnologías.”

Los jóvenes viven pegados al móvil. Es una extensión de sus manos, les conecta con el mundo y les hace sentirse integrados. Están enganchados al teléfono y, en algunos casos, esa dependencia ha derivado en adicción. Según un estudio sobre conductas patológicas en Internet, realizado por la ONG Protégeles, que colabora en programas de la Comisión Europea, el 21,3% de los jóvenes está en riesgo de convertirse en adicto a las nuevas tecnologías. Y el 1,5% ya lo es. No controlan su conducta, lo que afecta al trabajo y a las relaciones personales.

España, a la cabeza de Europa

España es el país con mayor número de smartphones en la Unión Europea. Hay 23 millones de estos dispositivos. El 87% de la población española lo tiene a mano las 24 horas del día y el 80% admite que lo primero que hace por la mañana es coger su teléfono inteligente, según el informe La sociedad de la información en España 2014 de Telefónica.

El auge de las nuevas tecnologías ha modificado las conductas de comunicación. Según este mismo informe, el 35% de los españoles prefiere comunicarse mediante mensajes, mientras que el 33,5% se decanta por las llamadas telefónicas. Lo que ha pasado de moda es la comunicación en persona: solo el 24% de los españoles prefiere hablar cara a cara.

https://elpais.com/elpais/2015/06/24/masterdeperiodismo/1435159121_214029.html

- «La tecnoadicción está afectando compulsivamente a las nuevas generaciones»

El Observatorio de Contenidos Televisivos Audiovisuales reclama que el uso de las pantallas en la infancia sea regulado.

Muchos menores juegan con móviles y tablets incluso antes de cumplir los tres años. Entonces, ¿hace falta educar a los jóvenes en las nuevas tecnologías? Para el Observatorio de Contenidos Televisivos Audiovisuales (OCTA) la respuesta es clara: sí, y no solo a los jóvenes, sino a toda la sociedad. Con unas consecuencias aún desconocidas en áreas como la neuropsicología, padres e hijos comparten ya la adicción a las pantallas: nadie está haciendo buen uso de ellas.

«La tecnoadicción es una nueva realidad que afecta compulsivamente a las nuevas generaciones», asegura el Observatorio. Por ello, reclama que el uso de las pantallas en la infancia y adolescencia quede regulado en el Pacto Educativo. Y no sólo a nivel técnico, sino también a nivel moral, ético o

físico. Entre otros puntos, piden que, ante los avances de la neurociencia, se informe a todos los educadores de los beneficios y riesgos de su uso.

http://www.abc.es/sociedad/abci-tecnoadiccion-esta-afectando-compulsivamente-nuevas-generaciones-201705092152_noticia.html

- "La tecnoadicción surge cuando no le damos al cerebro otra alternativa”

Las tecnologías de entretenimiento se han vuelto uno de los mayores desafíos para padres y educadores en nuestros días.

¿Existe un problema real en torno a las tecnoadicciones o ciberadicciones? Desde la Fundación Aprender a Mirar (FAAM) –cuyo ámbito de actuación es la defensa de los derechos del consumidor audiovisual-, aseguran que sí, y que de no poner remedio podrían ir a peor en los próximos años. Su delegado en Aragón y abogado experto en nuevas tecnologías, Juan Boza, ha comenzado a impartir ciclos abiertos dirigidos a padres y profesores en los que trata de dar algunas claves para combatirlo.

Como explica el experto: “surge cuando utilizamos los dispositivos móviles para realizar tareas para las que no son totalmente necesarios”. Algo que resulta muy habitual en nuestros días y, cada vez, a edades más tempranas.

http://www.heraldo.es/noticias/aragon/2017/04/02/tecno-adicion-surge-cuando-damos-alcerebro-otra-alternativa-1167818-300.html

- ¿Adicto al móvil? En lugar de desconectar, aprende a priorizar.

Esforzarse en mantener límites estrictos entre la vida online y 'offline' también puede generar estrés y ansiedad

Estamos hartos de escuchar que dependemos en exceso de la tecnología, que los niños pasan demasiado tiempo delante de las pantallas y que vivir en las redes sociales aumenta las posibilidades de sentir envidia, frustración y tristeza. El grueso de los estudios científicos hasta el momento defiende estas conclusiones y alerta de las consecuencias negativas que pueden derivarse de abusar de la tecnología. Pero la solución no tiene por qué ser desconectar, obligarse a no mirar el móvil y no consultar el correo fuera del trabajo. En su lugar, algunos expertos defienden la necesidad de aprender a priorizar y compaginar la realidad online y offline.

Regular el uso del móvil en lugar de dejar de utilizarlo cuando estás con otras personas podría reducir los niveles de ansiedad que genera no estar atendiendo a las notificaciones. "Mi consejo es que cada cual gestione su propia vida. Si dejar de mirar el buzón de entrada o no contestar a un

mensaje en tu tiempo de descanso te va a provocar todavía mayor estrés, hazlo", comenta Santi García, cofundador de Future For Work Institute, en un reportaje reciente publicado en EL PAÍS.

https://retina.elpais.com/retina/2017/08/30/talento/1504087145_736668.html

5. Tecnoadicciones

5.3 Pautas y recomendaciones

PAUTAS Y RECOMENDACIONES PARA FAMILIAS Y EDUCADORES

La prevención familiar y escolar es una parte fundamental ante el desarrollo de cualquier adicción. Es necesario conocer las causas, consecuencias o riesgos que se sumen al hacer un uso incorrecto o excesivo de las TIC. Describiremos algunas pautas de actuación a nivel preventivo dirigido tanto a familias como a educadores y menores.

Sabemos que la oferta es tan variada, atractiva e interesante que no puede estar exenta de problemas. La participación en redes sociales, la descarga y escucha de música, la televisión, las apuestas on line, el visionado de películas y telefilmes forma parte de esta oferta.

Veamos algunas de las pautas y recomendaciones.

- Usar herramientas de control parental en el ámbito de las TIC, instalando aplicaciones que impidan el acceso del usuario a páginas que pueden ser perjudiciales para el menor.
- Diseñar contratos o acuerdos de conducta que regulen el comportamiento relacionado con el uso de las tecnologías, aceptando por parte de los implicados las conductas y normas a las que se comprometen, así como asumir las consecuencias de su incumplimiento.
- Propiciar mover alternativas de ocio más saludables como el teatro, el cine, la lectura, el deporte, etc., fomentando las relaciones sociales o participaciones en grupo.
- Limitar el uso de los dispositivos electrónicos y establecer horarios de conexión a internet.
- Las familias tienen que dar buen ejemplo en los hábitos sobre el uso de las TIC, compartiendo momentos y realizando actividades con ellos para comprobar cómo se maneja en el uso de las TIC.
- Educar emocionalmente a los menores, ayudándoles a identificar las diferentes emociones y ayudarles a gestionar el enfado, la ira o la frustración. Pero también fomentando la empatía y la comunicación, como formas adaptativas para desarrollar el

Copyright 2026

autocontrol y así evitar la tecnoadicción.
- Educar a los menores en valores de respeto, confianza, solidaridad, cooperación, , responsabilidad,...)
- Sensibilizar sobre el problema de la tecnoadicción, promoviendo actitudes positivas y facilitándole ejemplos de casos reales que han acontecido, y vean las consecuencias múltiples y directas de la adicción a las TIC.
- Proponer actividades relacionadas con la competencia sociemocional, fomentando las relaciones interpersonales, para evitar el aislamiento que lleva un uso abusivo de las TIC. Desde el ámbito educativo debe desarrollarse habilidades sociales como la asertividad, la empatía o la escucha activa.
- Crear un grupo de ciberayudantes en el centro que se encargue de informar, detectar y asesorar a los demás alumnos sobre esta temática. Con la finalidad de que hagan un buen uso de las TIC.

Las familias son parte de la solución, por eso te adjuntamos un tríptico a modo de ejemplo con una información básica que deben conocer y que está relacionado con los dos anteriores módulos. Ahora adáptalo a tu centro.

https://alumnosayudantes.files.wordpress.com/2015/03/triptico-uso-redes-sociales-padres2.pdf

6. Ciberbullying, sexting y grooming

Copyright 2026

6.1 Definición y conceptos

DEFINICIÓN Y CONCEPTOS

Es indudable que el acceso de la información a través de internet ha permitido una nueva forma de comunicación global que facilita el acceso al conocimiento. Hay que buscar espacios positivos para que el uso de las TIC sea verdaderamente una oportunidad. La sociedad tiene que ser capaz de hacer de esto una experiencia por y para el desarrollo de una adecuada alfabetización.

El uso del móvil, internet y las redes sociales pueden aportar aspectos positivos, pero no se puede obviar, y forma parte del proceso educativo, que pueden existir una serie de riesgos. En el anterior tema hablamos de las posibles tecnoadicciones, ahora vamos a profundizar sobre **tres situaciones extremas que se pueden producir en la red: Ciberbullying, sexting y grooming.**

a- Ciberbullying

Es el acoso entre menores que se produce a través de medios tecnológicos. Por uso y difusión de información lesiva o difamatoria en formato electrónico a través de los medios de relación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de dispositivos móviles o la publicación de vídeos o fotografías en plataformas electrónicas de difusión de contenidos.

Para que se defina como **ciberacoso** tiene que ser una agresión psicológica, **sostenida y repetida en el tiempo, perpetrada por uno o varios individuos contra otro**s, utilizando para ellos las nuevas tecnologías. Si la agresión fuera puntual, evidentemente habría que buscar soluciones, pero no se debería considerar como acoso.

Conductas que provocan ciberbullying:

- Amenazar
- Insultar
- Subir una foto sin permiso o trucada
- Crear websites o grupos difamatorios
- Robar contraseñas
- Suplantar la identidad

Copyright 2026

- Seguir enviando correos o mensajes a alguien que no quiere recibirlos
- Acechar y acosar a través de las redes
- Excluir intencionadamente a alguien de un grupo
- Envío de rumores o cotilleos
- Compartir información secreta
- Grabar y compartir vídeos de peleas o tipo sexual.

¿Por qué es tan peligroso? * No siempre hay intención de causar tanto daño, a veces la conducta desencadenante parece inocente. * Su efecto es duradero, se mantiene a través de las redes durante mucho tiempo. * Se extiende por las redes sociales sin control y la audiencia se expande. * Favorecen el anonimato * No hay enfrentamiento personal, a la cara * Quien lo causa se siente impune. * No se produce un contagio físico de las emociones ya que las claves socioemocionales propias de la empatía (llanto, expresión de la cara,..) no son visibles para el agresor.

¿Qué consecuencias tiene? * En las víctimas provoca serios daños emocionales que lesionan la autoestima, pudiendo ser la causa de enfermedades como la depresión y en casos extremos el suicidio * Estrés postraumático * Delirio de persecución * Insomnio * Cambios de personalidad que puede a llegar a destruir o anular a la persona del menor * Sensación de inferioridad respecto al resto del entorno * Nerviosismo e hipersensibilidad a toda injusticia * Incapacidad para disfrutar y estar seguro de lo que se es y se hace * Miedo general

Para los agresores las consecuencias pueden ser penales…

La edad penal en España se establece en los 18 años pero a partir de los 14 se pueden exigir responsabilidades, aplicando un sistema jurídico particular.

Los menores de 14 años también responden de los delitos cometidos ante la fiscalía de menores.

Son los padres o tutores legales los que asumen la responsabilidad civil.

El ciberacoso no está tipificado como tal en el Código penal al ser un fenómeno moderno.

La mayor parte de los delitos cometidos a través de las tecnologías de la información sí lo están. Por ejemplo, el artículo 143 del Código Penal castiga con pena de prisión de cuatro a ocho años al que induzca al suicidio de otro. No importa el mecanismo utilizado, o si se induce a éste en persona, verbalmente, por chat, por SMS.

Según el Código Penal español, los **delitos informáticos que podrían encajar con esta figura** delictiva, si bien no exactamente son:

- Delitos contra la intimidad: El descubrimiento y revelación de secretos o la vulneración de la intimidad de las personas.

- Amenazas.
- La alteración, destrucción o los daños en datos, programas o documentos electrónicos ajenos. En este tipo delictivo se incluirían conductas como, por ejemplo, los actos de sabotaje contra soportes electrónicos, o la introducción de virus electrónicos para causar daños.
- La pornografía infantil, que se ha visto favorecida por el anonimato que proporciona la red.
- Delitos contra el honor: Las injurias y las calumnias. Generalmente las que se cometen en redes sociales, foros o por correo electrónico.
- Coacciones

También en el artículo 173.1, pudiera ser aplicado para referirnos a esta figura: “El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años”.

Otros casos, en el 197.1 del CP: para contemplar aquellos casos, en el que alguien pueda descubrir los secretos o vulnerar la intimidad de otro.

Perfil del acosador:

El perfil genérico del acosador es el de una persona fría, con poco o ningún respeto por los demás y que disfruta persiguiendo a una persona determinada, ya tenga relación directa con ella o sea una completa desconocida.

El acosador disfruta y muestra su poder persiguiendo y dañando psicológicamente a esa persona.

Según Rodríguez López en su libro El Acoso moral define a estas personas como " resentidas, frustradas, envidiosas, celosas o egoístas, necesitadas de admiración, reconocimiento y protagonismo y lo que quieren es figurar, ascender o aparentar, aun cuando simplemente deseen hacer daño o anular a otra persona".

En el caso del ciberacosador se siente en una posición de poder desde el anonimato que se percibe mientras se está “en línea”. Durante todo ese tiempo va recopilando toda la información posible acerca de su víctima, fundamentalmente en aquellos aspectos que forman parte de su vida privada y de sus movimientos en la Red.

Además es cobarde, ya que se oculta tras el aparente anonimato y falsificación de identidad que proporciona internet.

Este vídeo te invita a reflexionar acerca del Cyberbullying. Si no eres capaz de decirlo en persona, ¿por qué hacerlo en intenet?:

https://www.youtube.com/embed/E3Z6f-KIIQI?rel=0

La víctima: La víctima se siente indefensa, en muchos casos culpable. Entiende este alumno que ha hecho algo mal, se lo merece puesto que nadie le apoya. Su aislamiento psíquico, su falta de comunicación, el desconocimiento de éstos sobre los hechos, la falta de solidaridad entre compañeros, socavan la fuerza de la víctima. En principio, no se puede afirmar que exista un perfil psicológico que predisponga a una persona a ser víctima de acoso u hostigamiento. Esto quiere decir que cualquier persona en cualquier momento puede ser víctima. Nada tiene que ver la imagen que pretende proyectar el acosador de su víctima con la realidad. Mientras que esa imagen pretende reflejar una persona poco inteligente y holgazana, los acosados a menudo suelen ser inteligentes y trabajadores.

En cualquier caso el acosador no actúa nunca solo, sino que más bien es el acosado quien lo está. Es la pasividad de los demás la que refuerza el acoso.

El espectador:

En los nuevos protocolos y programas de convivencia se está insistiendo en una figura que hasta ahora no estaba siendo considerada, y esta es la del testigo.

En los centros educativos los testigos son compañeros que se alinean con el acosador para no tener problemas, y a la vez conviven dentro del anonimato que les hace creer ser más impunes.

b- Sexting:

Se origina en un menor que **envía imágenes o vídeos sexuales propios**. Para ello utiliza el móvil y a través de redes sociales como Whatsapp, Line, SnapChat, Instagram, Telegram… es delito porque se considera como pornografía infantil.

Esta práctica está realmente extendida entre los jóvenes, y aunque el eslogan es **no lo produzcas, no lo transmitas y no lo provoques**, los niños y adolescentes lo realizan sin ser conscientes sus consecuencias.

De esta manera **el sexting se convierte en una práctica de riesgo. Los problemas más habituales son:**

- Daños al honor y a la propia imagen
- Pérdida de intimidad y privacidad
- Sextorsión: personas que te chantajean por esas imágenes
- Ciberbullying: personas que te acosan, insultan y molestan
- Implicación en delitos de pornografía infantil si eres menor de edad

A continuación damos **diez razones para no sextear**:

http://www.pensarantesdesextear.mx/prevencion-10-razones-no-sexting/

Muy a menudo el alumnado no acepta ese riesgo, de hecho es muy común entre los adolescentes hacer sexting. Ahora te proponemos un **decálogo para sextear de forma segura**:

http://www.sextingseguro.com/consejos-sextear-nudes-con-menos-riesgos/

c- Grooming.

Es **acoso sexual que se produce en los espacios virtuales**. Es acoso ejercido por un adulto y se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor. Se podría decir que son situaciones de acoso con un contenido sexual explícito o implícito.

Fases: 1. Contacto y acercamiento del ciberacosador que finge ser atractivo para el menor. 2. Consigue en el transcurso de la relación que el menor le envíe alguna fotografía comprometida. 3. Si el menor no accede a sus pretensiones sexuales, le chantajea con las fotos. 4. Mediante amenazas el ciberacosador puede acceder a todos sus caprichos sexuales, llegando en algún caso, incluso a contactar físicamente con el menor.

Consejos para los alumnos: 1. Mantener los datos en privado. 2. No molestar o insulta a otros con dispositivos. 3. No responder a mensajes o llamadas de desconocidos. 4. Si es algo importante hablar con un adulto de confianza. 5. La opción GPS se debe utilizar con precaución. 6. Cuidado con la webcam, tapa siempre la cámara. 7. Tener precaución al conectarse a redes WIFI o Bluetooth

Encuestas sobre comportamiento de los niños en las redes sociales revelan que a la vez que se hacen mayores aumenta el contacto con desconocidos. El salto de las 12 a los 14 años puede quintuplicar ese contacto que estaría en zona de riesgo.

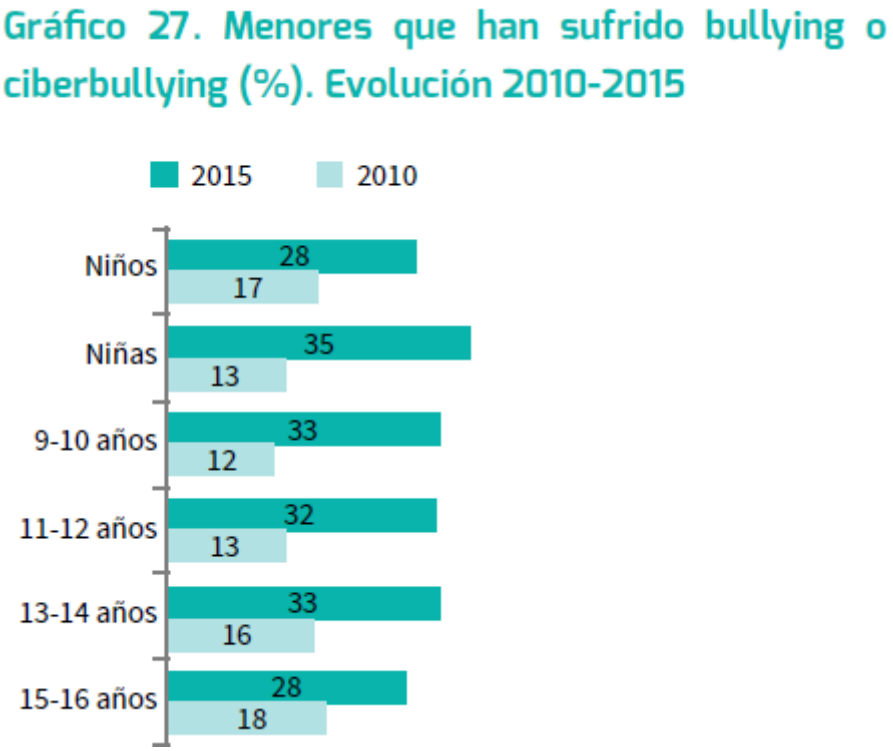
Observa esta imagen del Estado de México:

Copyright 2026


PARA ACERCARSE
A TUS HIJOS
LOS ACOSADORES
USAN LAS FORMAS
MÁS DESCARADAS.
Hablá con ellos antes
que otros lo hagan.
EL PELIGRO ESTÁ AHÍ
AUNQUE NO LO VEAS.
#CONECTATESEGURO
GOBIERNO NACIONAL

6.2 Datos y ejemplos

ALGUNOS DATOS Y EJEMPLOS REALES DE SITUACIONES DE RIESGO



El ciberbullying, según ha podido medir el estudio, **es más probable entre las chicas** (35%, frente al 29% de chicos), quienes también se ven más afectadas por ello (26%, frente al 22% de los chicos).

Sin embargo, el ciberbullying parece disminuir a partir de los 15/16 años (un 6%, frente a un 12% de la media), y también disminuye a la mitad en la adolescencia el porcentaje de menores que dice sentirse disgustado por esta experiencia.

Además del ciberbullyng, también se ha preguntado a menores de edad por otros riesgos derivados del uso de internet o del teléfono móvil como imágenes de contenido sexual (un 52 % reconoció su visión); encuentros con desconocidos contactados en la red (11 %), o el envío de

Copyright 2026

mensajes sexuales o sexting (31 %).

El ciberbullying sigue siendo el fenómeno que más daño creen que causa (24%).

Y un último dato bastante ejemplificador: la edad de inicio de acceso a internet se sitúa actualmente en 7 años.

Fuente: Informe Net Children Go Mobile

Veamos algunos **ejemplos de casos reales**:

- Ciberbullying en niños de nueve años.

http://www.lavanguardia.com/local/girona/20160203/301865681908/ciberbullying-ninos-girona-whatsapp.html

Unos niños de 4º de primaria acosaban dentro y fuera del aula a través de Whatsapp. Al tomar el centro medidas punitivas las familias de los acosadores amenazan a la dirección del centro con denuncias.

- Uno de cada cuatro casos de acoso se produce en la red.

http://www.elmundo.es/sociedad/2016/09/20/57e10015468aeb59718b4650.html

El ciberacoso está abierto las 24 horas. El 92% de las víctimas sufre algún tipo de secuela psicológica, como ansiedad, la más común, tristeza, soledad y baja autoestima.

Ademas, un 10% de las víctimas ha tenido conductas autolesivas, pensamientos suicidas e incluso intentos de acabar con su vida como forma de huir y acabar con la situación.

- Víctimas del 'sexting' con sólo 13 años: los peligros de compartir contenido sexual a través del móvil.

http://www.lasexta.com/noticias/nacional/victimas-del-sexting-son-solo-13-anos-los-peligros-de-compartir-contenido-sexual-a-traves-del-movil_20170517591c5ccf0cf249bae19ecbaf.html

Si los chicos se aíslan o se vuelven agresivos, cuidado, porque pueden pertenecer al 21% de los jóvenes que han sufrido alguna vez ciberacoso.

Fijar unas **normas de uso del móvil** o vigilar sus aplicaciones son algunas de las pautas básicas para evitar que algo tan útil se convierta en un verdadero problema.

6.3 Pautas y recomendaciones

PAUTAS Y RECOMENDACIONES PARA FAMILIAS Y EDUCADORES

De nuevo **son los adultos los que deben estar atentos al desarrollo de su hijo o alumno**. No sólo porque puede sufrir una situación de riesgo, grooming, sexting sino porque pueda ser acosado en la red.

Y aunque la mayoría de los casos educamos para no ser acosado, las probabilidad de que un niño o adolescente sea el acosador es mucho mayor.

Como **detectar si puede existir ciberacoso**:

1. Cambios en sus hábitos:

• En el uso de dispositivos móviles o de Internet • De asistencia a clase • Por ausencia en actividades hasta ese momento preferidas • En altibajos en los tiempos de estudio y en el rendimiento del trabajo escolar • De variaciones en sus actividades de ocio habituales • De regularidad en la cantidad de comida y maneras de comer • Por permutas en los grupos de iguales, en ocasiones antagónicos • En relación con los adultos, en cuanto a la frecuencia y dependencia de ellos • En cuanto a su capacidad de concentración y de mantenimiento de su atención • Por modificación de sus costumbres de ocupación de su tiempo libre • En estados de humor • Por variabilidad de grupos de referencia

2. Cambios en el estado de ánimo:

• Fundamentalmente en el humor • Momentos de tristeza y/o apatía e indiferencia • En actitudes de relajación y tensión, incluso de reacción agresiva inusual • Excesivas reservas en la comunicación

Copyright 2026

3. Cambios en su red social:

• Intercambios extraños de red social y/o por repentina pobreza, ausencia de amistades y de relaciones sociales • Falta de defensa ante supuestas bromas públicas u observaciones públicas, inocuas aparentemente a ojos de los adultos • Miedo u oposición a salir de casa.

4. Cambios físicos o en sus pertenencias:

• En su lenguaje corporal ante determinadas presencias: hombros encorvados, cabeza gacha, falta de contacto en ojos, rechazo de la presencia pública • En la ocupación de espacios escolares: cercanía a adultos, miedo a recreos, ocupación de rincones, paredes y espacios protegidos y controlables visualmente • De ocultamiento especial cuando se comunica por Internet o móvil • Explosiones agresivas momentáneas • Manifestaciones de enfermedad o dolencias frecuentes • Pérdida y/o deterioro de pertenencias físicas, lesiones físicas frecuentes sin explicación razonable

5. Síntomas físicos:

• Síntomas neurológicos: cefaleas intensas y prolongadas, mareos, pérdida de fuerza en extremidades inferiores. • Síntomas gastrointestinales: dolor abdominal intenso y continuado, pérdida de apetito. • Pérdida de peso • Insomnio Si se detecta algunos de estos síntomas el adulto tendrá que acercarse al niño intentado transmitir confianza, y una vez iniciado el contacto alejarlo de la culpabilidad de lo que está sucediendo. Fuente:

http://www.chaval.es/chavales/sites/default/files/Guia_Actuaci%C3%B3n_contra_Ciberacoso_vf_pi.pdf

Copyright 2026

7. Ciberayudantes: Un programa de centro

Copyright 2026

7.1 Contexto del proyecto y del centro

CONTEXTO DEL PROYECTO Y DESCRIPCIÓN DEL CENTRO EDUCATIVO Y SU ENTORNO

Nuestro instituto está situado al norte de la ciudad, en el primer barrio bioclimático construido en Zaragoza. Un centro de reciente creación en una zona residencial inaugurado en el años 2000.

El IES Parque Goya en su relación con el entorno busca respuestas a las necesidades de sus alumnos, y a la vez ser centro educativo de referencia junto al resto de centros, en definitiva ser un espacio integrado en la vida del barrio.

El Instituto desarrolla el Plan de coordinación con los centros de primaria adscritos cuya transición se hace de forma ordenada, especialmente en la atención a la diversidad y la acogida de alumnado, familias y profesorado nuevo.

Además nuestras prioridades se centran en grandes programas y proyectos que la mayoría se desarrollan en los centros de primaria adscritos al Instituto, y que redundan en la adquisición de las competencias clave. Hablamos del **British Council, Desarrollo de Capacidades, grupo de lectura "Leer juntos" y en especial de nuestro plan de convivencia**, en el que los **alumnos ayudantes** tienen un papel relevante en la cooperación entre iguales, en el **desarrollo de la inteligencia emocional y en la mejora del clima de convivencia del centro.**

Nuestro proyecto persigue desarrollar una **estrategia de participación y empoderamiento de los adolescentes**, apoyada en las buenas prácticas e iniciativas para hacer de Internet un entorno saludable y seguro con la creación de un **grupo de ciberayudantes**. Trabajamos contenidos relacionados con los riesgos y utilidades del uso de las redes sociales en el alumnado de secundaria, con la implicación de este grupo de alumnos. Por otro lado, este programa busca la colaboración de las familias a través del grupo de lectura de padres y profesores " Leer juntos" y la

realización de talleres.



El enlace al Blog del programa:

http://alumnosayudantes.wordpress.com/

Grado de participación de las familias implicadas directamente en el proyecto.

Las familias están representadas en el centro a través del Consejo escolar. Su representante en la comisión de convivencia sirve de enlace para la promoción de estas iniciativas. Colaboran a través del AMPA y de la asociación de vecinos.

Asisten a charlas y colaboran en el observatorio sobre el estado de la convivencia en el centro, en nuestro blog, en la página web y utilizar de forma asidua el correo electrónico corporativo.

Participan de manera activa a través de la biblioteca y de la tertulia “Leer juntos".

Grado de implicación del resto de la comunidad educativa.

La implicación del profesorado del centro es fundamental para el desarrollo del proyecto, especialmente **los tutores** que son las personas responsables de poner en marcha estas iniciativas en la sesión de tutoría. La planificación de las actuaciones que se están llevando a cabo en el aula, se organizan desde las reuniones de tutores con una periodicidad semanal, coordinados

por la **jefatura de estudios y el departamento de orientación**.

Este Programa **se extiende a los centros de primaria adscritos con quienes trabajamos nuestras propuestas en colaboración con el grupo de Ciberayudantes**. Hacemos intercambios con otros centros a través de los Encuentro Provinciales de Ayudantes y mediadores, dos de los cuales hemos organizado en nuestro centro. Contamos con la ayuda inestimable de Pantallas Sanas, que ha promovido esta labor de cibervoluntariado. Creamos materiales disponibles en el blog que permiten ser replicados en otros centros (spot publicitario, guía didáctica, enlaces...)

Copyright 2026

7.2 Marco teórico

MARCO TEÓRICO

¿Cuántas veces hemos escuchado que la conflictividad entre los jóvenes aumenta cada día?. Con frecuencia nos encontramos en los centros educativos alumnos/as que se pelean o discuten por diferencias personales o por malentendidos.

La forma que tienen algunos de resolverlo es a través de la violencia, terminando frecuentemente con una expulsión del centro. Sin embargo, los conflictos no quedan resueltos.

La conflictividad es un proceso dinámico y forma parte de la vida de los centros. En este proceso, se desarrollan capacidades y habilidades de cooperación, de colaboración, de comunicación y de expresión de sentimientos que predisponen a facilitar un acuerdo mutuo. La resolución de conflictos debe entenderse como una herramienta de prevención de nuevos problemas que pueden aparecer si la situación que en un principio ha originado el conflicto no está bien resuelta por las dos partes implicadas. Como diría Martin & Puig 2002 **«El conflicto no es únicamente inevitable, sino que, además, es necesario para mejorar la vida colectiva»**.

Además, existen otras situaciones en las que la convivencia se ve dañada por el acoso escolar, el maltrato, el aislamiento, la exclusión social,... y que surgen fundamentalmente fuera de la vista de los profesores, en contextos poco vigilados como son los pasillos, el patio , salidas del centro, etc.

Para dar respuesta a estas situaciones es necesario la incorporación de programas preventivos para la mejora de la convivencia, que permita por un lado a los alumnos/as otras formas alternativas de resolución de conflictos y por otro lado que eviten la aparición de situaciones de maltrato.

La puesta en marcha de estos programas preventivos para la mejora de la convivencia está basada en sólidos **fundamentos teóricos y metodológicos**, algunos de los cuales haré referencia a continuación.

1º Los nuevos enfoques para abordar la resolución de los conflictos y el maltrato tienen que basarse en modelos de **mediación y ayuda entre iguales**. Se trataría de estrategias para asistir a los alumnos en situación de debilidad, maltrato e indefensión . 2º Estos modelos deben apoyarse

Copyright 2026

en valores prosociales de respeto, ayuda, diálogo, tolerancia y solidaridad, con una finalidad muy clara: fomentar una cultura del diálogo, la empatía y escucha activa.

3º Estos modelos ponen en valor el empoderamiento de los adolescentes. Entendido este como un proceso que **les permite sentirse cómplices y responsables del buen funcionamiento de la convivencia.**

4º A nivel metodológico, utilizamos la **Pedagogía de aprendizaje y servicio solidario**. "una metodología que combina en una sola actividad el aprendizaje de contenidos, competencias y valores con la realización de tareas de servicio a la comunidad y con una utilidad social.

En definitiva, estos programas tienen un carácter eminentemente preventivo y proactivo, en el sentido de que actúa a priori, anticipa los problemas e intenta resolver el futuro. Ve los conflictos como una ocasión y como una oportunidad.

Copyright 2026

7.3 Justificación

JUSTIFICACIÓN

Según la Asociación de Usuarios de Internet el 50% de los niños menores de 10 años ya tiene un smartphone y con 14 años, este porcentaje se eleva al 90%. “El 40% de los niños de entre 10 y 12 años accede a contenidos de carácter sexual explícito y más del 30% comparte imágenes de otros sin ser conscientes del riesgo que eso conlleva.

Nadie duda de los beneficios derivados de la utilización del móvil que les facilita el trabajo o les permite relacionarse y divertirse. Sin embargo no está exento de riesgos. El uso excesivo, las amenazas a la privacidad y acceso a contenidos inapropiados, pueden conducir a formas más graves como las adiciones, el grooming, el sexting y especialmente el ciberbullying.

En este contexto se hace necesario abordar estos problemas desde una perspectiva educativa frente a una visión punitiva o de prohibición.Pero también, respetando las directrices que marca la UE en un reciente estudio publicado en 2016. Se trata del informe “Cyberbullying among Young People”, donde se propone que las buenas prácticas para combatir el ciberbullying se basen en la atención a las víctimas y protección a la infancia, y a campañas de sensibilización y las políticas educativas. Una buena combinación de estas ofrece los mejores resultados, siempre y cuando se involucre también a niños, niñas y adolescentes como parte de la solución y no se les trate como meros objetos a proteger. Y esto es precisamente lo que nosotros venimos realizando desde hace años.

Desde hace el curso 2011-12 venimos aplicando en el IES Parque Goya una serie de programas preventivos Alumnos ayudantes y Ciberayudantes que tratan de mejorar el clima de convivencia tanto en el entorno real como en el virtual. Y que pretender prevenir comportamientos de riesgo que dañen la convivencia entre iguales (como el maltrato, el aislamiento, la exclusión social o el ciberacoso.)

En este contexto, se hace necesario elaborar un diagnóstico de los usos del smartphone y de los hábitos seguros por parte de adolescentes y, asimismo, conocer la percepción que de dichos usos y hábitos seguros tienen sus madres y padres. Es importante, determinar el conocimiento que el alumnado tiene de los riesgos del uso de las distintas redes sociales, su reacción ante los mismos, así como tomar medidas de carácter preventivo para hacer de internet un espacio saludable y seguro.

Copyright 2026

Tenemos que ayudar a nuestros menores a tener una relación positiva y saludable en el uso de las redes sociales. Es importante ayudar a nuestros hijos y alumnos a ser conscientes de sus riesgos, a saber controlarse y a seguir disfrutando de otras actividades. Pero además lo queremos hacer dando mayor participación e implicación de los propios menores.

Copyright 2026

7.4 Objetivos

OBJETIVOS

El objetivo general del proyecto es promover buenas prácticas que permitan el desarrollo de una buena salud digital, apoyadas en estrategias innovadoras. Además pretendemos invitar a la comunidad educativa a desarrollar actividades y recursos con y en la Red sobre los ámbitos más importantes de la educación para la salud a partir de campañas de prevención que surgen del propio alumnado, y otras iniciativas docentes, sobre todo en lo que concierne a la acción tutorial.

Queremos **dar protagonismo a los adolescentes**, para que sean ellos quienes hagan propuestas concretas, especialmente al grupo de alumnos ayudantes, y también a las familias a través del programa “Leer juntos”.

Objetivos específicos
* Dar respuesta a situaciones que dañan la convivencia como el maltrato, el aislamiento, peleas por diferencias personales, incorporando medidas preventivas que mejoren esta situación. * Fomentar una cultura de diálogo, la escucha activa, el interés por el compañero basado en valores prosociales de respeto, ayuda y solidaridad. * Prevenir la aparición de comportamientos de riesgo social, tales como: maltrato, acoso, ciberbullying, sexting, grooming etc. * Iniciar una estrategia de participación y protagonismo de los adolescentes, apoyada en las buenas prácticas para hacer de Internet un entorno saludable.
* Invitar a la comunidad educativa a desarrollar actividades de prevención propuestas por el alumnado. * Crear recursos con y en la Red sobre los ámbitos más importantes de la educación para la salud. * Elaborar otras iniciativas docentes, especialmente realizadas desde la acción tutorial. * Realizar una experiencia pionera de innovación y empoderamiento en los adolescentes que servirá como recurso educativo a sus iguales a partir de la creación de Equipos de Cibervoluntariado. * Desarrollar iniciativas innovadoras basadas en la creación de audiovisuales, en la utilización de las TICS y de las redes sociales educativas. * Implicar a las familias en las distintas iniciativas que se presentan. * Hacer de la lectura, a través del grupo “Leer Juntos”, una herramienta de acercamiento y de reflexión sobre la red a toda la Comunidad Educativa.

Copyright 2026

7.5 Metodología

METODOLOGÍA

Nuestro proyecto se sustenta en los siguientes **principios metodológicos**:

- Que garantice la funcionalidad de los aprendizajes, y que estos estén vinculados a los problemas importantes de la vida cotidiana: el uso inadecuado de las redes sociales.
- Que permita un enfoque globalizador e integrador entre distintos contenidos de las diferentes áreas y que permitan desarrollar las competencias clave.
- Que fomenten el papel activo y participativo del alumnado.
- Que incida en actividades que permitan la indagación, el planteamiento y resolución de problemas derivados de la red, así como la búsqueda, selección y procesamiento de la información.
- La utilización de las herramientas que nos proporcionan las TICs como el blog, Twitter o diferentes redes sociales, nos puedan servir como instrumento de trabajo para explorar, analizar e intercambiar información.
- Los métodos de trabajo guardan una estrecha relación con el clima del aula, donde la convivencia constituye uno de los aprendizajes esenciales en la educación básica. Debe haber equilibrio entre el trabajo personal y el cooperativo.

Las **estrategias metodológicas** que hemos utilizado son:

- Pedagogía del aprendizaje-servicio. Se trata de una metodología de enseñanza y aprendizaje mediante la cual los jóvenes desarrollan sus conocimientos y competencias a través de una práctica de servicio a la comunidad (TAPIA, 2000).

Se trata, por lo tanto, de sostener simultáneamente una intención pedagógica de mejorar la calidad de los aprendizajes y una intención solidaria de ofrecer una respuesta participativa a una necesidad social. Un buen programa de aprendizaje-servicio les permite a los jóvenes aprender contenidos académicos y, a la vez, realizar tareas importantes y de responsabilidad en su comunidad y en la propia institución educativa.

Otras **metodologías que empleamos** son las siguientes.

- Trabajo colaborativo en red utilizando la tecnología de Google Drive

Copyright 2026

- Tutoría entre iguales
- Integración de las tics a partir del uso del Blog, del Twitter y de Redes sociales. En cuanto a la estructura básica que configura cada una de nuestras iniciativas siguen el siguiente esquema:
- **Sensibilización e información**: Se trata de una primera etapa de acercamiento a la problemática del uso de las redes sociales por parte de todos los miembros de la comunidad educativa. Es necesario que desde el centro se trate el tema en reuniones de equipo y que, en conjunto, se planteen las bases del programa durante las primeras semanas del curso.
- **Aprobación del proyecto y de las actuaciones que lo componen**.
- **Formación a profesores, alumnos y padres**.
- **Desarrollo del proyecto**: Las tutorías de grupo van a ser una herramienta para encaminar y dirigir el proceso.
- **Evaluación del programa**: Se realizara una evaluación conjunta (equipo docente y alumnado) sobre la eficacia y la eficiencia del proyecto, valorando y concretando los resultados obtenidos en relación con el planteamiento inicial.

RECURSOS: * Portátil, proyector y pantalla. * Cartulinas de colores. * Fichas para el alumno. Pizarra digital. * Sala de informática. * Cámara de vídeo y de fotos. * Móvil.

AGRUPAMIENTO.

- Por parejas: búsqueda de información en internet.
- En grupo: conclusiones consensuadas
- En grupo: lluvia de ideas.
- Gran grupo: visionado de vídeos. Análisis y debate final, donde los portavoces de cada grupo exponen sus conclusiones.
- En grupo: exposición oral de los trabajos

Copyright 2026

7.6 Actividades realizadas

ACTIVIDADES REALIZADAS

1. Observamos. Observatorio sobre el uso de redes sociales en la ESO.

Cuestionario On-line elaborado por los alumnos de psicología sobre las conductas que se desarrollan a través de la red. Posteriormente serán los propios alumnos de secundaria quienes completarán el cuestionario en la sesión de tutoría.

El alumnado en grupos revisará los resultados globales del cuestionario y reflexionará sobre los usos de internet por un lado, y los riesgos y problemas que con mayor frecuencia han surgido. En gran grupo se pondrán en común las ideas aportadas por todos y se recogerán las conclusiones a las que han llegado.

Enlace cuestionario para profesores.

https://docs.google.com/forms/d/1i7iQ-yhICbgFV8oyW0TCz7FJMVjeuBkojY/viewform

Enlace últimos resultados del alumnado.

https://alumnosayudantes.files.wordpress.com/2015/01/resultados-cuestionario-redes-sociales-12-2014b.pdf

Enlace al cuestionario de alumnos.

https://alumnosayudantes.wordpress.com/cibervoluntariado/iniciativa-1/

Copyright 2026



2. Visionamos cortos y reflexionamos.

Esta iniciativa tiene como finalidad la de visualizar vídeos publicados en internet donde se aprecian diferentes usos de las redes sociales que realizan los adolescentes. Servirán de base para poder analizar y reflexionar sobre las prácticas que se hacen de ellas. Para ello utilizaremos distintas guías didácticas que hemos elaborado en el centro y que se pueden descargar desde nuestro blog.

VIDEO 1. ¿Anonimato? Una reunión con la profesora

https://www.youtube.com/embed/TT-t6HNwbts?rel=0

VIDEO 2. ¿Tienes privacidad de verdad en las redes sociales?

https://www.youtube.com/embed/_VAgyuNjnoY

VÍDEO 3. No lo digas por internet

https://www.youtube.com/embed/E3Z6f-KIIQI

VÍDEO 4. Ciberbullying.

https://www.youtube.com/embed/9bgdOuBn4Q4?rel=0

VÍDEO 5. El cartero. Grooming.

Copyright 2026

https://www.youtube.com/embed/jFDkS6qWn9I

VÍDEO 6. El peligro de las redes sociales.

https://www.youtube.com/embed/Ak3qp4qRAiY?rel=0

VÍDEO 7. Seguridad de los niños en las redes sociales.

https://www.youtube.com/embed/tuJG1M0broo?rel=0

VÍDEO 8. Piénsalo antes de publicar algo.

https://www.youtube.com/embed/-L93JZc-Kgo?rel=0

VÍDEO 9. Antes de colgar tu imagen en la web.

https://www.youtube.com/embed/n_q-HJQe4rM?rel=0

Guía didáctica 1. https://alumnosayudantes.files.wordpress.com/2014/05/guia-didactica-uso-redes-sociales.pdf

Guía didáctica 2. https://alumnosayudantes.files.wordpress.com/2015/02/guc3ada-del-vc3addeo-peligros-de-las-redes-sociales-eso.pdf

3. Leemos para reflexionar.

La lectura de noticias, historias o cuentos relacionados con las redes sociales constituye una propuesta didáctica eficaz para sensibilizar a nuestro alumnado sobre el uso adecuado de las redes sociales. Además favorece la reflexión sobre algunas cuestiones que pueden afectar al uso inadecuado de las mismas.

A través del análisis de distintos tipos de textos se trabaja además la competencia en comunicación lingüística. Para ello se han diseñado dos tipos de actividades:

A) El comic de la Patrulla-K. https://alumnosayudantes.files.wordpress.com/2015/03/guc3ada-de-cc3b3mic-la-patrulla-k.pdf

B) Noticias de prensa.

https://alumnosayudantes.files.wordpress.com/2015/03/ciberacoso-a-travc3a9s-de-la-prensa.pdf CIBERACOSO A TRAVÉS DE LA PRENSA: Guía didáctica.

Imputan a dos chicas de 14 y 15 años de Tamarite por amenazar de muerte a otra menor a través de las redes. HERALDO 2018

Imputado un menor en Málaga por distribuir imágenes pornográficas suyas en una red social. SUR 2018

La edad ideal para tener el primer móvil es a partir de los 15 años. ABC 2018

Casi la mitad de los menores abusa de la tecnología. ABC 2018

Un millar de jóvenes daneses, imputados por compartir porno infantil en un chat. EL MUNDO 2018

Decálogo para el buen uso del móvil en niños y adolescentes. VALENCIA NOTICiAS 2017

Adolescentes: La vida en el móvil. EL MUNDO 2017

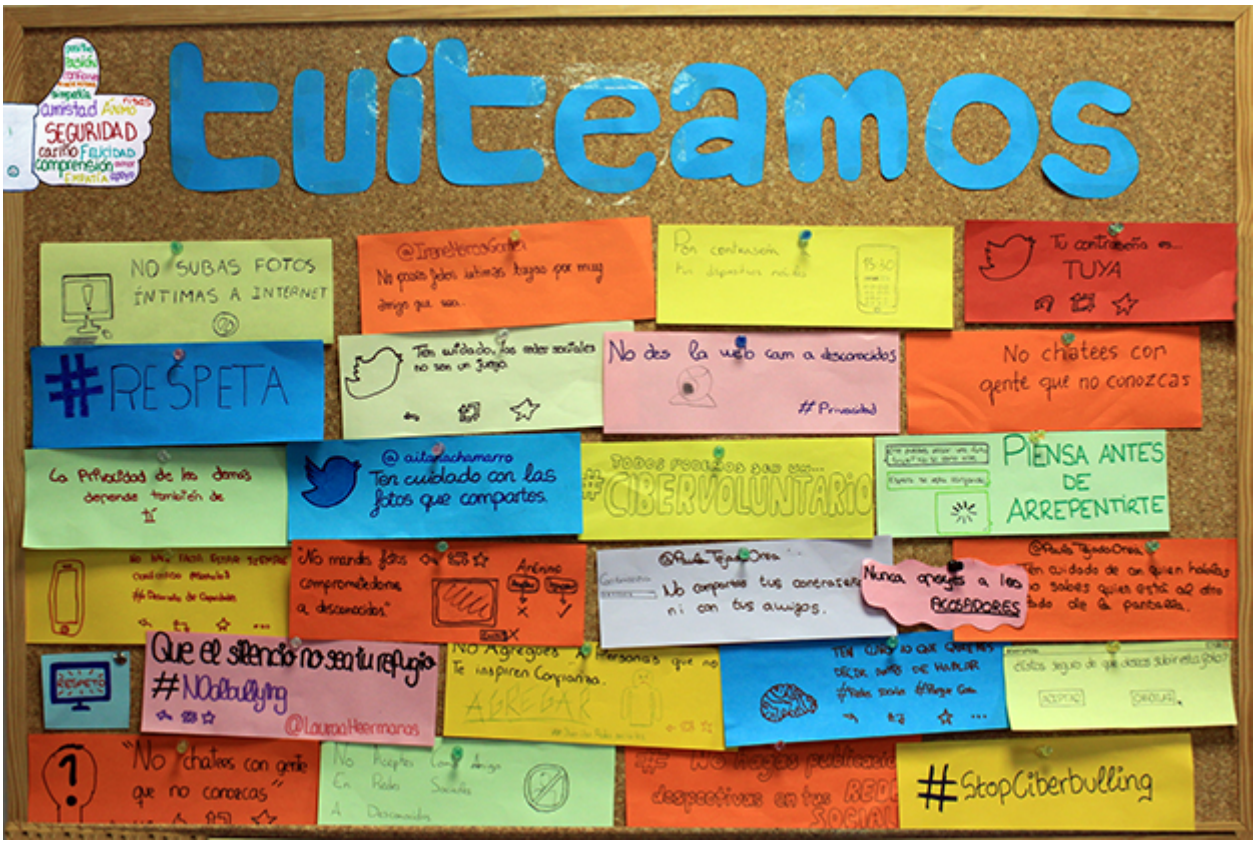
El 21% de los adolescentes españoles están en riesgo de ser adictos a Internet. EL PAIS 2013

La lección de privacidad de una profesora se hace viral. YAHOO 2013

4. Tuiteamos.

Con esta iniciativa simulando a la red social Twitter, queremos fomentar que se haga un uso adecuado de internet. Después de revisar los consejos y decálogos de buenas prácticas en redes sociales de las páginas web recomendadas y que aparecen debajo, los alumnos elaborarán un mural por clase, en el que aportarán mensajes propios en los que se describan normas que hagan de internet un entorno más seguro. Esta actividad podría realizarse paralelamente desde la red social EDMODO para subir los mensajes. Todos ellos serán publicados en nuestro blog. Desde este curso además contamos con una cuenta de Twitter: @iespgoya

Copyright 2026


tuiteamos
NO SUBAS FOTOS ÍNTIMAS A INTERNET
#RESPETA
Ten cuidado con las fotos que compartes
No chatees con gente que no conozcas
PIENSA ANTES DE ARREPENTIRTE
#CIBERVOLUNTARIO
Que el silencio no sea tu refugio
#NObullying
@LauraHermanos
#StopCiberbulling



MI MÓVIL

¿QUÉ PUEDE PASAR SI...

...LO TRAIGO AL INSTITUTO?

PUEDE DESPARECER

Lo pierdo, o alguien se lo lleva...

SE PUEDE ROMPER

Se cae al suelo, al váter, me lo tiran jugando...

PUEDE SONAR

Olvido quitar el sonido y me suena en clase...

NO HABLO CON NADIE

Mirando el móvil se me olvida que tengo gente cerca que busca mi compañía

INCUMPLO NORMAS

Pronto o tarde lo acabo mirando en cualquier sitio

ME PUEDEN SANCIONAR

Si me pillan con él me sancionarán según el reglamento

...LO DEJO EN CASA?

NO DESAPARECE

Cuando vuelva a casa seguro que está donde lo dejé

NO SE ROMPE

Al volver a casa, seguro que funcionará igual que siempre

NUNCA SONARÁ

Llego a casa y tengo un montón de mensajes...

HABLO CON LA GENTE

Me relaciono con todo el mundo cara a cara, sin trampa ni cartón

CUMPLO LA NORMA

Como no está permitido su uso, pues no lo uso

NO ME SANCIONAN

Por este motivo seguro que hoy no me sancionarán

DEJAR EL MÓVIL EN CASA ES LA MEJOR OPCIÓN. SI TIENES QUE LLAMAR A TU FAMILIA, O ELLOS TIENEN QUE NOTIFICARTE ALGO, USAD EL TELÉFONO DEL CENTRO.

NETIQUETA. https://create.piktochart.com/output/29052800-netiqueta

5. Jugamos.

A través de esta iniciativa queremos que nuestro alumnado participe de forma lúdica a partir de dos tipos de juegos.

El primero de ellos es el “Juego del PRIVIAL”. Se trata de un juego on line similar al Trivial sobre el uso de redes sociales que permitirá jugar a los alumnos por parejas o grupos de 4 alumnos y que tiene como finalidad cuidar la privacidad.



El segundo tipo de juego es el KAHOOT! “¿Y tú qué sabes sobre el uso de las redes sociales?” Se trata de un juego de preguntas y respuestas por equipos de cuatro, para realizar utilizando un smartphone o tablet. Buena parte de la preguntas han sido elaboradas por los ciberayudantes..



EDUCAPLAY. La ruleta de las redes sociales.
https://es.educaplay.com/es/recursoseducativos/3555372/html5/la_ruleta_de_redes_sociales.htm#!
QUIZIZZ: Privacidad e identidad digital
https://quizizz.com/admin/quiz/5acddb8c4644110019a2b59f/privacidad-e-identidad-digital

Juego con FLIPQUIZ.

1. Redes sociales 2. TIC 3. Internet

6. Creamos Cibercortos:

Diseño y elaboración de producciones audiovisuales propias. Algunos de los vídeos y animaciones que hemos realizados están publicados en Youtube y se muestran a continuación.

Proyecto Ciberayudantes:

https://www.youtube.com/embed/DKWJ2J9ExBo?rel=0

Andrea y Diana dan su visión del programa.

https://www.youtube.com/embed/QiFxwgIAi_w

Motivos por los que utilizan las rede sociales.

https://www.youtube.com/embed/EHDHoR8YvwY

Escenificación en mediación en redes sociales

https://www.youtube.com/embed/MzESkr4Krzc

1,78 https://goanimate4schools.com/player/embed/08GoB3OI3AH4

Huella digital. https://goanimate4schools.com/player/embed/0OyyyEVbCp_c

“De ayudantes a ciberayudantes”:

https://www.youtube.com/embed/TIjCCr4Jy2c?rel=0

Spot “Me gusta , no me gusta”.

https://www.youtube.com/embed/MgpqtmdUWXQ?rel=0

Animación: “Buenas prácticas de internet”.

https://www.youtube.com/embed/MIdhs2unQfI?rel=0

Animación: “Reglas de oro para uso de internet”

https://www.youtube.com/embed/01yConkn3Bg?rel=0

Spot: “Basta ya de machismos en whatsapp”.

https://www.youtube.com/embed/Qz89d-jNfvg?rel=0

7. Colaboramos con la Familias.

La implicación de las familias es fundamental. Por eso organizamos iniciativas que promuevan el uso adecuado de internet en el hogar. Algunas de ellas son las siguientes:

- Charla informativa a las familias sobre el uso de las redes sociales a cargo de la Policía Nacional dentro del Plan Director.
- Taller formativo sobre el uso de redes sociales para familias realizado por el grupo de convivencia con la participación de los ciberayudantes.
- Elaboración conjunta de folletos que recojan buenas prácticas de internet en familia”.

https://alumnosayudantes.files.wordpress.com/2015/03/triptico-uso-redes-sociales-padres2.pdf

- Grupo de lectura “Leer juntos” de padres y profesores en el que se propone la lectura de dos obras que tratan sobre el uso de redes sociales y adolescente: Pomelo y limón y

Croquetas y whatsapp de la escritora zaragozana Begoña Oro. En ambas historias, leídas también en clase por los alumnos, las familias y los profesores se ponen en la piel de los adolescentes a través de la ficción. Esa visión tan cercana a la realidad les sirve como reflexión del uso que su hijo o alumno puede hacer de un blog o del whatsapp. Aunque es una tertulia literaria y no una escuela de familias, el hecho de que padres e hijos hayan leído las mismas novelas les proporciona la posibilidad de hablar del tema y así compartir lo que cada uno conoce del mismo. Además padres, profesores y alumnos asisten en diferentes momentos al encuentro con la autora, un motivo más de acercamiento y de complicidad de nuestra comunidad educativa y un posterior encuentro con la autora.



8. Creamos equipo de Ciberayudantes. Formación de los futuros ciberayudantes a través de la red social educativa Edmodo.

Uno de los aspectos clave del programa es la formación de un equipo de Ciberayudantes. Todos ellos tienen experiencia como alumnos ayudantes.

- Queremos destacar que su rol tiene una **doble función**: **Ayudar , asesorar, detectar** situaciones de riesgo y mediar entre alumnos más pequeños por un lado. Y por otro lado **informar** directamente a través de charlas sobre temas de ciberseguridad, partiendo de la base que su incidencia entre el alumnado tiene mayor calado que si viene de los adultos.
- Pero ¿Cuáles son los temas más importantes que se abordan en esta formación?

- PRIVACIDAD e IDENTIDAD DIGITAL : Datos personales, derecho a la imagen, configuración de perfil, contactos,..
- REPUTACIÓN DIGITAL Y RESPONSABILIDAD PENAL.
- REDES SOCIALES PAUTAS Y NORMAS DE CONDUCTA. NETIQUETA

Creemos necesaria la participación del alumnado en el desarrollo de este proyecto en colaboración con los tutores. Al menos han dedicado una sesión a modo de charla con el resto de los alumnos, para comentarles sobre algunos consejos, pautas y normas de utilización de las TIC y más concretamente en el uso de las redes sociales, tomando como referencia los contenidos relativos a la privacidad, uso de contraseñas, webcam, configuración de perfil, acceso a contenidos inadecuados, envío de comentarios e imágenes,...

Consultamos al correo de ciberayudantes@iesparquegoya.es. Espacio de consultas de los alumnos cuando tengan problemas con el uso de las redes sociales.

CASO PRÁCTICO. Gestión de la identidad. Mediación de ciberayudantes.

Ya hemos visto cómo gestionar la privacidad e identidad digital. A continuación vamos a verlo de una manera práctica, a través de algunos casos prácticos, que nos van a permitir prevenir, detectar y actuar ante un caso de este tipo.

Mario es un chico de 15 años que, como casi todos los adolescentes en la actualidad, mantiene una relación continua con las nuevas tecnologías: utiliza redes sociales de forma diaria para contactar con sus amigos y con grupos con los que se siente identificado, interactuando normalmente con el mundo virtual tanto con personas conocidas como desconocidas.

Actualmente cursa tercero de ESO y, aunque es buen estudiante, ha sido acusado por una compañera Marta por haber subido una foto a Instagram en la que ella aparecía fumando con sus amigos. Se siente molesta y ahora ella va vertiendo a través de las redes comentarios despectivos sobre Mario.

Al día siguiente de que se publicaran estos comentarios, Andrea, una alumna ciberayudante ha recibido dichos comentarios por un grupo de Whatsapp . Lo ha comentado con otra ciberayudante Diana y están dispuestas a mediar entre los dos.

Andrea, una buena amiga de Mario, habla con él en la hora del recreo.

-Mario tío, no veas la que has liado. ¡Se te ha ido la olla! Todo el mundo ha visto la foto de Marta fumando, y ya sabes que a ella no le gusta que se suban fotos suyas fumando. Además, acaba de dejarlo hace unos días. -Bah, me da igual... Ella siempre está chuleándose con el cigarrillo. Va de más guay. Y encima cuando se encuentra conmigo, me echa el humo a la cara. Así que no me arrepiento... -Quizá ahora no te arrepientas pero...¿no has pensado que esto puede traerte

consecuencias? -Si, ya lo sé. Va subiendo comentarios sobre mi persona que nos son ciertos y si sigue así, pienso denunciarla. Al fin y al cabo yo solo he subido una foto suya fumando. -Claro, pero lo has hecho sin su consentimiento. ¿Quieres que hable con ella para ver qué solución podemos dar?

En el segundo recreo Andrea y Diana se reúnen con Mario y Marta, para tratar de llegar a un acuerdo.

-Hola chicos. Queríamos hablar un momento con vosotros porque hemos vista la foto que tú has subido y hemos leído los comentarios que Marta has compartido por whatsapp. -Estoy seguro de que escribiste todo aquello porque estabas enfadada pero tienes que comprender que no ha sido la mejor forma para demostrarlo. -Todo lo que publicamos en la red influye en la imagen que damos a los demás, en nuestra reputación… ¿eres consciente de que esto puede afectarte de forma negativa? -Puff… yo que se… estaba muy cabreado… tenía que haberme relajado antes de subir nada. -Si…ahora no podemos volver atrás, pero espero que puedas aprender de esta experiencia… Todo tiene consecuencias . -Y tú Marta, ¿crees que con los comentarios que has publicado es la mejor manera de resolver tu conflicto con Mario? -Supongo que los comentarios que he hecho no son muy afortunados, pero lo que ha hecho Mario no tiene desperdicio.

VER MÁS INFORMACIÓN ACTUALIZADA DESDE EL BLOG

7.7 Criterios y herramientas de evaluación.

CRITERIOS Y HERRAMIENTAS DE EVALUACIÓN

Con carácter general y al final del desarrollo del proyecto se realizará su evaluación. **Por parte de los alumnos:**

A final de curso los alumnos rellenarán un cuestionario sobre el estado de convivencia del centro en que se incluyen cuestiones para valorar el proyecto y el grado de utilidad que ha tenido para ellos

Los alumnos ciberayudantes rellenarán un cuestionario específico que servirá exclusivamente para valorar el proyecto y el grado de utilidad que ha tenido para ellos. **Por parte de los profesores.**

El equipo docente del centro cumplimentará un cuestionario sobre el estado de convivencia del centro a final de curso donde constará una parte específica relativa a la valoración del proyecto, otra relativa a los aspectos que han mejorado la convivencia y una última relativa a las propuestas de mejora.

Los tutores cumplimentarán un cuestionario específico que servirá exclusivamente para valorar el proyecto y el grado de utilidad, así como para aportar propuestas de mejora.

Por parte de las familias. Las familias del centro cumplimentarán un cuestionario sobre el estado de convivencia del centro a final de curso donde constará una parte específica relativa a la valoración del proyecto y otra relativa a los aspectos que han mejorado la convivencia

Procedimientos e instrumentos de valoración. Después de algunos años de la puesta en marcha de estos programas de convivencia, creemos necesario comprobar el grado de eficacia de los mismos. Para ello nos hemos servido de algunos procedimientos y herramientas. Somos conscientes que puedan adolecer de la eficacia y fiabilidad que nosotros hubiéramos deseado. No somos especialistas pero nos servimos de algunos cuestionarios que desde el centro se han elaborado para tener un diagnóstico del estado de la convivencia del centro, que nos facilitara la puesta en marcha de las iniciativas que hemos señalado anteriormente. Algunos de los procedimientos e instrumento utilizados son los siguientes.

Copyright 2026

- Cuestionarios estado convivencia
- Seguimiento de la convivencia
- Cuestionario redes sociales
- Cuestionarios ayudantes y ciberayudantes
- Observatorios de niveles sobre la convivencia.

Cursos que el proyecto lleva en ejecución y continuidad

El proyecto de Ciberayudantes se **inició en el curso 2013-2014**, a partir de la iniciativa propuesta por el programa Pantallas Sanas sobre cibervoluntariado. Dirigida a toda la comunidad educativa. Pantallas Sanas es una iniciativa de Cine y Salud, donde se aborda la fenomenología de las pantallas y las nuevas tecnologías desde el punto de vista de la promoción de la salud, con el objeto de abordar aspectos que van desde los hábitos y la sociabilidad a los consumos y las adicciones en el uso de las Tecnologías de la Información y el Conocimiento.

Durante el pasado curso se realizó la fase de detección de necesidades surgidas en las juntas de evaluación y en las reuniones de tutores, como consecuencia de un uso inadecuado de las redes sociales por parte de nuestro alumnado. Se acordó desarrollar medidas de carácter preventivo desde la tutoría con la finalidad de hacer de internet un entorno saludable y seguro.

Aprovechando la existencia en nuestro centro del programa de Alumnos Ayudantes, que lleva funcionando desde el curso 2011-2012, y del que forman parte 35 alumnos del centro que han recibido formación específica, hemos querido buscar su implicación en el proyecto de Ciberayudantes. También hemos contado con la colaboración de profesores y alumnos del programa de desarrollo de capacidades, de psicología de 1º de Bachillerato y con los tutores y alumnos de 1º y 2º de ESO.

Por otro lado venimos desarrollando desde la apertura del centro el Programa de EL CINE COMO HERRAMIENTA DE EDUCACIÓN PARA LA SALUD, organizado por el Gobierno de Aragón, desde la Dirección General de Salud Pública y la Dirección General de Política Educativa y Educación Permanente. El Programa Cine y Salud tiene por objeto tratar desde el cine la prevención de los problemas de salud más relevantes en la adolescencia. Ha supuesto un gran impulso el Primer Premio Cibervoluntariado por unas Pantallas Sanas 2014, concedido por el Departamento de Salud del Gobierno de Aragón dentro del programa Cine y Salud al proyecto Ciberayudantes de nuestro centro. Gracias a él hemos podido desarrollar nuevas propuestas didácticas que han dado continuidad durante el presente curso.

Se espera que el proyecto continúe a través de la formación de futuros alumnos ayudantes que serán además ciberayudantes en próximas convocatorias. Estas iniciativas se incluirán en el Plan de Acción Tutorial en todos los niveles de secundaria, pero especialmente en 1º y 2º. Además se han realizado actividades tutoriales de nuestros ciberayudantes con los alumnos de 6º de primaria del CEIP Agustina de Aragón, CEIP Catalina de Aragón y CEIP Parque Goya durante lops dos últimos

cursos.

Copyright 2026

7.8 Resultados y conclusiones

RESULTADOS Y CONCLUSIONES

A partir de los resultados obtenidos en los diferentes cuestionarios y su posterior análisis sobre el estado de la convivencia en el centro, disponemos de una mayor información sobre conflictos generados desde las redes sociales.

Por este motivo, decidimos crear un observatorio para conocer específicamente el uso que hacen nuestros alumnos de internet. Los resultados de este cuestionario realizado por los alumnos de 1º de ESO están disponibles en el blog de alumnos ayudantes.
http://alumnosayudantes.wordpress.com/

Con los datos obtenidos en los cuestionarios cumplimentados por los alumnos de 1º, podríamos hacer un **retrato robot a modo de diagnóstico de un alumno de 1º de ESO recién llegado** al instituto sobre el uso que hace del móvil y de las redes sociales. Los resultados son muy similares del año 2014 y 2016.

- Se trata de un alumno que se ha registrado con menos de 11 años a un RS con permiso de los padres (82%).
- Utiliza mayormente whatsapp, youtube e Instagram.
- En Snapchat se incorporan después.
- Facilitan muchos de sus datos personales incluido correo y teléfono.
- Pasan un promedio de más de 5 horas conectados a la semana.
- Utilizan las RRSS principalmente para chatear, mantenerse en contacto con otros, ver vídeos y fotos y para temas de estudios.
- Desconocen la existencia de buena parte de los riesgos que acompañan al uso de las redes sociales.

Comparativamente **los datos de los cuestionarios cumplimentados por los mismos alumnos en 3º de ESO en 2016 reflejan algunas diferencias**. Hay que tener en cuenta, que un tercio son alumnos nuevos o repetidores.

Copyright 2026

- Algunos datos como el intento de robo de datos personales (8) se mantienen en porcentajes similares, pero han aumentado las propuestas sexuales no deseadas (6- 21). Entendemos que son alumnos mayores que han ampliado sus contactos con desconocidos (19- 36) y por tanto están asumiendo más riesgos.
- Sin embargo disponen de menos cuentan falsas (19-14) y dicen tener un mejor control de la información (86-92) que introducen. Ha disminuido el porcentaje tanto de alumnos que insulta y amenaza (13-12), como el que los recibe (26-22)
- Nos alegra saber que ha subido el porcentaje de los alumnos que están dispuestos a ayuda a alguien acosado en la red. (35-41)
- Finalmente y en relación al conocimiento que tienen de los riesgos, el ciberbullying (53-83) es un término que ya es conocido de forma generalizada, pero aun confunden lo que es el sexting (37-50) y el grooming,(15-22) aunque para muchos sobre todo el término sexting es conocido. Cosa que también ocurre con los adultos.

Un programa de estas características debe de contar necesariamente con la valoración que hacen los propios protagonistas para poder medir sus beneficios. Su opinión es muy importante para conocer las claves de su eficacia en el centro y creemos estar en el buen camino.

A continuación os vamos a mostrar lo piensan los propios ciberayudantes, aquellos que tienen más experiencia y que están en cursos superiores.

- La gran mayoría cree que **figura del alumno ayudante y ciberayudante** es conocida en la comunidad educativa.

Manifiestan que **han intervenido entre 1 y 5 casos en un año.**

*El tipo de casos en los que han intervenido están relacionados con el acoso, con discusiones, sexting, conflictos, ciberacoso, burlas, insultos y personas aisladas**. Les resultaron más difíciles de intervenir cuando se involucraba gente de fuera o cuando los chicos tenían problemas personales.

- En relación a los problemas producido en el último año relacionados con el uso de la TICs, piensan que se producen entre muchas y bastantes veces los siguientes:

| Problema | Porcentaje | |--||--| |Acceso a contenidos inadecuados o ilícitos|33%| |Intercambio de imágenes con contenido sexual|16%| |Insultos y amenazas|67%| |Contactos con adultos que han fingido la edad|12%| |Amenazas a la privacidad: robo, publicación y difusión de datos personales|33%| |Tecnoadicciones|50%| |Ciberbullying|28%|

- Muchos de ellos consideran suficiente la **formación recibida** y se sienten implicados y comprometidos.
- Gran parte de ellos no ha encontrado **dificultades en sus intervenciones y se sienten valorados** por sus compañeros, por sus profesores y por sus familias.

Copyright 2026

- Para el 87% de los ciberayudantes **la convivencia en el centro ha mejorado** entre bastante y mucho.

CONCLUSIONES FINALES

1. **Disminución de las situaciones que dañan la convivencia**. Gracias a estos programas de convivencia se han reducido las situaciones que dañan la convivencia en el centro tal y como los datos mostrados anteriormente.
2. **Cultura del diálogo y mayor interés del alumnado**. Estas actuaciones están generando una cultura del dialogo y de la ayuda entre iguales. No en vano hay un 10% de alumnos ayudantes y cada vez es mayor el interés mostrado por el alumno en participar en el programa de Alumnos ayudantes. Unos 60 alumnos forman parte de él (casi un 10% del total).
3. **Detección y reducción de comportamiento de riesgo**. Aunque seguimos observando comportamiento de riesgo, tales como insultos y amenazas, gracias a estos programas tenemos más capacidad para detectarlos y para evitar que estos se extiendan.
4. **Implantación de las actuaciones en la Acción tutorial**. Estamos consiguiendo que la formación en educación emocional se vaya incorporando a las sesiones de tutoría.
5. **Implicación de las familias**. A través del Consejo escolar, el Ampa, comisión convivencia, las charlas a padres,.. estamos implicando a las familias.
6. **Mayor implicación y participación del alumnado.** Uno de los objetivos prioritarios del programa de ayudantes y ciberayudantes era dar más protagonismo al alumnado. Estamos satisfechos por la implicación, la participación y compromiso de todos ellos. en las decisiones que se tomen en la relación con la convivencia.
7. V**isibilización de las actuaciones**. En relación a este punto creemos que estos programas son suficientemente conocidos por la comunidad educativa, pero también ha tenido una repercusión mediática. Nosotros seguimos apostando por incorporar nuevas iniciativas en las que estamos trabajando, tales como la elaboración de animaciones y videojuegos relacionados con el uso de las redes sociales, y próximamente publicaremos un corto sobre estos programas con el fin de promocionarlos y al que os invitamos a visionar en cuanto se publique.

Copyright 2026

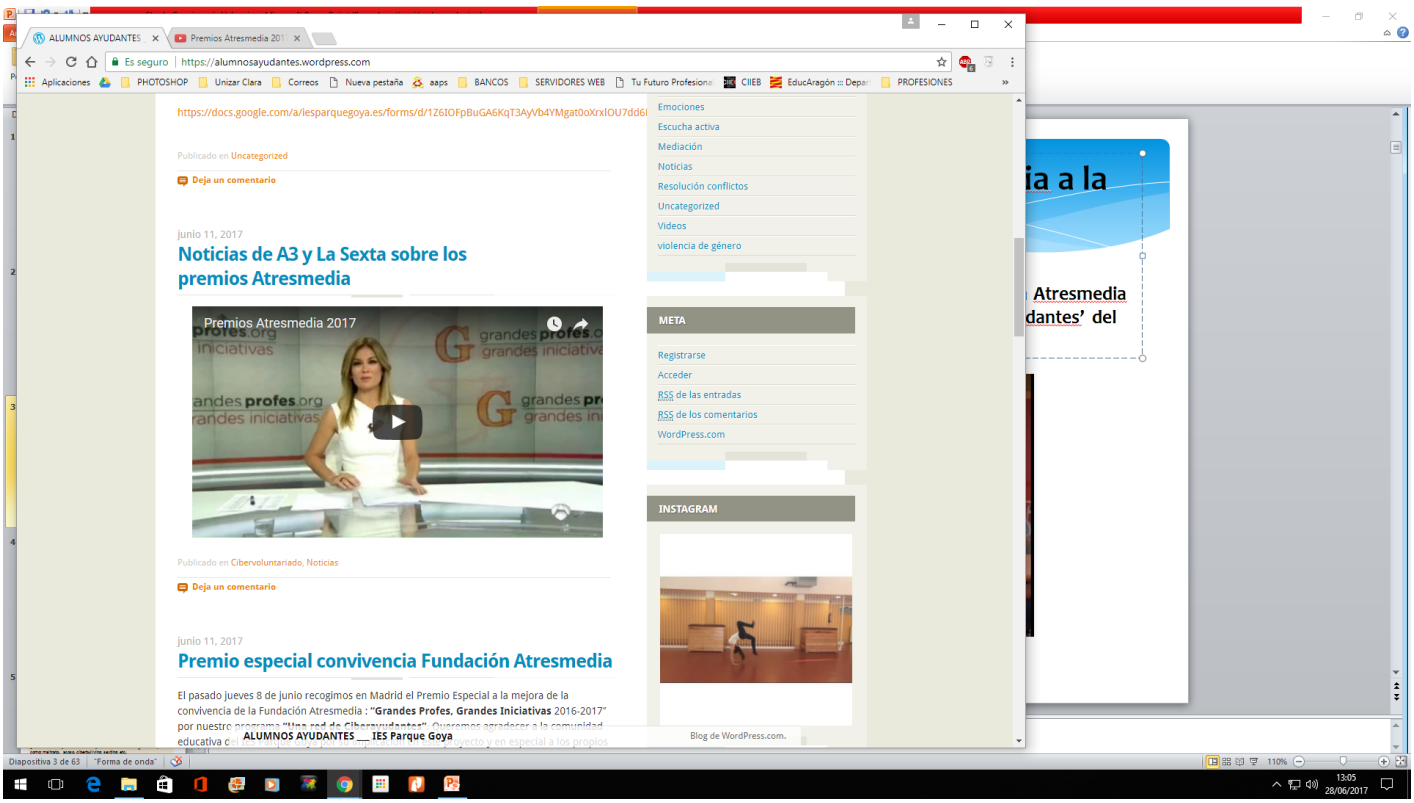
7. Ciberayudantes: Un programa de centro

7.9 Repercusión en medios de comunicación.

REPERCUSIÓN MEDIOS DE COMUNICACIÓN

Premio Especial Fundación Atresmedia a la ‘Mejora de la Convivencia Escolar’. Junio 2017 La iniciativa ganadora en la categoría de Premio Especial Fundación Atresmedia a la ‘Mejora de la Convivencia Escolar’ ha sido ‘Una red de ciberayudantes’ del IES Parque Goya de Zaragoza.

http://fundacion.atresmedia.com/actividades/educacion/grandes-iniciativas/premio-especial-fundacion-atresmedia-%E2%80%98mejora-convivencia-escolar%E2%80%99_2017061200520.html





Copyright 2026

Glosario

Copyright 2026

Glosario

Glosario y recursos

GLOSARIO

Acosador. Menor o menores que instigan o acosan de forma reiterada a otro menor.

Acoso escolar o bullying. Continuado y deliberado maltrato verbal, físico O psicológico que recibe un niño/a por parte de otro u otros menores.

Android. Sistema operativo diseñado principalmente para dispositivos móviles.

Antivirus. Aplicación cuya finalidad es la detección, bloqueo y eliminación de virus informáticos y otros códigos maliciosos.

App. Abreviatura de Aplicación. Esta abreviatura está muy extendida en el argot actual de los dispositivos móviles.

Banner. Anuncio gráfico que aparece en determinadas direcciones web, caracterizado por contener imágenes que buscan un impacto visual.

Bloqueo En el contexto de Internet: forma de impedir el acceso a un tipo de información determinada: una web, un mensaje de correo, un tipo de servicio, etc.

Ciberbullying. Daño intencional y repetido infligido por parte de un menor o grupo de menores hacia otro menor mediante el uso de medios digitales.

Cortafuego. Pasarela que limita el acceso a y desde una red según unas determinadas directrices de seguridad. En Internet es el programa o dispositivo hardware que nos protege de accesos no autorizados a nuestro ordenador a la vez que evita que se envíen datos a Internet sin nuestro permiso.

Contenidos falsos. Informaciones erróneas o falsas, inapropiadas para el menor, que circulan por Internet y llegan fácilmente a un gran número de receptores debido a la naturaleza del contenido y la tendencia a propagarse rápidamente.

Contenido inapropiado. Material percibido por el menor de edad que sea dañino para él. Son las imágenes y estímulos que provocan un perjuicio en el menor; peligros que circulan por la Red, y las características de la información que contienen.

Copyright 2026

Control parental. Herramienta informática personalizada para filtrar e impedir que los usuarios menores de edad puedan acceder a determinadas páginas Web con contenidos inapropiados.

Consentimiento. Manifestación libre y expresa por la que un titular autoriza el tratamiento de sus datos personales o las de un menor a su cargo.

Ciberbullying. Fenómeno por el que un menor es amenazado, acosado, avergonzado u hostigado por otro menor, a través de internet o dispositivos móviles.

Contraseña. Cadena de caracteres que identifican a un usuario determinado.

Datos personales. Información de cualquier tipo referida a una persona física.

Dirección IP. Identificador de un ordenador o dispositivo en una red.

Droga. Cualquier sustancia introducida en el organismo que provoca una alteración del funcionamiento natural y del sistema nervioso, lo que conlleva un riesgo para la salud física y psicológica.

Espectador. Sujetos pasivos que de forma indirecta están presentes en una situación de ciberacoso, bien alentando al acosador, o permaneciendo impasibles ante dicha situación.

Etiquetar. Nombrar públicamente a un amigo que aparece en una foto, vídeo o comentario de una red social de pertenencia. El etiquetado consiste en colocar el nombre del contacto sobre el contenido en que aparezca, generando de esa forma un link directo con su cuenta personal de esa red social.

Eyeballing. Reto viral que consiste en la introducción de alcohol de alta graduación en la córnea como si fuese un colirio, con la finalidad de provocar una borrachera con mayor rapidez. Esta práctica puede causar lesiones graves en la vista...

Groomer. Fenómeno a través del cual un adulto contacto con un menor por la red con el objeto de establecer una relación erótica o/y sexual.

Geolocalización. Aplicación que permite, desde cualquier dispositivo conectado a la red, obtener información acerca de la localización real de una persona.

Grooming. Conjunto de técnicas de engaño y persuasión que utiliza un adulto para ganarse la confianza y disminuir las inhibiciones del menor y obtener de él un beneficio de índole sexual, que es la finalidad que persigue.

IOS. Sistema operativo de Apple diseñado originalmente para iPhone, iPad, iPod y Apple TV.

Copyright 2026

Ingeniería Social. Consiste en obtener información de los usuarios a través de engaños y manipulaciones, por ejemplo, simulando una llamada o un correo electrónico desde nuestro banco, para conseguir las claves de acceso a la cuenta.

Juegos de azar. Juegos de apuestas donde la búsqueda de beneficio económico trae consigo el riesgo de ser engañado, o de perder cantidades considerables de dinero. Se basan en modelos de 'captación', ofreciendo a los jugadores atractivos premios a cambio de juegos y apuestas sencillas.

Leyendas urbanas. Historias extravagantes pero verosímiles, que supuestamente han ocurrido, dadas siempre como verdaderas.

Market. Sitio web y tienda online donde se pueden adquirir aplicaciones y juegos para dispositivos móviles.

Mensajes en cadena. Tipos de correo basura cuyo fin es la propagación, fraude y/o coacción de alguna manera a los receptores para que los reenvíen a otro grupo de personas.

Mensajería instantánea. Programas que permiten conversar de forma online (chatear), o enviar mensajes cuando no se está conectado a la vez, de persona a persona o en grupos.

Netiqueta. Conjunto de normas y reglas de comportamiento de un usuario dentro del contexto de Internet: listas de correo, foros, correo electrónico, redes sociales, etc.

Oxy-shots. Reto viral que consiste en inhalar chupitos de alcohol a través de un sistema de inhalación como los asmáticos, para absorber el alcohol más velozmente por vía aérea. Esta práctica puede dañar el sistema nervioso y provocar patologías pulmonares graves.

Página web. Documento o información electrónica que contiene texto, sonido, vídeo, programas, enlaces, imágenes etc. al que puede accederse mediante un navegador.

PEGI. Pan European Game Information es un sistema europeo para clasificar el contenido de los videojuegos y otro tipo de software de entretenimiento.

Perfil. Es la identidad que una persona tiene en una red social.

Perfil de usuario. Conjunto de datos, incluidos aquellos de carácter personal, que los usuarios de la red introducen en el momento de su registro en alguna web o red social.

Pop-up. Ventana emergente que suele mostrarse en una web sin que el usuario lo haya solicitado.

Pornografía. Obras que contienen imágenes sexuales explícitas con el fin de provocar la excitación del receptor, no adecuadas para menores de edad, y cuyo acceso está prohibido por la Ley.

Copyright 2026

Privacidad. Control de la información que posee un determinado usuario que se conecta a Internet, interactuando por medio de diversos servicios en línea con los que intercambia datos durante la navegación.

Red. Grupo de dispositivos informáticos conectados entre sí a través de línea telefónica o cable con el objetivo de comunicarse y compartir recursos. Internet es una inmensa red.

Red Social. Sitio web que ofrece una serie de funcionalidades y servicios de comunicación que permiten mantener el contacto con otros usuarios pertenecientes a la misma red.

Seguridad informática. Disciplina que integra diversas técnicas, dispositivos y herramientas con el objeto de asegurar la integridad y privacidad de la información integrada en un sistema informático.

Sexting. Envío de contenidos de tipo sexual (principalmente fotografías y/o vídeos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles.

Spam. Correo no deseado o información no deseada que se suele recibir por correo electrónico.

Spyware. “Software espía”. Se trata de una aplicación informática que roba información valiosa de un equipo informático, sin consentimiento ni conocimiento del usuario, vulnerando de este modo su privacidad.

Troyano. Aplicación informática con aspecto de ser inofensiva y útil, pero que tras su instalación realiza diferentes acciones que afectan a la privacidad y confidencialidad del usuario afectado.

Víctima. Menor que sufre los abusos, amenazas o extorsiones por parte de otro u otros menores.

Violencia. Empleo intencional de la fuerza o poder físico que pueda causar daños físicos o psicológicos. Son todas las acciones que son el resultado de una relación de poder, incluidas las amenazas o la intimidación.

Viral. Grabaciones difundidas a una enorme cantidad de personas, y compartidas a través de la Red. Se plantean como retos o desafíos en cadena, y su contenido varía enormemente, lo cual supone también un riesgo potencial para la población menor de edad.

Web. Red informática mundial que distribuye documentos de hipertexto o hiper-medios interconectados y accesibles vía Internet.

Web-Cam. Cámara de fotos y de grabación que se conecta al PC

WEBGRAFÍA Y RECURSOS COMPLEMENTARIOS

Copyright 2026

Chaval.es. es un portal web de referencia centrado en el buen uso de las TIC (Tecnologías de la Información y la Comunicación); perteneciente a Red.es (Ministerio de Industria, Energía y Turismo). http://www.chaval.es/chavales/

Pantallas Amigas. Iniciativa que tiene como misión la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia. Algunas de sus actividades principales son la creación de recursos didácticos, sesiones y jornadas formativas y estudios, con especial énfasis en la prevención del ciberbullying, el grooming, el sexting, la sextorsión y la protección de la privacidad en las redes sociales. http://www.pantallasamigas.net/

Oficina de Seguridad del Internauta. https://www.osi.es/

Portal web Sexting . http://www.sexting.es/

Portal web Sextorsión. http://www.sextorsion.es/

Guía para usuarios sobre identidad digital y reputación online (INTECO). http://www.incibe.es/

Cuida tu imagen online. http://www.cuidatuimagenonline.com/

Protección de la privacidad. http://www.proteccionprivacidad.com/

Red.es. es una entidad pública empresarial adscrita al Ministerio de Industria, Energía y Turismo (MINETUR), que desarrolla un extenso conjunto de programas para que la sociedad española se beneficie al máximo de las posibilidades que ofrecen las Tecnologías de la Información y la Comunicación (TIC). www.red.es

Ciberbullying.com. Portal web especializado en ciberbullying que ofrece información, recursos, consejos, bibliografía, casos, etc. Este portal forma parte de The School Safety Net proyect, financiado por la Comisión Europea en el marco del Programa de Aprendizaje Permanente. www.ciberbullying.com

Guía ciberbullying: prevenir y actuar. Guía de recursos didácticos para centros educativos, relacionados con el ciberbullying elaborada por el Colegio Oficial de Psicólogos de Madrid, en colaboración con la Fundación Atresmedia.http://www.copmadrid.org/webcopm/recursos/Cib

Copyright 2026

Guía de actuación contra el ciberacoso para padres y educadores. Guía completa publicada por el Instituto Nacional de Tecnologías de la Comunicación (INTECO), donde se ofrecen recomendaciones para padres y educadores sobre cómo prevenir y actuar ante el ciberacoso.

http://xuventude.xunta.es/uploads/Gua_de_actuacin_contra_el_ciberacoso.pdf

EMICI (Protocolo de actuación escolar ante el ciberbullying). Protocolo de actuación escolar ante el ciberbullying desarrollado por el Equipo Multidisciplinar de Investigación sobre ciberbullying: http://stopcyberbullying.org

Stop Ciberbullying. Tutorial sobre la detección e intervención en casos de ciberbullying:

http://www.savethechildren.es/

Portal especializado en ciberbullying. Portal web que nos ofrece directrices e información sobre ciberbullying, para abordarlo por edades, vídeos, artículos, etc. Ofrece un espacio para preguntas y dudas sobre el riesgo, ofreciendo asesoramiento, recursos escolares, orientaciones para padres y expertos. https://www.commonsensemedia.org/

Simulador de privacidad. http://www.simuladordeprivacidad.com/

e-Legales. http://www.e-legales.net/

Oficina de Seguridad del Internauta (OSI).

http://www.osi.es/es/reporte-de-fraude/formulario-de-alta-de-incidentes-generales

Grupo de Delitos Telemáticos (GDT) http://www.gdt.guardiacivil.es/webgdt/pinformar.php

Brigada de Investigación Tecnológica (BIT) : delitos.tecnologicos@policia.es

Grupo de Delitos Telemáticos Guardia Civil: www.gdt.guardiacivil.es/webgdt/pinformar.php

Brigada de Investigación Tecnológica Policía Nacional: delitos.tecnologicos@policia.es

Blog de Seguridad en Internet y Protección de menores: www.elblogdeangelucho.com

Cómo funciona un antivirus: www.youtube.com/watch?v=xZECq69Um2A#t=249

Copyright 2026

Blog con información sobre las estafas relacionadas con envío de mensajes SMS Premium

www.afectadosporlospremium.com

Stop Grooming! Blog puesto en marcha por PantallasAmigas.net cuyo objeto es informar sobre el fenómeno del grooming. stopgrooming.wordpress.com

Educared. Programa de la comunidad educativa gestionado y dirigido por la Fundación Telefónica con una amplia gama de recursos para los docentes.

www.educared.net/asp/global/portada.asp

Guía de recursos didácticos para docentes. La web Formación del Profesorado es un servidor que pertenece al Centro de Información y Comunicación Educativa (CNICE). Entre otros servicios ofrece material didáctico con el que el profesorado planifique sus clases en función de los objetivos y necesidades de aprendizaje propias del aula.

http://www.formacion.pntic.mec.es/

Guía de recursos para navegación segura, y protección del menor. Web del Ministerio de Ciencia y Tecnología cuyo objetivo es suministrar información necesaria para conseguir que los niños estén protegidos frente a contenidos y contactos nocivos en el uso de Internet.

http://www.navegacionsegura.es/red/indexintro.ph

Guía para padres e hijos con documentos y recursos para uso responsable de TIC. En esta página ofrecen recursos y consejos a padres e hijos para un uso responsable de las TIC, documentos didácticos útiles para prevenir los riesgos en la utilización de la Red, juegos y actividades para enseñar el manejo tecnológico a través del entretenimiento, y otras herramientas para una aproximación correcta a las nuevas TIC.

http://www.hijosdigitales.es/2014/06/cuales-son-los-contenidos-inapropiados-mas-demandados-por-los-menores/

ORGANISMOS Y ENTIDADES DE REFERENCIA

Portal del Ciudadanos. Comunidad de Madrid. Portal del Ciudadanos. Comunidad de Madrid (Servicios al Ciudadano; Menores y Tecnologías): www.madrid.org

Copyright 2026

Asociación dedicada a la seguridad infantil en Childnet International. La misión de esta asociación sin ánimo de lucro es trabajar y orientar a los niños, adolescentes y los padres en el uso de las TIC, previniendo posibles adicciones y consecuencias nocivas de un mal uso de las tecnologías. www.childnet.com

tecnoadicciones.com: Portal especializado donde se ofrece ayuda e información sobre las adicciones a las nuevas tecnologías. www.tecnoadicciones.com.

Estudio de EU Kids Online. Estudio del 2011 de EU Kids Online (financiado por la CE).

www.lse.ac.uk/

Video Game Addiction. Portal especializado en la adicción a los videojuegos. Ofrece información sobre los síntomas, señales de alerta, consecuencias psicológicas y sociales, tratamiento adecuado, además de varios artículos informativos de la materia.

www.video-game-addiction.org/

Centro de seguridad en Internet. Dossier informativo (Marzo 2012-Junio 2014). Centro de seguridad en Internet.

www.centroInternetsegura.es/descargas

www.guiavideojuegos.es

Time to Change. Campaña para cambiar el estigma de la salud metal y la discriminación en la que se puede encontrar indicaciones sobre cómo enfocar el tema del suicidio y la autolesión con responsabilidad para evitar un comportamiento imitador (en inglés).

www.time-to-change.org.uk

BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.Guía sobre el uso de las Cookies.

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

Guía sobre seguridad y privacidad de las herramientas de geolocalización. Observatorio de la Seguridad de la Información.

https://radiosyculturalibre.com.ar/biblioteca/INFOSEC/guia_sobre_seguridad_y_privacidad_de_las_herramientas_de_geolocalizacion.pdf

Instituto Nacional de Tecnologías de la Información INTECO. (2012). Guía para usuarios: identidad digital y reputación online.

http://www.albacetejoven.es/archivos/uploads/guia_identidad_reputacion_usuarios_INTECO.pdf

Report: Teens and Mobile Apps Privacy (2013).
http://blogs.law.harvard.edu/youthandmediaalpha/projects/online-privacy/new-report-teens-and-mobile-apps-privacy/

Sección española del proyecto EU Kids online. (2011). Informe EU Kids online.

http://www.ehu.es/es/web/eukidsonline

Internet en la vida de nuestros hijos. Fernando García 2010

http://www.bibliotecaspublicas.es/villanuevadelpardillo/imagenes/Internet-en-la-vida-de-nuestros-hijos.pdf

JORGE TOLSA 2012.Los menores y el mercado de las pantallas: una propuesta de conocimiento integrado. http://www.revistacomunicar.com/pdf/2012-03-menores-mercados.pdf

ELVIRA MIFSUD. (2012). Introducción a la seguridad informática. Seguridad de la información/Seguridad informática. Creative Commons.
http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?format=pdf

BONNAFONT, G. (1992). Video games and the child. Paper presented at Myths and Realities of Play Seminar. London." Libro en el que se explica todo lo relacionado con los videojuegos, la niñez y la adolescencia. Habla de los mitos y las realidades existentes referentes a esta temática.

HOLLOWAY,D., GREEN, L. Y LIVINGSTONE, S. (2013). Zero to eight. Young children and their internet use. LSE, London: EU Kids Online.

http://www.open.edu/openlearn/ocw/pluginfile.php/559256/mod_resource/content/3/Zero%20to%20Eight.pdf

Copyright 2026

RODRIGO RON, ANTÓN ÁLVAREZ, FÉLIX MUÑOZ. "Niños, adolescentes y redes sociales. ¿Conectados o atrapados?" ESIC 2013

JOSÉ MANUEL PÉREZ TORNERO Y SANTIAGO TEJEDOR (EDS.). "Guía de tecnología, comunicación y educación para profesores" UOC. 2014

GUILLERMO CÁNOVAS. (2014). "Cariño, he conectado a los niños. " e-book . 2014

FERNANDO GARCÍA FERNÁNDEZ ."Las redes sociales en la vida de tus hij@s Cómo conseguir que se relacionen on-line de forma segura y responsable." 2010

VIDEOS DE INTERÉS

Acceso a redes sociales. Guillermo Cánovas

https://www.youtube.com/watch?v=3-u4jX35BTA

Dispositivos móviles. Guillermo Cánovas

https://www.youtube.com/watch?v=07eliJWVO6I

La adicción a las nuevas tecnologías. Guillermo Cánovas

https://www.youtube.com/watch?v=vCAy0Ql_Mbs

Más confianza. Guillermo Cánovas

https://www.youtube.com/watch?v=JSZhFiukFrs

Esto es lo que una red social puede hacer con tus datos. Guillermo Cánovas

https://www.youtube.com/watch?v=0zJZfLXVyAE

BLOGS DE REFERENCIA

Blog de alumnos ayudantes IES Parque Goya.

https://alumnosayudantes.wordpress.com/

Uso seguro y responsable. Jesús Prieto

Copyright 2026

https://jprietoblog.wordpress.com/

Copyright 2026

Glosario

Créditos

Autores: Antonio Martínez Ramos y Jesús Prieto González.

Cualquier observación o detección de error en soporte.catedu.es

Los contenidos se distribuyen bajo licencia **Creative Commons** tipo **BY-NC-SA** excepto en los párrafos que se indique lo contrario.