GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es

"Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad"

[Red.es]

MONOGRÁFICO MEDIACIÓN PARENTAL

MONOGRÁFICO MEDIACIÓN PARENTAL

1. Objetivo del monográfico

«Describir las principales características y formas de mediación parental y educación digital, identificando las principales carencias en la mediación parental y la educación digital actual; así como estrategias, herramientas y recursos para prevenir riesgos y lograr un uso responsable y seguro de las nuevas tecnologías por parte de los menores.»

2. Conceptualización y descripción del riesgo

La familia y los centros educativos tienen un papel fundamental en la socialización del menor, así como un protagonismo absoluto en la prevención de conductas de riesgo como el uso irresponsable de las nuevas tecnologías[1]. Por ello, la educación en el uso de las nuevas tecnologías debe ser algo prioritario en la etapa en la que nos ha tocado vivir. Una educación digital que debe vehicularse a través de una doble vertiente:

- Educación tecnológica: enseñando a los menores a utilizar las tecnologías con las garantías adecuadas de seguridad, privacidad y prevención.
- Educación conductual: mostrando a los menores el respeto a la privacidad, la imagen, la netiqueta o buenos modales en la Red, etc.

Así, en este proceso educativo deben estar necesariamente implicados todos los agentes que tienen algo que aportar en la educación del menor: padres/madres, tutores, educadores y otros profesionales.

Definición de mediación parental

La **mediación parental** se puede definir como «el proceso por el cual los responsables de la educación digital del menor, acompañan a éste en su proceso de alfabetización digital, le educan para que realice un uso responsable y seguro de las nuevas tecnologías y velan para impedir que los riesgos de las TIC se materialicen y en caso de ocurrir, ofrecer soluciones».

[1] Madrid Salud, Instituto de Adicciones. Guía para familias. TIC: Prevención de usos problemáticos. Recuperado de: http://www.madridsalud.es/publicaciones/adicciones/doctecnicos/TIC.pdf

Alfabetización digital

Los responsables de la educación del menor, tienen la obligación legal y moral de educar también en el ámbito de las nuevas tecnologías, incluyéndolo como un apartado más de la educación general que procuran al menor. Así, deben acompañar al menor en el proceso de alfabetización digital, entendiéndose como el proceso por el cual las personas adquieren los conocimientos y habilidades necesarias para desenvolverse en la interacción con las nuevas tecnologías[2]. Por otro lado, hay que entender que actualmente el concepto de enseñanza y formación se ha modificado sustancialmente, por lo que la alfabetización digital es un proceso con dos características fundamentales:

- El aprendizaje en esta alfabetización digital se producirá a lo largo de toda la vida, por la velocidad de cambio constante del entorno digital y su influencia en el analógico o físico.

- Debemos aprender a aprender, es decir, a autoformarnos. Adquirir habilidades de autoaprendizaje en el entorno digital es tan importante como la enseñanza de los propios contenidos.[3]

Los responsables de la educación del menor deben conocer las herramientas tecnológicas y los programas y aplicaciones que los menores utilizan, para poder educarle en el uso seguro y responsable de las mismas.

Además, deben establecer normas y límites claros y consensuados para el uso de estas nuevas tecnologías, con el fin de prevenir riesgos como el abuso o la dependencia, el uso en situaciones inadecuadas, la disminución del rendimiento académico o la alteración de los horarios y los hábitos fisiológicos y sociales.

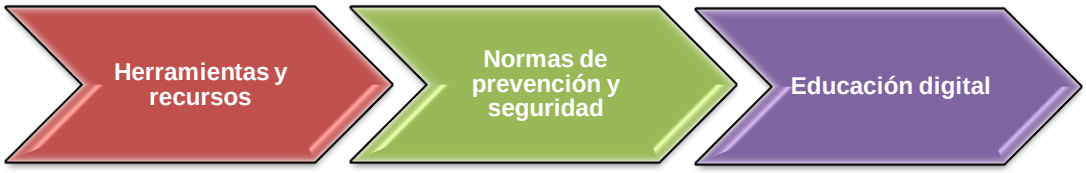
Para una adecuada mediación parental, los responsables de la educación del menor deben conocer las herramientas de control parental disponibles y su configuración, con el fin de reforzar la educación digital aportada, y las nomas y límites establecidos en el uso de las TIC por parte del menor.

---

[2] Fundación Telefónica (2012). Alfabetización digital y competencias informacionales. Recuperado de: https://ddv.ull.es/users/manarea/public/libro_%20Alfabetizacion_digital.pdf

[3] Junta de Castilla y León (2011). Manual: las TIC en Educación. Recuperado de: http://www.jcyl.es/web/jcyl/binarios/158/396/Manual%20Las%20TIC%20en%20Educacion%20Programa%20Aprende.pdf?blobheader=application%2Fpdf%3Bcharset%3DUTF-8&blobheadername1=Cache-Control&blobheadername2=Expires&blobheadername3=Site&blobheadervalue1=no-store%2C

El no poner en práctica una adecuada mediación parental por parte de los responsables de la educación del menor, puede conducir al establecimiento de una



serie de riesgos en su interacción con las TIC. Si al menor no se le proporciona la guía necesaria, no sabrá cuáles son los límites, lo que está bien o mal, las responsabilidades y consecuencias de sus actos en Internet o los peligros a los que puede exponerse. Esta es la definición de un concepto muy actual, el de "*huérfanos digitales*".

Ejes de la mediación parental

Llevar a cabo una mediación parental adecuada y eficaz no se basa tan sólo en conocer las herramientas de control parental existentes - herramientas tecnológicas que permiten a los responsables de la educación del menor controlar, orientar, filtrar o limitar las interacciones del menor con las TIC así como el contenido, programas y servicios a los que accede- y su uso y configuración por parte de los responsables de la educación del menor. Por el contrario, una adecuada mediación parental debe reunir tres niveles o ejes[4]:

- Educación digital: conductual y tecnológica, a la hora de interactuar con las TIC.
- Pautas y normas de prevención y seguridad en el uso de las TIC.
- Herramientas y recursos para la educación digital, entre las que estarían las herramientas de control parental.

[4] Comisión Europea (2011). *Evaluación comparativa de las herramientas de control parental*. Recuperado de: http://sipbench.eu/index.cfm/secid.3

3. Datos de situación y diagnóstico

El inicio de las interacciones con Internet por parte de los menores es cada vez más temprano. Con escasa edad comenzamos a permitir a los niños y niñas que interactúen con los juegos o vídeos de las tabletas, móviles o portátiles. Las empresas no son ajenas a este hecho y comercializan productos y dispositivos tecnológicos, como móviles y tabletas[5], con los que los niños pueden conectarse a la red a edades cada vez más tempranas.

En este sentido, resulta interesante que conozcamos algunos **datos relevantes** en cuanto al uso de las nuevas tecnologías por parte de los menores[6]:

Porcentaje de menores usuarios de TIC por sexo y edad
Año 2014

	Uso de ordenador	Uso de Internet	Disposición de móvil
Total	93,8	92,0	63,5
Sexo			
Niños	93,9	92,3	61,9
Niñas	93,6	91,6	65,3
Edad			
10	90,7	89,3	23,9
11	92,4	88,5	40,4
12	94,3	92,4	64,3
13	94,7	92,2	78,7
14	95,6	93,7	85,6
15	95,2	96,0	90,3

- A partir de los 10 años de edad el 23,9% de los niños ya tiene su propio teléfono móvil.

- La media en España para que los niños tengan su primer móvil, en el año 2011, era a los 11,2 años de edad, y se alertaba que la tendencia era a seguir disminuyendo, con lo que en 2014 se estima que la media bajaría hasta los 9

[5] Noticia Europapress. *Imaginarium presenta un phablet como el Galaxy Note, pero para niños*. Recuperado de: http://www.europapress.es/portaltic/gadgets/noticia-imaginarium-lanza-paquito-mix-primer-phablet-ninos-20141024103628.html

[6] INE (Instituto Nacional de Estadística) (2014). Encuesta *sobre Equipamiento y Uso de las Nuevas Tecnologías de la Información y la Comunicación en los Hogares*. Recuperado de: http://www.ine.es/prensa/np864.pdf

años de edad. [7]Así, casi el 24% de los menores de 10 años poseen *smartphone* e incrementa a un 90,3% a los 15 años de edad.[8] [9]

- A los 13 años de edad, cuando aun legalmente en España no pueden estar dados de alta ni usar muchos de los servicios que ofrece Internet como las Redes Sociales, tener cuenta en Google o servicios de correo electrónico que tanto utilizan, casi el 80% de los menores ya tienen un móvil que les ofrece todas estas características y sus riesgos añadidos.

- En relación a la mediación parental y al uso de herramientas de control parental en los hogares españoles, se arrojan los siguientes resultados[8]:

    1. En cuanto al uso de herramientas de control parental, solo el 38,1% de los encuestados usa herramientas de control parental que limitan contenidos inapropiados a los menores y el 19,2% usa software para controlar las webs que visita el menor.

    2. En relación a la educación digital, el 79,1% explica a los menores por qué unas web son buenas y otras no, el 68,7% explica a los menores formas de usar Internet de manera segura, el 66,4 % se sienta con el menor mientras navega vigilando pero sin participar y el 53,8 % le pregunta qué haría en determinadas situaciones problemáticas en Internet.

    3. En relación a las autorizaciones de los responsables de los menores en cuanto al uso de distintos servicios de Internet, el 53,9% permiten usar Messenger y WhatsApp en cualquier momento al menor, el 53,3% a ver vídeos en cualquier momento por Internet, el 52,9% a navegar por Internet y el 27,1% a tener su propio perfil en una red social.

---

[7] INTECO (2011). *Estudio sobre hábitos seguros en el uso de Smartphones por niños y adolescentes españoles*. Recuperado de: http://www.protecciononline.com/galeria/proteccion_online/Estudio-sobre-el-uso-de-smartphones-por-los-ninos-y-adolescentes.pdf

[8] Ministerio del Interior (Junio 2014). *Encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España*. Recuperado de: http://www.interior.gob.es/documents/10180/2563633/Encuesta+sobre+h%C3%A1bitos+de+uso+y+seguridad+de+internet+de+menores+y+j%C3%B3venes+en+Espa%C3%B1a/b88a590a-514d-49a2-9162-f58b7e2cb354

[9] INE (Instituto Nacional de Estadística) (2014). *Encuesta sobre Equipamiento y Uso de las Nuevas Tecnologías de la Información y la Comunicación en los Hogares*. Recuperado de: http://www.ine.es/prensa/np864.pdf

- Los niños se conectan habitualmente desde el hogar, y de manera secundaria lo hacen en el colegio o en casa de algún amigo. La mitad de los chavales accede a diario a Internet, y pasan, de media, 14,5 horas a la semana conectados, con mayor intensidad el fin de semana que los días de diario.[10]

De este modo, el panorama actual y la tendencia del futuro es a que todo esté conectado en Internet, y que "todo esté en Internet". Este panorama al que los menores no son ajenos, ni deben serlo, aumenta sin embargo exponencialmente los peligros asociados al uso de esta interconectividad.

Esta situación actual en la que nos encontramos, hace completamente imprescindible la existencia de una educación y guía en el uso de las nuevas tecnologías a los menores, tanto desde las familias, como desde los centros educativos, aunando esfuerzos en la prevención de los riesgos asociados a dicha interacción con las TIC.

4. Ejemplos de casos reales

En este apartado exponemos algunas noticias de casos reales relacionados con la mediación parental, con objeto de concienciar del riesgo de no practicar una mediación parental eficaz y adecuada ante el uso de las TIC por parte de los menores.

Las consultas médicas de adolescentes adictos a los videojuegos "online" se han triplicado en Cataluña en cinco años[11]

En los casos más extremos los chicos han tenido que ser rescatados por la policía de la habitación, llevan años sin comer con la familia o han perdido el control de los esfínteres por estar delante de la pantalla. En los últimos dos años se está viendo un comportamiento similar con las redes sociales.

El aislamiento en la habitación durante largas horas encadenando partidas de diferentes partes del mundo lleva a estos jóvenes a una desconexión total del entorno llegando, en los casos más extremos, a obligar a intervenir

[10] Instituto Nacional de Tecnologías de la Comunicación INTECO (2009). *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres*. Recuperado de: http://www.pantallasamigas.net/estudios-realizados/pdf/inteco-estudio-uso-seguro-tic-menores.pdf

[11] Fuente: http://www.lavanguardia.com/vida/20140413/54405725221/triplican-adolescentes-adictos-videojuegos.html

a la policía para conseguir que el joven salga de su encierro. Algunos afectados reconocen que hace años que no comen con la familia e incluso ha habido casos de jóvenes que se han hecho sus necesidades encima ante la imposibilidad de desengancharse de la pantalla. La mayoría de expertos consultados puntualizan que los casos más extremos suelen tener asociadas otras patologías y aseguran que se trata de un problema que va en aumento y al que se le están sumando en los últimos dos años la adicción a las redes sociales.

El móvil, uno de los principales conflictos que llevan a las familias a mediación[12]

El uso del teléfono móvil se ha convertido en una de las cuatro principales causas de conflicto con hijos adolescentes que llevan a las familias españolas a recurrir a servicios de mediación, junto a los problemas con los estudios, con las tareas en el hogar o de relaciones interpersonales.

Así lo han explicado este martes la coordinadora del servicio de Mediación de UNAF, Ana María del Campo; y el responsable del área de mediación entre padres y adolescentes de la organización, Gregorio Gullón; junto a la vocal de FAPROMED, Ana Cobos; en una rueda de prensa para reivindicar la implantación del 21 de enero como día europeo de la mediación a fin de difundir estos servicios, avanzar en normativa y unificar criterios.

Según ha señalado Gullón, en los servicios de mediación con adolescentes de UNAF, que han tratado a medio millar de familias en los últimos 8 años y cuya demanda se ha incrementado exponencialmente en el último lustro; cada vez son más los casos de problemas desencadenados por el uso de las nuevas tecnologías y, en particular, del *smartphone*.

El experto plantea que los padres se encuentran ante una "paradoja" problemática, ya que por un lado, "sienten la necesidad de cortar un uso inadecuado del teléfono móvil" y, por otro, quieren que su hijo lo tenga para poder tenerle localizado.

[12] Fuente: http://www.europapress.es/epsocial/familia-00324/noticia-uso-movil-ya-principales-conflictos-llevan-familias-mediacion-expertos-20150120132500.html

Emilio Calatayud: "La edad mínima que debería pactarse para usar un móvil son los 14 años"[13]

Los teléfonos móviles, que permiten estar conectado a la red las 24 horas del día, cada vez llegan antes a manos de nuestros hijos. Pero esto no debería ocurrir de cualquier manera. Padres y menores deberían pactar sus condiciones de uso. Es más, según el juez de menores Emilio Calatayud, «la edad mínima que debería pactarse para poder usar un móvil son los 14 años». «Es crucial que las autoridades trabajen por un pacto de uso de los dispositivos para los menores y, para todos, recuperar el sentido común. El acceso a la red es algo muy bueno pero también muy peligroso», advierte. El magistrado ha alertado asimismo de que «los dispositivos móviles son una herramienta muy poderosa para delinquir o ser víctima de un delito y es responsabilidad de los padres proteger a los menores educándoles e imponiéndoles condiciones de uso».

5. Estrategias, pautas y recomendaciones para la mediación parental

Existe una regla básica de prevención en el uso seguro de las TIC normalmente conocida como la "regla de las tres R":

- **R** de regular: regular el acceso, el tiempo de conexión, los contactos.
- **R** de reducir: reducir los riesgos de las TIC con las recomendaciones generales de prevención.
- **R** de recursos: dotar al menor de recursos, para que sea el mismo el que vele por su propia seguridad.

[13] Fuente: http://www.abc.es/familia-padres-hijos/20141211/abci-telefono-emilio-calatayud-201412101530.html

Tenido como marco de referencia este punto de partida y tal como se explica en el primer apartado, para que la mediación parental sea adecuada y la prevención eficaz, debe establecerse una intervención basada en tres ejes:

- Educación digital: conductual y tecnológica.
- Pautas y normas de prevención y seguridad en el uso de las TIC.
- Herramientas y recursos para la educación digital.

A lo largo de este apartado se presentan un conjunto de estrategias, pautas y recomendaciones que ayuden a padres, madres, tutores y educadores a prevenir los riesgos en materia de seguridad TIC en general por medio de la instauración de mecanismos adecuados de mediación parental en particular.

Educación digital

A muchos adultos, padres y educadores, el boom de las nuevas tecnologías, las redes sociales y la "sociedad conectada", les ha pillado por sorpresa y sin estar informados y formados en ellas, o simplemente no le dan la importancia y utilidad que tienen en la sociedad actual. Padres con edades avanzadas, que o bien no usan la tecnología o bien no quieren usarla, no deben utilizarlo como una excusa, ya que deben asumir la educación digital de sus hijos, para lograr que se conviertan en ciudadanos digitales responsables.

Un ejemplo claro es el de las normas de circulación: hay adultos que no conducen y no por eso desconocen las principales normas de circulación y se las inculcan y enseñan a sus hijos para protegerles de los respectivos peligros. Igual pasa con las nuevas tecnologías, aunque no se utilicen, se deben tener unos mínimos conocimientos para poder comprenderlas y para poder enseñar y guiar a los menores.

La educación digital de los menores, descuidada hasta la actualidad, se configura cada vez más como uno de los aspectos más importantes a tener en cuenta en la educación general del menor. Así, la educación en el uso seguro de las nuevas tecnologías debe realizarse siempre en una doble vertiente, donde no debemos descuidar ninguna de las dos:

Educación digital conductual

La familia tiene una enorme importancia socializadora para los menores[14]. La sociedad en la que vivimos es cada vez más compleja y con la llegada de las nuevas tecnologías hemos incorporado una necesidad más que anteriormente no existía.

Con educación conductual hacemos referencia a enseñar a los menores a utilizar las nuevas tecnologías con sensibilidad, respeto, empatía y siguiendo las normas básicas de civismo y educación también en Internet.

En este punto es necesario recordar que:

- Los padres comparten la educación de los menores con otros agentes. Si en los primeros años la influencia de la familia es prácticamente absoluta, poco a poco van incorporándose otros espacios y otras instituciones: la escuela, las amistades, actividades extraescolares, medios de comunicación, modas y tendencias juveniles…

- Cuanto mayor sean las influencias externas, más sentido cobra la labor educativa de la familia en relación al uso de las nuevas tecnologías.

Por ello, en la educación conductual de los menores, vamos a abordar las principales estrategias de mediación parental de los responsables de la educación del menor y sus efectos sobre la conducta de éste, las normas y límites que deben establecerse en

[14] Inmaculada Sánchez Espejo (2008). *La familia como primer agente socializador*. Cuadernos de docencia – Revista digital de educación. Nº 10

el uso de las TIC para el menor, qué es la netiqueta y su relevancia, y por último la importancia de la comunicación familiar en el ámbito de las TIC.

Estilos educativos de mediación parental

Los estilos educativos de mediación parental se pueden definir como "la forma regular de actuar de los padres ante sus hijos, de interactuar con ellos, en las situaciones cotidianas, con el fin de enseñarles y prepararles para el mundo en el que vivimos, el analógico y el digital".

El estilo de mediación parental depende en gran medida del carácter que tiene el padre/madre, pero también hay otros factores que tradicionalmente han influido en el estilo educativo de los padres: el cómo el adulto interpreta las conductas de los niños, manera de concebir la vida y el mundo al que se van a incorporar los niños, por parte de los padres, el pasado de los padres y la relación de éstos con sus progenitores, carácter, personalidad, temperamento, etc.

Sin embargo, el ámbito de las nuevas tecnologías es un nuevo territorio de educación que los padres están aún explorando y empezando a incorporar en sus hábitos educativos generales. Por lo que no tienen experiencia previa en él, y en muchas ocasiones están aprendiendo a la par que los menores o incluso por detrás de ellos, teniendo una falta de referencias, información y experiencia previa.

Básicamente se pueden distinguir 4 tipos de estilos de mediación parental[15], cada uno con sus particularidades y con sus efectos a la hora de educar al menor en el ámbito de las TIC:

- **Estilo autoritario**. Se caracteriza por normas rígidas y abundantes impuestas, no se dialoga ni hay negociación, inflexibles en la aplicación de las mismas, utiliza sobre todo el castigo y las críticas, escaso contacto emocional con los hijos, no se tienen en cuenta los intereses y preferencias del niño y se es demasiado exigente para el nivel de madurez del niño. Se les advierte de que las TIC tienen sus riesgos, pero sin especificar ni aclararlos, ni tampoco la forma de autoprotegerse, basándose la prevención en la prohibición en el

[15] MacCoby, E. E. y Martin, J. A. (1983). *Socialization in the context of the family: parent-child interaction*. En E. M. Hetherington & P. H. Mussen (Eds.), Handbook of Child Psychology, Vol. IV: Socialization, Personality and Social Development (4ª ed. pp. 1-101). Nueva York: Wiley.

acceso a las TIC en muchos de los casos. No se les imparte educación conductual ni educación tecnológica, por lo que aprenden el uso de las TIC sin la guía por parte de los responsables de su educación.

Los efectos de este estilo sobre la forma en la que el menor interactuará con las nuevas tecnologías pueden ser: son obedientes en su interacción con las TIC cuando están presentes los padres o tutores, pero en ausencia de estos, se vuelven temerosos e irresponsables, ya que no se les enseña autocontrol, buscan y generan contenido inapropiado, pueden ejercer formas de acoso y *ciberbullying,* no dan el valor adecuado a lo que comparten en la Red y no utilizan la netiqueta y normas de buena educación, ya que no se les han enseñado los límites ni han tenido una guía adecuada. Tienen baja autoestima, escasas habilidades sociales y pueden refugiarse en el uso de las TIC para aislarse del contacto social físico. No recurren a los padres o responsables cuando algo les molesta o no entienden en la Red, o tiene un problema con las TIC ya instaurado.

- **Estilo permisivo**. Se caracteriza por mucho afecto y contacto emocional, se rigen por los intereses y preferencias del niño, escaso control de la actividad del menor con las TIC, falta de normas o son difusas, poco exigentes, se le deja al menor explorar e interactuar a su antojo, evitan los conflictos, la negociación y permiten hacer al niño, delegando en otros (profesionales: docentes, amigos, pediatra…) la educación de los hijos en el ámbito de las nuevas tecnologías, amparándose en su desconocimiento, edad, falta de importancia de los riesgos de las TIC, etc.

  Los efectos de este estilo de mediación parental sobre la forma en la que el menor interactuará con las nuevas tecnologías pueden ser: utilizan las TIC a su antojo, sin tener límites ni normas, y si se marcan horarios o límites no lo aceptan, teniendo bruscos comportamientos y una escasa tolerancia a la frustración. No conocen previamente la existencia de riesgos en el uso de las TIC, exploran Internet sin límites, exponiéndose constantemente a riesgos (*ciberbullying, grooming*, estafas…) y contenido inapropiado. Son candidatos a abusar de las TIC y a padecer en el futuro conductas adictivas a las nuevas tecnologías.

- **Estilo indiferente o negligente**. Se caracterizan por implicarse muy poco en la educación y crianza de los hijos en general y en el ámbito de las TIC en particular, no establecen normas ni límites en el uso de las TIC, no le dan importancia a los riesgos de las mismas y también tienen una escasa comunicación con los hijos en relación a las nuevas tecnologías. No enseñan a los menores normas de comportamiento en interacción en la Red, ni cuáles son los riesgos ni la forma de protegerse. Pueden imponer castigos o límites severos en el uso de las TIC sin justificación adecuada.

  Los efectos de este estilo de mediación parental sobre la forma en la que el menor interactuará con las nuevas tecnologías pueden ser: tienen baja autoestima, no acatan ninguna norma ni límite, tienen escasa empatía y son muy vulnerables a los conflictos sociales y personales, por lo que son buenos candidatos a riesgos como el *ciberbullying* (tanto víctima como agresor) y al uso abusivo de las TIC. No saben cuáles son los riesgos a los que se exponen en la Red por lo que desconocen las pautas y recomendaciones para el uso seguro de las nuevas tecnologías. Pueden ser candidatos a exponerse a contenido inapropiado de las comunidades peligrosas *online*. No recurren a los padres o responsables cuando algo les molesta o no entienden en la Red, o tiene un problema con las TIC ya instaurado.

- **Estilo democrático**. Se caracterizan por ser bastante afectuosos y tener muy buena comunicación con los hijos, se les educa en la autonomía y la independencia mostrándoles cuáles son los peligros de Internet y cómo autoprotegerse de ellos, normas y límites claros, bien definidos y justificados o razonados con sus hijos en el uso de las TIC, los que a veces además participan del establecimiento de los mismos, controlan el comportamiento de sus hijos en la Red y dan pautas de buena conducta *online,* usan herramientas de control parental de forma consensuada con el menor y utilizan el refuerzo de forma adecuada y el castigo de igual manera. Les enseñan desde pequeños a utilizar los distintos dispositivos y navegan con ellos para aprender conjuntamente de las nuevas tecnologías. Les otorgan la privacidad necesaria en el uso de las TIC cuando la edad, el nivel de madurez y de conocimiento de Internet es el adecuado. Cuando algo lo desconocen, procuran informarse de ello para explicárselo al menor. Practican una adecuada educación digital con el menor.

Los efectos de este estilo de mediación parental sobre la forma en la que el menor interactuará con las nuevas tecnologías pueden ser: tienen una adecuada empatía con los demás, tienen buena competencia digital y habilidades sociales y tecnológicas, conocen los riesgos de Internet y la forma de prevenirlos, si algo no entienden o les molesta o tienen un problema con las TIC, tienen más posibilidades de acudir a los padres o tutores o a algún adulto cercano para solucionarlo, buen desarrollo moral y sentido de la responsabilidad, usan por tanto las TIC de forma educada y siguiendo las normas de la netiqueta. Utilizan las TIC, tanto en el hogar como fuera de él, siguiendo las directrices marcadas por los progenitores. Si acceden a contenido inapropiado es de forma pasiva o accidental.

Una última cuestión que hay que dejar bien clara es que el estilo de mediación parental no es el único factor influyente en la conducta de los hijos. No se debe estigmatizar al padre/madre o tutor por ello, pero lo que sí está claro, es que es un factor importante y que además es un factor que se puede controlar en cierta medida, por lo que a igualdad del resto de condicionantes, los beneficios para los niños serán mayores con un estilo educativo de las TIC democrático.

Límites y normas esenciales en la mediación parental

Por su parte, los límites y normas en mediación parental deben atender a los siguientes aspectos:

- **Establecer horarios y situaciones en las que se conectará a Internet**, independientemente de que esté en el hogar o fuera de él y del dispositivo que se utilice. Hay que evitar horarios en los que se pueda afectar a su descanso, a su rendimiento académico, a la realización de otras actividades familiares y de ocio, o simplemente por educación. Esto último es lo que se ha venido a llamar *phubbing*[16] utilizar las nuevas tecnologías en situaciones en las que puede ser considerada una falta de educación.

  Del mismo modo también se debe limitar o acotar la cantidad de horas de conexión ya que, además de quitar tiempo de otras actividades al menor,

[16] Definición y aparición del concepto de *Phubbing.* Recuperado de: http://es.wikipedia.org/wiki/Phubbing

igualmente necesarias, *el uso excesivo de las nuevas tecnologías puede conducir a alteraciones y trastornos físicos, así como psicológicos, como es el abuso o la adicción a las nuevas tecnologías*[17]. Para ampliar información, recomendamos la lectura del monográfico "Tecnoadicciones".

- **Establecer edades a las que el menor podrá acceder a la Red, tener su primer móvil**, tableta, portátil o cuenta en la red social de moda, entre otros servicios. Así, cada familia debe establecer sus propios límites y edades atendiendo siempre a la lógica y el sentido común. La tecnología no debe servir para aparcar a los niños en ella y que sea un entretenimiento más. Por el contrario, los padres deben usarlas con ellos para que éstos sean capaces de emplearlas de forma segura y competente, convirtiéndose así en un elemento de uso y disfrute más de toda la familia.

- **Limitar programas, aplicaciones, webs y servicios en función de la edad**. Así, cuando surjan programas o aplicaciones nuevas, los padres deberán informarse de sus condiciones de uso, de qué edad es a partir de la cual se puede utilizar o la recomendada, al igual que se hace o debe hacerse con las películas y los videojuegos.

- **Limitar la "subida" de datos personales y de imágenes a la Red** para salvaguardar la privacidad familiar y personal del menor es algo completamente imprescindible en la actualidad. Para ampliar información al respecto, consultar el monográfico "Gestión de la privacidad e identidad digital".

- **Educar a los menores en la sensibilidad y el respeto.** Debemos indicarles que todos tenemos nuestros derechos, también en Internet y que aquello que no nos gustaría que nos hicieran a nosotros, no debemos hacerlo, ni en el mundo físico ni en el digital.

- **Enseñar a los menores a no responder a las provocaciones y a los malos modos de otros.** A pesar de ello, deben conocer aquellos mecanismos

17 Echeburúa, E. (2010) Adicción a las nuevas tecnologías y a las redes sociales en jóvenes: un nuevo reto. Revista española de drogodependencias. 37(4) Págs. 435-447.

disponibles para dar solución a aquellas situaciones en las que se vulneren sus derechos en la red.

- **Educación en un ocio saludable.** Será necesario ofrecer alternativas de ocio a los menores con el fin de evitar el uso abusivo de las TIC.

Además de todo lo anterior no hemos de olvidar que los responsables del menor deben ser un buen ejemplo. Los padres han de tomar conciencia de que son personas muy significativas y de referencia para sus hijos y que por lo tanto son modelos a imitar. Esto supone que han de prestar mucha atención a los mensajes que sobre las nuevas tecnologías se transmiten en la familia, así como al propio uso que de estas nuevas tecnologías se haga en presencia de los hijos.

Netiqueta: educación y buena conducta en la Red

A la hora de interactuar en Internet, hay unas normas no escritas a las que se les ha denominado **netiqueta**, son como las normas cívicas o de urbanidad del mundo digital. Usando buenos modales, facilitamos la convivencia online, cuestión que debemos inculcarles a los menores también. Algunas de las directrices que como padres, madres o tutores hemos de trasladar a los menores en este sentido son:

1. En la Red, hay que tratar a los demás como nos gustaría ser tratados.

2. Escribir en mayúsculas en las nuevas tecnologías significa “gritar”, por lo que no es adecuado utilizarlas.

3. Hay que pensar antes de escribir opiniones, comentarios, etc. Igual que en la vida real, existen muchas formas de expresar nuestra opinión e incluso defenderla, sin faltar ni molestar a nadie.

4. No todos los servicios que ofrecen las nuevas tecnologías tienen las mismas reglas de buen uso. Lo que es válido en una red social no tiene por qué serlo en un blog o en un chat. Es conveniente conocer las normas de uso, prohibiciones y limitaciones antes de usar un servicio.

5. No somos el centro de atención del ciberespacio. Hay que aprender a ser pacientes y a pedir las cosas con respeto y educación. La inmediatez es una de las ventajas y desventajas de Internet, hay que educarles a ser pacientes.

6. No hay que facilitar nunca datos personales de terceros, a no ser por permiso o encargo explícito de éstos.

7. Siempre que se comparte el conocimiento o trabajo de otros, hay que asegurarse que podemos hacerlo y, por supuesto, citar la fuente original

8. Hay que respetar los horarios de todos, igual que no llamamos a un amigo a las 2 de la madrugada entre semana, tampoco habrá que mandarle un WhatsApp o un SMS.

Para ampliar información al respecto, consultar el monográfico “Netiqueta: comportamiento en línea”.

Comunicación familiar

Es imprescindible que en la educación de los hijos haya una comunicación familiar fluida y bidireccional. Así, hay que darles opciones para que puedan expresarse, dialogar y preguntar. La comunicación familiar contribuye a que se establezcan y se estrechen unos vínculos que facilitarán que los hijos recurran a los padres en caso de necesidad o problemas. Y esto es igualmente aplicable en el ámbito de las nuevas tecnologías.

De este modo, uno de los pilares clave de la prevención es transmitir a los hijos una información clara y objetiva respecto a estos riesgos y cuáles son las consecuencias del uso inapropiado de las nuevas tecnologías. Para ello, es imprescindible que, al menos uno de los dos progenitores, tenga unos conceptos mínimos de las TIC, ya que es fundamental que se establezca un vínculo de confianza con el menor en todos estos temas. Antes de ofrecer nuestra perspectiva y darles la información oportuna, debemos informarnos de qué conocen, qué quieren y deben saber y su percepción personal sobre los riesgos de las nuevas tecnologías.

En este sentido, la información que debemos transmitirles en relación a los riesgos de las TIC debe ser:

- Desmontar opiniones e ideas equivocadas que tienen sobre el uso de las TIC.

- Informar a los hijos sobre los riesgos físicos y psicológicos del uso excesivo e irresponsable.

- Ayudarles a comprender los riesgos de una conducta inadecuada en la Red: imposibilidad de borrar de la Red lo compartido y colgado, las posibles denuncias y consecuencias legales, las consecuencias para los afectados y su entorno, el detrimento de la propia imagen al obrar de mala fe, consecuencias en el futuro personal y laboral, etc.

El hecho de que a los menores se les considere nativos digitales no quiere decir que sean *competentes digitales*. La competencia digital se refiere a las capacidades y habilidades para interactuar con las herramientas tecnológicas, con la finalidad de sacarles el máximo provecho y hacerlo de una forma segura.

Educación digital tecnológica

La segunda de las vertientes educativas a llevar a cabo dentro de la educación digital es la **educación tecnológica,** una tarea que se lleva a cabo normalmente desde los centros educativos pero que no por eso se debe desatender desde la familia. La educación tecnológica es la enseñanza del uso adecuado de los distintos programas informáticos, servicios de Internet y dispositivos que utilizamos para conectarnos a Internet. Así, dentro de la educación tecnológica, se debe enseñar cuestiones básicas como:

- **Dispositivos:** funcionamiento de los distintos dispositivos tecnológicos, mantenimiento de los mismos y cuestiones relacionadas con la seguridad y protección de la información sensible y confidencial que en ellos pueda existir (actualizaciones, cuentas de usuario, antivirus).

- **Programas informáticos:** funcionamiento de los distintos programas informáticos que al menor le puedan resultar de utilidad (navegadores, buscadores, procesadores de texto, programas de presentación de trabajos, antivirus, etc.)

- **Servicios de Internet:** funcionamiento de dichos servicios que el menor pueda utilizar, apertura de perfiles, gestión de los datos que en ellos se puedan publicar o facilitar, cierre de sesiones, gestión adecuada de contraseñas, opciones de bloqueo, denuncia, cierre, configuración de los perfiles, forma de acceso y distintas posibilidades que ofrezca el servicio.

La edad a la que debemos enseñar a un menor a utilizar los dispositivos tecnológicos es “cuanto antes”. Indicar una edad exacta a la que empezar a enseñarles estas cuestiones informáticas es muy difícil, ya que dependerá de muchos factores: del interés del propio niño/a, de si tenemos dispositivos en casa o no para poder enseñarle, de los mayores o menores conocimientos de los padres o incluso de la disponibilidad de los mismos. A pesar de ello, la necesidad de educar en tecnología debe hacerse patente desde el comienzo del uso de la misma por parte del menor.

Algo en lo que tenemos que incidir y enseñarles en cada acción que lleven a cabo con las nuevas tecnologías son la seguridad del dispositivo que utilicen y la importancia de la privacidad y los datos personales.

La seguridad del dispositivo

En cuanto a la seguridad del dispositivo que utilicen para conectarse a Internet debemos enseñar a los menores a:

- Proteger el dispositivo con contraseñas, cuentas de usuario propias, establecer sistemas de bloqueo de pantalla para casos de robo o pérdida, etc.
- Cerrar las sesiones que abran en aquellos servicios que sea preciso y en aquellos ordenadores o dispositivos que son de otras personas, de cibercafés, de amigos, en *Wifis* libres, etc.
- Utilizar aplicaciones específicas que permiten añadir un plus de seguridad a los documentos, imágenes, contactos, vídeos… que pueda contener el dispositivo.
- Pensar antes de compartir información y de acceder a servicios web o páginas no confiables.
- Leer los permisos que se otorgan, las políticas de privacidad y de uso de los servicios web, a desconfiar de los programas y archivos de descarga de la Red, a pasar el antivirus de todo aquello que llegue a sus dispositivos para evitar infecciones, etc.
- Apagar el dispositivo cuando no se utilice, al igual que el *Wifi*, el *bluetooth,* GPS, etc.
- Mantener sus contraseñas en secreto y no compartirlas con los demás.

- Tener un buen antivirus, herramientas *antimalware,* bloqueo de publicidad y *antipop-ups,* etc., a hacer exámenes del dispositivo de vez en cuando si no se tienen programados y a tenerlos bien actualizados.

- Obviar todas aquellas notificaciones que puedan llegar solicitando datos, descargas de programas, aplicaciones o juegos, cuando pidan activar el GPS o los datos de geolocalización.

- Leer y buscar noticias sobre seguridad de los dispositivos, en definitiva, a generar una cultura de seguridad en la conexión y uso de Internet.

Para ampliar información sobre este tema, recomendamos la lectura del monográfico "Protección ante virus y fraudes".

La privacidad y la importancia de los datos personales

Hay que ser muy insistentes con ellos en el tema de la privacidad de sus datos personales y de la información familiar:

- No compartir imágenes propias, o imágenes de la familia o de terceros sin el permiso de ellos, ni tampoco a etiquetar a otros sin su consentimiento.

- Avisar a los amigos de que no compartan fotos o vídeos en los que salga él/ella sin su conocimiento.

- No divulgar información personal sobre los horarios, el lugar de residencia, el teléfono, el colegio o instituto, los hábitos diarios, las amistades…

- Diferenciar los conceptos de íntimo (aquello que a lo mejor puede compartir con su grupo de amigos cercanos) y privado (aquello que no se debe compartir).

- Enseñarles a configurar la privacidad de aquellos servicios web que utilicen y que lo permiten, como por ejemplo las redes sociales.

- A informar a los padres y a denunciar todos los atentados contra su privacidad y contra la de su familia.

- A desconfiar en Internet de quien está al otro lado, nunca se tiene el 100 % de seguridad de con quien se está hablando, así que no se deben facilitar datos personales.

Para ampliar información, recomendamos la lectura del monográfico “Gestión de la privacidad e identidad digital”.

Principales recomendaciones para una adecuada y eficaz mediación parental

Vamos a ver las principales recomendaciones para evitar los riesgos de las nuevas tecnologías en los menores y que los responsables de su educación practiquen una adecuada y eficaz mediación parental.

- **Sea el mejor ejemplo para sus hijos.** No podemos exigir normas a los menores que posterior o anteriormente nosotros no cumplimos.

- **Los dispositivos deben ser de uso común en la familia, no privativos.** Se debe evitar en la medida de lo posible que haya ordenador, tablet, videoconsola, televisión… en la habitación del menor. Se debe pactar que deje el móvil fuera de su habitación o lugar de trabajo en los ratos de estudio o de trabajo. Además de los riesgos de las TIC, exponemos al menor a un descenso del rendimiento académico.

- **No demonice las nuevas tecnologías.** Prohibir o impedir el acceso es una estrategia errónea ante los riesgos de las nuevas tecnologías. Hay que fomentar el uso responsable de las mismas.

- **Establezca reglas y límites.** Hay que estar informados, coordinarse entre los progenitores y hacer partícipe al menor del establecimiento de las normas, para que aumenta la probabilidad de acatarlas. Hay que establecer edades, horarios y normas de uso, en la familia y el hogar, y fuera del hogar. Use programas y aplicaciones de control parental que garanticen el cumplimiento de las normas establecidas y ayuden a saber cómo son las interacciones del menor con la Red.

- **Elija contenidos apropiados para su edad.** Busque sitios web, aplicaciones, videojuegos y programas adecuados a su edad en relación a su contenido.

Haga caso de las indicaciones y de códigos como el código PEGI en el caso de los videojuegos.

- **Preocúpese de conocer el entorno digital y la tecnología.** Es necesario informarse, seguir webs, blogs y organizaciones de referencia, que actualicen conocimientos sobre nuevas tecnologías, campañas en marcha, alertas, casos, noticias, etc.

- **Interésese por lo que hace en Internet y con las nuevas tecnologías.** Las TIC no deben producir una brecha generacional entre los miembros de la familia, deben ser un tema común, que se comparta y usen en familia, y que estrechen relaciones.

- **Ayúdele a pensar críticamente sobre lo que encuentran en la Red.** No todo es cierto en Internet, hay que fomentar el espíritu crítico y la búsqueda de información basándose en distintas fuentes y en fuentes de entidad y prestigio en la materia. Enséñele la importancia de conocer y leer las condiciones de uso de los servicios que se utilicen y los permisos que se conceden para evitar sorpresas y pérdidas de privacidad.

- **Transmita confianza al menor.** Hágale entender que puede recurrir a la familia también ante los problemas y dudas que puedan surgir en el ámbito de las TIC.

- **Enséñele a mantener la información personal en privado.** Enséñele la importancia de no compartir información personal y familiar como domicilio, nombres, teléfonos, costumbres, horarios, colegios y lugares de trabajo…, de gestionar adecuadamente las redes sociales y servicios que use en Internet, de cerrar sesiones y cuentas cuando no sea su dispositivo, a usar *nicks* o alias e imágenes de perfil que no sean la propia, y las consecuencias posibles de compartir dicha información personal y familiar.

- **Conozca cómo se presentan a sí mismos en las Redes Sociales y su actividad en ellas.** Cuáles son sus contactos, lo que comparten, las imágenes que suben, los perfiles que visitan, cómo se describan y lo que comentan, etc.

- **Discreción en la publicación de fotografías.** Hay que sensibilizarlos para que no compartan imágenes propias con poca ropa, en determinadas posturas, imágenes en las que salen terceros sin permiso, etc.

- **Recuérdeles que deben respetar a los demás.** Debemos convertirlos en ciudadanos digitales responsables. Deben comportarse como lo hacen en la vida física, y no "pisar" los derechos de los demás ni hacer lo que no le gustaría que le hicieran.

- **Enséñele a no fiarse al 100% de con quién habla en Internet.** En el mundo digital hay programas para trucar todo, la imagen, el audio, el vídeo… con lo que cualquiera puede hacerse pasar por otro, engañar *(grooming),* robar la identidad de alguien conocido (suplantación), etc.

- **Enséñele a crear contraseñas seguras y robustas y a proteger sus dispositivos.** Tener contraseñas inseguras, es como dejar la puerta de casa abierta, y arriesgarse a que nos roben toda la información o los perfiles. Hay que proteger los dispositivos con los que accedemos a la Red, para evitar pérdidas de información o virus informáticos con los que luego controlen nuestros dispositivos para poder cometer fraudes y delitos en nuestro nombre. Muéstrele la importancia de tener los dispositivos que no se estén utilizando desconectados de Internet y apagados, así como desconectadas todas sus opciones de conectividad si no se utilizan (*Wifi,* GPS, *Bluetooth,* etc.). Enséñele a usar programas originales, a actualizar los programas, antivirus y sistemas operativos, y reducir el riesgo de infecciones no clicando en adjuntos de desconocidos o enlaces de dudosa procedencia.

- **Enséñele la importancia de tener un equilibrio en el tiempo de uso de las TIC.** Las TIC tienen muchas potencialidades y usos positivos, pero si se invierte demasiado tiempo en ellas, además del riesgo de afecciones físico-psicológicas, se pierde cosas del mundo físico o analógico.

Principales recomendaciones de mediación parental por grupos de edad

Infantil (3 a 5 años)

- Hay que transmitirles a estas edades que los dispositivos que puedan utilizar para conectarse a Internet (*smartphone,* tableta, ordenador, videoconsola,

Smart tv…) deben utilizarlos solo en presencia de algún adulto, haciéndoles comprender que Internet tiene sus riesgos y que es mejor por su propia seguridad que esté un adulto presente mientras lo utilice.

- Es necesario crear para estas edades, entornos e interfaces adecuadas a su edad, de manera que sean sencillas de utilizar y seguras, eliminando la posibilidad de la publicidad y de enlaces externos que pongan en riesgo al menor y al dispositivo. Para esto es necesario crear cuentas de usuario en el dispositivo y organizar el entorno de trabajo del menor. Se pueden eliminar los iconos de acceso a la Red y dejar algún acceso directo a buscadores infantiles específicos y seguros para su edad. También se debe configurar el navegador que utilice para acceder a la Red (Internet Explorer, Mozilla, Chrome…) en sus opciones de control parental; añadir *plugins* o programas que bloquean la publicidad, los molestos pop-ups, robapáginas, banners, etc., y acudir a las opciones de configuración del control parental del sistema operativo que use.

- Enseñarles que no se debe proporcionar información personal y/o familiar a través de la red, incluidas fotografías o cualquier tipo de documento por correo electrónico, WhatsApp, etc., con información privada. La privacidad propia y de los demás es algo en lo que hay que insistirles desde pequeños.

- Es bueno recordarles, que por debajo de 14 años no pueden abrirse cuentas en determinados servicios de la Red como las redes sociales, WhatsApp, Gmail… y que tampoco deben usar el de sus padres, ya que cualquier acto inadecuado la responsabilidad del mismo será para los padres, además de que no es legal en España, por lo que si se permite, se le estará enseñando a "saltarse" la legislación desde bien pequeño.

- Hay que decir a los niños y niñas que si alguien o algo les hace sentir mal estando conectados a Internet se lo comuniquen a un adulto. Hay que hacerles entender que a esa edad pueden sucederles cosas malas en la Red y que no necesariamente pasan por su culpa, por lo que deben comunicarlo para ponerlo freno.

Primaria (6 a 12 años)

- Es la etapa en la que verdaderamente comienzan a interactuar con Internet, con lo que es la mejor etapa para empezar a inculcar una serie de valores y normas de buen uso y comportamiento ante las TIC en los menores.

- Igual que en el ciclo de edad anterior es conveniente configurar cuentas de usuario, entornos de trabajo, eliminar publicidad, activar filtros y opciones de control parental, etc.

- Hay que enseñarles normas de buena conducta en la Red para evitar riesgos y sucesos innecesarios. La netiqueta (conjunto de normas de buena educación en la Red) es algo que deben aprender desde bien pequeños.

- A estas edades sigue siendo necesaria una supervisión de los adultos acerca de lo que los menores hacen en Internet. Debe ser algo consensuado y pactado con el menor, no se espía al menor, se vela por su seguridad en las TIC.

- A esta edad empieza a ser fundamental insistir en la importancia de temas como la seguridad del dispositivo, la privacidad propia y de los demás, el contactar con personas desconocidas en la Red, etc., ya que es posible que sean víctimas de intentos de *grooming* a estas edades si no hay una supervisión adecuada. Hay que insistirles en la necesidad de que no se fíen de nadie que hayan conocido exclusivamente por la Red, y menos quedar físicamente con ellos.

- Es la franja de edad de los videojuegos y las videoconsolas. Hay que remarcar que las modernas videoconsolas tienen acceso a la Red por *Wifi* y también webcam, con lo que tienen los mismos riesgos que un ordenador o *smartphone.* Además se deben supervisar y adquirir los videojuegos en función de la edad del menor y del contenido que tengan, atendiendo a las indicaciones del código PEGI, e igualmente para los juegos online.

- También en esta franja hay muchos menores que comienzan a tener un móvil, con lo que habrá que hablar de la seguridad en estos dispositivos, de los riesgos específicos, de un uso y un consumo responsable, de marcar normas de uso, etc.

- Es muy importante a esta edad establecer límites de uso de las nuevas tecnologías, recordarles que deben usarse con sentido común, sin abusar de ellas y sin restar tiempo a otras actividades, evitando la dependencia, el cansancio, afecciones físicas por el abuso, disminución del rendimiento académico, etc.

Secundaria (13 a 16 años)

- Es la franja de edad en la que legalmente pueden empezar a utilizar servicios de la Red como las redes sociales o los servicios de mensajería instantánea. Es necesario establecer en el hogar una serie de límites y normas de uso de las TIC, tanto de sus propios dispositivos como de los que usen en otros lugares.

- Es necesario conversar sobre las TIC en la familia con la idea crear un vínculo en estos temas y facilitar el hecho de que acudan a los adultos en caso de problemas o dificultades antes las TIC.

- Puede ser interesante crear una especie de manifiesto recogido en un documento tangible, en cooperación con el menor, de buenas prácticas ante las TIC, donde se motive al joven para su firma y compromiso desde la familia y sirva de recordatorio.

- Seguir insistiendo en estas edades en temas como la seguridad informática, el *sexting* que se suele iniciar como práctica en esta franja de edad, la privacidad sobre todo en redes sociales y con el tema de las imágenes y vídeos, el *ciberbullying* y la buena educación en el uso de las TIC, el asumir la responsabilidad de los propios actos también en la Red, el conocer las consecuencias legales de los actos inadecuados en Internet, el no abusar demasiadas horas con las TIC estableciendo límites horarios, etc.

- Es necesario controlar el tipo de descargas que realizan de la Red con la finalidad de evitar las descargas ilegales y la entrada de virus y de malware en los dispositivos.

- Respecto al tema del acceso a páginas con contenido inadecuado del tipo de violencia, xenofobia, terrorismo, anorexia y bulimia, modas absurdas y peligrosas, pornografía, etc., esta edad es la más crítica. Ellos quieren conocer,

explorar, experimentar, además de tener cierta tendencia al riesgo y es necesario que aprendan a discernir, pero es importante que lo hagan desde una visión crítica, y esto requiere que haya habido previamente un proceso de formación y una conciencia adecuada, que se adquiere si se ha seguido una trayectoria en ese sentido desde pequeños, tanto desde la familia como desde la escuela.

- Es igualmente importante que sepan ver que todo lo que hay en Internet no tiene por qué ser cierto o real, deben aprender a contrastar, a buscar buenas fuentes de información, etc.

Bachiller (17-18 años)

- A esta edad empiezan a tener un buen nivel de madurez para identificar y protegerse de los peligros de la Red. En aquellas familias en las que haya hermanos de distintas edades, puede ser muy útil que los hermanos mayores se involucren en la educación en el ámbito de las TIC de sus hermanos más pequeños.

- A estas edades, sin restarles ni la privacidad ni la autonomía que demandan, habrá que seguir insistiendo en los principales temas tratados en las anteriores franjas de edad: privacidad, seguridad, buena educación, no abuso de las TIC, etc.

- La comunicación con ellos a estas edades debe ser fluida, ya que es una de las principales carencias, por lo que es conveniente transmitir confianza y servirlos de punto de apoyo en aquellas situaciones en las que se presenten problemas o puedan estar molestos con algo que les haya pasado con las TIC. Se les debe de informar cuáles son los canales de denuncia que tienen para comunicar hechos contra sí mismos o contra otros, las consecuencias legales de sus acciones cuando pasan a la mayoría de edad y la responsabilidad de sus propios actos en la Red.

Herramientas y recursos de mediación parental

Cuando hablamos de mediación parental indudablemente pensamos rápido en los programas y aplicaciones de control parental, pero considerar dentro de este grupo a los programas de control parental exclusivamente sería un grave error ya que existe

un abanico mucho más amplio de recursos del que los responsables de la educación del menor se pueden servir para protegerle de los riesgos de las nuevas tecnologías.

Así, los recursos para la mediación parental serían todos aquellos que ayudan al adulto a guiar y educar al menor en sus interacciones con las TIC y a prevenir los riesgos y solucionar los que se produzcan. Luego restringirnos sólo a los programas de control parental, aunque sean una parte destacada de los recursos, sería un error.

Entendiéndolo así, podemos considerar recursos para la mediación parental a:

- Webs y blogs de organizaciones dedicadas a la prevención de los riesgos de las TIC, con continuas campañas y actualizaciones que conviene consultar y seguir para estar informados.
- Estudios, noticias y estadísticas publicadas para conocer la situación actual y los hábitos y riesgos existentes.
- Guías y manuales sobre educación en el uso de las TIC.
- Recursos para educar a los menores como vídeos, juegos, cuentos, cómics, videotutoriales, concursos…
- Herramientas de control parental.
- Herramientas específicas de seguimiento y supervisión de la actividad en las redes sociales.
- Cursos, charlas y jornadas online y/o presenciales sobre los riesgos de las nuevas tecnologías.
- Navegadores infantiles, buscadores infantiles y redes sociales infantiles, que ya incorporan filtros y parámetros de control parental.
- Entornos seguros para los sistemas operativos de los móviles y tabletas y apps de control parental.
- Opciones de denuncia: webs de las fuerzas y cuerpos de seguridad, opciones de denuncia y bloqueo de servicios y redes sociales, organizaciones que facilitan la denuncia de acosadores y/o de contenido, etc.

- Herramientas, programas y aplicaciones para la protección de la información y la seguridad de los dispositivos.

Control parental

Se llama *Control Parental* a cualquier herramienta o programa tecnológico que permita a los padres controlar y/o limitar el uso que un menor pueda hacer del dispositivo o de Internet.

Hoy en día tenemos una grandísima oferta de programas de control parental, tanto de forma gratuita como de pago, pero también podemos encontrar opciones de control parental en muchos dispositivos y programas que ya veníamos utilizando.

Podemos encontrar herramientas de control parental en:

- Los principales sistemas operativos que utilizamos (Windows, MacOS, Android, Linux, iOS…)
- *Plugins* o programas que se anexionan a nuestros principales navegadores (Internet Explorer, Google Chrome, Mozilla Firefox…) permitiendo opciones de control parental para la navegación.
- Herramientas web y *software* específico, de pago o gratuitos, que descargamos en nuestros dispositivos (ordenadores, tabletas y móviles) y nos ofrecen multitud de opciones.
- *Routers*, que proporcionan el acceso a Internet, que ofrecen opciones de control parental.
- Opciones de control parental que brindan los principales Proveedores de Servicios (ISP), aquellas compañías que nos ofrecen la conexión a Internet en nuestros dispositivos y que también brindan opciones y programas de control parental a los usuarios.
- En las actuales videoconsolas, así como en las modernas Smart Tv o la TDT, ofrecen opciones de control parental que deben ser exploradas y configuradas.

Funciones de los programas de control parental

- **Bloqueo de palabras clave.** Consiste en bloquear el acceso a las páginas que contengan aquellas palabras que creamos que llevan asociados contenidos inapropiados (sexo, apuestas, drogas, casino,…). Tiene dos pegas importantes: una, es que con ésta técnica se pueden producir numerosos "falsos positivos", es decir, corremos el peligro de bloquear contenidos que pueden no ser nocivos para los menores ya que se bloquean las palabras aisladamente, sin tener en cuenta el contexto en el que se hayan integradas, y dos, hay muchas páginas que tienen contenido inapropiado y no incluyen las palabras clave en su contenido, por lo que programa no las bloquea y el menor podrá acceder a ellas.

- **Control del tiempo.** Podemos limitar el tiempo que se conecte un determinado dispositivo a Internet, estableciendo los días de la semana y el horario específico para cada uno de los días. Resulta muy útil cuando no queremos que el menor se conecte cuando está solo.

- **Bloqueo de programas y aplicaciones.** Podemos bloquear que se ejecuten en el dispositivo determinados servicios y programas del tipo mensajería instantánea, correo electrónico, descarga de programas, juegos, reproductores de vídeo y audio, etc.

- **Listas blancas y negras.** Permiten la configuración de listas positivas (blancas), a las que se permite el acceso y listas negativas (negras), a las que se deniega.

    1. Las listas negras consisten en determinar las páginas a las que se restringe el acceso. Debido a la rapidez con la que se añaden cada día contenidos y páginas a la Red es prácticamente imposible tenerlas actualizadas.

    2. Las listas blancas son más restrictivas pero aseguran la denegación de acceso a determinados contenidos. A través de esta opción, el menor solo podría ingresar en las webs y servicios que hayamos introducido nosotros manualmente en el programa de control parental para ese dispositivo.

- **Etiquetado de páginas.** Todas las páginas contienen una serie de etiquetas de clasificación que determinan el contenido de la misma. Con esta técnica se permite el bloqueo por parte de navegadores y herramientas a páginas que contengan ciertos contenidos determinados por los padres/educadores.

- **Registros.** Realiza un recuento de las páginas que han sido visitadas o a las que se ha intentado visitar. Sirve para revisar y comprobar los hábitos de navegación de los menores. Esta técnica no precisa que el menor sea consciente de que los contenidos están siendo limitados, pero la base de una navegación segura es el diálogo entre padres/educadores y menores.

- **Monitorización.** Son herramientas que realizan un seguimiento de la actividad del menor al usar la Red y el dispositivo. Por ejemplo, registran todas las páginas web visitadas para posteriormente poder supervisar los hábitos de navegación de los menores, los términos de búsqueda que utiliza, los perfiles en redes sociales que visita, pueden hasta informar de las conversaciones en chats, mensajería, etc.

- ***Keyloggers.*** Un *keylogger* es un *software* o *hardware* que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo en el que se haya instalado, es decir, nos puede dar un informe de todo el texto que se ha tecleado con el teclado del dispositivo.

- **Herramientas que bloquean la información que sale del ordenador.** Son aplicaciones que impiden difundir información personal y sensible. Esto es especialmente útil a la hora de cumplimentar formularios y hojas de registro en Internet o comprar a través de Internet con la tarjeta de crédito. Puede ser utilizado tanto para la red, como para el correo electrónico, como para los *chats,* etc.

- **Navegadores infantiles.** Son herramientas que dan acceso a páginas adecuadas para los niños y adolescentes. Tienen un diseño y características apropiadas al público menor y permiten el uso de diferentes perfiles, en función de la edad del usuario.

Ejemplo de configuración de herramienta de control parental: Qustodio

Existen muchos programas y aplicaciones de control parental en el mercado, muchos de ellos con muchas y muy buenas funcionalidades, algunos de ellos son gratuitos y otros de pago, algunos tienen las dos versiones, la gratuita y luego, con más funcionalidades, la de pago.

Quizás, debido a su sencillez, a la gran cantidad de funciones que tiene y a que es multiplataforma, es decir, que desde una misma cuenta y panel de control, se pueden configurar y controlar distintos dispositivos como el ordenador, la tableta y el *smartphone*, mostramos *Qustodio*.

Lo primero que se debe hacer es crear cuentas de usuario en los dispositivos que vaya a utilizar el menor, protegiendo la del adulto (administrador) con contraseña, ya que el menor debe acceder al dispositivo a través de esas cuentas de usuario, y configuraremos el control parental para esa cuenta de usuario. Para ello podemos consultar los siguientes enlaces:

- Crear cuentas de usuario en Windows
- Crear cuentas de usuario en Mac
- Crear cuentas de usuario en Android para tablets
- Crear cuentas de usuario en Android para móviles versión 5.0

Una vez creadas las cuentas de usuario, tenemos que instalar Qustodio en los distintos dispositivos que vaya a utilizar el menor y queramos supervisar, configurar y limitar, estando disponible para los sistemas operativos que muestra la siguiente imagen. Para ello, acudimos a http://www.qustodio.com/es/family/downloads y descargamos la versión adecuada al dispositivo.

Una vez instalado en los dispositivos, desde nuestro PC podemos crear una cuenta de usuario con un correo electrónico y una contraseña, para, desde esa cuenta, configurar todos los parámetros en cada uno de los dispositivos y usuarios.

A partir de aquí, podemos entrar en nuestra cuenta de Qustodio en el siguiente enlace, acceso, e ingresar nuestro correo electrónico y contraseña para acceder al panel de control.

Una vez hemos accedido, nos saldrán los distintos dispositivos donde tenemos instalado el programa, y en cada uno de ellos, los menores que hayamos añadido. Desde ahí, tenemos una serie de pestañas superiores “Resumen de actividad”, “Actividad social”, “Navegación” y “Cronología de actividad” que nos informan de la actividad del menor en ese dispositivo. Y una última pestaña “Reglas” en las que podremos configurar el control parental con las opciones que nos ofrecen para: Navegación Web, Límites de uso, Programas, Monitoreo Social, Llamadas y SMS, Localización y Botón de Pánico.

En la pestaña de *Navegación web* pondremos los sitios web que no queramos que visiten, establecer categorías por palabras clave, añadir excepciones, etc.

En la pestaña *Límites de uso* podremos establecer el calendario semanal de horas que permitiremos que ese dispositivo se conecte a Internet. Podemos establecer también permisos de conexión, bloqueos de tiempo, bloqueos de dispositivo completo y alertas, que nos llegarán a nuestra cuenta de correo electrónico vinculado, como se muestra en las siguientes imágenes.

En la pestaña *Programas* se puede bloquear el acceso a determinados programas o aplicaciones que consideremos que el menor no debe acceder (programas del PC o aplicaciones del móvil o la tableta como *Snapchat, WhatsApp*…)

La pestaña *Monitoreo Social* nos permite hacer un seguimiento de la actividad del menor en la Red Social de Facebook.

Desde la pestaña de *Llamadas y SMS* podemos configurar la supervisión de las llamadas y los SMS recibidos, así como bloquear llamadas entrantes, llamadas salientes, los SMS entrantes o bloquear números de teléfono determinados, tal y como se muestra en las imágenes.

La pestaña de *Localización* nos permite hacer un seguimiento de los terminales móviles en función de su geolocalización y actualizar esta geolocalización con la frecuencia que nosotros marquemos.

Y, por último, la pestaña *Botón de pánico*, nos sirve para configurar una aplicación para el terminal móvil que utilice el menor, en la pantalla de inicio de Qustodio del móvil para que, en caso de necesidad y de que el menor lo apriete, mande un correo y un SMS con la geolocalización de móvil hasta 4 correos electrónicos y 4 móviles que nosotros marquemos como de confianza.

Para completar más información sobre las funcionalidades y opciones de Qustodio, acceder al siguiente enlace: Cómo funciona Qustodio.

También señalar que los centros educativos tienen la posibilidad de participar en el **Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos**[18], 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. En el marco de este Plan los miembros de las Fuerzas y Cuerpos de Seguridad realizan charlas, visitas y actividades en centros escolares, dirigidas tanto al alumnado como al resto de la comunidad educativa (directivos, personal docente y Asociaciones de Madres y Padres de Alumnos). Como medidas adicionales, se contemplan acciones de sensibilización y formación dirigidas a concienciar sobre el "uso responsable de las nuevas tecnologías y los riesgos que las mismas pueden implicar, promoviendo, a su vez, la comunicación a su entorno familiar, educativo o a las Fuerzas de Seguridad de los hechos de los que pueden ser víctimas o testigos.

6. Mecanismos de respuesta y soporte ante un incidente

A continuación, si los padres, madres, tutores o educadores son conscientes de que el menor ha sufrido un incidente relacionado con el uso de las TIC, deben tener en

[18]Ministerio del Interior. Instrucción nº 7/2013 de la Secretaría de Seguridad, sobre el "Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos". Recuperado de: http://www.interior.gob.es/documents/642012/1568685/Instruccion_7_2013.pdf/cef1a61c-8fe4-458d-ae0d-ca1f3d336ace

cuenta una serie de indicaciones para que su actuación sea adecuada y dé respuesta y soporte a la situación dada. Así, la ausencia de una adecuada mediación parental puede propiciar el desarrollo de incidentes vinculados al uso de las TIC tales como *ciberbullying* o ciberacoso escolar, *sexting*, *grooming,* tecnoadicciones, suplantación de identidad, establecimiento de vínculos con comunidades peligrosas, infección por virus o fraudes, acceso a contenidos inapropiados o aquellos relacionados con una inadecuada gestión de la privacidad o identidad digital, entre otros. De este modo, aunque cada incidente, dada su naturaleza y características propias, debe abordarse de una forma diferente, podemos ofrecer unas pautas generales sobre cómo abordarlos a modo de orientación:

1. **Escuche y dialogue**. Pregunte a su hijo lo que está sucediendo, escúchele atentamente y ayúdele a expresar emociones y preocupaciones (use frases como «Cuéntame más sobre eso»). Para facilitar el diálogo muéstrese sereno y adopte una actitud de comprensión y atención, no es el momento de juzgarle. Si encuentra reticencias al diálogo los adolescentes tienen su propia dinámica social que generalmente no incluye a sus padres- promueva que hable con amigos u otros adultos de confianza para que le ayuden a gestionar la situación.

2. **Refuerce su autoestima y no le culpabilice**. Asegúrese de que entiende la problemática asociada al incidente y haga hincapié en que no está solo, que usted está allí para ayudarle a resolver la situación con la dignidad y el respeto que toda persona se merece. Si bien él puede haber cometido errores en ningún caso justifican lo que le está sucediendo. Sea positivo, reconozca su valentía por haber pedido ayuda y/o dejarse ayudar y hágale saber que se solucionará.

3. **Actué, trace un plan**. Actúe inmediatamente, no espere a que el incidente cese por sí solo porque el problema podría agravarse. Proponga una respuesta eficaz a la situación y cuente con la cooperación de su hijo para llevarla a cabo. Asegúrese de que el menor entiende cuáles son los siguientes pasos a realizar. El objetivo es que salga reforzado y se sienta parte de la solución.

4. **Comunique la situación al centro educativo**. En caso de que el incidente esté vinculado con el centro educativo es muy importante que sean conocedores de la situación, ya que la escuela es el principal lugar de relación del menor. La mayoría de los centros educativos están sensibilizados sobre el ciberacoso y muchos de ellos disponen de protocolos de actuación en sus planes de convivencia. Cuando

hable con el centro educativo sobre la situación de su hijo trate de no sobrerreaccionar, tenga presente que lo más importante es trabajar conjuntamente para resolver la situación – déjeles claro que usted está para ayudar y que confía en el centro educativo de la misma manera en que espera que ellos confíen en usted.

5. **Comunique lo ocurrido a su pediatra.** En caso de que el incidente haya afectado a la salud del menor este debe ser valorado por su pediatra para tratar los síntomas que tiene, para prevenir que la situación empeore y para ayudarle en los pasos a seguir.

6. **Aconséjele sobre cómo actuar ante futuras situaciones**. Se trata de evitar que el problema se reproduzca en el futuro. Trasládele las recomendaciones oportunas para minimizar las probabilidades de que vuelva a ocurrir. Ayúdele a aprender de sus errores sin culpabilizarle, haciéndole saber que todos nos equivocamos y que lo valiente es aprender de los errores.

7. **Busque la ayuda de expertos**. Las siguientes entidades disponen de «Líneas de Ayuda» conformadas por abogados, psicólogos y expertos en seguridad infantil con la que sensibilizar, informar y mediar ante incidentes con las TIC:

    a. Fundación ANAR: www.anar.org

    b. Padres 2.0 (ONG): http://padres20.org

    c. Pantallas Amigas: http://www.pantallasamigas.net

    d. Fundación Alia2: www.alia2.org

8. En situaciones graves puede notificarlo en:

    a. Fiscal de Menores: goo.gl/U9YZm6

    b. Policía: www.policia.es/

    c. Guardia Civil: www.gdt.guardiacivil.es

9. **Asegúrese que se siente cómodo solicitando su ayuda**. Si el menor presiente que se meterá en problemas o que perderá algún privilegio (como el acceso a Internet o el teléfono móvil) al comunicarle algún incidente en el que se haya visto

involucrado, será más reticente a solicitar su ayuda. Lo que puede provocar que intente resolverlo por sí mismo acrecentando el problema.

Para ampliar información referente a cada uno de los riesgos anteriormente mencionados y poder acceder a los mecanismos de respuesta y de soporte ante incidentes relacionados con los mismos, se recomienda la lectura de los monográficos "Ciberacoso escolar: *ciberbullying*", *"Sexting", "Grooming",* "Suplantación de identidad", "Gestión de privacidad e identidad digital", "Comunidades peligrosas", "Protección ante virus y fraudes", "Tecnoadicciones", "Netiqueta" y "Acceso a contenidos inapropiados".

7. Marco legislativo aplicable a nivel nacional y europeo.

En primer lugar debemos considerar que la mediación parental es una cuestión de la que no existe una normativa y legislación específica, pero sí existe normativa relacionada que afecta a la labor educativa en el ámbito de las nuevas tecnologías por parte de los responsables de la educación de los menores.

Nuestros actos en Internet y en el uso de las nuevas tecnologías, tienen consecuencias bien reales para nosotros mismos, para nuestro entorno más cercano y también para terceros.

Estas consecuencias también tienen sus responsabilidades y pueden ser sancionadas. En la Red parece igualmente, que la falsa sensación de seguridad que nos transmite, posibilita el que no exista legislación al respecto de los actos que en ella se llevan a cabo, pero es totalmente falso.

Es importante transmitir tres mensajes muy claros a los menores:

1. Internet es un espacio regulado por la Ley.

2. En Internet no existe el anonimato absoluto.

3. Puede haber consecuencias legales y penales de sus actos en la Red.

Es igualmente importante que los usuarios menores sepan que este tipo de conductas pueden y deben denunciarse. Por ello, padres y educadores deben unir esfuerzos en pos de un uso de las TIC por parte de los menores seguro y legal.

Debemos de inculcar en los menores la idea de sanción para aquellos comportamientos reprobables en el uso de las TIC, y lejos de quedarnos solo en el aspecto legal, debemos de transmitirles que la posible sanción puede aplicarse en una triple vía: sanción en la familia, sanción en el centro educativo (si atañe a la comunidad educativa) y sanción legal.

En este sentido, veamos la normativa relacionada con tres niveles de responsabilidad distintos: responsabilidades de los padres, de los centros educativos y del propio menor.

Responsabilidades de los padres[19]

En relación a los padres, nuestro Código Civil, en su artículo 154 lo deja bastante claro: “Los hijos no emancipados están bajo la potestad de los padres”.

La patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad, y con respeto a su integridad física y psicológica. Esta potestad comprende los siguientes deberes y obligaciones:

- Velar por ellos, tenerlos en su compañía, alimentarlos, educarlos y procurarles una formación integral.
- Representarlos y administrar sus bienes.

[19] INTECO (2012). *Guía de actuación contra el ciberacoso. Padres y educadores*. http://xuventude.xunta.es/uploads/Gua_de_actuacin_contra_el_ciberacoso.pdf

Si los hijos tuvieran suficiente juicio, deberán ser oídos siempre antes de adoptar decisiones que les afecten. Los padres podrán, en el ejercicio de su potestad, recabar el auxilio de la autoridad."

De aquí se desprende la necesidad lógica de que los padres, mientras tengan bajo su guarda a los menores, deben estar atentos a las actividades de sus hijos con Internet y las nuevas tecnologías de la información y la comunicación, tanto desde el punto de vista legal como del sentido común.

En la *Ley Orgánica 5/2000, de 12 de enero, de Responsabilidad penal de los menores*, establece, en su artículo 61.3 lo siguiente: "Cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guardadores legales o de hecho, por este orden. Cuando éstos no hubieran favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el juez según los casos".

Así pues, en la responsabilidad civil, en el pago de las responsabilidades que pudiesen corresponder, actuarán de forma solidaria los padres juntamente con sus hijos.

Responsabilidad de los centros educativos[20]

En el artículo 1902 del Código Civil se establece:

El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.

En el artículo 1903 del Código Civil se establece:

"Las personas o entidades que sean titulares de un centro docente de enseñanza no superior responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del centro, desarrollando actividades escolares o extraescolares y complementarias"

[20] García Ingelmo, Francisco, M. (2008) "*Responsabilidad legal de los menores*". Recuperado de: http://www.e-legales.net/responsabilidad-penal-de-los-menores.shtml

En la *Ley Orgánica 5/2000, de 12 de enero, de Responsabilidad penal de los menores*, establece, en su artículo 61.3 habla de guardadores, concepto en el que se pueden incluir a los centros docentes durante el horario escolar.

RD 732/1995, de derechos y deberes de los alumnos y normas de convivencia de los centros, en su Art. 46: "Podrán corregirse, de acuerdo con lo dispuesto en este título, los actos contrarios a las normas de convivencia del centro realizados por los alumnos en el recinto escolar o durante la realización de actividades complementarias y extraescolares.

Igualmente, podrán corregirse las actuaciones del alumno que, aunque realizadas fuera del recinto escolar, estén motivadas o directamente relacionadas con la vida escolar y afecten a sus compañeros o a otros miembros de la comunidad educativa".

Este artículo deja bien claro la necesaria implicación de los docentes en el uso inadecuado de las TIC por parte de los menores, fuera del centro y del horario escolar, siempre que afecte a otros compañeros, profesores o a la dinámica habitual del curso escolar.

Ley 2/2010, de 15 de junio, de Autoridad del Profesor de la Comunidad de Madrid. En sus artículos 5 y 6 se ratifica al docente como una autoridad pública y con presunción de veracidad.

Estas dos últimas normativas, dejan bien clara una cuestión:

- Los centros educativos son competentes para la corrección disciplinaria de todo tipo de *ciberbullying* y otros actos inadecuados a través de las TIC, que afecte a la comunidad educativa (todos).

Responsabilidad de los menores[21]

El menor, aun teniendo la condición de menor de edad, debe ser responsable, moralmente, de todos sus actos. Solo, a partir de los 14 años podrá tener también responsabilidad penal. Antes de los 14 años son inimputables.

[21] García Ingelmo, Francisco, M. (2008) "*Responsabilidad legal de los menores*". Recuperado de: http://www.e-legales.net/responsabilidad-penal-de-los-menores.shtml

Las sanciones que pueden establecerse a un menor son muy variadas, y vienen establecidas en el Art. 7 de la Ley Orgánica 5/2000, de 12 de enero, de responsabilidad penal de los menores. Algunas de ellas son:

- Internamiento (en régimen cerrado, semiabierto o abierto).
- Internamiento terapéutico.
- Tratamiento ambulatorio.
- Asistencia a un centro de día.
- Permanencia de fin de semana.
- Libertad vigilada.
- Prohibiciones de aproximarse o comunicarse.
- Prestaciones en beneficio de la comunidad.
- Realización de tareas socio-educativas.
- Amonestaciones, etc.

Otras normativas a destacar

Existen distintas legislaciones a nivel europeo y español que afectan a las interacciones de los menores con Internet, y al papel de los padres y educadores en el control de dichas interacciones:

- Ley Orgánica 1/1996 de Protección Jurídica del Menor:
    1. Los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo.
    2. Los padres o tutores y los poderes públicos velarán porque la información que reciban los menores sea veraz, plural y respetuosa con los principios constitucionales.
- Ley 5/2014, de 9 de octubre, de Protección Social y Jurídica de la Infancia y la Adolescencia de Castilla-La Mancha.

- Código Penal: delitos relativos a la prostitución y corrupción de menores. Artículos 187.1 y 189.4.
- LOPD, Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.
- Ley 1/82 de Protección Civil del Derecho al Honor, a la Intimidad Personal, Familiar y a la Propia Imagen.
- Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.
- Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual.

8. Organismos, entidades y foros de referencia

ORGANISMO / DETALLE
Chaval.es (www.chaval.es) Iniciativa del Ministerio de Industria, Energía y Turismo, puesta en marcha por Red.es para responder a la necesidad de salvar la brecha digital entre padres, madres, tutores y educadores respecto al avance de los menores y jóvenes en el uso de las TIC. Ofrece recursos de sensibilización y formación sobre el ciberacoso.
Oficina de Seguridad del Internauta (www.osi.es) Oficina de Seguridad del Internauta que ofrece una enorme variedad de recursos e información sobre todo lo relativo a la seguridad en las TIC.
INCIBE (www.incibe.es) Portal web del Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE). En su web encontrarás guías, estudios y todos los recursos relacionados con la ciberseguridad.
Pantallas Amigas (www.pantallasamigas.net) 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. Dispone de una línea de ayuda para niños y adolescentes ante situaciones de peligro en Internet.

CyL Digital (www.cyldigital.es)

Web de CyL Digital, dependiente de la Junta de Castilla y león, que ofrece formación presencial y a distancia para padres y educadores sobre temas relativos a las nuevas tecnologías y los menores.

Internet sin riesgos (www.internetsinriesgos.com)

Web dependiente del Cabildo de Tenerife y de la Universidad de La Laguna, que ofrece gran variedad de recursos y formación online para padres y educadores sobre los riesgos de las nuevas tecnologías.

Ciberfamilias (www.ciberfamilias.com)

Web dedicada a la información a familias sobre todo lo relativo a las nuevas tecnologías y sus riesgos, que ofrece gran cantidad de recursos y consejos para la seguridad en Internet y los dispositivos que usamos para conectarnos.

Internet Segura (http://www.educa.jcyl.es/es/webs-tematicas/ciberacoso)

Web de la Junta de Castilla y León que ofrece un programa con recursos para la navegación segura y para los centros educativos.

Hijos digitales (www.hijosdigitales.es)

Blog creado por S2 Grupo, empresa de seguridad de la información, que ofrece a padres e hijos menores de edad contenidos actualizados y relevantes sobre seguridad en el uso de las nuevas tecnologías.

Kiddia (www.kiddia.org)

Blog dependiente de la Junta de Andalucía que ofrece un gran variedad de recursos a padres y menores: guías, teléfonos de ayuda, concursos, vídeos, eventos, formación, etc.

9. Más información

Presentamos a continuación una relación de documentos y recursos para ampliar información sobre mediación parental:

RECURSO / DETALLE
Monográfico: "Protección ante virus y fraudes" Guía para aprender herramientas, sistemas y pautas para proteger a los menores ante virus informáticos y situaciones de fraudes por Internet.
Monográfico: "Acceso a contenidos inapropiados" Guía para establecer pautas para controlar el acceso a contenidos inapropiados a menores de edad, así como acciones para una navegación segura en Internet.
Monográfico: "Gestión de la privacidad e identidad digital" Guía para aprender y transmitir la importancia de que los menores gestionen su visibilidad, reputación y privacidad en la red, así como su huella digital en Internet.
Monográfico: "Netiqueta: comportamiento en línea" Guía para aprender las principales normas de comportamiento en la red, cuya finalidad es respectar a los demás y transmitir la importancia de conductas ciberresponsables por parte de los menores; incidiendo en los procesos de comunicación online.
Monográfico: "*Grooming*" Guía para describir las principales características y manifestaciones de prácticas de *grooming* en la red, identificando las consecuencias para menores; así como estrategias, herramientas y recursos para prevenir y afrontar una situación de acoso sexual de un menor en la red.
Monográfico: "Ciberacoso escolar (*Ciberbullying*)" Guía para conocer y obtener pautas para proteger a los menores ante un acoso entre iguales producido a través de Internet o redes sociales; analizando las principales consecuencias a nivel

psicológico, educativo, social, etc.; así como las implicaciones legales.

Monográfico: "*Sexting*"

Guía para identificar las actuaciones catalogadas como sexting, aportando pautas y estrategias para que padres, madres, tutores y educadores puedan prevenir y actuar ante estas situaciones de riesgo.

Monográfico: "Suplantación de identidad"

"Guía para conocer las principales pautas que padres, madres, tutores y educadores pueden realizar para que los menores gestionen adecuadamente su identidad en la red; así como la detección de identidades falsas, robo de identidad y suplantación.

Monográfico: "Tecnoadicciones"

Guía para abordar las principales adicciones como riesgos a los que se enfrentan los menores tanto en el entorno de internet (redes sociales, juegos online…) como en el uso de dispositivos móviles y otras adicciones.

Monográfico: "Comunidades peligrosas en línea"

Guía para sensibilizar sobre los riesgos de interactuar con comunidades peligrosas en Internet, establecer criterios para que padres, madres, tutores y educadores puedan evaluar una comunidad, red o sitio web que contenga algún tipo de peligrosidad y ofrecer recomendaciones para prevenir y para responder ante esta problemática.

10. Bibliografía

Cervera, L. (2009). "Lo que hacen tus hijos en Internet". Ed.: Integral. Barcelona.

Comisión Europea (2011). *Evaluación comparativa de las herramientas de control parental*. Recuperado de: http://sipbench.eu/index.cfm/secid.3

Echeburúa, E. (2010) *Adicción a las nuevas tecnologías y a las redes sociales en jóvenes: un nuevo reto*. Revista española de drogodependencias. 37(4) Págs. 435-447.

Fundación Telefónica (2012). *Alfabetización digital y competencias informacionales.* Recuperado de: https://ddv.ull.es/users/manarea/public/libro_%20Alfabetizacion_digital.pdf

García Fernández, Fernando (2010). “Internet en la vida de nuestros hijos. ¿Cómo transformar los riesgos en oportunidades?”. Foro Generaciones Interactivas.

García Ingelmo, Francisco, M. (2008) “*Responsabilidad legal de los menores*”. Recuperado de: http://www.e-legales.net/responsabilidad-penal-de-los-menores.shtml

García, F. y Bringué, X. (2007). “Educarhij@sinteractiv@s”. Ed.: Rialp. Madrid.

http://www.interior.gob.es/documents/10180/2563633/Encuesta+sobre+h%C3%A1bitos+de+uso+y+seguridad+de+internet+de+menores+y+j%C3%B3venes+en+Espa%C3%B1a/b88a590a-514d-49a2-9162-f58b7e2cb354

Inmaculada Sánchez Espejo (2008). *La familia como primer agente socializador*. Cuadernos de docencia – Revista digital de educación. Nº 10

Instituto Nacional de Estadística INE (2014). *Encuesta sobre Equipamiento y Uso de las Nuevas Tecnologías de la Información y la Comunicación en los Hogares*. Recuperado de: http://www.ine.es/prensa/np864.pdf

Instituto Nacional de Tecnologías de la Comunicación INTECO (2007). *Guía para la protección legal de los menores*. Recuperado de: https://www.incibe.es/file/KzUa3p_LcPrLSDCfeJCkbA

Instituto Nacional de Tecnologías de la Comunicación INTECO (2009). *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres*. Recuperado de: http://www.pantallasamigas.net/estudios-realizados/pdf/inteco-estudio-uso-seguro-tic-menores.pdf

Instituto Nacional de Tecnologías de la Comunicación INTECO (2010). *Estudio sobre hábitos seguros en el uso de smartphones por niños y adolescentes españoles*. Recuperado de: http://www.menoreseninternet.com/descargas/estudio_smartphones_menores.pdf

Instituto Nacional de Tecnologías de la Comunicación INTECO. (2008). *Guía sobre cómo activar y configurar el control parental de los sistemas operativos.* Recuperado de https://www.incibe.es/file/csra6um3wQbMlxpjOX2pMw

Instituto Nacional de Tecnologías de las Comunicación INTECO (2012). *Guía de actuación contra el ciberacoso*. *Padres y educadores*. Recuperado de: http://xuventude.xunta.es/uploads/Gua_de_actuacin_contra_el_ciberacoso.pdf

Jaúdenes, M. (2006). “Cómo usar las nuevas tecnologías en la familia”. Ed.: Palabra. Madrid.

Junta de Castilla y León (2011). Manual: las TIC en Educación. http://www.jcyl.es/web/jcyl/binarios/158/396/Manual%20Las%20TIC%20en%20Educacion%20Programa%20Aprende.pdf?blobheader=application%2Fpdf%3Bcharset%3DUTF-8&blobheadername1=Cache-Control&blobheadername2=Expires&blobheadername3=Site&blobheadervalue1=no-store%2C

Livingstone, S., Haddon, L., Görzig, A., Ólafsson, K. (2010).“Risks and safety on the internet: The perspective of European children. InitialFindings”. LSE, London: EU Kids Online.

Madrid Salud, Instituto de Adicciones. *Guía para familias. TIC: Prevención de usos problemáticos.* Recuperado de: http://www.madridsalud.es/publicaciones/adicciones/doctecnicos/TIC.pdf

Ministerio del Interior (Junio 2014). *Encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España*. Recuperado de:

Monsoriu Flor, M: (2007).Cómo Controlar lo que hacen tus hijos con el ordenador: Técnicas de hacker para padres. Ed. Creaciones Copyright.

PROTÉGELES Y ACPI (Acción Contra la Pornografía Infantil) Noviembre 2012. *Seguridad infantil y costumbres de los menores en Internet* Estudio realizado a 4.000 menores de entre 10 y 17 años de ambos sexos.