Asociación Profesional Española de Privacidad

# Cuestiones y recomendaciones básicas para padres y educadores sobre el uso de redes sociales e Internet por los menores

**Elaborada por la Comisión de Menores APEP**

**GUÍAS APEP** **Guía nº 1:**

**Autores:**
María Arias Pou
David González Calleja
Alicia Piña Pérez
Cristina Ribas Casademont
María Suárez Pliego
Silvia Telechea Dayuto

# ÍNDICE

# INTRODUCCIÓN:

Internet ha venido para quedarse. Ha cambiado nuestra forma de comunicarnos, de procesar la información y, en definitiva, de ver y experimentar el mundo.

Esta nueva sociedad hace que hablemos de “inmigrantes digitales” y “nativos digitales”. Los primeros, creen perdida la batalla de entender y comprender el vertiginoso cambio que el s. XXI les ha deparado. Los segundos, han nacido con un perfil en redes sociales y un smartphone o tablet bajo el brazo.

Con independencia del grupo con el que te hayas identificado, debes saber que tanto tú como tus hij@s y alumn@s necesitáis aprender, experimentar, vivir y descubrir conjuntamente todo lo que Internet os puede aportar.

Tampoco podemos olvidar que Internet, así como las demás tecnologías que de él dependen, son herramientas que han sido creadas por personas ajenas que, en la mayoría de los casos, viven en otro país. Y aunque para ti muchos de estos servicios son gratuitos, a cambio les cedes algo de incalculable valor: tus datos personales y los datos personales de otros.

En ocasiones, el desconocimiento y la inconsciencia llevan a que expongamos excesiva e innecesariamente a toda la familia. En otras, el miedo y la desconfianza llevan a que perdamos las oportunidades que Internet nos ofrece a nosotros y a nuestr@s hij@s, que acaban quedándose sol@s, desprotegid@s e indefens@s en la Red.

# LO QUE PUEDES OBTENER DE INTERNET

♦ **Aprovecha sus posibilidades:**

- Para comunicarte:
  - Es económico.
  - Accesible desde muchos lugares.
  - No tiene barreras.
  - Te ayuda a relacionarte y a conocer gente nueva.
  - Es global: Puedes conocer gente de otro país, cultura, o contactar con la familia y amigos en tiempo real.

- Para obtener información:
  - Nuevos recursos, nuevas páginas y contenidos actualizados.
  - De fácil acceso y abundante

  Atención: Es necesario que los adultos controlen y supervisen los contenidos y búsquedas que los menores obtienen de y realizan en la Red. Hay que enseñar a contrastar la información, pues no toda es cierta o real.

- Como entretenimiento
  - Juegos y apuestas online, comunidades virtuales y de *sandbox* inundan nuestra Red.

  Atención: Es imprescindible controlar y evitar un uso abusivo porqué pueden ser herramientas altamente adictivas.

- Como potente herramienta de educación.
  - Ofrece variedad de contenidos.
  - Muchísima información y recursos interactivos.
  - Es el lugar idóneo para encontrar y difundir conocimiento.

♦ **Aprende y enseña a gestionar sus riesgos:**

- Comparte tus conocimientos y recursos con tus hij@s.
- Enséñales a protegerse en la Red y acompáñales en esta aventura.
- Conviértete en su aliado/a y déjaselo bien claro.
- Respeta la privacidad de tus hij@s, es su derecho y tu deber.
- Enséñales a ser responsables con sus datos, su privacidad y la de los demás.
- Y que no hagan en Internet lo que no les gustaría que le hicieran a él/ella. [Nota: Su vida “real” es Internet.]

# ENSÉÑALES A CONOCER SUS DERECHOS Y A RESPETAR LOS DERECHOS DE LOS DEMÁS

Hoy en día existen multitud de dispositivos tecnológicos que permiten conectarnos a Internet desde cualquier parte del mundo y a una edad muy temprana. También podemos compartir todo tipo de contenido (vídeos, fotografías, conversaciones, comentarios…), sea propio o ajeno.

Como muestra de ello, observa la siguiente fotografía que refleja el tráfico global de Internet:

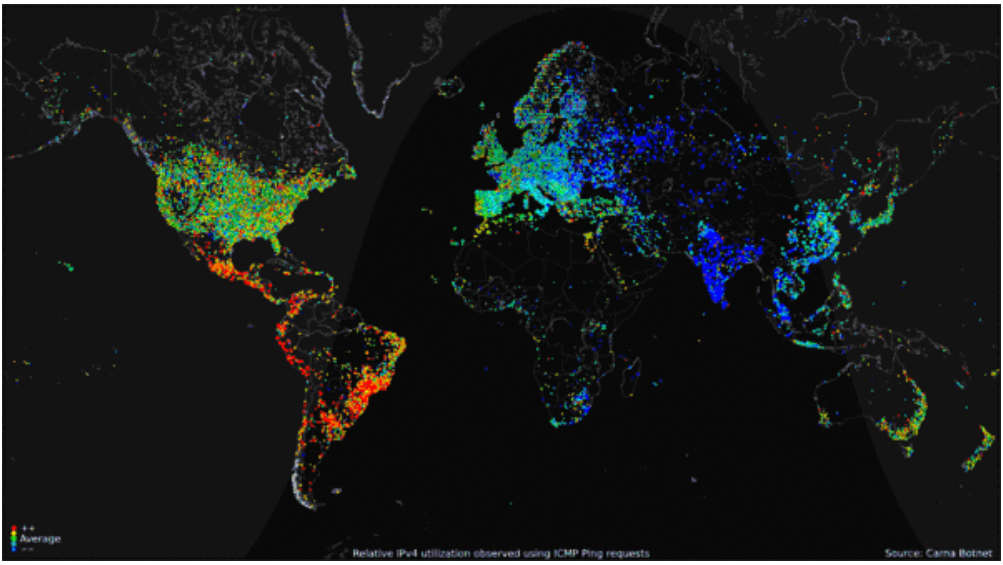



*Imagen extraída del portal Carna Botnet, Internet Census of 2012*
*http://internetcensus2012.bitbucket.org/images/geovideo.gif*

♦ **Si eres educador, padre o madre, pregúntate:**

- **¿Saben nuestros menores cuáles son sus derechos y obligaciones al usar las TIC?**

♦ **Lo que deben saber los menores:**

- **¿Qué es un dato personal?**

  Es cualquier información que identifica o permite identificar a una persona física concreta. [Por ejemplo: nombre, DNI, dirección postal o electrónica, número de teléfono, fotografía, grabación de voz, etc.]

- **¿Qué es el derecho a la protección de datos personales?**

  Es un derecho fundamental que reconoce a las personas la facultad de controlar sus datos personales y la capacidad para disponer de ellos. Se recoge en el art. 18.4 de la Constitución Española y se desarrolla en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- **¿Por qué son importantes nuestros datos personales**?

  Porque ofrecen información sobre tus gustos, tu familia, tu vida, dónde vives y qué haces. Si te das cuenta, continuamente nos solicitan datos personales para poder realizar cualquier actividad, ya sea para abrir un perfil en redes sociales, jugar a un videojuego, utilizar una aplicación, ir al gimnasio, a la biblioteca o al centro comercial. Enséñale a pedir información sobre la finalidad para la que usarán sus datos, pues muchas personas y organizaciones que no conocen pueden solicitarles multitud de datos personales para objetivos bien distintos. Los menores deben facilitar únicamente los datos estrictamente necesarios y desconfiar del que no le informa sobre para qué los recaba.

- **Todos nuestros datos personales nos atañen y, en general, para utilizarlos y/o hacerlos públicos se necesita nuestra autorización**:

  En general, para que los demás puedan utilizar nuestros datos personales deben:

  - Informarnos sobre para qué quieren nuestros datos y cómo los utilizarán; y
  - Solicitar nuestro consentimiento.

Además, hay que tener en cuenta:

- Si es un menor de 14 años: se necesita la autorización del padre, madre o tutor. [Por ejemplo, para crear un perfil en redes sociales o abrir una cuenta de correo electrónico]
- Si es un mayor de 14 años: no se necesita autorización parental pero sí comprobación de la edad.

Atención: Los padres y tutores deben realizar tareas de control y supervisión porque, hasta los 18 años, pueden ser responsables de los daños que puedan causar sus hij@s a través de las TIC.

- **Que el material que difunda en las redes sociales lo comparta de manera responsable [Pensar antes de enviar]**
  - Compartir vídeos y fotografías: enséñale a conocer las consecuencias de publicar fotos y vídeos de los que mañana o en un futuro pueda arrepentirse.
  - Enséñale a pedir autorización a las personas que aparezcan en la fotografía o en el video. Y si no le dan permiso, que se abstenga de publicarlos.
  - Enséñale que los contenidos son propiedad de sus autores. Siempre que quiera difundir alguna fotografía o vídeo que no sea suyo, debe pedir autorización al autor.
  - Enséñale que, una vez publicado, se deja de tener control sobre este material. Un borrado posterior puede resultar imposible y los perjuicios causados difícilmente reparables. Internet es como un vaso derramado.- Por mas que lo intentes, nunca se puede recoger todo el contenido que había en el. Siempre queda algo fuera.
  - Sé cuidadoso con los videos y fotografías que tú mismo/a compartes de tus hij@s y alumn@s en Internet. Lo que hoy puede resultar gracioso, mañana puede ponerles en peligro o resultar de otro modo realmente perjudicial.
  - Publicar comentarios y conversaciones: Valorar si el comentario puede dañar la honorabilidad del otro, ser una falta de respeto y/o constituir delito de injurias o calumnias. Los comentarios deben ser constructivos y respetuosos con los demás.

## CONOCE Y ENSÉÑALES LAS CONDUCTAS QUE PODRÍAN SER ILÍCITAS

- **Ciberacoso:** Lo que para unos niños puede ser una broma, para la víctima supone un problema psicológico que dificulta su desarrollo emocional y sus relaciones sociales. El acoso que ocurre en Internet también ocurre en la vida real pero los efectos son de mayor magnitud. Puede constituir un delito contra la integridad moral.

- **Uso de imágenes:** Enviar o compartir con otros la imagen de una persona sin su autorización así como contenidos ajenos puede ser ilícito y suponer la comisión de infracciones civiles, administrativas e incluso penales.

- **Ataques a la intimidad:** Entrar en el correo electrónico o en el perfil en la red social de otra persona sin su consentimiento, independientemente de los métodos utilizados, es un grave ataque a su intimidad y puede constituir delito.

- **Incitación al odio:** Los menores han de respetar y apoyar a todos aquellas personas que pertenezcan a algún colectivo que, por la razón que sea, estén en una situación de marginalidad o de exclusión. No hay nada atractivo en fomentar conductas o difundir mensajes de odio.

- **El honor y la libertad de los demás:** Aunque a menudo se tienda a minimizar la importancia de determinadas actuaciones en Internet, insultar y amenazar a una persona son actitudes que tienen trascendencia penal.

- **La actitud de los demás:** Es importante que los niños entiendan que todas estas actitudes no deben aplaudirse. Muchas veces, el autor de estos hechos busca el reconocimiento de sus compañeros y lo que se les debe transmitir es todo lo contrario: la crítica y el reproche de este tipo de actitudes.

- **Robo de identidad:** En Internet es muy fácil suplantar la identidad de otro y hacerse pasar por un tercero, esto no es un juego, pueden incurrir en infracciones civiles, administrativas y penales.

# FAQs SOBRE EL TIEMPO DE CONEXIÓN A INTERNET

♦ **¿Cuándo y cuánto tiempo es recomendable que juegue con la videoconsola?**

El juego virtual es una actividad divertida y productiva para los menores. Debes recordar que, en los días de colegio, tendrá deberes que hacer. Dialoga con él/ella y acordad un horario y duración prudencial de juego durante el fin de semana.

♦ **¿Qué hago si sobrepasa el tiempo de juego que hemos pactado?**

Es recomendable que no hagas concesiones: sus próximas partidas deberían ser más cortas y, si continúa desobedeciendo, plantéate instalar mecanismos de control parental que programen la desconexión de su consola u ordenador.

♦ **¿Qué síntomas indican un abuso de las TIC y del juego virtual?**

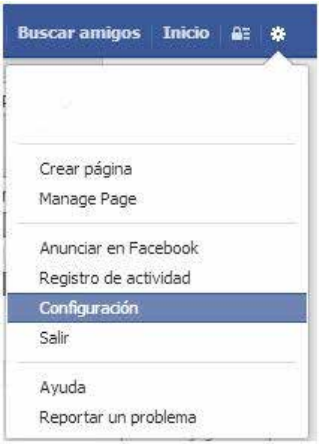
Pasar un rato con la videoconsola y navegar por Internet no tiene por qué ser contraproducente, pero dejará de ser una experiencia positiva si detectas que declina invitaciones para jugar con sus amigos, relacionarse con los demás o incluso, salir de casa. Especialmente, si:

- Dedica muchas horas a navegar por Internet;
- El rendimiento escolar y sus notas han empeorado;
- Se relaciona poco con vosotros y con sus amigos;
- Te presta poca atención antes y durante una partida; o no reacciona a ningún otro estímulo;
- Se muestra más irascible, apático/a o eufórico/a en las partidas que en cualquier otra situación.

♦ **¿Qué recomendaciones se deben tener en cuenta?**

- Vigila el tiempo que dedica a navegar por Internet. Es razonable que le permitas navegar un rato cada día en función de su edad pero, por ejemplo, ponle un horario de uso.

- Ten presente que podrá necesitar tiempo extra para completar cualquier trabajo del cole. En estos casos, define un tiempo adicional a condición de que se levante y descanse un rato al cabo de una hora. De todos modos, puedes controlar cómo avanza con sus tareas utilizando como excusa el *"¡toca una pausa!"*
- Plantéate si, por la edad de tu hij@, conviene facilitarle un *smartphone*, en qué condiciones y con qué tipo de controles.
- No seas alarmista, pero sí caut@. Empieza por establecer normas en casa, p.ej. que ningún dispositivo quedará encendido por la noche, y que permanecerán en la sala de estar (o cualquier otra zona común); así, evitarás que su sueño se altere y le provoque una disminución de la capacidad de atención y participación en el colegio (y en las notas).
- Ante cualquier indicio de que los alicientes de tu hij@/alumn@ se reducen casi exclusivamente a los videojuegos, sé consciente de que ello es síntoma de adicción a este tipo de entretenimientos. En tu mano está proponerle otras alternativas lúdicas. Motívale para descubrirlas y hazle saber que no puede depender de los videojuegos para ser feliz.
- No te conformes con que tu hij@/alumn@ destine más tiempo a Internet que a cualquier otra actividad que implique relacionarse con los demás. ¡Es una equivocación! Habla con él/ella y muéstrale con qué otras aficiones puede llegar a pasarlo en grande.
- Si nunca has puesto en práctica estas recomendaciones, intenta aplicarlas. Para obtener resultados, deben interiorizarse como hábitos de vida saludables.



# CONOCE LAS HERRAMIENTAS Y AYÚDALE A:

- **Configurar el perfil en las redes sociales, configurando el nivel de privacidad:**
  Puede decidir qué información quiere compartir y con quién. Por defecto, muchas redes sociales ofrecen el perfil *"abierto a todos"*. Es tan sencillo como cerrarlo y restringirlo a aquellas personas que selecciones.
- **Configurar los grupos en los que se participa:**
  Sólo debe compartirse la información personal que sea estrictamente necesaria, sin proporcionar dónde vive, dónde estudia ni su número de teléfono.
- **Conocer y usar los filtros de seguridad:**
  No todas las páginas web que están disponibles en Internet son fiables. El reto consiste en aprender a identificar las que son buenas. Puedes lograrlo con estos métodos:
  - Candado verde: Si en la barra de tu navegador aparece este símbolo, los datos personales que introduzcas en la web estarán protegidos
  - HTTPS:// Si la URL de la web empieza por https:// en color verde, significa que utiliza protocolos de seguridad y de cifrado de la información. Todos los datos personales y contraseñas que proporciones pasaran por un túnel en el que la información no podrá ser interceptada ni utilizada por personas maliciosas.


  - Dominio: Comprueba que el dominio que aparece sea el correcto y que antes de la terminación del dominio aparezca el nombre de la entidad o página. [Ejemplo de web falsa: www.apep.cl.es. Ejemplo de web fiable: www.apep.es ]
  - Apps: Actualmente existen en el mercado aplicaciones específicas que detectan las páginas web inseguras.
- **Elegir contraseñas adecuadas:**
  La contraseña es una herramienta para proteger el perfil de usuario en una red social. Debes elegir una contraseña robusta que se componga de varios tipos de caracteres. Las más seguras son las que combinan caracteres nu-

méricos, alfanuméricos (Mayúsculas y minúsculas) y especiales (€,@,$,&). El mínimo de caracteres recomendado es de 6 u 8.


Ejemplo:


- **Cuando navega en otro ordenador:**
  Antes de irse se deben cerrar bien todas las sesiones (por el apartado *"cerrar sesión"* o *"salir"*, nunca clickando directamente en la crucecita roja de la pantalla), eliminar el historial de navegación y las *cookies*. En caso contrario, habrás dejado tu rastro y tus datos personales en el equipo.

- **Usar *nickname*:**
  Para proteger debidamente su identidad en la Red y sus datos personales es muy recomendable que en lugar de su nombre y apellidos utilice un *nickname* o apodo.

- **Evitar fraudes online**
  Recuérdale que si recibe un correo electrónico en el que le invitan a rellenar un formulario con sus datos personales, de la familia o de sus amigos, no debe contestarlo porque puede tratarse de un fraude. Si tiene dudas, anímale a que lo consulte contigo o el adulto que le acompañe en sus tareas educativas.

# RECURSOS WEB DE INTERÉS

- Protección de menores en Internet
  - Agencia Española de Protección de Datos. www.tudecideseninternet.es
  - Agencia Vasca de Protección de Datos www.avpd.euskadi.net (Kontuzdatos)
  - Autoridad Catalana de Protección de Datos www.apd.cat/es (Privacidad para jóvenes)
  - Secretaría de Estado de Telecomunicaciones www.chaval.es
  - Oficina de Seguridad del Internauta https://www.osi.es/es/proteccion-de-menores
  - Instituto Nacional de Ciberseguridad www.incibe.es
  - Orange Navega Seguro www.blog.orange.es/navegacion-segura/
  - El Blog de Angelucho www.elblogdeangelucho.com
  - TenCuidado www.tencuidado.es

- Programas y herramientas
  - Filtro publicitario Ad Block www.adblockplus.org/es
  - Creador online de contraseñas seguras www.password.es
  - Comprobar fortaleza y seguridad de las contraseñas www.passwordmeter.com
  - Información sobre el significado de las etiquetas de los videojuegos www.pegi.info/es

- Organizaciones
  - Pantallas amigas www.pantallasamigas.net
  - Fundación Alia2 www.alia2.org
  - Padres 2.0 www.padres20.org
  - La Familia Digital www.lafamiliadigital.es
  - Protégeles www.protegeles.com
  - Internet sin Acoso www.internetsinacoso.com
  - Comisión de menores APEP www.apep.es