UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica

Universitat Politècnica de València

Protección del menor en la red

Proyecto Final de Carrera

Ingeniería Informática

Autor: Maria Morant Llorca

Director: Juan Vicente Oltra Gutiérrez

Julio 2013

Resumen

El objeto del presente Proyecto de Fin de Carrera es la obtención del título de Ingeniero en Informática expedido por la Universidad Politécnica de Valencia.

Hoy en día, los avances de la web y las TIC han convertido Internet en una herramienta cotidiana y casi imprescindible para la mayoría de nosotros: organizamos nuestros viajes, eventos y quedadas, buscamos trabajo, recuperamos contactos, jugamos en línea con nuestros amigos o felicitamos sus cumpleaños gracias a los recordatorios de las redes sociales. Además, a través de éstas compartimos nuestros pensamientos y gran cantidad de información y contenido personal.

Sin embargo, si debemos destacar lo usuarios más activos en esta nueva generación de medios de comunicación, estos serían los menores de edad, o tal como se les denomina comúnmente, los nativos digitales. Estos niños y adolescentes han nacido ya con las nuevas tecnologías y, probablemente por su inmadurez y desconocimiento, sean los más vulnerables a sufrir alguno de los riesgos que se pueden presentar al hacer uso de las nuevas tecnologías.

Esta memoria pretende recoger los peligros más importantes a los que se puede enfrentar un menor en la red, y plantear las recomendaciones básicas y consejos a seguir para navegar de la forma más segura posible.

Además, analizaremos los términos y condiciones de las redes sociales más importantes e indagaremos en nuestro código penal para saber en qué medida se representan los delitos derivados de las malas prácticas en Internet y que afectan directamente a un menor de edad.

Palabras clave: menores, redes sociales, software, control parental, ciberacoso, grooming, phising, spam, pornografía infantil, legislación, ley, términos, Servicio, TOS, www

Tabla de contenidos

1. Introducción 10
2. Legislación 18
2.1 Introducción 18
2.2 Convenio de Ciberdelincuencia 19
2.2.1 Definición 19
2.2.2 Código penal 22
2.3 Ley orgánica de protección de datos (LOPD) 24
2.3.1 Introducción 24
2.3.2 La ley orgánica de protección de datos y los menores 25
2.3.3 Recomendaciones AEPD 27
2.3.4 Marco internacional 28
2.4 Ley de Servicios para la Sociedad de la Información y de comercio electrónico (LSSICE) 30
2.4.1 Introducción 30
2.4.2 La Ley LSSICE y los menores 32
2.5 Ley de propiedad intelectual 33
2.5.1 Introducción 33
2.5.2 La Ley de propiedad intelectual y los menores de edad 33
3. TOS de las redes sociales 35
3.1 Definición TOS 35
3.2 Criterios utilizados para el análisis de TOS 35
3.3 Creación de perfiles falsos 36
3.4 Casos de estudio 37
3.4.1 Facebook 37
3.4.2 Tuenti 49
3.4.3 Twitter 55
3.4.4 Instagram 64
3.4.5 Servicios Google: Google+ 70
3.4.6 Servicios Google: YouTube 76
3.4.7 Habbo Hotel 82
3.5 Conclusiones 92

4. Software de Control Parental 93
4.1 Introducción al Control Parental 93
4.2 Criterios de clasificación del software de Control Parental 94
4.3 Probando el Software 99
4.3.1 Windows 7 + Windows Live Protección Infantil 99
4.3.2 Norton Online Family 109
4.3.3 K9 Web Protection 119
4.3.4 Qustodio 127
4.4 Inventario software de Control Parental 137
4.4.1 Net Nanny 137
4.4.2 McAfee Family Protection 138
4.4.3 PC Pandora 139
4.4.4 bSecure 139
4.4.5 Cybersitter 140
4.4.6 Control Kids 141
4.4.7 MintNanny 141
4.4.8 Gnome-Nanny 142
4.4.9 Pure Sight 142
4.4.10 Spector Pro 143
4.4.11 Trend Micro Guardian 143
4.4.12 Web Watcher 144
4.4.13 OTROS – Navegadores y Complementos de navegador 145
4.5 Conclusiones 146
5. Casos de estudio 148
5.1 Introducción 148
5.2 Ciberacoso o ciberbullying 149
5.2.1 Definición 149
5.2.2 Algunos datos 154
5.2.3 Cómo detectarlo 164
5.2.4 Consejos y recomendaciones 166
5.2.5 Estudio de casos 170
5.2.6 Enlaces de interés 177
5.3 Grooming 179
5.3.1 Definición 179
5.3.2 Algunos datos 183
5.3.3 Cómo detectarlo 188

5.3.4 Consejos y recomendaciones 188
5.3.5 Estudio de casos 190
5.3.6 Enlaces de interés 196
5.4 Otros 197
5.4.1 Pornografía Infantil 198
5.4.2 Sexting 202
5.4.3 Spam 207
5.4.4 Phishing 212
5.4.5 Happy Slapping 215
5.4.6 Robo de identidad 216
6. Bibliografía 219

1. Introducción

Internet se ha convertido en una de las herramientas más importantes en la vida de muchas personas. A través de Internet podemos comunicarnos con otras personas en cualquier lugar del mundo y de forma inmediata, investigar y recaudar información o simplemente entretenernos delante de la pantalla. A día de hoy, las ventajas y oportunidades que nos proporciona la red son casi ilimitadas, pero para llegar a este punto, Internet ha tenido que sufrir una evolución importante desde los inicios de la WWW (*World Wide Web* o simplemente conocida como *Web*) hasta tal y como la conocemos hoy en día. No se trata únicamente de las mejoras tecnológicas que han permitido este cambio constante a través de los años, sino del cambio de la forma de ver las cosas en cuanto al servicio a los internautas se refiere.

La Web fue creada a finales de los años 80 por el físico inglés **Tim Berners-Lee** y por el ingeniero industrial belga **Robert Cailliau**. Esta primera fase, conocida como la Web 1.0, en sus inicios se caracterizaba por estar formada por un conjunto de páginas traducidas a documentos simples constituidos únicamente por textos. Para interpretar estas páginas, ya existían unos navegadores específicos muy rápidos, como por ejemplo el ELISA.

Tras la aparición del lenguaje HTML (*HyperText Markup Language*), las páginas web que únicamente contenían textos, evolucionaron en otras mucho más ricas en cuanto a contenido y, por tanto, más agradables a la vista. Este nuevo conjunto de documentos estarían comunicados mediante enlaces, y se podrían visualizar a través de los nuevos navegadores visuales más sofisticados como las primeras versiones de Internet Explorer o Netscape.

Sin embargo, estas páginas web presentarían una importante limitación, y es que se trataba únicamente de páginas web estáticas de sólo lectura. Estos primeros sitios web eran desarrollados principalmente para fines comerciales, poco actualizados, cuyo objetivo era el de difundir información.

Eran administrados por un *Webmaster*, que debía tener unos conocimientos avanzados en informática, y era el único encargado de su diseño y de todo el contenido que se mostraba en ellos. Por tanto, el usuario no podía interactuar con estas páginas y toda la información contenida se encontraba limitada a lo que el *Webmaster* decidía publicar.

A modo de resumen, podemos enumerar las principales características que presentaba la Web 1.0 de la siguiente manera:

- Páginas de sólo lectura.
- Páginas estáticas.
- Páginas escritas en lenguaje HTML.
- Otros formularios HTML vía email.
- Uso de *framesets* o Marcos.
- Libro de visitas online o guestbooks. Era lo más parecido que podríamos encontrar en cuanto a la interacción con el usuario se refiere. No se podían añadir comentarios ni cualquier otro tipo de *feedback*.
- Botones *GIF*, con una resolución típica de 88x31 píxels.
- El contenido de las páginas web muy pocas veces se actualizaba.

A partir del 2001, nació lo que se conoce como *fiebre punto-com* o de las "compañías cibernéticas", lo que provocó un cambio de enfoque sobre lo que hasta el momento se entendía por páginas web. Llegados a este punto, el éxito de estas compañías cibernéticas dependía, en muchos casos, de páginas webs más dinámicas y que permitiesen conocer la opinión de los usuarios.

Para conseguir este objetivo, entraron en acción los CMS (*Content Management System*), programas que permiten crear una estructura de soporte para la gestión de contenidos por parte de los administradores, editores y demás participantes en las páginas web, principalmente. De esta forma, dejábamos atrás los sitios estáticos y poco actualizados para utilizar nuevas páginas HTML dinámicas creadas desde una actualizada base de datos.

En esta nueva generación de Webs, los contenidos ya no son responsabilidad de un único *Webmaster*, sino que éstos son compartidos y producidos, además, por los propios usuarios del portal. La interacción de todos estos usuarios da lugar a lo que conocemos por comunidad virtual, concepto imposible de concebir en las antiguas web estáticas en las que los usuarios se limitaban a la observación pasiva de contenidos que se había creado para ellos.

Esta nueva forma de ver las cosas es lo que se conoce por Web 2.0., término popularizado por **Dale Dougherty**, vicepresidente de O'Reilly Media, en una conferencia en la que hablaba del renacimiento y evolución de la Web en el año 2004. En 2005, el fundador de esta empresa, **Tim O'Reilly**, definía el concepto de Web 2.0 como "una serie de aplicaciones y páginas de Internet que utilizan la inteligencia colectiva para proporcionar servicios interactivos en red dando al usuario el control de sus datos" (O'Reilly, 2005).

Por tanto, las características que definen las Web 2.0 serían:

- Páginas dinámicas que permiten la retroalimentación de contenido: más información, comentarios, etc.
- El sitio debe estar preparado para la entrada de cualquier persona.
- Los propios usuarios deberán ser los encargados de controlar su información
- La información debe poderse introducir y extraer fácilmente.
- Basada exclusivamente en la Web, accesibles enteramente desde un navegador

El término Web 2.0 estará pues estrechamente asociado al fenómeno social que vivimos hoy en día. Existen gran cantidad de aplicaciones web que nos permiten compartir gran cantidad de información y cuyo diseño se centra en el usuario y la colaboración en la WWW.

Entre los servicios que proporciona este nuevo enfoque de web, además de todas las comunidades, servicios y aplicaciones web que permiten una interacción entre usuarios, destacamos:

- **Wikis**: Se trata de espacios webs corporativos, en los que varias personas elaboran contenidos de forma asíncrona. El usuario podrá crear o modificar contenidos ya publicados de forma sencilla, únicamente seleccionando la opción de edición.
- **Mashups**: Son páginas web o aplicaciones que utilizan y combinan datos, presentaciones y funcionalidad de otras fuentes para crear nuevos servicios. Sus características principales son la combinación, la visualización y la agregación.
- **Folcsonomías**: Se trata de un estilo de categorización cooperativa de contenido de sitios mediante descriptores, más conocidos como tags o etiquetas.
- **Blogs**: Son espacios webs personales en los que el usuario autor puede escribir artículos, noticias o impresiones de forma cronológica. Además, los lectores podrán publicar comentarios en cada una de las entradas del blog y de esta forma el autor podrá interaccionar con ellos. Al conjunto de blogs publicados en Internet se le llama blogosfera.
- **Redes sociales**: Se trata de aplicaciones online que permite a los usuarios del servicio generar un perfil público, compartir información, comunicarse

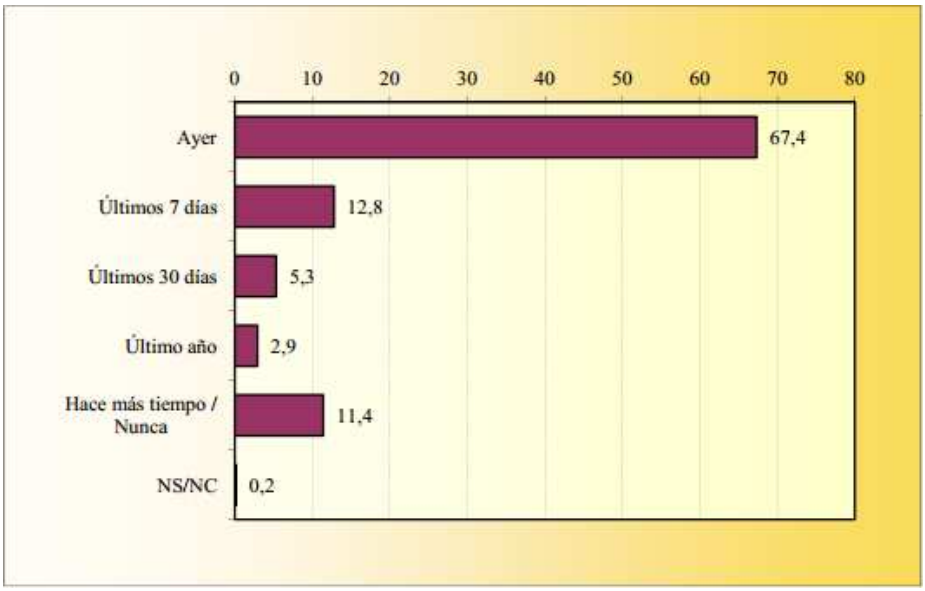
con otros usuarios, colaborar en la generación de contenidos y participar de forma espontánea en movimientos sociales y corrientes de opinión.

- **Entornos para compartir recursos**: Entornos que nos permiten almacenar recursos o contenidos en Internet, compartirlos y visualizarlos en todo momento. Este material podría tratarse de documentos, vídeos, fotos, agregadores de noticias, almacenamiento online, presentaciones, plataformas educativas, aulas virtuales o encuestas online.

De entre los servicios que acabamos de citar, destacamos el uso de redes sociales. Como hemos definido, las redes sociales son sitios web donde cada usuario tiene una página donde publica contenidos y se comunica con otros usuarios, y cada vez las utilizamos más en nuestro día a día para estar actualizados sobre lo que ocurre con las personas de nuestro entorno. Según recoge el estudio *Navegantes en la red* realizado por AIMC (Asociación para la Investigación de Medios de Comunicación) en su oleaje publicado en Marzo de 2013, el 67,4% de los encuestados acceden a diario a las redes sociales:

P. Sin contar el día de hoy ¿cuándo ha sido la última vez que ha accedido a una red social de Internet?		
	Absolutos	**%**
BASE	33.254	100,0
Ayer	22.397	67,4
Últimos 7 días	4.257	12,8
Últimos 30 días	1.775	5,3
Último año	968	2,9
Hace más tiempo / Nunca	3.801	11,4
NS/NC	56	0,2

15º Encuesta Navegantes en la Red (AIMC, 2013): *Tabla último acceso a Redes Sociales*



15º Encuesta Navegantes en la Red (AIMC, 2013): *Gráfico último acceso a Redes Sociales*

Además, existen varios tipos de redes sociales según el público o usuarios al que van destinadas y el contenido que se aloja e intercambia en las mismas. Así, observamos la existencia de dos grandes grupos: las **redes sociales generalistas o de ocio** y las **profesionales**.

Aunque cada una de ellas presenta sus propias características conceptuales y estructurales, ambos grupos comparten los elementos básicos de toda red social. Según la guía legal "Redes sociales, menores de edad y privacidad en la red", publicada por el *Observatorio de la Seguridad de la Información* del Instituto Nacional de Tecnologías de la Comunicación (INTECO), sus principales características son:

- Tienen como finalidad principal **poner en contacto** e **interconectar** a personas, de forma que a través de la plataforma electrónica se facilite la conexión de forma sencilla y rápida.
- Permiten la **interacción** entre todos los usuarios de la plataforma, ya sea compartiendo información, contactando o facilitando contactos de interés para el otro usuario.
- Permiten y fomentan la posibilidad de que los usuarios inicialmente contactados a través del mundo online, **acaben entablando un contacto real**, del que muy probablemente nacerán nuevas relaciones sociales.
- Permiten que el contacto entre usuarios sea **ilimitado**, en la medida en la que el concepto espacio y tiempo se convierte en relativo al poder comunicar desde y hacia cualquier lugar, así como en cualquier momento, con la única condición de que ambas partes acepten relacionarse entre sí.
- Fomentan la **difusión viral de la red social**, a través de cada uno de los usuarios que la componen, empleando este método como principal forma de crecimiento del número de usuarios. (INTECO, 2008)

Una vez conocidos los elementos básicos que la componen, estudiaremos las particularidades de las redes sociales generalistas, cuyo grado de crecimiento ha sido el más destacado en los últimos años, llegando a formar plataformas que alcanzan ya el billón de usuarios activos (como Facebook a fecha de marzo de 2013):

- Su objetivo principal es el de facilitar y potenciar las relaciones personales entre los usuarios que la componen. Es común añadir a nuestros contactos gente de nuestro entorno, amigos, familiares, compañeros de clase, compañeros del trabajo, etc. En definitiva, mantener el contacto e información actualizada sobre la gente con la que nos relacionamos.

- Permite organizar eventos offline a través de una plataforma online, como podrían ser fiestas o quedadas.

- Muchas ofrecen gran cantidad de aplicaciones, juegos y funcionalidades.

- Algunas ponen a disposición del usuario parte del código abierto, de forma que los propios usuarios puedan desarrollar sus aplicaciones para ser ejecutadas dentro de la red.

- Tienen un factor cultural importante, pues la capacidad para añadir enlaces musicales, fotográficos o periodísticos pueden servirnos para descubrir nuevos grupos, leer fragmentos de prensa de interés o conocer lugares que no habíamos visto nunca.

- Pueden llegar a presentar un efecto psicológico importante, sobre todo entre los usuarios más tímidos que se atrevan a expresar por escrito sus pensamientos y sentimientos mejor que en la vida real.

Es por todo esto que las redes han pasado en muchos casos a complementar o incluso a sustituir otros medios de comunicación entre los usuarios, sobre todo entres los más jóvenes de la sociedad.

Estos jóvenes, nacidos a partir de los 80 o 90, son los denominados **nativos digitales**. Cada vez es más habitual utilizar esta expresión en el lenguaje común para hablar de los jóvenes que, desde muy temprana edad, utilizan masivamente las nuevas tecnologías y los nuevos medios de comunicación en su estilo de vida. De esta forma, se rodean y utilizan desde muy pequeños los ordenadores, videojuegos, cámaras o teléfonos móviles de última generación y, además, desarrollan otra manera de pensar y de entender el mundo de como lo hacen sus padres.

Los jóvenes de hoy en día sienten la necesidad de compartir en todo momento sus emociones y pensamientos, y lo hacen a través de las redes sociales,

aplicaciones de difusión de contenidos o servicios de mensajería instantánea. Además, venden y compran en línea, encuentran empleos, amigos y ligues a través de Internet y lo hacen en su día a día, como parte de su vida cotidiana.

Otro ejemplo claro lo observamos en los juegos. Mientras que los primeros juegos eran lineales, con un objetivo fácilmente identificable, los juegos más recienten son mucho más complejos e implican la participación y coordinación de un gran número de jugadores conectados en línea. Hasta las videoconsolas de última generación precisan de una constante actualización online de software para hacer frente a las nuevas y constantes demandas de sus usuarios.

Además, ya no cuenta únicamente el tiempo que los menores pasan delante de la pantalla del ordenador. Con la aparición de los teléfonos móviles inteligentes de última generación, más conocidos como **smartphones**, éstos mantienen una conexión prácticamente permanente a la red y están enterados a tiempo real de todo lo que pasa a su alrededor y con las personas de su entorno.

Es por ello, que la mayoría de ellos únicamente ve las ventajas y oportunidades que todo esto conlleva: un mundo de información a su alcance, posibilidad de comunicación constante con sus amigos, vídeos, juegos, etc. Sin embargo, no hay que menospreciar los riesgos y peligros reales que lo que se pueden estar enfrentando al exponer gran cantidad de información personal y sensible sobre todo a través las redes sociales:

- En muchos casos, los usuarios hacen completamente públicos datos y características personales que nunca revelarían en su vida offline, como podrían ser datos relativos a su ideología, orientación sexual y religiosa.
- Existe la posibilidad que estos datos puedan ser utilizados por terceros con fines ilícitos.
- Posibilidad que otros publiquen en la Red información falsa o no autorizada sobre nosotros, generando situaciones jurídicas perseguibles que pueden llegar a derivarse de este hecho.
- Desconocimiento por parte del usuario de la cesión de derechos plenos e ilimitados sobre todos los contenidos propios alojadas en las plataformas sobre las que se registran, de manera que éstos pueden ser explotados económicamente por parte de la red social.
- Huella digital de todo el contenido que publicamos.

Aparte de los riesgos genéricos que acabamos de citar, cabe destacar los problemas de ciberacoso, grooming y pornografía infantil que se agravan con el uso de las nuevas tecnologías. Se trata de peligros que han existido siempre,

desde mucho antes de la aparición de Internet. Sin embargo, los agresores o acosadores de este tipo de prácticas se adaptan a los nuevos medios tecnológicos para perseguir su objetivo, consiguiendo así que cualquier paso en su empeño por humillar o extorsionar a su víctima cobre mucha más relevancia.

Por todo esto, los padres y educadores tienen la labor y el deber de educar desde la infancia a estos jóvenes internautas en aspectos de seguridad, privacidad y protección de derechos de las personas.

A veces son los propios padres o educadores los que desconocen todos estos riesgos, por lo que también deberán informarse sobre la materia y educar y orientar así a los menores cuando empiecen con su andadura por Internet.

Esta memoria intenta recoger y definir todos aquellos problemas principales a los que se exponen los menores al utilizar las nuevas tecnologías y proponer algunos consejos o recomendaciones para evitarlos en la medida de lo posible. Además, probaremos y comentaremos algunas herramientas de control parental que ayudarán a los padres a controlar el contenido al que acceden sus hijos y así poder orientarles y ayudarles en la toma de decisiones a la hora de utilizar las redes sociales y, en general, a la hora de navegar por la Red.

También se analizarán los Terms of Service de las redes sociales más importantes para conocer el grado en el que cedemos el derecho de nuestros datos y contenido, así como la huella digital de todo aquello que publicamos. Hay que tener en cuenta que estos términos pueden ser cambiados por los administradores de la red social en cualquier momento, por lo que hay que revisar constantemente el contrato de registro que aceptamos a la hora de darnos de alta en este tipo de servicios online.

Finalmente, comprobaremos hasta qué punto está reflejado en nuestro código penal vigente todas aquellas acciones ilícitas que se cometen utilizando las nuevas tecnologías y que afectan directa o indirectamente a un menor de edad.

2. Legislación

2.1 Introducción

De forma coloquial, se define como delito informático a toda aquella acción, típica, antijurídica y culpable que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes en Internet. Sin embargo, actualmente no existe en nuestro ordenamiento jurídico ningún título específico que los contenga.

El debate existente a día de hoy radica en la consideración de estos crímenes informáticos como un nuevo delito o si son delitos clásicos cometidos a través de un nuevo medio que, en este caso, serían las nuevas tecnologías.

Desde el Grupo de Delitos Telemáticos de la Guardia Civil española (https://www.gdt.guardiacivil.es/webgdt/legislacion.php), se defiende la postura de que "lo que califica al tipo no es su naturaleza sino el medio comisivo y la metodología que requiere su investigación" (GDT de la Guardia Civil, 2011). Por ello, clasifican como delito informático "todos aquellos delitos cometidos a través del medio telemático y cuya vía probatoria se sustenta en la prueba informática" (GDT de la Guardia Civil, 2011).

Teniendo en cuenta esta clasificación podemos encontrar en el Código Penal vigente multitud de penas aplicables cuya comisión, en determinadas circunstancias, exige la metodología de investigación informática.

Debido a la velocidad de los avances informáticos y la mayor relevancia que va obteniendo este concepto, urgió la redacción de un convenio en el que se expusiese todos estos delitos informáticos así como los tipos penales que han de considerarse como tales. Así mismo, el 23 de noviembre de 2001 fue promulgado el Convenio de Ciberdelincuencia realizado por el Consejo de Europa y del que hablaremos más detenidamente en su subapartado correspondiente.

Además, existe un cuerpo legislativo que complementa a los tipos penales y que pretende regular aspectos de la Sociedad de la Información. Cabría destacar entre ellos la ley de protección de datos a la que dedicaremos otro punto de este apartado.

Probablemente los usuarios más vulnerables a ser víctimas de este nuevo concepto de delito informático sean los menores de edad, y más hoy en día con el gran auge de las redes sociales en las que se comparte tanta información. En el ciberespacio, encontramos distintos tipos de riesgos a los

que pueden enfrentarse. En el apartado *ciberderechos* de la web www.delitosinformaticos.com encontraremos la siguiente clasificación:

1. Contenidos inadecuados: pornográficos, violentos, racistas, sectas, relacionados con las drogas, …
2. Abuso físico: Podría pasar que un menor se encuentre con invitaciones de personas que desean citarse con ellos mientras chatean. El potencial contacto con pedófilos es uno de los peligros más importantes.
3. Acoso: a través de e-mails, fotos, chats, redes sociales…
4. Información personal: Por las condiciones de madurez que puede presentar un menor de edad, éstas lo hacen más vulnerable a la hora de facilitar cierto tipo de información personal que le puede poner en peligro a él mismo y a su familia. (Delitos Informáticos, 2013)

Es por esto, que los menores necesitan tener una buena educación tecnológica y navegar de forma segura. Existen infinidad de consejos y manuales por la red que ayudan a esta causa y a la que nos dedicaremos en su apartado correspondiente de esta memoria.

Entremos pues ahora a analizar en profundidad cada una de las leyes o convenios que reflejen los posibles cibercrímenes que podemos encontrar hoy en día y, más concretamente, las que pueden llegan a involucrar la participación directa o indirecta de un menor.

2.2 Convenio de Ciberdelincuencia

2.2.1 Definición

Conscientes de los profundos cambios provocados por la digitalización, convergencia y la globalización continua de las redes informáticas y los riesgos que estos conllevan, los Estados miembros del Consejo de Europa firmaron, junto a otros Estados signatarios, el denominado "Convenio sobre la ciberdelincuencia" (2001).

Este convenio fue originalmente firmado en Budapest el 23 de noviembre de 2001 y a lo largo del tiempo ha sido ratificado por un gran número de países.

La idea de la redacción del convenio surge tras la necesidad de aplicar una política penal común frente a la ciberdelincuencia. Entenderemos por ciberdelincuencia a la comisión de delitos utilizando las redes

informáticas y la información electrónica y en la que las pruebas relativas a estos delitos sean almacenadas y transmitidas por medio de dichas redes.

A su vez, se pretende garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales entre los que encontramos el derecho de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad.

En este convenio se acotan los delitos informáticos en cuatro grupos y se definen los tipos penales que han de considerase como delito informático. Estos son:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

    - Acceso ilícito a sistemas informáticos.
    - Interceptación ilícita de sistemas informáticos.
    - Interferencia en el funcionamiento de un sistema informático.
    - Abuso d dispositivos que faciliten la comisión de los anteriores delitos.

2. Delitos informáticos.

    - Falsificación informática mediante la introducción, alteración, borrado o supresión de datos informáticos.
    - Fraude informático mediante la introducción, alteración, borrado de datos informáticos, o la interferencia en sistemas informáticos.

3. Delitos relacionados con el contenido.

    - Producción, oferta, difusión, transmisión, adquisición o tenencia, en sistemas o soportes informáticos, de contenidos de pornografía infantil.

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Desde el año en que se redactó el convenio original hasta el día de hoy, la red ha sufrido un cambio importante. La evolución de la web 1.0 a las redes sociales supone la aparición de nuevos escenarios que dan lugar a situaciones de vulneración de derechos. El mayor ejemplo es el de la conducta *grooming* o acoso de menores en la red que hoy en día tiene una gran importancia en la lucha contra la pornografía infantil. Es por ello, que el convenio ha precisado de alguna revisión para adaptarlo a los nuevos tiempos y las nuevas tecnologías.

Centrándonos en el tema que nos concierne sobre la protección del menor en la red, encontraremos en el artículo 9 de una ratificación del convenio de 2010 los delitos relacionados con la pornografía infantil:

Artículo 9. *Delitos relacionados con la pornografía infantil.*

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,

d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de:

a) Un menor comportándose de una forma sexualmente explícita;

b) una persona que parezca un menor comportándose de una forma sexualmente explícita;

c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

3. A los efectos del anterior apartado 2, por «menor» se entenderá toda persona menor de dieciocho años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años.

4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2. (Ratificación Convenio de Ciberdelincuencia, 2010)

En el siguiente punto de este subapartado citaremos los tipos penales existentes en el Código Penal vigente que más se aproximan a lo que refleja el convenio.

2.2.2 Código penal

De los distintos enfoques o puntos de vista que existen actualmente sobre lo que se podría entender por delito informático, quizá el que goza de mayor aceptación por el consenso alcanzado sea el Convenio sobre Ciberdelincuencia que acabamos de comentar en el punto anterior.

Actualmente, los tipos penales de nuestro Código Penal que más se aproximan a lo que refleja el Convenio y, en concreto, a lo relacionado con la problemática de la pornografía infantil son los siguientes:

CAPÍTULO V: DE LOS DELITOS RELATIVOS A LA PROSTITUCIÓN Y LA CORRUPCIÓN DE MENORES

Artículo 189

1. Será castigado con la pena de prisión de uno a cinco años:
    a. El que captare o utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.
    b. El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

2. El que para su propio uso posea material pornográfico en cuya elaboración se hubiera utilizado menores de edad o incapaces, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.
3. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:
    a. Cuando se utilicen a niños menores de 13 años.
    b. Cuando los hechos revistan un carácter particularmente degradante o vejatorio.
    c. Cuando los hechos revistan especial gravedad atendiendo al valor económico del material pornográfico.
    d. Cuando el material pornográfico represente a niños o a incapaces que son víctimas de violencia física o sexual.
    e. Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

f. Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho o de derecho, del menor o incapaz.

7. Será castigado con la pena de prisión de tres meses a un año o multa de seis meses a dos años el que produjere, vendiere, distribuyere, exhibiere o facilitare por cualquier medio material pornográfico en el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada. (Código Penal, Art. 189)

Sin embargo, el Grupo de Investigación informática de la Guardia Civil Española amplía la definición de delito informático y atribuye a la misma las siguientes conductas reflejadas en el Código Penal:

CAPÍTULO II: DE LOS ABUSOS SEXUALES

Artículo 181

1. El que, sin violencia o intimidación y sin que medie consentimiento, realizare actos que atenten contra la libertad o indemnidad sexual de otra persona, será castigado, como responsable de abuso sexual, con la pena de prisión de uno a tres años o multa de dieciocho a veinticuatro meses.
2. A los efectos del apartado anterior, se consideran abusos sexuales no consentidos los que se ejecuten sobre personas que se hallen privadas de sentido o de cuyo trastorno mental se abusare, así como los que se cometan anulando la voluntad de la víctima mediante el uso de fármacos, drogas o cualquier otra sustancia natural o química idónea a tal efecto. (Código Penal, Art. 181)

CAPÍTULO IV: DE LOS DELITOS DE EXHIBICIONISMO Y PROVOCACIÓN SEXUAL

Artículo 186

El que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menos de edad o incapaces, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses. (Código Penal, Art. 186)

CAPÍTULO V: DE LOS DELITOS RELATIVOS A LA PROSTITUCIÓN Y LA CORRUPCIÓN DE MENORES

Artículo 187

1. El que introduzca, promueva, favorezca o facilite la prostitución de una persona menor de edad o incapaz será castigado con las penas de uno a cinco años y multa de doce a veinticuatro meses. La misma pena se impondrá al que solicite, acepte u obtenga a cambio de una remuneración o promesa, una relación sexual con persona menor de edad o incapaz. (Código Penal, Art. 187)

Artículo 189

4. El que haga participar a un menor o incapaz en un comportamiento de naturaleza sexual que perjudique la evolución o desarrollo de la

> personalidad de éste, será castigado con la pena de prisión de seis meses a un año. (Código Penal, Art. 189)

Como vemos, la problemática de la pornografía infantil se intenta resolver aplicando las penas que se exponen en los diferentes puntos o artículos del Código Penal de nuestro país. Además, existe un cuerpo legislativo complementario a los tipos penales que pretende regular aspectos de la Sociedad de la Información tan importantes para la investigación como son la conservación y cesión de datos de tráfico de internet, y la protección de datos personales. Hablaremos de ellos en su apartado correspondiente.

2.3 Ley orgánica de protección de datos (LOPD)

2.3.1 Introducción

La **Ley Orgánica de Protección de Datos de Carácter Personal** fue aprobada el 13 de diciembre de 1999, se publicó en el Boletín Oficial del Estado el 14 de diciembre de 1999 (BOE nº 298) y entró en vigor el 14 de enero del año 2000.

Más conocida como ley LOPD, es la norma que regula en España el régimen jurídico aplicable al tratamiento de los denominados *datos de carácter personal*. En este documento se define dato personal como "Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables" (LOPD, 1999). Serían ejemplos de datos personales los nombres y apellidos de una persona, DNI, dirección, huella, imagen, voz, etc.

Así pues, se establecen las condiciones en que se deben recoger, tratar y ceder este tipo de datos para no perjudicar con ellos los derechos fundamentales y libertades públicas de los ciudadanos, especialmente su derecho al honor e intimidad personal y familiar.

Con la entrada en vigor de la LOPD, se adaptó definitivamente la legislación española a los requisitos exigidos por la Directiva 95/46/CE para todos los Estados Miembro de la Unión Europea.

La LOPD está estructurada en 49 artículos, 7 títulos, 6 disposiciones adicionales, 3 disposiciones transitorias, 1 disposición derogatoria y 3 disposiciones finales. Se regulan las siguientes cuestiones:

- **Título I**: Disposiciones generales
- **Título II**: Principios de la protección de datos
- **Título III**: Derechos de las personas
- **Título IV**: Disposiciones sectoriales
- **Título V**: Movimiento internacional de datos
- **Título VI**: Agencia de protección de datos
- **Título VII**: Infracciones y sanciones

Como se viene comentando en puntos anteriores, los menores de edad son más ingenuos y por tanto, en términos generales, más vulnerables y propensos a facilitar cierto tipo de información personal que les puede poner en peligro a ellos y a sus familias. Por tanto, la ley LOPD dedica un artículo para regular la participación de éstos en la red.

2.3.2 La ley orgánica de protección de datos y los menores

En el artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, encontraremos el apartado correspondiente al consentimiento para el tratamiento de datos de menores de edad.

Este artículo se divide en cuatro puntos.

En el punto 1 se clasifica a los menores de edad en dos grupos:

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela.

   En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores. (LOPD, 1999)

Como vemos, el artículo 13.1 hace una distinción entre menores y mayores de 14 años, ya que considera que a partir de esta edad, el menor tiene unas *condiciones de madurez suficientes* para que puedan consentir por sí mismos el tratamiento de sus datos personales.

En cambio, los menores de 14 años no presentan estas *condiciones de madurez suficientes* descritas en el Código Civil y, por tanto, la

responsabilidad de otorgar este permiso recaerá sobre los mismos padres o tutores legales del menor.

En el segundo punto del artículo se hace referencia al tipo de datos que se pueden obtener del menor y para qué finalidad:

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior. (LOPD, 1999)

En este artículo 13.2 se observa cómo se vuelve a destacar la obligación del usuario manipulador de los datos de pedir consentimiento formal de los padres o tutores del menor para los casos en que se quiera tratar información, ya sea del mismo menor de 14 años o en el caso que se traten datos que afecten a terceras personas del entorno familiar de éste.

El siguiente punto del artículo hace referencia de manera indirecta al cumplimiento del deber de información expuesto en esta misma Ley Orgánica de Protección de datos. Esto es, "El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal..." (LOPD, 1999)

Debido al nivel de entendimiento que puede tener un menor de edad, será responsabilidad del usuario de los datos el expresarse de forma que resulte perfectamente comprensible para el menor al que se refieren los datos:

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo. (LOPD, 1999)

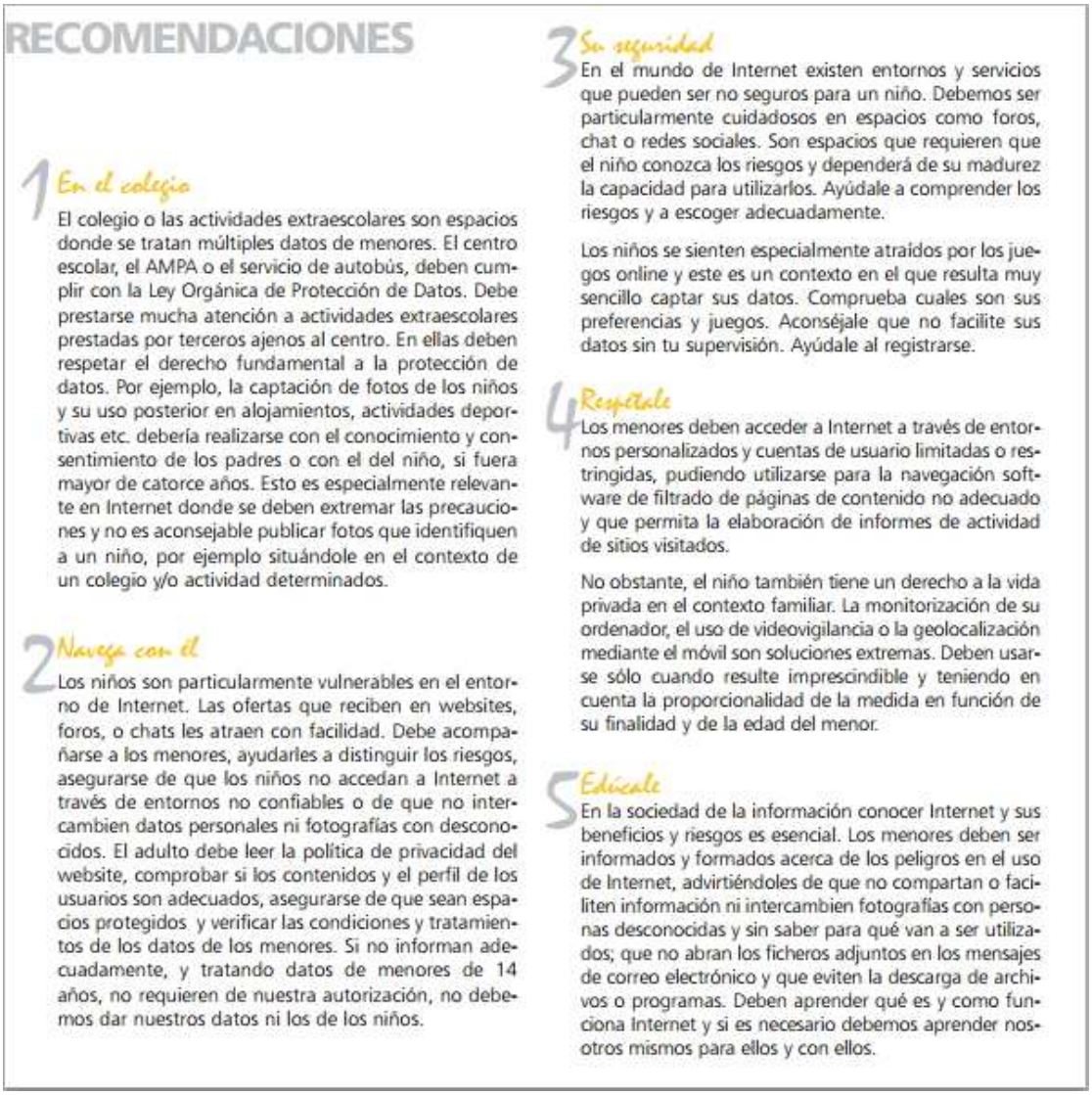
Finalmente, en el último punto de este artículo 13, se recuerda la obligación por parte del responsable del tratamiento de los datos de garantizar que se ha comprobado la edad del menor así como la autenticidad del consentimiento correspondiente:

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales. (LOPD, 1999)

Cabe destacar que, según lo establecido en esta LOPD, una vez hemos otorgado el consentimiento para el tratamiento de nuestros datos, en cualquier momento posterior se puede revocar o retirar.

2.3.3 Recomendaciones AEPD

La Agencia Española de Protección de Datos, conscientes de los riesgos que conlleva el uso de las nuevas tecnologías y de las redes sociales por parte de menores de edad, publica una lista de recomendaciones a seguir a la hora de garantizar una navegación segura:



RECOMENDACIONES

1 En el colegio

El colegio o las actividades extraescolares son espacios donde se tratan múltiples datos de menores. El centro escolar, el AMPA o el servicio de autobús, deben cumplir con la Ley Orgánica de Protección de Datos. Debe prestarse mucha atención a actividades extraescolares prestadas por terceros ajenos al centro. En ellas deben respetar el derecho fundamental a la protección de datos. Por ejemplo, la captación de fotos de los niños y su uso posterior en alojamientos, actividades deportivas etc. debería realizarse con el conocimiento y consentimiento de los padres o con el del niño, si fuera mayor de catorce años. Esto es especialmente relevante en Internet donde se deben extremar las precauciones y no es aconsejable publicar fotos que identifiquen a un niño, por ejemplo situándole en el contexto de un colegio y/o actividad determinados.

2 Navega con él

Los niños son particularmente vulnerables en el entorno de Internet. Las ofertas que reciben en websites, foros, o chats les atraen con facilidad. Debe acompañarse a los menores, ayudarles a distinguir los riesgos, asegurarse de que los niños no accedan a Internet a través de entornos no confiables o de que no intercambien datos personales ni fotografías con desconocidos. El adulto debe leer la política de privacidad del website, comprobar si los contenidos y el perfil de los usuarios son adecuados, asegurarse de que sean espacios protegidos y verificar las condiciones y tratamientos de los datos de los menores. Si no informan adecuadamente, y tratando datos de menores de 14 años, no requieren de nuestra autorización, no debemos dar nuestros datos ni los de los niños.

3 Su seguridad

En el mundo de Internet existen entornos y servicios que pueden ser no seguros para un niño. Debemos ser particularmente cuidadosos en espacios como foros, chat o redes sociales. Son espacios que requieren que el niño conozca los riesgos y dependerá de su madurez la capacidad para utilizarlos. Ayúdale a comprender los riesgos y a escoger adecuadamente.

Los niños se sienten especialmente atraídos por los juegos online y este es un contexto en el que resulta muy sencillo captar sus datos. Comprueba cuales son sus preferencias y juegos. Aconséjale que no facilite sus datos sin tu supervisión. Ayúdale al registrarse.

4 Respétale

Los menores deben acceder a Internet a través de entornos personalizados y cuentas de usuario limitadas o restringidas, pudiendo utilizarse para la navegación software de filtrado de páginas de contenido no adecuado y que permita la elaboración de informes de actividad de sitios visitados.

No obstante, el niño también tiene un derecho a la vida privada en el contexto familiar. La monitorización de su ordenador, el uso de videovigilancia o la geolocalización mediante el móvil son soluciones extremas. Deben usarse sólo cuando resulte imprescindible y teniendo en cuenta la proporcionalidad de la medida en función de su finalidad y de la edad del menor.

5 Edúcale

En la sociedad de la información conocer Internet y sus beneficios y riesgos es esencial. Los menores deben ser informados y formados acerca de los peligros en el uso de Internet, advirtiéndoles de que no compartan o faciliten información ni intercambien fotografías con personas desconocidas y sin saber para qué van a ser utilizados; que no abran los ficheros adjuntos en los mensajes de correo electrónico y que eviten la descarga de archivos o programas. Deben aprender qué es y como funciona Internet y si es necesario debemos aprender nosotros mismos para ellos y con ellos.

En resumen se trata de concienciar a los menores de edad sobre los peligros que conlleva el uso de Internet. Por ello, hay que educarles y aconsejarles sobre la forma de actuar en determinados espacios como foros, redes sociales o chats.

Además, se aconseja que los padres naveguen con sus hijos para ayudarles a distinguir estos riesgos y evitar así posibles situaciones de peligro para el menor, sobre todo a la hora de compartir información, datos personales o fotografías.

Finalmente se recomienda la utilización de Software de filtrado de páginas de contenido inadecuado para menores de cierta edad que puedan resultar ofensivas para el niño.

2.3.4 Marco internacional

Si echamos un vistazo al problema del tráfico de datos de menores de edad a través de Internet a nivel internacional, encontraremos otras leyes o convenios que intentan regular el tratamiento de los mismos.

Entre ellas, cabría destacar ley federal denominada Childen's Online Privacy Protection Act (conocida por las siglas COPPA) promulgada el 21 de octubre de 1998 en Estados Unidos y efectiva desde el 12 de abril del año 2000.

En el número 16 de la revista Redseguridad (http://www.borrmart.es/articulo_redseguridad.php?id=393&numero=16) publicada por la editorial BORRMART (empresa editorial especializada en la edición de publicaciones técnicas de difusión nacional e internacional) se resume las principales cuestiones o ideas que recoge la ley de la siguiente manera:

- No se podrá recoger por Internet ninguna información o dato de carácter personal de menores de 13 años sin el permiso de sus padres o representantes legales.
- Los padres o representantes legales tienen el derecho a conocer qué información sobre sus hijos se les ha solicitado y qué uso se da a la misma.
- Los padres tienen el derecho de acceso a dicha información obtenida de sus hijos, así como el derecho a decidir sobre su cesión a terceros o sobre su cancelación.
- No se podrá solicitar en la recogida de datos de menores más información de la que sea razonablemente necesaria para el acceso a los sitios web y su participación en las actividades (como juegos o concursos) de los mismos.

- Las autorizaciones que, en cualquier caso, deban otorgar los padres o representantes de los menores, deber ser verificables, por ejemplo, con una autorización firmada enviada por correo ordinario o fax, o por medio de llamada telefónica. También se podría verificar con el número de una tarjeta de crédito o enviando un e-mail, ya sea firmado digitalmente o acompañando una clave que la empresa otorgue únicamente al padre para prestar dicho consentimiento.
- Los sitios web y los servicios on-line deben exhibir una política de privacidad bien definida. En cuanto a ésta, debe indicarse quién realiza la recogida de los datos (incluyendo los datos de contacto de la empresa); el tipo de datos de carácter personal que se solicitan, el uso posterior que se le va a dar a dicha información, si la información va a ser cedida a terceros; y las advertencias de que no se va a solicitar más información de la que sea estrictamente necesaria para los usos y que los padres tienen los derechos de acceso, cancelación y oposición a la recogida de datos. Se deberá indicar la forma de ejercitar dichos derechos.

Se exceptúan de la solicitud de autorización de los padres los siguientes casos:

- La recogida de la dirección de correo electrónico de menores de edad para actuaciones concretas y aisladas.
- La participación de menores en promociones o el envío de mensajes de correo electrónico siempre que los padres hayan sido notificados previamente de dicha posibilidad.
- En los sitios de chat controlados, si se omite toda información que permita identificar al usuario y si la que se almacene para dichos servicios se elimina posteriormente de los registros del proveedor de servicios de Internet.
- Cuando sea necesario para proteger la seguridad del menor o del sitio web. (Red Seguridad, 2005)

La regulación marcó un antes y un después en la protección de datos de menores de edad.

La Comisión Federal de Comercio (FTC), que tiene autoridad para emitir normas y hacer cumplir la COPPA, anunció en septiembre de 2011 la primera propuesta de cambios desde que se emitió la ley en el año 2000. Estos cambios consistían en ampliar el significado de aquello que entendemos por *recoger* datos de niños o menores de edad. Además, presentaba un requisito de *retención y eliminación de datos*, que consistiría en mantener la información obtenida de los menores sólo durante el tiempo necesario para alcanzar el propósito para el que se recogió así como añadir el requisito de que los operadores se aseguren que toda aquella información revelada a terceros cuenta con los procedimientos razonables para proteger dicha información.

A nivel de la Unión Europea, el mismo artículo del número 16 de la revista **Redseguridad** (BORRMART, S.A.) comenta que se deberá tener

en cuenta el Dictamen 3/2003 relativo al Código de Conducta de la Federation of European Direct Marketing (FEDMA) sobre la utilización de datos personales en la comercialización directa, emitido por el Grupo 29 de la Comisión Europea, donde la Organización Europea de Consumidores (BEUC) consideró que las medidas del código no ofrecían un nivel de protección lo bastante elevado en su opinión, y citaba la COPPA Act estadounidense, como modelo a seguir.

2.4 Ley de Servicios para la Sociedad de la Información y de comercio electrónico (LSSICE)

2.4.1 Introducción

La Ley de Servicios de la Sociedad de la Información y del comercio electrónico tiene como objeto "la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información" (LSSICE, 2002) tal y como se anuncia en el Artículo 1 del Capítulo 1 de la ley que nos ocupa.

La Ley entiende por "servicio de la sociedad de la información", toda actividad que cumple con los siguientes requisitos:

- Recibe una contraprestación económica.
- La actividad se realiza a distancia (no presencial).
- Por medios electrónicos o telemáticos.
- A petición individual del destinatario del servicio. (LSSICE, 2002)

En la Ley se exponen una serie de infracciones clasificadas según la gravedad de las mismas. Por ejemplo, se consideraría una infracción grave "el incumplimiento significativo de lo establecido en los párrafos a) y f) del artículo 10.1" (LSSICE, 2002). Esto sería:

Artículo 10. Información general.

1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la

información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío o en su caso aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia. (LSSICE, 2002)

En cambio, se considerarían infracciones leves "no informar de la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo, o en los párrafos a) y f) cuando no constituya infracción grave" (LSSICE, 2002). Esto sería:

b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

d) Si ejerce una profesión regulada deberá indicar:

1.º Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

2.º El título académico oficial o profesional con el que cuente.

3.º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente. (LSSICE, 2002)

Atendiendo a la gravedad de las infracciones cometidas, se aplicará la multa correspondiente según la siguiente clasificación:

a) Por la comisión de infracciones muy graves, multa de 150.001 hasta 600.000 euros.

La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, multa de 30.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, multa de hasta 30.000 euros. (LSSICE, 2002)

2.4.2 La Ley LSSICE y los menores

Si leemos la Ley con detenimiento, observaremos que no dedica ningún capítulo exclusivamente a contemplar el comportamiento cuando se trata con menores de edad.

Sin embargo, encontraremos en el apartado II de la EXPOSICIÓN DE MOTIVOS de la Ley una pequeña mención donde se expone que "sólo se permite restringir la libre prestación en España de servicios de la sociedad de la información procedentes de otros países pertenecientes al Espacio Económico Europeo en los supuestos previstos en la Directiva 2000/31/CE, que consisten en la producción de un daño o peligro graves contra ciertos valores fundamentales como el orden público, la salud pública o la protección de los menores" (LSSICE, 2002).

Además, en el Artículo 18.2 del Capítulo III (Códigos de Conducta), también encontraremos un condicionante a la conducta teniendo en cuenta la protección de los menores y la dignidad humana:

CAPÍTULO III

Códigos de conducta

Artículo 18. *Códigos de conducta*

1. Las Administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional. Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información.

2. En la elaboración de dichos códigos, habrá de garantizarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas, cuando afecten a sus respectivos intereses.

Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias. Los poderes públicos estimularán, en particular, el establecimiento de criterios comunes acordados por la industria para la

clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos. (LSSICE, 2002)

2.5 Ley de propiedad intelectual

2.5.1 Introducción

El ministerio de educación, cultura y deporte de España define la propiedad intelectual como "el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación" (Ministerio de Educación, Cultura y Deporte, 2013).

Estos derechos otorgan a los autores de las creaciones un reconocimiento por su obra, así como una retribución económica por la realización de las mismas. A raíz de ello y debido a la necesidad de proteger estos derechos, se emitió la llamada Ley de Propiedad Intelectual.

Encontramos por primera vez una regulación sobre los derechos de Autor en España dentro de la Ley 22/11, de 11 de noviembre de 1987 sobre la Propiedad Intelectual. Con los años esta ley sufrirá varias modificaciones hasta llegar a la Ley de Propiedad Intelectual que conocemos hoy en día, debidas, en gran parte, a los grandes avances tecnológicos y de difusión que hemos sufrido a través de los años. Esta ley la podremos encontrar en el "REAL DECRETO LEGISLATIVO 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia" (Ley de Propiedad Intelectual, 1996).

2.5.2 La Ley de propiedad intelectual y los menores de edad

Cuando un menor de edad presenta una obra de propia creación, este deberá tener la misma igualdad que cualquier otro autor a reclamar sus derechos.

Sin embargo, la ley solamente se contempla los casos para menores de edad entre 16 y 18 años. Podremos encontrar el texto correspondiente en el artículo 44 de la Ley:

Artículo 44. Menores de vida independiente.

> Los autores menores de dieciocho años y mayores de dieciséis, que vivan de forma independiente con consentimiento de sus padres o tutores o con autorización de la persona o institución que los tengan a su cargo, tienen plena capacidad para ceder derechos de explotación. (Ley de Propiedad Intelectual, 1996)

Por tanto y, al igual que pasaba con la ley LOPD, la responsabilidad de salvaguardar los derechos de autor de un menor que no cumpla con las condiciones expuestas en el artículo anterior recaerá sobre los padres o tutores legales del mismo.

3. TOS de las redes sociales

3.1 Definición TOS

Los TOS (*Terms of Service*) o *Condiciones de uso* de un servicio web se trata de un contrato o acuerdo entre el proveedor del servicio y el usuario final, en el que se enuncian las normas o reglas que el usuario debe cumplir a la hora de utilizar el producto. Estos términos pueden llegar a abarcar un gran número de temas; desde las bases de un comportamiento ético y aceptable online hasta hacer referencia a las políticas de marketing de la empresa o violación de copyright.

El incumplimiento del mismo por parte del usuario conlleva penalizaciones, llegando a poder ser privado de la utilización del servicio.

Los términos del acuerdo, que suelen estar muy condicionadas a las leyes vigentes, pueden ir cambiando en el tiempo, y será responsabilidad del proveedor del servicio el notificarlo a sus usuarios.

Muchas páginas web puramente informativas no suelen tener un apartado de condiciones de uso. En cambio, los proveedores de Internet y todos aquellos sitios web que almacenan información personal de un usuario lo tienen; en particular, las redes sociales, subastas online y sitios de transacciones financieras, que necesitan mantener un alto nivel de confianza entre los usuarios.

3.2 Criterios utilizados para el análisis de TOS

A continuación vamos a analizar los TOS asociadas a las redes sociales más relevantes en la actualidad. En ellas, analizaremos los términos referentes a todas aquellas prácticas que involucren la participación de un menor y el protocolo de actuación en caso de detectar comportamientos ofensivos o malintencionados que puedan dañar o poner en peligro al usuario.

Para ello, analizaremos las condiciones de uso de cada servicio prestando atención a los siguientes puntos:

- Edad mínima para utilización del servicio.
- Consentimiento paterno para el uso del servicio por menores de cierta edad.
- Cómo informar de algún comportamiento ofensivo o inadecuado.

- Identificación de participantes (a través de la información del dispositivo desde el que se conecta)
- Filtrado de material ofensivo. Por ejemplo, anuncios o publicidad para adultos.
- Huella digital. ¿Qué pasa con el material subido a la red una vez eliminada una cuenta?
- Responsabilidades de tipo legal.

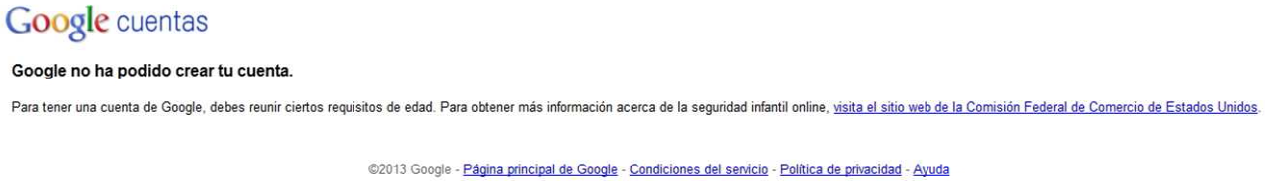
3.3 Creación de perfiles falsos

A la hora de analizar los TOS para algunas de las redes sociales más relevantes en la actualidad, crearemos unos perfiles falsos de usuarios para intentar violar las condiciones referentes a la edad de acceso y comprobar así las verdaderas barreras existentes a la hora de acceder a la web social por parte de un menor.

Para ello, se han creado los siguientes cuatro perfiles:

Como todos los servicios que almacenan datos personales de usuario, hemos tenido problemas a la hora de crear las cuentas de usuario de los niños de 9 años, puesto que en las condiciones de uso de Google, la edad mínima para utilizar cualquiera de sus servicios es de 13 años.

Si indicábamos la edad real de los niños de 9 años, el navegador nos redirigía a la siguiente pantalla:



Por tanto, nos ha bastado indicar algunos años de nacimiento anteriores y nos ha dejado completar el alta sin problemas.

Analizaremos estas condiciones en profundidad en el subapartado correspondiente.

3.4 Casos de estudio

3.4.1 Facebook

Desde que a finales de septiembre de 2006 la hasta entonces red social destinada a universidades se abriese a todos los usuarios de Internet, *Facebook* se ha convertido probablemente en la plataforma social más importante y relevante que haya existido hasta el momento.

Actualmente Facebook ronda ya los 1000 millones de usuarios.

Su gran repercusión requiere una extensa y detallada definición de términos y condiciones así como de política de privacidad, que nos permita a los usuarios saber exactamente a qué nos exponemos al hacer uso de sus servicios. Esta declaración la podemos encontrar en su totalidad en el mismo portal web, y se puede consultar sin estar registrado como usuario.

A continuación nos centraremos en los criterios citados anteriormente.

3.4.1.1 Facebook – Edad mínima

Tal como se indica en el apartado *Seguridad de la cuenta y registro* del vigente documento de términos del servicio, el usuario se

compromete a seguir una serie de reglas, entre las que se cita “No utilizarás Facebook si eres menor de 13 años”.

Tal y como se indica en los términos, se trata de un mero compromiso por parte del usuario, pero en ningún momento se pide ningún comprobante para demostrar que éste cumple los requisitos mínimos a la hora de registrarse.

Veamos un ejemplo claro de cómo un usuario que no cumple la edad mínima se puede registrar sin apenas algún tipo de obstáculo.

Recordemos a José:

José tiene 9 años y, por tanto, no debería poder tener acceso a esta red social.

José, como cualquier otra persona que se quiere registrar entra en la página de inicio de Facebook e introduce sus datos:

Justo abajo del formulario donde se indica la fecha de nacimiento aparece una pequeña explicación del porqué es necesario introducir la edad al registrarse. Aunque aquí no se indica la edad mínima que se debería tener para poder utilizar el servicio, sí que anuncia que Facebook utilizará esta información para intentar adecuar los contenidos a mostrar a cada uno de sus usuarios. De esta forma, en teoría se debería evitar publicidad o anuncios no recomendados para usuarios menores de cierta edad.

Una vez introducidos todos los datos necesarios, José hace *click* sobre el botón *Regístrate* y automáticamente le salta el mensaje:

Si José cierra la pestaña y con la misma sesión del navegador vuelve a entrar en la página de inicio para volver a intentarlo de nuevo, vuelve a aparecer un mensaje de nuevo indicando que el usuario no cumple los requisitos mínimos para utilizar el servicio:

Esta vez, José abre una nueva sesión en el navegador y prueba suerte de nuevo falsificando su año de nacimiento, de tal forma que pretenda tener una mayor edad a la mínima permitida:

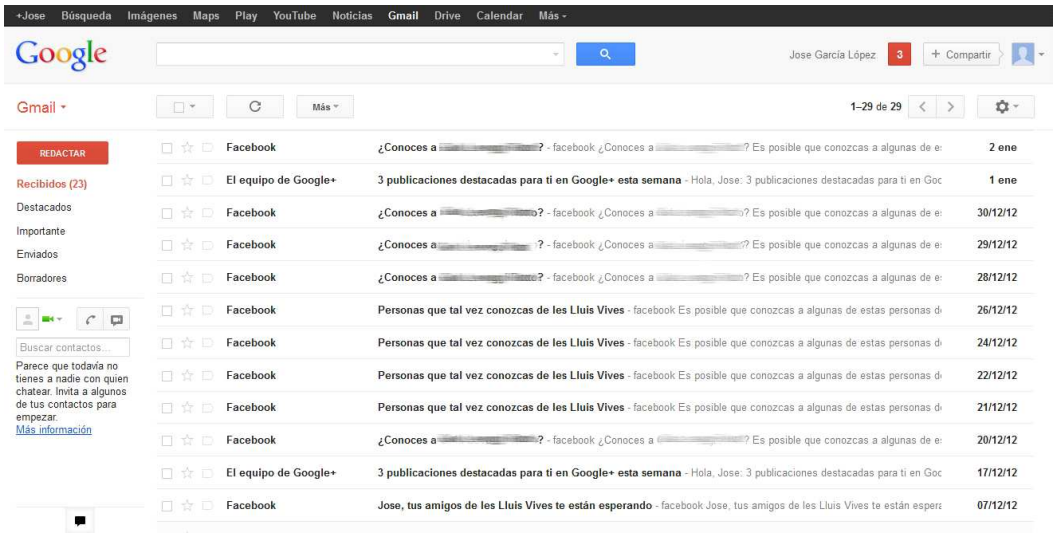
Esta vez nos dejará proceder sin problema:

Tras haber indicado que José tiene supuestamente 15 años, en el segundo paso de finalización de registro Facebook nos ofrece la posibilidad de indicar a qué instituto acude el usuario. En este caso, nos inventamos que José es un estudiante del instituto “Lluís Vives”:

Tras seleccionar el instituto, automáticamente Facebook nos sugiere posibles compañeros asociados a la red de ese mismo centro:

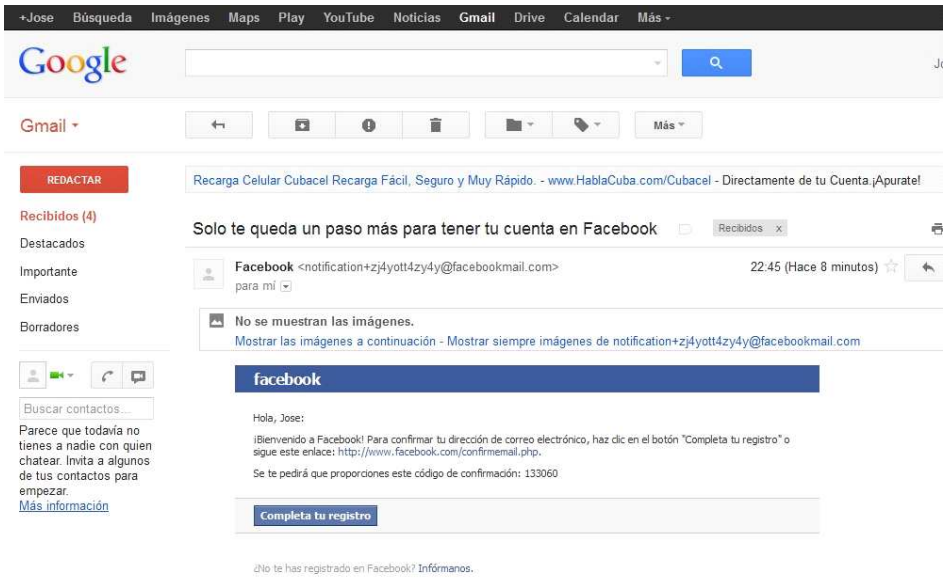
Este paso puede considerarse un servicio bastante útil para todos aquellos alumnos reales del centro que deseen establecer amistad con otros compañeros pero, debido a la falta de verificación de los datos introducidos por el usuario a la hora de registrarse, este paso podría considerase al mismo tiempo igual de peligroso, pues se están exponiendo menores de forma pública a cualquier usuario decidido a falsificar su información.

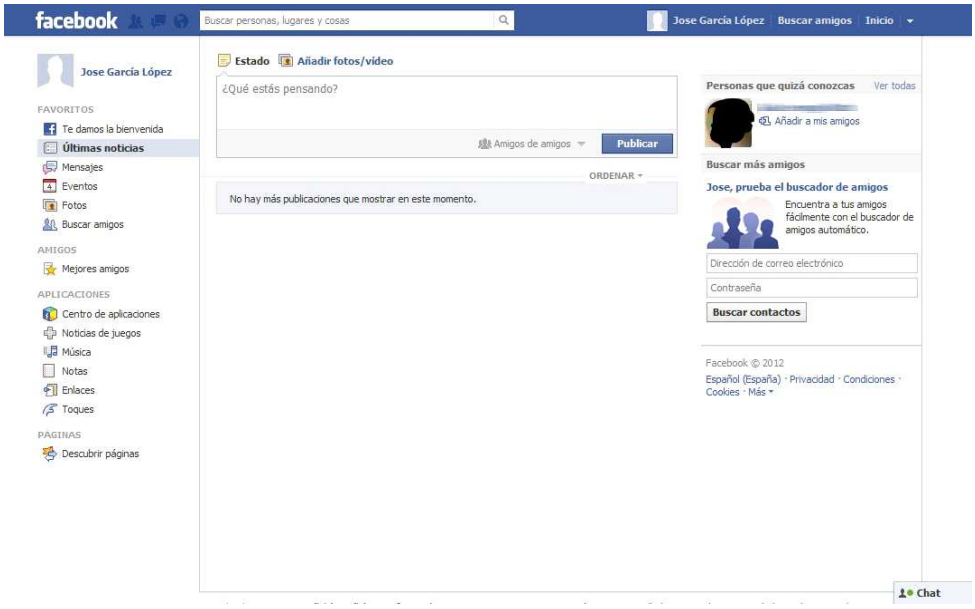
Si José omite este paso y accede a su cuenta de correo electrónico en unos días, Facebook le habrá enviado repetidos e-mails recordando de nuevo los compañeros que puede que conozca del mismo centro:



Por tanto, se trata de una exposición continua de usuarios menores de edad.

Finalmente y para acabar con el registro, Facebook nos enviará a nuestro correo un electrónico un e-mail con un enlace de activación de la cuenta. José ya tiene acceso a Facebook:





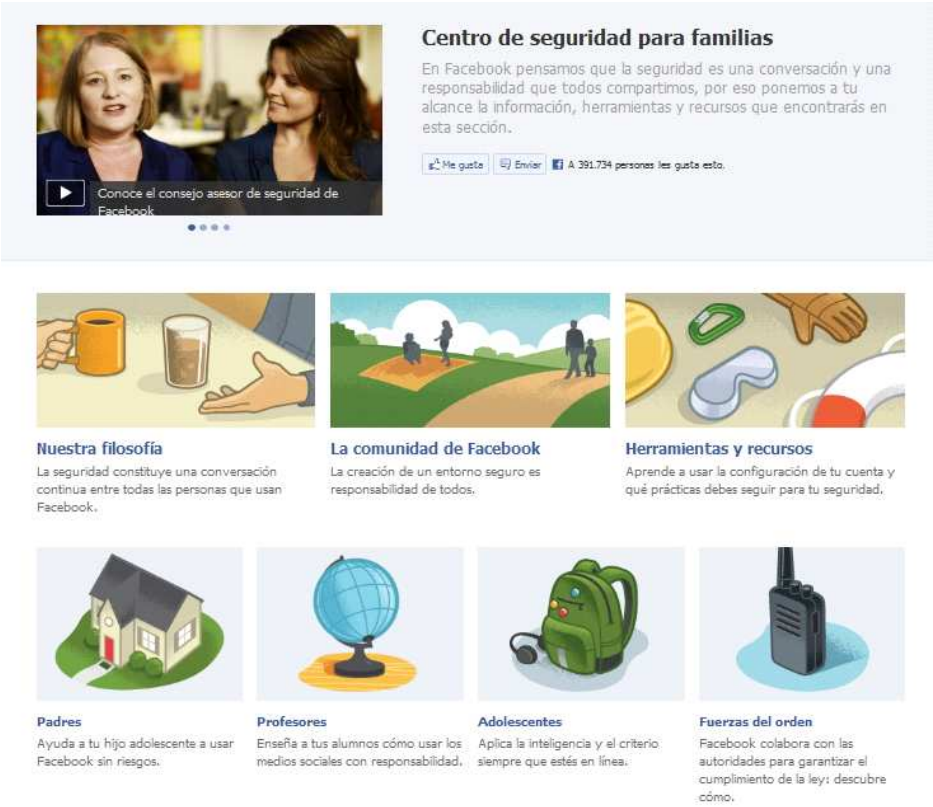
3.4.1.2 Facebook – Consentimiento paterno

A diferencia de otras redes sociales, Facebook no dispone de ningún documento para padres de menores de cierta edad que deseen otorgar el permiso correspondiente a sus hijos para utilizar el servicio, siendo conscientes de todas las ventajas y peligros que puede conllevar su uso.

Sin embargo, presenta una amplia guía para padres y profesores sobre cómo orientar a un menor a la hora de utilizar el servicio y la red en general de forma segura.

Para ello, habría que visitar el apartado *Los menores y la seguridad* del portal (actualmente localizado en la URL: https://www.facebook.com/about/privacy/minors):

Si seleccionamos el enlace *Centro de Seguridad* incluido en esta introducción, la página nos enviará al apartado correspondiente donde podremos encontrar información más detallada y por categorías sobre el tema:



Además, podemos encontrar en la misma gran cantidad de enlaces de otros documentos o sitios web destinados exclusivamente a la protección del menor en la red, así como información sobre cómo

actuar si observamos comportamientos inadecuados o peligrosos que involucren de forma directa o indirecta a un menor. Comentar que se trata de sitios web norteamericanos principalmente y que por tanto toda la información contenida en los mismos está relacionada con las leyes aplicables en el país.

3.4.1.3 Facebook – Denuncia social

Uno de los peligros a los que nos exponemos a la hora de publicar fotos, comentarios o información general sobre nosotros mismos, es la crítica social. Esta puede ser inofensiva; simples bromas o comentarios entre amigos y compañeros.

Sin embargo, existe la posibilidad que algún otro usuario haga uso de nuestra información para ofender o difamar acerca de nosotros.

Para estos casos, Facebook propone una serie de pasos a seguir para ayudarnos a denunciar estos comportamientos.

Denuncia contenido ofensivo o abusivo

Infórmanos acerca de cualquier contenido que suponga una infracción de las Condiciones de Facebook. El método más eficaz para denunciar contenido abusivo es hacerlo directamente desde el área de Facebook en la que lo hayas encontrado, mediante el enlace Denunciar que encontrarás cerca de la publicación, biografía o página.

Si recibes un mensaje de acoso de uno de tus amigos de Facebook, puedes hacer clic en el enlace Denunciar, situado junto al nombre del remitente del mensaje, y eliminar a esa persona de tu lista de amigos. Al denunciar un mensaje por acoso, se añade automáticamente al remitente a la lista de bloqueados. También puedes usar la opción Denunciar/bloquear que aparece debajo del icono de engranaje en la parte superior derecha de la biografía de todos los usuarios.

Las denuncias son confidenciales. El usuario en cuestión no sabrá que lo has denunciado. Una vez enviada la denuncia, investigaremos el caso y determinaremos si el contenido debe o no eliminarse tomando como referencia las Condiciones de Facebook. Investigamos cada una de las denuncias para determinar cuál es la línea de acción adecuada.

Denuncia social

La denuncia social es una función de la herramienta de denuncia que te ayuda a resolver problemas con publicaciones, biografías y otro contenido del sitio. Si quieres denunciar contenido que no te gusta pero que no incumple las Condiciones de Facebook, te facilitamos que te comuniques con la persona que publicó dicho contenido. Por ejemplo, si estás denunciando una foto en la que apareces, puedes enviar fácilmente un mensaje a la persona que la publicó para que sepa que no te gusta. En la mayoría de los casos, si lo pides, eliminarán la foto.

En casos de bullying o acoso, si no te sientes cómodo comunicándote con la persona directamente, puedes utilizar la herramienta de denuncia

social para obtener ayuda de un padre, profesor o amigo de confianza. Puedes compartir ese contenido y un mensaje explicando la situación con una persona de confianza. También tienes la opción de bloquear a la persona que ha publicado el contenido y denunciarlo a Facebook, para que podamos llevar a cabo la acción correspondiente, si procede.

En el apartado de *Facebook y el cumplimiento de la Ley* del centro de seguridad, se indica que en casos de emergencia pueden llegar a proporcionar información a los agentes del orden público, para poder evitar así situaciones extremas que impliquen un riesgo inmediato de sufrir daños, prevención del suicidio y la recuperación de niños desaparecidos.

3.4.1.4 Facebook – Identificación por IP

En el apartado *Otros tipos de información que recibimos sobre ti* de la Política y uso de datos se indica que cada vez que nos conectamos a Facebook estamos enviando la información del dispositivo u ordenador que estamos utilizando para acceder al servicio.

Entre esta información se podría incluir la dirección IP y otra información relativa a nuestro servicio de Internet, nuestra ubicación, el tipo de navegador que utilizamos e incluso obtener nuestras coordenadas GPS u otros datos de ubicación.

Esta información, así como puede resultar útil a Facebook a la hora de sugerirnos otros usuarios de nuestra zona o filtrar publicidad que nos pueda resultar más interesante, también ayuda a mantener localizados a cada uno de los usuarios del servicio. De esta forma, en caso de situación de alerta que pueda resultar peligrosa para un menor o cualquier usuario en general que pudiese llegar a requerir la ayuda de las fuerzas del orden, aporta una información adicional que puede llegar a ser de gran utilidad.

3.4.1.5 Facebook – Filtrado de material ofensivo

En el subapartado *Información que decides compartir* de la *Política de uso de datos* se advierte que indicar la fecha de nacimiento a la hora de registrarse permite a Facebook la posibilidad de poder

mostrar anuncios y contenidos adecuados para la edad que indicamos tener.

Por tanto, si somos sinceros a la hora del registro encontramos así un filtro de material que podría resultar ofensivo o inadecuado para menores de cierta edad.

3.4.1.6 Facebook – Huella digital

En el subapartado *Compartir el contenido y la información* de los TOS se indica qué ocurre con toda la información y contenido que publicamos en Facebook.

Para conocer qué ocurre con toda esta información que compartimos una vez la eliminamos o nos damos de baja en el servicio nos centraremos en los siguientes puntos:

1. Para el contenido protegido por derechos de propiedad intelectual, como fotografías y vídeos (en adelante, "contenido de PI"), nos concedes específicamente el siguiente permiso, de acuerdo con la configuración de la privacidad y las aplicaciones: nos concedes una licencia no exclusiva, transferible, con derechos de sublicencia, libre de derechos de autor, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook (en adelante, "licencia de PI"). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta, salvo si el contenido se ha compartido con terceros y estos no lo han eliminado.
2. Cuando eliminas contenido de PI, este se borra de forma similar a cuando vacías la papelera o papelera de reciclaje de tu equipo. No obstante, entiendes que es posible que el contenido eliminado permanezca en copias de seguridad durante un plazo de tiempo razonable (si bien no estará disponible para terceros).

3.4.1.7 Facebook – Responsabilidad legal

En el subapartado *Conflictos* de los TOS se expone la responsabilidad de Facebook ante cualquier demanda o conflicto que involucre al servicio.

En él se recuerda que el único responsable de todo el material compartido en la red social es el propio usuario, ya sea ofensivo, inapropiado, obsceno, ilegal o inaceptable.

Por ello, al registrarnos estamos accediendo a librar a Facebook de toda responsabilidad por todos los posibles daños, pérdidas y gastos de cualquier tipo que se puedan derivar de alguna demanda

interpuesta por alguien como consecuencia del uso malintencionado del Servicio.

3.4.2 Tuenti

Tuenti es una red social española lanzada a finales de 2006. El sitio estaba enfocado principalmente a la población española, hasta que el 11 de julio de 2012 se anunció una renovación de la red social en la cual el nuevo Tuenti estaría abierto a toda Europa, América, y con una mayor oferta de idiomas.

Al principio, el sitio web iba dirigido a universitarios. Debido a su éxito, más tarde permitieron la entrada a más usuarios a través de una invitación. El 14 de noviembre de 2011 se eliminó esa restricción de forma que todos pudiesen acceder a la red social registrándose con su número de teléfono.

Actualmente cuenta con más de 14 millones de usuarios.

3.4.2.1 Tuenti – Edad mínima

Tal y como se advierte en las condiciones de uso del sitio, el acceso al mismo está prohibido a los menores de 14 años.

Al igual que pasa con Facebook, a la hora de registrarse no se pide ningún documento o información que acredite que realmente el usuario es mayor a la edad permitida. Por tanto el usuario se responsabilizará enteramente de dicha declaración.

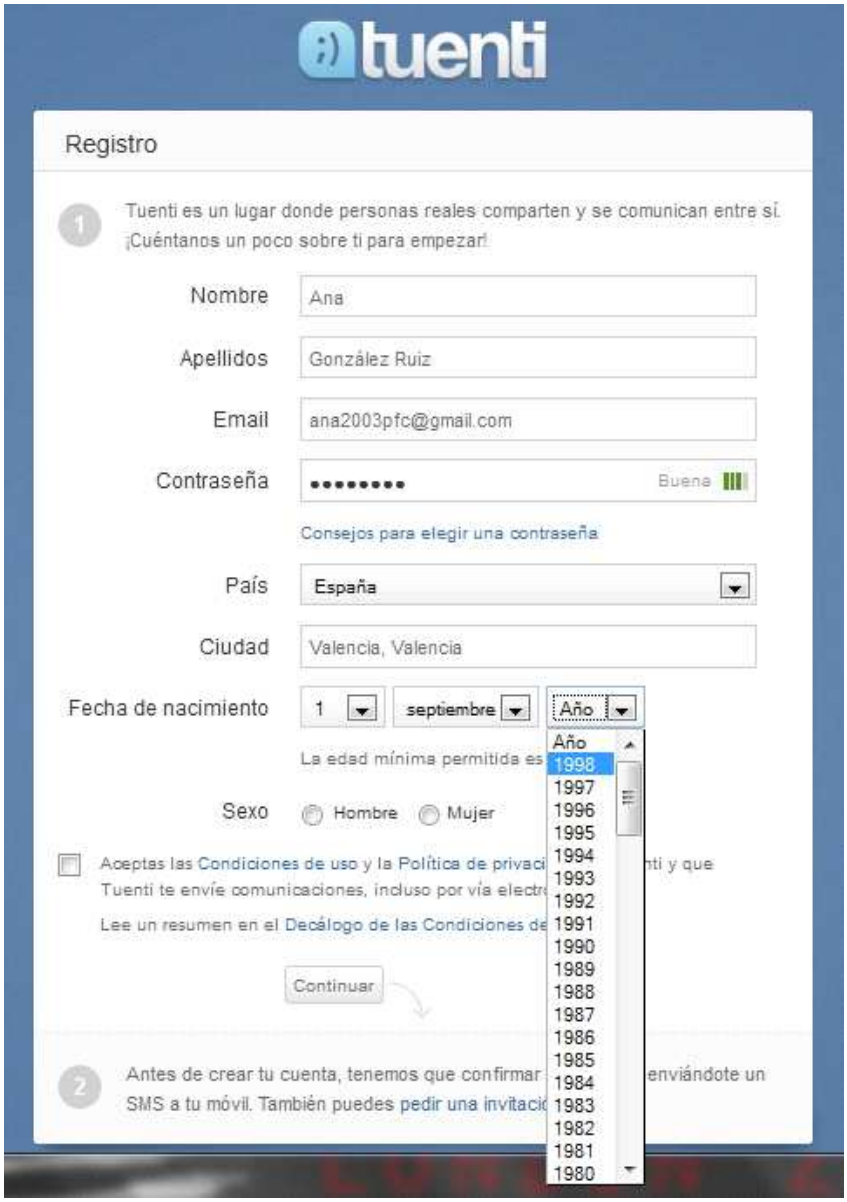
Como ejemplo, veamos esta vez cómo Ana, de 9 años, se puede registrar en Tuenti sin problemas.

Recordemos a Ana:

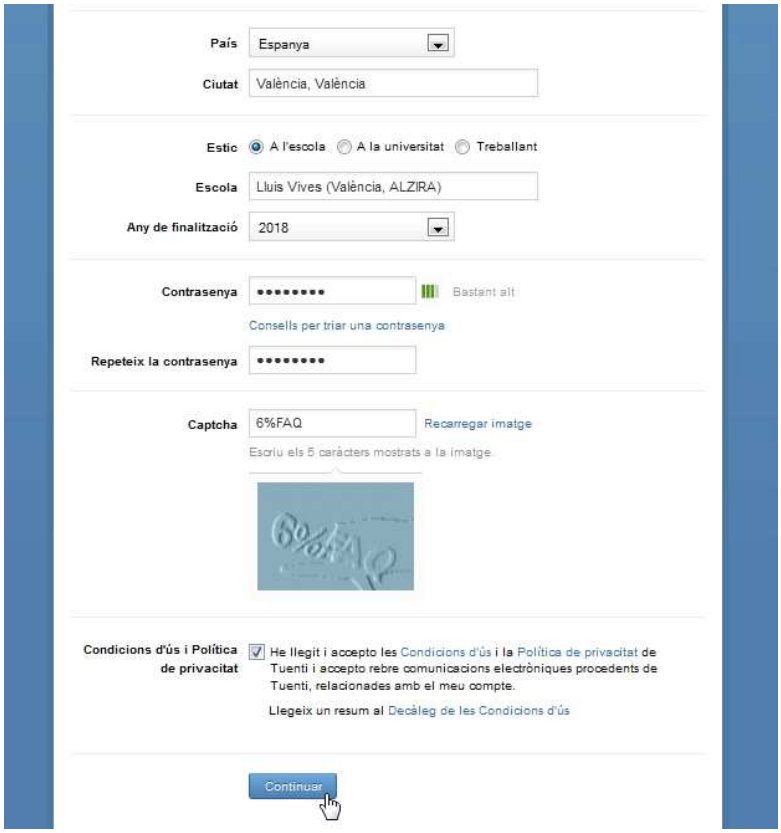
Ana tiene 9 años y, por tanto, no debería tener prohibido el acceso a esta red social.

Ana recibe una invitación por parte de una amiga para registrarse en el servicio y accede al portal. Empieza a introducir los datos, ya la hora de insertar la fecha de nacimiento vemos cómo solamente nos deja insertar un año menor a 1998 y que, por tanto, indicaría que el usuario es mayor de 14 años.

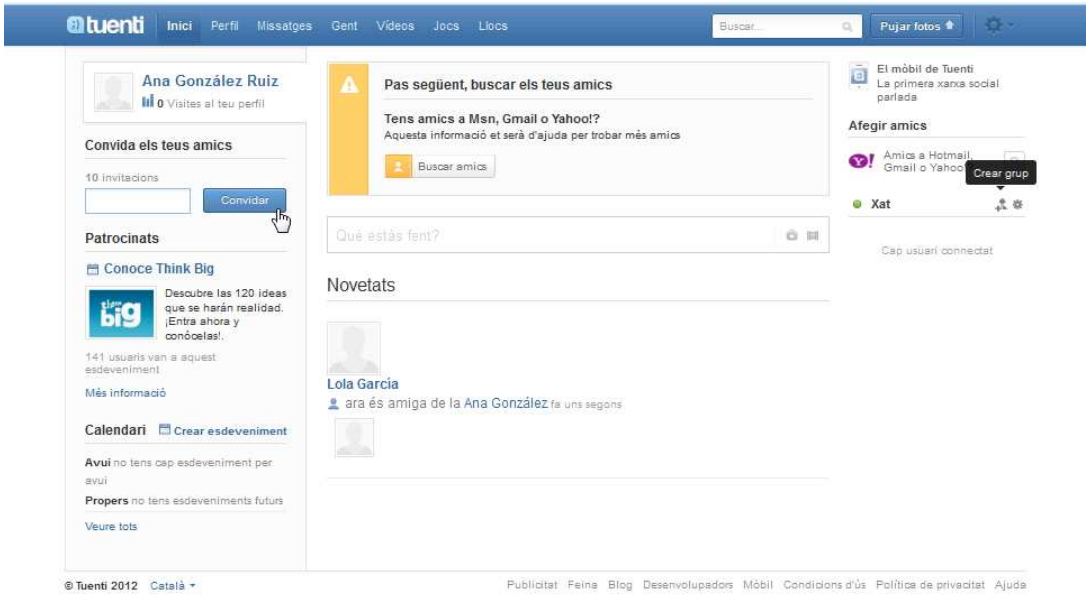
Ana quiere registrarse, por lo que directamente seleccionará el año máximo de nacimiento para acceder al portal:



Como ya hemos dicho que cumplimos la edad mínima, procedemos a finalizar el registro en el sitio web:



Y Ana ya está dentro:



Como vemos, nos ha resultado más rápido entrar en Tuenti que en Facebook, pues a la hora de registrarnos ya se nos está indicando que para poder formar parte de la red social debemos haber nacido

como muy tarde en el año 1998 y, por tanto, podemos seleccionar el año correcto en el primer intento de registro.

No obstante, se advierte que el equipo de portal puede ponerse en contacto con el usuario en cualquier momento para demostrar la edad real aportando la documentación pertinente, como copia o foto del DNI o documento equivalente. En caso de negar dicha petición por parte del usuario, el equipo de Tuenti se reserva el derecho a bloquear o cancelar el perfil del mismo.

3.4.2.2 Tuenti – Consentimiento paterno

Al contrario que Facebook, Tuenti permite el acceso al servicio a menores de la edad mínima indicada si se presenta el debido formulario que se puede descargar en el mismo portal web. En él, uno de los padres o tutor firmaría un consentimiento para que este usuario pueda utilizar el servicio y por tanto asumiría toda la responsabilidad del uso que el menor pueda hacer de él.

A su vez, la persona que firma la autorización deberá presentar también toda la documentación que se pertinente o necesaria para verificar su autenticidad y validez. Por ejemplo, copia o foto del DNI/pasaporte en vigor del padre, madre y/o tutor legal, copia o foto del Libro de Familia o documento equivalente, así como copia o foto del DNI/Pasaporte en vigor del menor, si lo hubiere.

Cualquier persona se puede descargar la autorización en el enlace de que aparece en los TOS del servicio:

tuenti

AUTORIZACIÓN DE PADRES/TUTORES DE MENORES DE CATORCE AÑOS.
D./Dª _____ , con DNI/pasaporte en vigor número _____, en mi condición de padre/madre/tutor/tutora de D./Dª_____, menor de 14 años, (en adelante el Menor) , con DNI/pasaporte en vigor número_____, y con dirección de correo electrónico de acceso a Tuenti _____@____.
En virtud del artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, LOPD), se recaba el consentimiento de los representantes legales del Menor, para garantizar su plena comprensión y aceptación de los extremos que se derivan del deber de

información establecido en la LOPD, y por la presente declaro:
Que CONSIENTO Y AUTORIZO EXPRESAMENTE a TUENTI TECHNOLOGIES, S.L. a tratar y almacenar los datos personales del Menor, recabados a través de su perfil en http://www.tuenti.com de acuerdo con las Condiciones de Uso y Política de Privacidad del Sitio Web, que se remiten anexas a este documento.
TUENTI TECHNOLOGIES, S.L. como responsable de los datos personales obtenidos a través del presente documento, le informa que los mismos, serán tratados y almacenados únicamente con la finalidad de garantizar que se ha comprobado de modo efectivo la edad del menor, así como la autenticidad del consentimiento prestado. La no remisión de esta autorización debidamente cumplimentada impedirá que el Menor pueda disfrutar de los servicios ofrecidos a través del Sitio Web.
Usted reconoce que podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición, así como los del Menor, y manifestar su negativa al tratamiento, remitiendo una solicitud, acompañada de su DNI a la siguiente dirección de correo electrónico: privacidad@tuenti.com.
En _____, a __ de _____ de _____.
Fdo:
Adjunto copia de mi DNI/pasaporte en vigor, Libro de Familia y copia del DNI/pasaporte en vigor del menor si lo hubiere.

3.4.2.3 Tuenti – Denuncia social

En el apartado *Responsabilidad por interacciones con otros usuarios* de los TOS se recuerda que el único responsable de las interacciones entre usuarios son los propios usuarios. Sin embargo, en caso de que algún usuario se sienta acosado, molestado o intimidado, se anima al mismo a comunicarlo de forma inmediata al equipo de Tuenti para que éstos tomen las mediadas oportunas.

Para ello, existen varios mecanismos de bloqueo y denuncia que están a disposición del usuario.

3.4.2.4 Tuenti – Huella digital

En el apartado *Contenido de los perfiles de los usuarios* se anuncia que al publicar contenido en el perfil de cualquier usuario (estados, fotos, textos vídeos, sonidos, dibujos, logos, etc.) el usuario conserva todos los derechos sobre los mismos y otorga a Tuenti una licencia limitada para reproducir y comunicar públicamente los mismos, para agregarles información y para transformarlos con el objetivo de adaptarlos a las necesidades técnicas del Servicio.

Esta licencia quedará resuelta al eliminar el contenido o al darse de baja en el Servicio. A partir de ese momento, Tuenti interrumpirá la

comunicación del contenido del usuario a la mayor brevedad posible.

A su vez, en el apartado *Baja en el servicio* de los TOS se exponen los pasos a seguir a la hora de desactivar una cuenta. Se puede elegir entre desactivar una cuenta de forma temporal o darla de baja de forma definitiva.

Si escogemos esta segunda opción, se perderá toda la información de la cuenta del usuario sin forma de recuperarla después. Toda esta información incluye las fotos y los comentarios que haya podido compartir el usuario a través de la red social

3.4.2.5 Tuenti – Responsabilidad legal

Tal como se expone en el apartado *Responsabilidades* de los TOS del Servicio, "Tuenti actúa como mero intermediario que pone a tu disposición su plataforma tecnológica, asumiendo única y exclusivamente la responsabilidad derivada de la diligencia que le pudiera ser exigible por ley. TUENTI no asumirá ninguna responsabilidad, ya sea directa o indirecta, derivada del mal uso que hagas del Servicio, del sitio web, de la aplicación móvil o de los contenidos allí alojados."

Tuenti se compromete a hacer todo lo razonablemente posible para vigilar la legalidad de los contenidos e información que se comunique a través del Servicio, pero, al no ser posible el control absoluto de los mismos, el usuario será el único responsable de la información, imágenes, comentarios, opiniones, alusiones o contenidos de cualquier tipo que comunique, aloje, transmita, ponga a disposición o exhiba a través del servicio web y/o aplicaciones móviles de Tuenti. Además, Tuenti no asume ninguna responsabilidad en la posible recogida y tratamiento de información de usuarios por parte de otros usuarios o por terceros.

3.4.3 Twitter

Twitter es una red social que permite enviar mensajes de texto plano de corta longitud llamados "tweets", que se muestran en la página principal del usuario. Actualmente, se le define como un servicio de

microblogging, que consiste en enviar y publicar mensajes breves (alrededor de 140 caracteres).

Twitter fue creado en marzo de 2006 y actualmente se calcula que cuenta con más de 200 millones de usuarios en todo el mundo.

Por defecto, los mensajes son públicos, por lo que hay que tener en cuenta todo los escribimos y publicamos ya que, como anuncia en sus términos del servicio, "Somos lo que twitteamos". Sin embargo, existe la posibilidad de bloquear los " tweets " y difundirlos de forma privada mostrándolo únicamente a nuestros seguidores.

Todo ello está expuesto en sus TOS y política de privacidad, de las que hablaremos a continuación.

3.4.3.1 Edad mínima

Tal y como se anuncia en el apartado *Nuestra política respecto a los niños* de la política de datos, Twitter no está dirigido a usuarios menores de 13 años.

Sin embargo, tampoco prohíbe expresamente el uso por parte de menores de esta edad.

Recordemos a José, de 9 años, que quiere abrirse una nueva cuenta en la red social:

Como vemos, a la hora de registrarse únicamente se le pide un *nickname*, un correo electrónico válido y una contraseña. En ningún momento nos pide la edad o el año de nacimiento.

José introduce sus datos y le da al botón “Regístrate en Twitter”.

Twitter revisa que no existe ningún otro usuario con los datos que el nuevo usuario acaba de introducir y, tras estas comprobaciones, da la bienvenida a José:

3.4.3.2 Consentimiento paterno

Si leemos con detenimiento los términos del servicio y la política de protección de datos, nos encontraremos que el Servicio no está

orientado ni dirigido a menores de 13 años. Además, no presenta ningún formulario de consentimiento para que los padres puedan otorgarles el mismo a los hijos para poder utilizar la red social.

Sin embargo, el Servicio sí que posee una política sobre el uso de datos de menores de esta edad y anima a los padres o tutores conscientes de la existencia de una cuenta del menor a reportarlo a través de la dirección de correo que nos facilita: privacy@twitter.com

De esta manera, Twitter procedería a la realización de lo necesario para borrar dicha información y dar de baja la cuenta del niño.

Además, presenta una guía (actualmente no disponible en Español) para padres y adolescentes en la que aporta consejos sobre el uso seguro de la red social. La misma se puede consulta en el siguiente enlace: https://support.twitter.com/articles/20169210-tips-for-parents.

3.4.3.3 Denuncia social

Aunque en los documentos de los términos del Servicio y Política de Privacidad de Twitter no mencione el cómo actuar ante una situación que podríamos considerar peligrosa para un usuario, sí que dedica varios apartados en el Centro de Ayuda del Servicio. En ellos encontraremos los pasos necesarios para reportar alguna Infracción o Comportamiento Abusivo que presenciemos en la red social.

Si entramos en el Centro de Ayuda, encontraremos un apartado denominado Políticas y Violaciones. Dentro del mismo, veremos que éste se divide en cuatro subapartados; Reglas y Políticas de Twitter, Directrices de Uso, Reportar una Infracción y Políticas del Anunciante.

En ellos encontraremos respuesta a muchas de las dudas que nos puedan surgir al utilizar el Servicio. El que más nos interesa para nuestro cometido será el de "Reportar una Infracción".

Como ocurre en la gran mayoría de TOS de redes sociales estudiadas, debe ser la propia víctima o los representantes legales de la misma los que reporten acerca del comportamiento abusivo que está recibiendo. Esto es así para evitar reportes falsos o no

autorizados por parte de terceras personas. Sin embargo, se anima a estos testigos a alentar a la víctima para reportar el abuso. Para ello, se dispone de un formulario a rellenar en el siguiente enlace: https://support.twitter.com/forms/abusiveuser

Tras un reporte, Twitter se compromete a revisar la cuenta reportada así como los tweets que el usuario desea que sean investigados. De esta manera, Twitter valorará si la cuenta ha cometido una infracción a las políticas del Servicio y, sólo en este caso, procederá a las acciones que crea convenientes. Estas pueden ir desde una advertencia al usuario hasta la suspensión permanente de la cuenta.

Cabe recordar que Twitter hace hincapié en que se permite a los usuarios la publicación de contenido ofensivo o potencialmente provocador. Además, Twitter por defecto no controla el contenido que se publica y tampoco retira el este tipo de contenido a menos que se violen ninguna de las normas establecidas en las condiciones y reglas del Servicio.

Para los casos menos graves en los que un usuario simplemente se sienta incómodo u ofendido por los tweets o comentarios de otro usuario, se recomienda utilizar las herramientas de Twitter para:

- Bloquear a un usuario:

Cómo bloquear usuarios en Twitter

Twittear

Para bloquear un usuario de Twitter:

1. **Inicia sesión** en tu cuenta de Twitter.
2. **Ingresa a la página de perfil** de la persona a la que deseas bloquear.
3. **Haz clic en el ícono de persona** de su página de perfil. Aparece un menú desplegable con acciones.
4. Selecciona **Bloquear** de entre las opciones listadas.

Los usuarios bloqueados no pueden:

- Agregar tu cuenta de Twitter a sus listas.
- Hacer que tus @respuestas o menciones aparezcan en tu pestaña de menciones (aunque estos Tweets pueden aparecer en búsquedas).
- Seguirte.
- Ver tu foto de perfil en su página de perfil o en su cronología.

- Dejar de seguir a alguien:

Para dejar de seguir desde tu lista de Siguiendo:

1. Haz clic en Siguiendo en tu página de inicio o de perfil.
2. Sitúa el cursor sobre el botón azul de **Siguiendo** que está al lado de cualquier usuario de tu lista de Siguiendo, el botón cambiará a un **Dejar de seguir** rojo.
3. **Haz clic en el botón** para dejar de seguir esa cuenta.

Para dejar de seguir desde la página de perfil de un usuario:

1. Ve a la página de perfil del usuario que quieres dejar de seguir.
2. Sitúa el cursor sobre el botón azul de **Siguiendo** en la esquina superior derecha, este se volverá rojo y mostrará **Dejar de seguir**.
3. **Haz clic en el botón** para dejar de seguir esa cuenta.

Para dejar de seguir mediante SMS/mensaje de texto:

- Si estás usando Twitter para SMS para seguir a otros, puedes elegir dejar de seguir al usuario enviando **NOSEGUIR nombredeusuario** al código corto de tu proveedor. (Ejemplo: **NOSEGUIR ayuda**)
- Si no quieres dejar de seguir al usuario completamente, sino solamente dejar de recibir sus actualizaciones por SMS, puedes enviar **DEJAR nombredeusuario** o **DESACTIVAR nombredeusuario** al mismo código corto. (Ejemplo: **DESACTIVAR ayuda** o **DEJAR ayuda**)
- Para conocer más sobre Twitter para SMS y comandos de texto por SMS, lee este artículo.

- Hacer nuestros Tweets protegidos o privados

¿Quién puede ver mis Tweets?

- Los **Tweets públicos** (la configuración por defecto) son visibles para todos, ya sea que tengan una cuenta de Twitter o no.
- Los **Tweets protegidos** sólo son visibles para seguidores de Twitter previamente aprobados. A continuación se puede ver la apariencia que tiene una cuenta con Tweets protegidos para personas que no sean seguidores aprobados.

Sin embargo, para los casos más graves o extremos que puedan llegar a la violencia o a hacer peligrar la seguridad de un usuario, Twitter aconseja el ponerse en contacto directamente con las autoridades locales. Estos serán los encargados de evaluar la gravedad del contenido o comportamiento y si éste constituye una violación a las leyes locales. En estos casos, Twitter se ofrece a trabajar con las autoridades si éstas contactan directamente con el Servicio, pudiendo proporcionar asistencia a su investigación y una guía para posibles soluciones.

Además, conscientes de la problemática del cyberacoso, lista algunos recursos en línea que pueden ayudar a lidiar con esta delicada situación:

- http://www.ciberbullying.net/
- http://bit.ly/fjM9FG
- http://www.internetsinacoso.es/

Otra de las cuestiones que más se comenta al hablar del peligro de las redes sociales es el de la **pornografía infantil**. Twitter, que también demuestra consciencia e intolerancia sobre el tema, dedica otro apartado de su Centro de Ayuda a proporcionar la información necesaria sobre cómo actuar al encontrarse con una situación que pueda asociarse a la explotación sexual de menores.

De esta forma, al tomar conocimiento de enlaces a imágenes o contenido que promueva esta práctica, Twitter los retirará del sitio sin previo aviso y lo reportará al Centro Nacional para Niños Desaparecidos y Explotados (NCMEC). Además, "suspenderá permanentemente las cuentas que promuevan o que contengan actualizaciones con enlaces a contenidos relacionados con explotación sexual de menores".

Para luchar contra este delito, Twitter anima a los usuarios a reportar cualquier indicio de esta práctica enviando un e-mail a la dirección de correo cp@twitter.com .

3.4.3.4 Identificación por IP

En la Política de Protección de datos del Servicio se informa que, cada vez que utilizamos el servicio, los servidores del Sitio graban automáticamente información de registro del usuario. Esta información puede incluir, entre otras cosas, la dirección IP completa del usuario, el tipo de navegador, sistema operativo, la web de procedencia, páginas web visitadas, ubicación, etc.

El Servicio anuncia que toda esta información, junto con todo el contenido compartido por un usuario, podrá ser conservada y revelada si se considera que es razonablemente necesaria para cumplir una ley, reglamento o requerimiento legal y, más importante, proteger la seguridad de cualquier persona.

3.4.3.5 Filtrado de material ofensivo

En los términos del Sitio se anuncia que los Servicios que utiliza el usuario pueden incluir publicidad relacionada con el contenido o información proporcionada a los Servicios.

Sin embargo, en ningún momento se anuncia ningún tipo de filtro aplicado a los mismos.

3.4.3.6 Huella digital

En el apartado 5 de los términos del Servicio relativo a los derechos del usuario, se informa que a la hora de compartir o exponer

contenido en el Sitio, estamos cediendo directamente a Twitter una "licencia mundial, no-exclusiva y gratuita (así como el derecho de sublicencia) sobre el uso, copia, reproducción, procesamiento, adaptación, modificación, publicación, transmisión, exposición y distribución de tal contenido a través de cualquier medio o método de distribución presente o futuro".

Además, a diferencia de otras redes sociales, esta licencia perdurará incluso una vez dada de baja la cuenta en el Sitio y dado pues por finalizado el contrato.

Tal y como se anuncia en el apartado 10 (Fin de la Aplicación de estas condiciones) de los TOS, al producirse una finalización de contrato con Twitter, "se producirá la terminación de las Condiciones incluyendo, sin limitación alguna, la licencia para utilizar los Servicios salvo en el caso de las cláusulas 4, **5**, 7, 8, 10, 11 y 12, que sobrevivirán a la terminación de estas Condiciones".

3.4.3.7 Responsabilidad legal

De igual forma que ocurre con la gran mayoría de redes sociales, Twitter deja en manos del propio usuario toda responsabilidad ante el acceso y uso de los Servicios o de cualquier Contenido.

Además, será el responsable de cualquier consecuencia que se derive de ello. Por ello se advierte al usuario, que a la hora de aceptar los términos y condiciones del servicio, éste entiende que el uso del mismo "puede exponerle a contenido ofensivo, dañino, erróneo o inapropiado, o en algunos casos, a mensajes etiquetados incorrectamente o engañosos. Bajo ninguna circunstancia asumirá Twitter responsabilidad alguna por el Contenido".

Podremos encontrar en el apartado de 11. *Renuncia y Limitación de Responsabilidad* de los TOS y, más concretamente en el subapartado C del mismo, información más detallada sobre la limitación de responsabilidad del Servicio web: "Con la mayor amplitud que permita la ley aplicable, las entidades de Twitter no serán responsables por ningún daño indirecto, incidental, especial consecuente o punitivo, o cualquier lucro cesante, en el que haya podido incurrirse de forma directa o indirecta, o cualquier pérdida de uso, fondo de comercio, o cualquier otra pérdida intangible como resultado de (i)…; (ii) cualquier conducta o contenido

generado por un tercero a través de lo Servicios, incluyendo, sin limitación alguna, toda conducta difamatoria, ofensiva o ilegal de otros usuarios o terceras partes; (iii)…"

Sin embargo, en la Política de Privacidad así como en el apartado de Centro de Ayuda del Sitio sí que informa que el Sitio se reserva el derecho de conservar o revelar información de un usuario si se considera que es razonablemente necesaria para cumplir con una ley. Por tanto, aunque se excluya de toda responsabilidad, sí que se muestra una actitud cooperativa a la hora de resolver cualquier conflicto que pueda llegar a afectar la seguridad de una persona.

3.4.4 Instagram

Instagram es una aplicación gratuita para compartir fotos. En ella, los usuarios podrán aplicar efectos fotográficos a sus imágenes tales como filtros, marcos y colores retro y vintage, y tendrán la opción de compartirla a través de redes sociales como Facebook, Twitter, Tuenti, Tumblr y Flickr.

La aplicación fue originalmente lanzada el 6 de Octubre de 2010 en la Apple App Store únicamente disponible para teléfonos iPhone y otros dispositivos Apple como iPad y iPod. A principios de Abril de 2012 se publicó también una versión para Android, que se puede adquirir en Google Play.

El 9 de Abril de 2012 se anunció que Facebook había adquirido la compañía, por lo que la política de privacidad de Instagram se actualizó para realzar esta unión.

Esta red social cuenta actualmente con más de 100 millones de usuarios a nivel mundial.

3.4.4.1 Edad mínima

La primera norma que aparece en los Términos de Uso de Instagram hace referencia a la edad mínima permitida para poder utilizar el

servicio. En este caso se indica que el usuario deberá tener más de 13 años.

Actualmente Instagram es una aplicación únicamente disponible a través de un dispositivo móvil, por lo que no podremos comprobar realmente las barreras que se le presentan a un menor de esta edad a la hora de registrarse.

Según las condiciones del Sitio, únicamente haría falta una dirección de correo electrónico válida y un nombre de usuario para dar de alta un nuevo registro.

3.4.4.2 Consentimiento paterno

Tal y como se anuncia en los términos del servicio, Instagram no va dirigido a menores de 13 años de edad. Tampoco presenta ningún formulario a rellenar por los padres en el que otorguen el permiso conveniente.

Sin embargo, sí que existe la posibilidad de que un padre con un hijo menor de 13 años registrado en el servicio obtenga acceso a la cuenta del mismo así como que pueda solicitar su eliminación.

Para ello, únicamente deberá mandar un correo electrónico a la dirección indicada en el apartado *Menores de edad* del Centro de Privacidad y Seguridad de Instagram con los siguientes datos:

- Nombre de usuario del menor

- Forma de identificación que pruebe que el menor no cumple con la edad mínima para utilizar el Servicio. Esto podría ser algún documento del colegio, certificado de nacimiento, etc.

3.4.4.3 Denuncia social

En Instagram, al igual que ocurre con el resto de redes sociales, podemos encontrarnos frente a situaciones que nos lleven a sufrir una experiencia negativa al utilizar el servicio, como son las peleas con otro usuario o el hecho de encontrar fotos ofensivas de alguien a quien seguimos.

Ante estas situaciones, tenemos la opción de **bloquear** al usuario en cuestión. Para ello, entraremos en su perfil con nuestro dispositivo móvil y seleccionaremos el botón que aparece en la parte superior derecha de la pantalla:

A continuación, seleccionaremos la opción "Bloquear usuario" de la pantalla siguiente:

Tras bloquear el usuario, éste no podrá buscar nuestro perfil ni seguirnos.

En el caso de ser conocedores de la creación de una cuenta cuya finalidad sea la de acosar a otro usuario o abusar de él, se anima al usuario a mandar una correo al Servicio con los datos necesarios para que Instagram la investigue y tome las medidas oportunas. Para ello, el usuario deberá adjuntar la siguiente información:

- Nombre del usuario que reporta
- Nombres de los usuarios de las cuentas que cometieron la infracción
- Incluir las URL de las imágenes o descripción de los comentarios abusivos o publicados en las cuentas de los usuarios

Tras el análisis de las cuentas reportadas, Instagram únicamente eliminará aquellas cuentas y contenidos que infrinjan las condiciones y normas del Servicio.

Si el conflicto ha ido demasiado lejos, Instagram anima los usuarios a ponerse en contacto con las autoridades locales, pues estas están en la mejor posición para valorar la amenaza y ayudar en caso necesario.

Además, Instagram se ofrece a trabajar con las autoridades siempre y cuando se soliciten dentro de un proceso legal válido. De esta manera, Instagram podrá proporcionarles la información que consideren necesaria para investigar el problema.

Además, en el apartado de "Información sobre cómo responder a conductas abusivas" del Centro de Ayuda del Servicio, encontraremos además una lista con enlaces de interés en los que podremos documentarnos sobre cómo actuar en estas situaciones.

- www.stopbullying.gov
- www.ncpc.org/cyberbulling
- www.cyberbulling.us
- www.connectsafely.org

Desafortunadamente, actualmente sólo se muestran enlaces de sitios de Estados Unidos de América.

3.4.4.4 Identificación por IP

En el apartado "Compartiendo tu información" de la política de privacidad, Instagram nos informa que cada vez que utilizamos cualquiera de sus Servicios automáticamente se registra información de nuestra sesión. Esta incluye, entre otras cosas, la información de las cookies, archivos de log, localización, identificador del dispositivo, etc.

Tal y como se comenta en el apartado anterior, esta información podrá ser transmitida a las autoridades si es requerida por las mismas a través de una solicitud legal válida.

Además, Instagram se reserva el derecho a compartir esta información en los casos que se considere necesario para:

- detectar, prevenir fraude u otra actividad ilegal
- proteger el propio Servicio así como al resto de usuarios, incluidas como parte de una investigación;
- prevenir la muerte o daño físico inminente

Esta información podrá estar accedida, procesada y retenida por un largo periodo de tiempo si forma parte de un proceso legal, investigación gubernamental o si alguna otra investigación en la que se considere que se están violando los términos del Servicio.

3.4.4.5 Filtrado de material ofensivo

En el apartado de "Derechos" de los TOS se anuncia que algunos de los Servicios de Instagram pueden presentar anuncios o promociones.

En general, estos anuncios irán vinculados a los Contenidos de cada usuario. Sin embargo, en ningún momento se informa que éstos puedan ser filtrados atendiendo a la edad del usuario.

3.4.4.6 Huella digital

En las condiciones del Servicio se informa del tratamiento del Contenido de cada usuario cuando éste desactiva o da de baja una cuenta.

Al finalizar el contrato con Instagram, las imágenes, comentarios y todo el contenido en general del usuario dejarán de estar disponibles a través de su cuenta. Sin embargo, todo este material podrá persistir en el Servicio si otros usuarios lo han compartido en sus respectivas cuentas.

Además, tanto Instagram como sus afiliados podrán retener la información del usuario por un tiempo razonable para la realización de *Backup*, archivos o fines de auditoría.

3.4.4.7 Responsabilidad legal

Al darse de alta en el Servicio, el usuario accede a cargar con toda la responsabilidad del uso que haga del mismo así como de todo el contenido que comparta en él. También será el único responsable de toda interacción con otros usuarios tanto en un entorno *online* como *offline*.

Por ello, en ningún caso Instagram se hará responsable por pérdida, daño o perjuicio, incluyendo lesiones personales o incluso la muerte.

Además, al aceptar el contrato el usuario accede a defender a Instagram, a petición del Servicio, contra cualquier reclamación, responsabilidad, daños, pérdidas y gastos que surja como consecuencia de la comisión de una infracción por parte del usuario. Se consideraría infracción actividades como el incumplimiento de los Términos de Uso, violación de cualquier derecho a terceros, violación de alguna ley, etc.

3.4.5 Servicios Google: Google+

Google+ (G+ o Google Plus) es una red social lanzada en junio de 2011 por Google Inc. En ella se pueden compartir fotos, comentarios e intereses y, además, permite los denominados *Hangouts*: un servicio de videollamada en el que pueden participar varios usuarios a la vez que pertenezcan al círculo de alguno de los participantes.

Desde julio de 2012 Google obliga indirectamente a crear un perfil de Google+ para poder utilizar completamente algunos de sus Servicios afiliados como YouTube. Esto disparó el número de usuarios de la red social, llegando a posicionarla actualmente como la segunda red social con más usuarios por detrás de Facebook.

Actualmente cuenta con más de 500 millones de usuarios, aunque este crecimiento de altas no ha conseguido aumentar el tiempo medio que cada usuario dedica a utilizar la red social que sigue siendo escaso desde su lanzamiento.

3.4.5.1 Edad mínima

A diferencia del resto de redes sociales estudiadas, no encontramos referencias a la edad mínima permitida para la utilización del Servicio ni en las condiciones ni en los Términos de Uso del mismo.

Tendremos que navegar por su Página Principal de la Ayuda de los Servicios Google para encontrar un apartado dedicado a las *Restricciones de edad en Cuentas de Google* dentro de las indicaciones de *Cómo empezar* a utilizar el Servicio.

Allí encontraremos la siguiente clasificación:

- **Estados Unidos**: 13 años o más
- **España**: 14 años o más
- **Corea del Sur**: 14 años o más
- **Países Bajos**: 16 años o más
- **Otros países**: 13 años o más

Estas restricciones de edad se aplicarán a algunos productos de Google que comparten un sistema de inicio de sesión único, tales como Google+, Gmail y YouTube.

Al crear una nueva cuenta de correo de Gmail, automáticamente nos aparecerá en la cabecera de nuestro navegador una cuenta Google+ asociada.

Al inicio de este apartado dedicado a analizar los Terms of Service de las redes sociales más relevantes, se crearon 4 perfiles de usuarios menores de edad y una cuenta de correo electrónico Gmail asociada a cada uno de ellos. Recordemos que dos de ellos tienen una edad inferior a la permitida y no nos resultó nada complicado burlar esta restricción.

3.4.5.2 Consentimiento paterno

No se han encontrado referencias a ningún tipo de consentimiento paterno para el uso de la red social en caso de jóvenes menores de la edad mínima permitida.

3.4.5.3 Denuncia social

Google+ tiene presente los peligros con los que se puede encontrar el usuario al utilizar un Servicio de estas características. Por ello,

presenta una lista de recursos para adolescentes, padres y educadores en su *Centro de Seguridad* para ayudar a evitar esta problemática.

La finalidad de todos estos consejos es conseguir alentar a los usuarios de la red social a hacer a un buen uso de la misma y navegar de forma segura y saludable.

En el texto referente a la *Política de Contenido y Conducta del Usuario* se informa, entre otras cosas que:

6. Protección de menores

No se permite la distribución de contenido que explote a los niños, como la pornografía infantil (incluida la pornografía infantil animada) ni de contenido que muestre a los niños en actitudes sexuales.

9. Material sexualmente explícito

No se permite la distribución de contenido que incluya desnudos, actividades sexuales explícitas o material sexual explícito. Tampoco se permite la publicación de contenido que genere tráfico a sitios pornográficos comerciales.

La imagen de los Perfiles de Google no puede incluir contenido ofensivo o destinado a un público adulto. Por ejemplo, no está permitido el uso de fotos que muestren primeros planos de las nalgas o el escote de una persona.

10. Acoso

No se permite el acoso hacia otros usuarios. Cualquiera que use Google+ para acosar a otras personas se expone a que se elimine el contenido ofensivo del sitio o a que se le prohíba utilizar dicho sitio. El acoso online es ilegal en muchos lugares y puede acarrear consecuencias graves en la vida real.

11. Violencia

No se permite la distribución de imágenes de violencia gratuita.

Sin embargo y siempre teniendo presente que no todos los usuarios cumplen con las normas y condiciones establecidas en el contrato, se presentan unas herramientas para reportar el contenido que infrinja estas directrices de forma que Google pueda tomar las medidas oportunas.

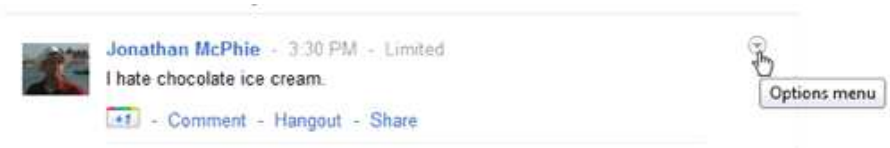
Se distinguen tres tipos de denuncias: las denuncias de comentarios, las denuncias de publicación o las denuncias de perfil. Veamos cómo actuar en cada una de las situaciones:

Denunciar un comentario

Pasa el ratón por encima del comentario, aparecerá una marca gris pequeña a la derecha. Haz clic en la marca para informar del uso inadecuado de ese comentario.

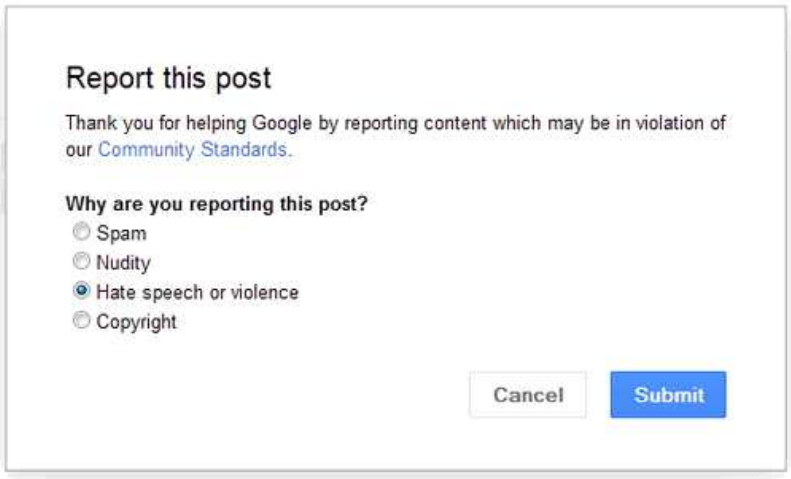
Denunciar una publicación

1. En la esquina superior de cada publicación podrás encontrar un pequeño círculo con un triángulo. Haz clic en este icono para mostrar un menú de opciones relacionadas con la publicación.



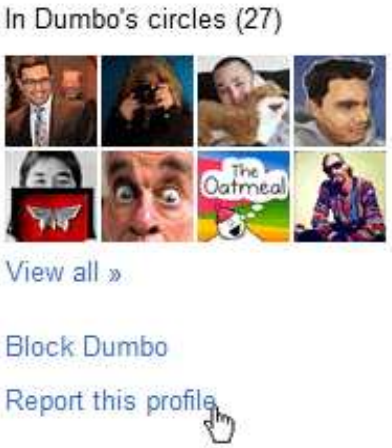
2. Haz clic en Informar de uso indebido.

3. Selecciona un motivo en el cuadro de diálogo.



Denunciar un perfil

Desplázate hasta el perfil que quieras denunciar. Debajo de la imagen del perfil, haz clic en Informar sobre este perfil.



3.4.5.4 Identificación por IP

Para mejorar el Servicio, Google recoge datos cada vez que utilizamos cualquiera de sus Servicios, como cuando visitamos una página web con servicios publicitarios de Google, visualizamos anuncios y contenidos Google e interactuamos con ellos, etc.

De entre la información que se recoge, podremos encontrar:

- Información detallada sobre cómo utilizamos el Servicio (consultas de búsqueda)
- Datos telefónicos
- Dirección IP

- Información relativa al dispositivo desde el que nos conectamos (tipo de navegador, idioma, fecha y hora de la solicitud, versión del sistema operativo, ID únicos y datos sobre la red, etc.

- Cookies

- Ubicación (a través de señales GPS, puntos de acceso Wifi,…)

En el apartado *Motivos Legales* de *Qué datos personales compartimos* (Política de Privacidad de Google), se declara que Google compartirá los datos personales de un usuario con empresas, organizaciones o personas físicas ajenas a Google en caso de ser necesario, entre otros casos, para:

- Cumplir cualquier requisito previsto en la legislación o normativa aplicable o atender cualquier requerimiento de un órgano administrativo o judicial

- Cumplir lo previsto en las Condiciones de Servicios vigentes, incluida la investigación de posibles infracciones

3.4.5.5 Filtrado de material ofensivo

Como hemos comentado en el punto anterior, Google obtiene información de los usuarios a través de las cookies.

Con esta información, Google trata de adaptar los anuncios publicitarios a la información que recoge sobre nuestra edad, sexo, localización, etc.

Una forma de poder filtrar parcialmente los anuncios a mostrar será a través del *Administrador de preferencias de anuncios*, en el que podremos suprimir algunas categorías de anuncios que aparecen asociados a nuestro perfil a través de la cookie.

Además, siempre podremos administrar también las cookies en nuestro navegador web.

3.4.5.6 Huella digital

En la política de privacidad encontraremos un apartado sobre *Cómo acceder a tus datos personales y actualizarlos*.

En él se informa que "Al prestar nuestros servicios, protegeremos tus datos procurando que no puedan ser eliminados de forma accidental o intencionada. Por este motivo, aunque elimines tus datos de nuestros servicios, es posible que no destruyamos de inmediato las copias residuales almacenadas en nuestros servidores activos ni los datos almacenados en nuestro sistema de seguridad".

Por tanto, nuestros datos permanecerán por un tiempo indefinido incluso después de haberlos eliminado.

3.4.5.7 Responsabilidad legal

A la hora de darnos de alta en el servicio, estamos aceptando un contrato en el que nos comprometemos a seguir unas normas de conducta adecuadas establecidas. Por tanto, seremos responsables del contenido que compartamos así como del uso que hacemos del Servicio.

3.4.6 Servicios Google: YouTube

YouTube es un sitio web en el que los usuarios pueden subir, comentar y compartir videos. Además, cada usuario puede suscribirse a los denominados "Canales" de otros usuarios e interactuar con ellos a través de comentarios o mensajes privados, por lo que en cierta manera, podríamos estar hablando de otra red social.

Fue creado en febrero de 2005, adquirido por Google Inc. en octubre de 2006 y ahora opera como una de sus filiales. Por ello, en la actualidad YouTube comparte Política de Privacidad y Condiciones del Servicio con todos los Servicios Google.

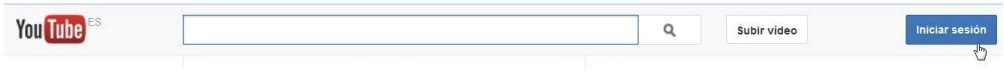
3.4.6.1 Edad mínima

Como hemos visto en el apartado Google+, la edad mínima para utilizar el Servicio es de 13 años.

Dicho esto, los menores de 13 años que accedan al portal tendrán prohibida la creación de una cuenta. Además, si llega a Google un video marcado para revisar (a través del reporte de otro usuario) y se determina que la edad declarada por el usuario al crear la cuenta no es cierta se procederá a la baja de la misma.

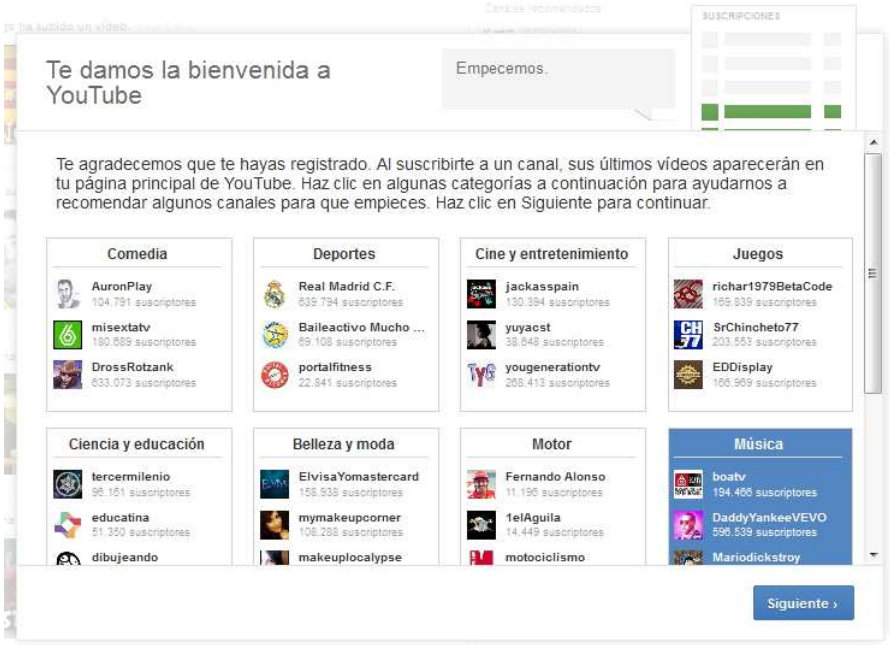
Cabe recordar, que actualmente se accede a YouTube a través de una cuenta Google+, por lo que cualquiera de nuestros cuatro perfiles de usuario tendría acceso al Servicio.

Recordemos a Ana (9 años). Accedemos al portal web y procedemos a iniciar sesión su cuenta:



Al seleccionar el botón de *Iniciar Sesión* que aparece en el borde derecho superior de la pantalla, nos pedirá los datos de inicio de sesión de nuestra cuenta Google:

Una vez introducidos nuestro correo electrónico y contraseña estaremos automáticamente *logueados*:



3.4.6.2 Consentimiento paterno

En los recursos para jóvenes, padres y educadores se insiste que para poder dar de alta una cuenta en el Servicio es necesario que los usuarios confirmen que tienen al menos 13 años. En ningún momento se incluyen aquellos menores de 13 años que presenten algún formulario o petición de padres o tutores legales otorgando su consentimiento.

3.4.6.3 Denuncia social

En el apartado de **Normas de las Comunidad YouTube** se establecen las pautas a seguir para evitar situaciones peligrosas e inaceptables. Entre ellas, cabe destacar:

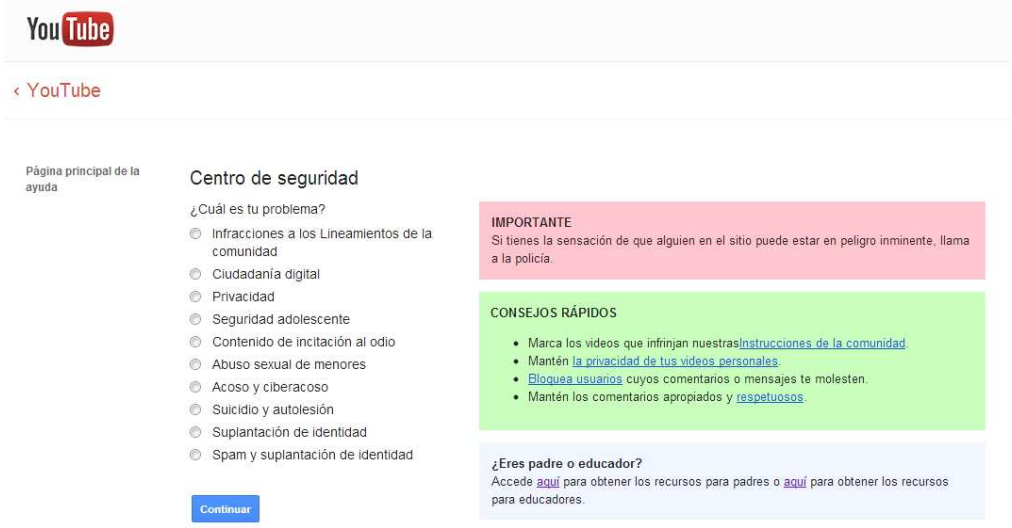
- YouTube no es un sitio destinado a la publicación de contenido pornográfico o sexualmente explícito… Ten en cuenta que trabajamos estrechamente con las autoridades y que notificaremos cualquier tipo de abuso de menores.

- No se permite la violencia explícita ni gratuita.

- No se toleran en modo alguno las amenazas, el comportamiento agresivo, el hostigamiento, el acoso, la invasión de la privacidad ni la revelación de información personal de otros miembros. Cualquier persona que incurra en alguno de los comportamientos anteriores puede ser expulsada de forma permanente de YouTube.

En el caso en que un usuario se encontrase con algún video con contenido inadecuado que infrinja las normas establecidas, se anima a reportarlo **marcando** el vídeo para que YouTube lo revise y tome las medidas oportunas.

Toda esta información la podremos encontrar ampliada en el apartado de *Seguridad* de YouTube.



Como se observa en la imagen anterior, el Centro de Seguridad dedica varios puntos a analizar cada una de las situaciones

peligrosas en las que se pudiera encontrar un usuario. Respecto al tema que nos concierne, encontramos varios apartados dedicados a los temas de *Seguridad adolescente*, *Abuso sexual de menores*, *Acoso y ciberacoso* y *Suicidio y autolesión*.

Además, añade recursos para padres y educadores y consejos para orientar a los jóvenes a navegar por el Servicio de forma segura.

De forma genérica, se recomienda seguir los siguientes pasos a la hora de actuar ante una situación de entre las que acabamos de presentar:

- Marcar contenido considerado inadecuado en las *Normas de Conducta del Servicio* así como aquellos vídeos en el que se expresan pensamiento suicidas.

- Bloquear a usuarios problemáticos (ej.: acosadores).

A continuación se indica cómo puedes bloquear a una persona en YouTube

1. Accede a la página de su canal, cuya URL es similar a www.youtube.com/user/NOMBRE.
2. En la pestaña "Feed" o "Destacados", haz clic en el menú desplegable **de NOMBRE**.
3. Haz clic en **Bloquear usuario**.

- Controlar los comentarios publicados en nuestro canal.

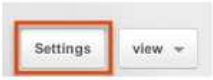
Cómo moderar los comentarios del canal

Para eliminar de tu perfil los comentarios de un usuario, sigue estos pasos:

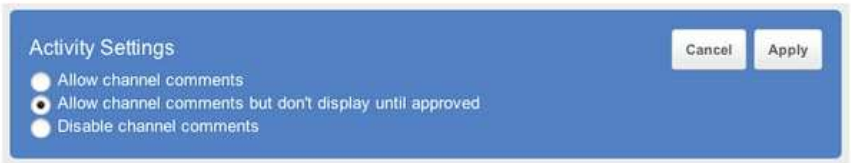
- Accede a la **página de tu canal**.
- Selecciona la **pestaña "Feed"**.
- Sobre tu historial de actividad, aparecerá un botón **Ver**. Si haces clic en él, verás una opción que permite visualizar **solo comentarios**.
- Si colocas el ratón sobre cualquier comentario, podrás hacer varias cosas con ese comentario (por ejemplo, **eliminarlo** o **marcarlo** como contenido inadecuado o como spam).

También puedes supervisar los comentarios antes de que aparezcan en tu canal. Esta opción te permitirá ver todos los comentarios que se publiquen en tu canal y darles el visto bueno antes de que aparezcan en él. Para ello, solo tienes que seguir estos pasos:

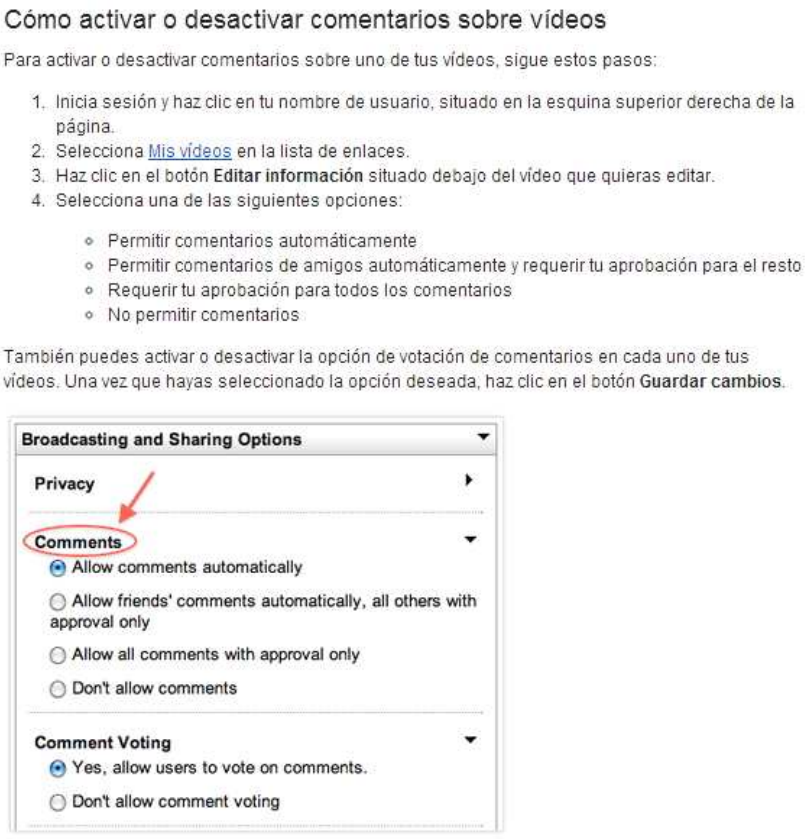
- Haz clic en tu nombre de usuario, situado en la esquina superior derecha de la pantalla.
- Selecciona **Mi canal** en el menú desplegable.
- Haz clic en el botón **Configuración** situado debajo del cuadro **Publicar un boletín**.



- Podrás elegir entre las siguientes opciones:
  - permitir que todos los comentarios del canal aparezcan en tu canal de forma automática,
  - permitir los comentarios del canal (solo tras tu aprobación),
  - desactivar por completo los comentarios del canal.



- Activar y desactivar los comentarios de los vídeos.



Cómo activar o desactivar comentarios sobre vídeos

Para activar o desactivar comentarios sobre uno de tus vídeos, sigue estos pasos:

1. Inicia sesión y haz clic en tu nombre de usuario, situado en la esquina superior derecha de la página.
2. Selecciona Mis vídeos en la lista de enlaces.
3. Haz clic en el botón **Editar información** situado debajo del vídeo que quieras editar.
4. Selecciona una de las siguientes opciones:
   - Permitir comentarios automáticamente
   - Permitir comentarios de amigos automáticamente y requerir tu aprobación para el resto
   - Requerir tu aprobación para todos los comentarios
   - No permitir comentarios

También puedes activar o desactivar la opción de votación de comentarios en cada uno de tus vídeos. Una vez que hayas seleccionado la opción deseada, haz clic en el botón **Guardar cambios**.

En la *herramienta de asistencia y seguridad* encontraremos más pautas a seguir a la hora de reportar comportamientos maliciosos. En cuanto a estas notificaciones, YouTube únicamente permite presentar una queja en nombre de un niño a los padres o tutores legales del menor.

El equipo de YouTube revisa los vídeos marcados 24h al día durante los 7 días de la semana y, a diferencia del resto de redes sociales estudiadas, se compromete a informar y trabajar estrechamente con las autoridades en situaciones en las que se presente cualquier tipo de abuso de menores.

3.4.6.4 Identificación por IP

Ídem que en caso de Google+. Recordemos que al tratarse de Servicios Google, ambos comparten la misma política de privacidad.

3.4.6.5 Filtrado de material ofensivo

Además de lo comentado en el apartado correspondiente de Google+, YouTube permite filtrar mediante la función *modo de seguridad* todo aquel contenido que no queremos que aparezca cuando utilizamos el Servicio.

Al activar este modo, no aparecerán en la búsqueda de vídeos todos aquellos que contengan material considerado potencialmente inaceptable o restringidos a usuarios mayores de edad.

3.4.6.6 Huella digital

Consultar apartado correspondiente a Google+.

3.4.6.7 Responsabilidad legal

Consultar apartado correspondiente a Google+.

3.4.7 Habbo Hotel

Habbo es una de las más grandes redes sociales en Internet enfocada a jóvenes y adolescentes. El servicio fue lanzado en el año 2000 y se ha llegado a expandir a 31 países.

Desde el año 2008, Habbo cuenta ya con más de 100 millones de cuentas de usuarios creadas, de las que el 90% pertenecen a jóvenes entre 13 y 18 años.

Al ser una red social que acoge a una gran mayoría de usuarios menores de edad, tiene una amplia guía de cómo hacer un buen uso del servicio y cómo actuar en determinadas situaciones de peligro o que nos hagan sentir incómodos. Veamos los puntos principales.

3.4.7.1 Habbo Hotel – Edad mínima

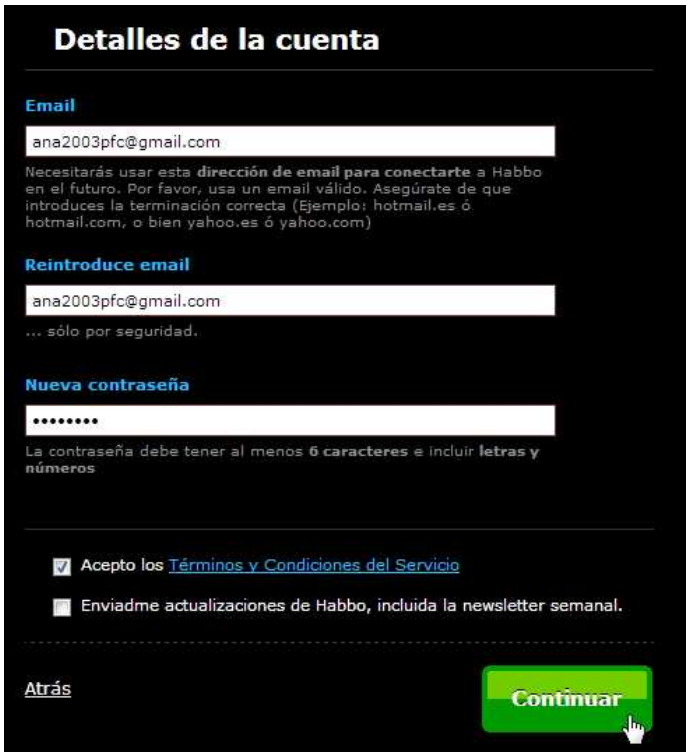
El Sitio Web y los servicios están pensados para mayores de 14 años. Ninguna persona menor de 14 años está autorizada para facilitar datos personales o publicar datos personales dentro del sitio web o de los servicios.

Al igual que para el resto de redes sociales ya comentadas, nos resultará fácil saltarnos esta norma. Veamos cómo Ana, de 9 años, intenta crearse un nuevo perfil de usuario:

Una vez introducida la fecha de nacimiento, el sistema percibe que el usuario es menor de edad y nos muestra el siguiente mensaje:

Hacemos un nuevo intento de registro, indicando esta vez que el usuario nació en el año 1998 y que, por tanto, tiene ya la edad

mínima para utilizar el Servicio. Esta vez no nos pide ninguna otra comprobación y nos damos de alta en el servicio sin problemas:



Ya somos parte de la red social.

3.4.7.2 Habbo Hotel – Consentimiento paterno

Para los jóvenes entre 14 y 18 años que deseen utilizar el servicio hay disponible en la web un formulario en el que los padres o tutores podrán otorgar la autorización pertinente.

Además la empresa Sulake, propietaria de la red social, se reserva el derecho a expulsar a todos aquellos que, teniendo menos de catorce años sean descubiertos por Sulake y no regularicen en setenta y dos horas su situación mediante dicha autorización.

AUTORIZACIÓN DE LOS PADRES O TUTORES LEGALES DEL MENOR QUE DESEA REGISTRARSE COMO USUARIO DE HABBO

1. DATOS DE LOS PADRES O TUTORES:

- Nombre y apellidos:
- D.N.I:
- Dirección:
- Teléfono/s:
- Correo electrónico:

2. DATOS DEL MENOR:

- Nombre y apellidos:
- D.N.I:
- Dirección:
- Teléfono/s:
- Fecha de nacimiento:
- Correo electrónico:

CONSIENTO EXPRESAMENTE la política de privacidad del sitio web www.habbo.es titularidad de SULAKE SPAIN S.L.U con CIF número B-63156319, con domicilio social en, calle C/ Francisco Remiro, 2 Modulo D, Planta 2ª Madrid 28028, disponible en http://www.habbo.es/papers/privacy cuyos principales aspectos se indican a continuación:
"El hecho de acceder al Sitio Web y/o utilizar los Servicios, y/o registrarte en el Sitio Web, significa que has leído, entiendes y aceptas, sin reservas de ninguna clase, esta Política de Privacidad, y CONSIENTES EN QUE RECOJAMOS Y TRATEMOS TUS DATOS PERSONALES Y TU INFORMACIÓN DE ACUERDO CON ESTA POLÍTICA DE PRIVACIDAD Y CON LAS LEYES ESPAÑOLAS, así como aceptas expresamente las medidas de seguridad que hemos implementado para hacer de Habbo Hotel un lugar seguro. Si no aceptas esta Política de Privacidad, no debes utilizar este Sitio Web ni los Servicios ofrecidos.
Sulake recoge determinada información de carácter personal (i) cuando te registras en el Sitio Web (a través del formulario correspondiente) para utilizar los Servicios; (ii) cuando compras Créditos o realizas cualquier pago para acceder a Servicios Adicionales; o (iii) a través de los correos electrónicos que nos envíes para contactar con nosotros.

Tus datos personales recogidos de acuerdo con esta Política de Privacidad serán incorporados a un fichero inscrito ante la Agencia Española de Protección de Datos, titularidad de Sulake Spain, S.L.U., con CIF número B-63156319, con domicilio social en Madrid 28028, calle C/ Francisco Remiro, 2 Modulo D, Planta 2ª Madrid.
De acuerdo con la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y su normativa de desarrollo, por la presente te informamos que tienes derecho a acceder, modificar, cancelar y oponerte a que se incluya tu información personal en nuestros ficheros. Para ejercer dichos derechos, puedes:(a) Acceder, rectificar, modificar o actualizar tus datos personales e información relativa a tu cuenta en el Sitio Web a través de la sección Ajustes dentro de tu cuenta de Usuario Registrado; o (b) Acceder, rectificar, modificar o cancelar tus datos personales poniéndote en contacto con nosotros enviándonos por correo postal a la dirección indicada arriba calle C/ Francisco Remiro, 2 Modulo D, Planta 2ª Madrid 28028"
En …….. a …. de …….. de 20….
Fdo: ……..
(Firma del padre, madre o tutor legal)
Anexo al presente documento debe figurar copia del documento que acredite la identidad de la persona que firma.

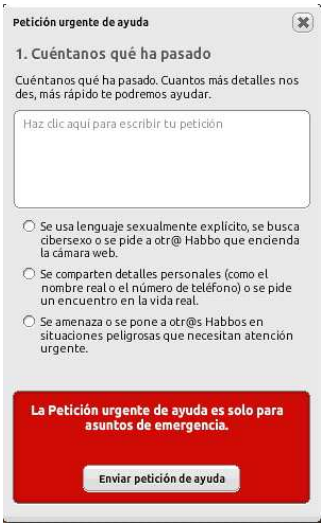
A pesar de que en la presente autorización se recogen los aspectos principales de la Política de Privacidad recomendamos leer el texto completo.

3.4.7.3 Habbo Hotel – Denuncia social

De las redes sociales estudiadas, Habbo probablemente sea la que tiene presente una mayor consciencia sobre los peligros que puede suponer el uso de este tipo de Servicios Web. Debido al público al que va enfocado esta red social en concreto, el Servicio presenta un

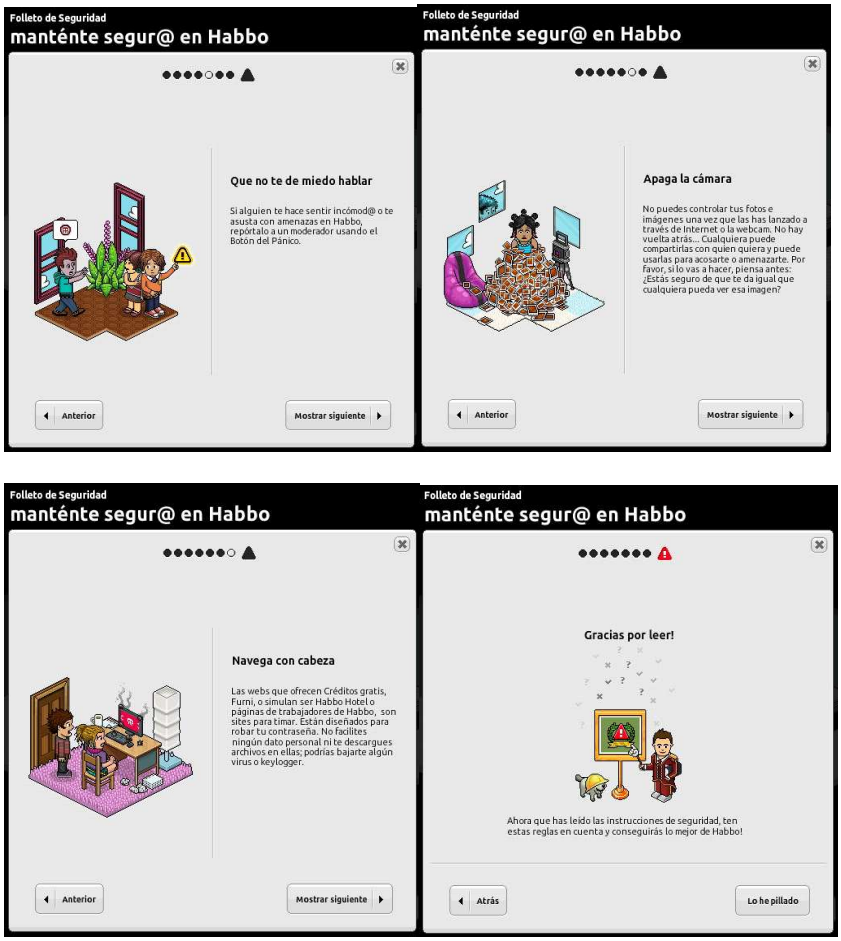
amplio despliegue de información sobre cómo interactuar de forma segura con otros usuarios de la red y asimismo cómo detectar ciertas actitudes inadecuadas que podrían llegar a crear una situación de peligro a el usuario. Es por ello, que el Servicio dispone siempre de forma visible en la pantalla el denominado *Botón del pánico* que invita al usuario a reportar cualquier comportamiento abusivo u ofensivo que pueda percibir en cualquier momento.

Si hacemos click sobre él, nos aparecerá la siguiente pantalla emergente:

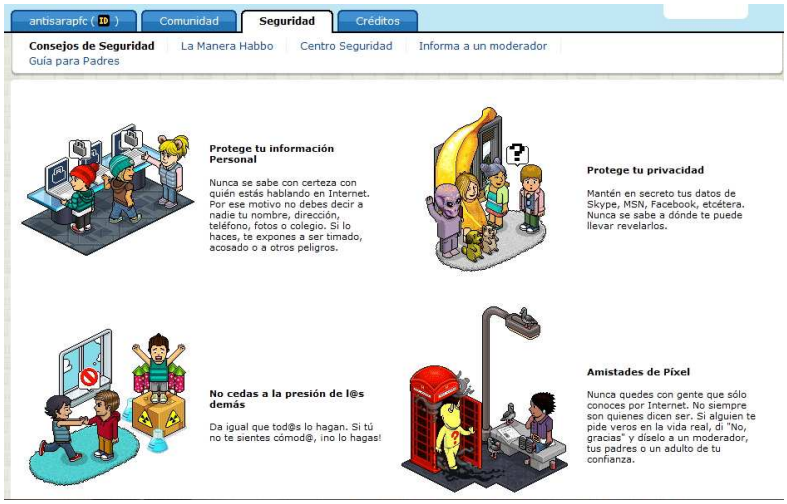


Al darnos de alta en el Servicio, una de las primeras pantallas de bienvenida nos obliga a pasar por un folleto de seguridad:

En él se enumeran de forma muy clara y sencilla algunos consejos sobre cómo hacer un uso seguro del Servicio, tales como no contar nunca las contraseñas de nuestras cuentas, no ceder a la presión de los demás, evitar enchufar la webcam con desconocidos, etc.

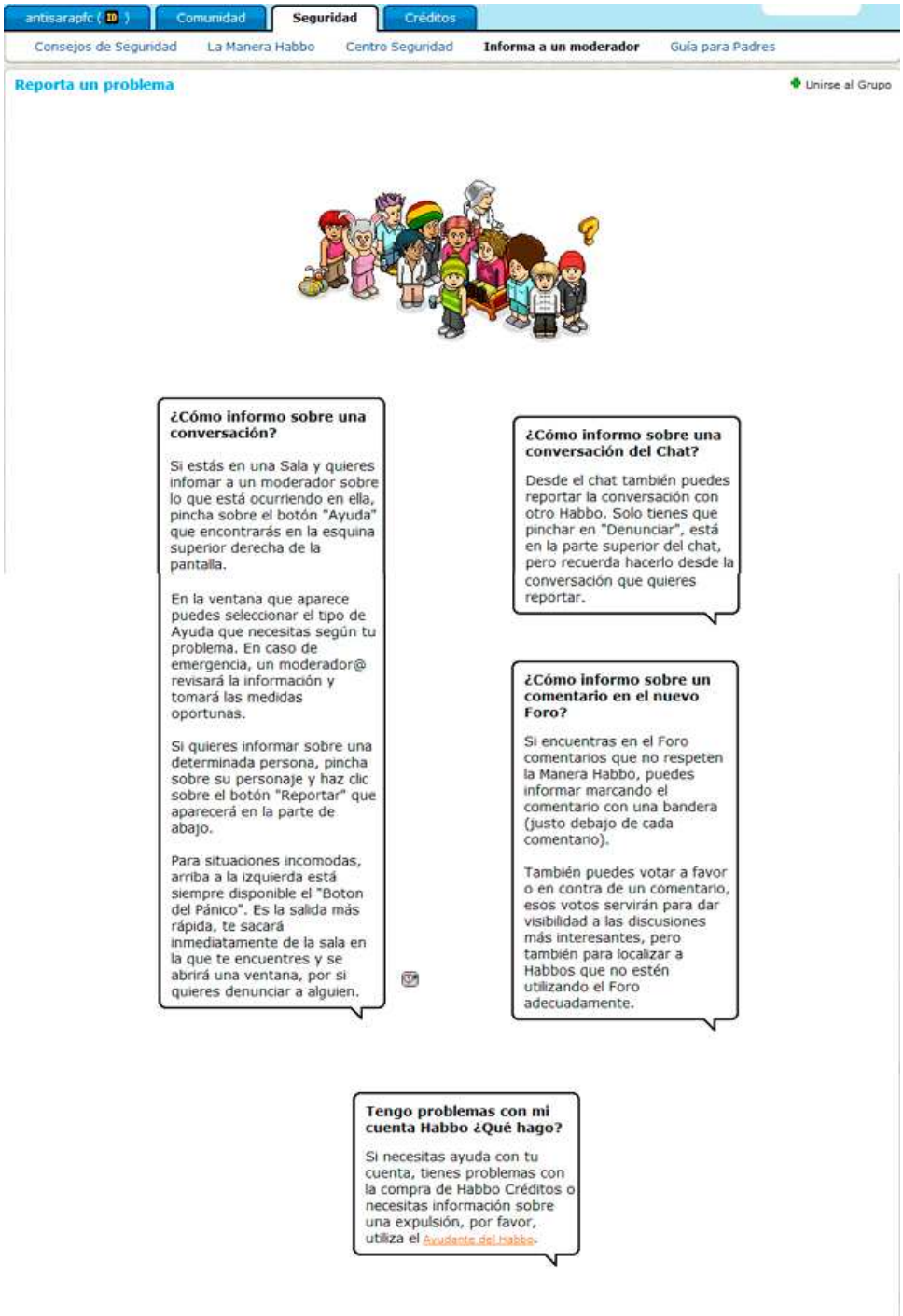


Este folleto se podrá consultar siempre que se quiera accediendo a la pestaña *Seguridad* del portal.



En este subapartado, además, encontraremos información más detallada sobre cómo informar y denunciar ciertos comportamientos o situaciones creadas utilizando el Servicio

(enlace *Informar a un moderador*) así como una amplia guía para padres y tutores:



3.4.7.4 Habbo Hotel – Identificación por IP

Cuando un usuario visita el Sitio Web o utiliza cualquiera de los Servicios del mismo, Sulake recopila automáticamente determinada

información, tales como su dirección IP, navegador utilizado, nombre de usuario, alias del personaje Habbo, horas de visita, páginas visitadas, lista de amigos, registro de transacciones si las hay, etc.

Toda esta información podrá ser retenida durante algún tiempo en caso de recibir algún requerimiento u orden correspondiente de una autoridad competente.

3.4.7.5 Habbo Hotel – Huella digital

Si leemos con detenimiento los TOS del Servicio, encontraremos qué pasa con nuestra información una vez nos damos de baja en el Servicio en el apartado Terminación y suspensión.

En este caso, Sulake cancelará las cuentas, usuarios y contraseñas que aparecían vinculadas al servicio que estamos dando de baja, así como todos los datos personales asociados a las mismas. Igualmente, Sulake se reserva el derecho a mantener en sus servidores nuestro perfil de usuario y contenido por un período razonable de tiempo después de la terminación del contrato en caso que reciban un requerimiento u orden correspondiente de una autoridad competente o en cualquier otro supuesto que exija la ley.

3.4.7.6 Habbo Hotel – Responsabilidad legal

Al igual que ocurre en la mayoría de redes sociales, Sulake no controla ni aprueba el contenido, mensaje, materiales, actividades o información que los usuarios finales del Servicio distribuyan o compartan en el Sitio Web, por lo que la empresa se excluye de toda responsabilidad respecto a cualquier demanda o reclamación relacionada con los mismos con su participación.

De esta forma, la responsabilidad de todo lo que se publique en el sitio web recaerá sobre el mismo usuario que decide compartirla.

3.5 Conclusiones

En general, todas las redes sociales estudiadas y analizadas en la presente memoria presentan unas normas de uso y conducta que el usuario se compromete a cumplir a la hora de utilizar sus servicios.

En todas ellas, la responsabilidad final del uso que hace cada usuario de las mismas así como de todo el material o contenido compartido recae sobre el mismo usuario. Por tanto, debemos ser cautos y pensar bien antes de publicar cualquier contenido de forma que no nos pueda perjudicar de ninguna manera.

Conscientes de los grandes peligros a los que se puede encontrar un usuario a la hora de navegar por la red y, más en concreto, al hacer uso de las redes sociales, casi todas las redes sociales relevantes en la actualidad presentan un apartado de *Seguridad* en el que se indican unas pautas a seguir a la hora de utilizar el Servicio de forma que se haga de la manera más saludable posible. Además, presentan una amplia guía para padres y educadores para que ayuden a los usuarios más vulnerables a concienciarse sobre los distintos peligros a los que se pueden enfrentar y cómo actuar en cada caso.

Finalmente, destacar que aunque cada una de las redes sociales presenta sus propias herramientas para el bloqueo de usuarios y administración de comentarios en caso de situaciones que nos incomoden, será nuestra responsabilidad el acudir directamente a las autoridades locales a la hora de reportar un abuso o comportamiento malintencionado que pensemos vaya más allá de una simple crítica o burla y pueda llegar a provocar una situación de daño o lesión al usuario.

4. Software de Control Parental

4.1 Introducción al Control Parental

Como se viene comentando a lo largo de esta memoria, la gran evolución de la web desde sus inicios hasta tal y como la conocemos hoy en día hace de ella una herramienta cotidiana para niños y adolescentes.

También, cada vez existen más dispositivos de uso diario tales como móviles o tabletas que nos permiten acceder y estar conectados a la red casi de forma permanente.

En los últimos años los menores dedican más y más tiempo a relacionarse y conocer gente nueva a través de las redes sociales, chats o foros de discusión. Además, utilizan la red como herramienta educativa para buscar información para trabajos escolares o simplemente para pasar el rato jugando a juegos online y entretenerse.

Es por todo esto que la probabilidad de que un menor o adolescente se exponga a contenido inadecuado para su edad es cada vez mayor.

Entenderíamos por contenido no apto para una menor de edad todo aquello relacionado con: pornografía, publicidad ofensiva, drogas, violencia, sectas, xenofobia o racismo así como todas aquellas páginas web de apuestas o compras online de las que se precisa de la introducción de números de tarjetas de crédito o datos personales y que resultan un tanto vulnerables para menores de edad que no poseen la madurez ni el criterio necesario para hacer uso de ellas.

A todo esto se le une todos los peligros comentados en otros subapartados de esta misma memoria que incluyen los riesgos a los que se exponen los menores como consecuencia del uso de redes sociales, como serían el ciberacoso, *grooming*, abuso o sobreexposición de información personal.

Como consecuencia de todo esto se crean unas herramientas de control parental que permite a los padres limitar, filtrar y controlar el contenido al que puede acceder el menor al utilizar la red. Además, la gran mayoría también permite limitar la cantidad de tiempo que éstos pasan delante de la pantalla así como bloquear el dispositivo si éstos sobrepasan este tiempo o simplemente enviar una notificación a los padres (por ejemplo, vía correo electrónico) para que éstos tomen las medidas oportunas.

Actualmente existen muchísimos programas y dependerá del grado de control que desee aplicar el padre el elegir uno u otro según se adecue a sus necesidades.

Hay que destacar que el uso de estas herramientas de control no son nunca 100% efectivas y, es por ello, que la solución principal y más importante para que nuestros hijos o menores a nuestro cargo hagan un buen uso de Internet pasa por una buena educación y concienciación sobre la materia. La mejor herramienta de prevención es el diálogo con ellos y haciéndoles ver los riesgos y peligros a los que se exponen. Además, sería conveniente hablarles sobre el uso del software de Control Parental. Como publica Cristina Polo en el artículo *Las mejores aplicaciones de Control Parental*, haciendo referencia en este caso a los adolescentes, "*es muy recomendable optar por una estrategia de supervisión más que de bloqueo, y siempre educar al menor en el uso del PC e Internet, haciéndole ver los riesgos y peligros, e instándole a conocer que el software de control parental está instalado y que es por su propia seguridad*" (Polo, 2013).

Todo este tema del diálogo cobra más importancia en estos adolescentes, pues es una época especialmente delicada en el desarrollo del joven y además puede que no todos los padres de los amigos del menor compartan la misma opinión sobre el uso de Internet y sus limitaciones. Habrá que tener en cuenta también en este caso el grado de control así como la constante monitorización de la actividad de éste, pues puede llegar a suponer una medida extrema que viole la privacidad del menor y que únicamente consiga mermar la confianza depositada en los padres.

4.2 Criterios de clasificación del software de Control Parental

Existe un gran número de opciones de configuración de herramientas de control parental que nos permiten clasificarlas.

Tras una pequeña investigación a través de blogs y artículos de revistas de tecnología (PC Actual: http://www.pcactual.com/), páginas web sobre seguridad de menores en la red (http://www.segu-kids.org/) o las mismas páginas web del producto en cuestión, se pueden definir los siguientes tipos de control parental y sus características:

- **Control de la navegación:** Esta opción nos permite filtrar todas aquellas páginas web cuyo contenido se considera inadecuado para menores de

cierta edad. A continuación mostraremos varios método de filtrado que, como veremos, se pueden combinar entre sí en algunas herramientas para una mayor flexibilidad de configuración:

- **Filtrado por listas blancas/negras**: En la lista blanca incluiremos todas aquellas páginas web a las que el menor tendrá siempre el accedo permitido, aunque ésta esté dentro de alguna de las categorías bloqueadas. Por el contrario en la lista negra añadiremos todos aquellos sitios a los que queramos denegar explícitamente el acceso.

- **Filtrar contenido por categorías**: Muchas herramientas incorporan una clasificación de sitios web por categorías. Se considerarían categorías, por ejemplo, los siguientes ítems: Educación, Redes Sociales, Armas, Apuestas, Drogas, Violencia, Pornografía, Noticias, Ocio, Juegos, etc. De esta forma, permite bloquear, controlar o permitir un conjunto de páginas web atendiendo a sus categorías.

- **Filtrado por *keywords* o palabras clave:** En esta ocasión la aplicación bloqueará aquellos sitios web o búsquedas que contengan cualquiera de las palabras que añadamos a la lista: porno, sexo, drogas, paliza, etc.

  Algunas aplicaciones incluso permiten personalizar el grado de severidad, es decir, la página se considerará como no apta en caso de sobrepasar las coincidencias con la palabra clave en cuestión un mínimo de veces establecido. De esta manera se evitarían los *falsos positivos*.

  Además, todo este filtro es posible gracias al sistema de autoetiquetado de contenidos. De esta forma se indica a las herramientas de filtrado qué sitios bloquear y cuáles no.

  Según la página web http://www.segu-kids.org/, "la tecnología de etiquetado más popular y estandarizada es RDF, una terminología descriptiva por la que los mismos proveedores de contenidos indican mediante etiquetas qué tipo de información está presente o ausente en sus sitios web" (SeguKids, 2008-2012) .

- **Bloqueo de aplicaciones:** En este caso el producto nos permitirá bloquear el acceso a ciertas aplicaciones, como los programas de mensajería instantánea, chat, e-mail, etc.

- **Limitación del tiempo de acceso:** En las herramientas que nos ayudan a controlar el tiempo de acceso, se permite establecer unos horarios en los que el menor podrá estar utilizando la red o directamente utilizando el dispositivo. Suelen ser bastante flexibles, pues generalmente podremos definir el periodo de uso para cada día de la semana. De esta forma podremos dejar a los menores a nuestro cargo utilizar más tiempo el ordenador o tableta el fin de semana y limitar más su utilización los días escolares.

- **Filtro de información saliente:** Estas herramientas permiten controlar la información que sale del ordenador o dispositivo de forma que se pueda impedir la revelación de cierta información personal. Un ejemplo del porqué nos podría resultar útil este tipo de control sería a la hora de evitar que los menores accedan a redes sociales o aplicaciones en las que no cumple con la edad mínima para su registro. De esta manera, en el software de protección el padre indicaría la edad real del menor que se está controlando y la herramienta detectaría la infracción en el caso de que el menor mintiese en su edad a la hora de darse de alta en un servicio.

- **Monitorización:** Quizá sea la práctica más extrema a la hora de controlar la actividad que realiza el menor en la red, pues afecta directamente a la privacidad del mismo y no es preventiva. En la monitorización la herramienta guarda toda actividad que realiza el joven: las páginas web que visita y la hora en la que lo hace, búsquedas que realiza e incluso en algunos casos hasta se monitoriza las redes sociales y mensajería instantánea así como los atajos y comandos de teclado que ejecuta.

  Como hemos comentado, se trata de un sistema de vigilancia extremo que podríamos evitar utilizar tras un buen diálogo con el menor y su pertinente concienciación de los peligros a los que se expone a la hora de utilizar estos servicios.

- **Control de la actividad en redes sociales:** No todas las herramientas lo poseen aunque cada vez existen más productos destinados a ello. Estas herramientas permiten avisar a los padres cada vez que su hijo hace nuevos amigos, comenta en muros, resulta etiqueto en alguna foto, asiste a eventos y todo aquello que se pueda llegar a hacer en la red social en la que está registrado. Con esto se intentan controlar y

solucionar principalmente los problemas de ciberacoso que tanto preocupan hoy en día.

- **Envío automatizado de informes:** Aunque en la gran mayoría de herramientas existe un apartado de informes donde se registra la actividad del menor, algunos presentan la posibilidad de programar el envío de un informe diario o semanal automatizado al correo electrónico de los padres.

- **Tipos de software parental:**

    - **Local:** Se trata de herramientas que deberemos instalar en nuestro equipo desde el que gestionaremos toda la configuración. Por tanto, únicamente podremos cambiar opciones o revisar la actividad del menor ejecutando el software en el lugar en el que lo hemos instalado.

    - **Nube:** Al contrario que ocurre en el software parental local, en este caso únicamente instalaremos la herramienta en los dispositivos que vaya a utilizar el menor y toda la gestión de la misma se realizará desde la web del desarrollador o el producto. De esta manera, podremos ajustar y controlar la actividad del menor desde cualquier equipo o dispositivo con acceso a Internet. Este tipo de software es el más utilizado en los productos de última generación.

- **Filtrado y control sobre otros dispositivos móviles:** Debido al gran auge de los smartphones y tabletas, actualmente las herramientas más conocidas presentan también versión para estos dispositivos. Por lo general suelen aportar opciones de configuración más reducidas aunque en ellas no echaremos de menos las más básicas como el filtrado de contenido inadecuado.

Tras la clasificación que acabamos de presentar, cabría mencionar que los menores de avanzada edad con los conocimientos necesarios podrían llegar a saltarse todo el tipo de control y de filtros. Una forma sería, por ejemplo:

- Utilizar **distribución Linux** de tipo **Live CD**: Con esto, el menor podría arrancar este sistema operativo únicamente insertando el USB o CD/DVD correspondiente sin necesidad de instalar nada y pasando a tener acceso completo a la red sin control o límite alguno.

Para evitar estos casos, deberemos seguir los siguientes pasos:

- Acceder a la *BIOS* del PC

- Definir el disco duro como única unidad de arranque posible
- Añadir una contraseña.

De esta forma, el menor ya no podrá deshacer estos cambios ni utilizar esta alternativa.

OTROS

Tras ver la clasificación más importante sobre las opciones de configuración que presentan las herramientas más relevantes, veremos otros tipos de controles más simples aunque con opciones son mucho más limitadas.

- **Navegadores y buscadores infantiles:** Se trata de herramientas que únicamente permiten el acceso a páginas adecuada para niños y jóvenes adolescentes. Algunas incluso permiten definir el perfil del menor, de forma que se presentará el diseño y las características apropiadas según la edad del joven.

  El lado positivo es que muchos de ellos son simplemente ejecutables que no precisan de ninguna instalación.

  Sin embargo, bastaría tener unos conocimientos básicos para instalar cualquier otro navegador y saltarnos de esta forma todo el filtrado de contenido que nos proporcionan estas herramientas. Por tanto, probablemente estos navegadores únicamente tengan sentido en niños con una edad poco avanzada.

- **Filtrado desde los DNS:** Este procedimiento consiste únicamente en modificar los servidores DNS que sirve el router al asignar las IPs por DHCP. De esta manera quedarían protegidos todos los dispositivos de casa contra conexiones no deseadas y a nivel de red. Existen algunas herramientas que utilizando este método bloquean todos aquellos sitios fraudulentos, filtran la conexión por categorías y controlan el tiempo de uso de Internet.

  Al igual que ocurre con los navegadores infantiles, bastaría tener unos conocimientos apropiados para modificar manualmente los DNS y saltarnos así esta protección. La única manera de evitar esta situación pasaría por contar con un router con cortafuegos integrado en el que deberemos bloquear el puerto que usa el protocolo DNS (TPC 53) además de los cambios comentados en el párrafo anterior.

4.3 Probando el Software

Tras el análisis que acabamos de hacer en el subapartado anterior sobre los diferentes tipos de configuraciones que podemos encontrar en las mejores herramientas de control parental, vamos a presentar un inventario sobre alguna de las aplicaciones que podemos encontrar hoy en día y sus características.

Como veremos, algunas de ellas son completamente gratuitas. Para utilizar algunas más completas, sin embargo, deberemos pagar una cuota anual, aunque éstas generalmente suelen presentar una versión gratuita un poco más limitada. Finalmente, también encontraremos algunas herramientas totalmente de pago sin opción a descarga de prueba.

Para ver cómo funcionan, seleccionaremos las 4 herramientas gratuitas más relevantes y analizaremos su funcionamiento así como sus limitaciones.

4.3.1 Windows 7 + Windows Live Protección Infantil

Windows es actualmente, con diferencia, el sistema operativo más utilizado en el mundo.

OS Platform Statistics

2013	Win8	Win7	Vista	NT*	WinXP	Linux	Mac	Mobile
May	7.9%	56.4%	2.1%	0.4%	15.7%	4.9%	9.7%	2.6%
April	7.3%	56.4%	2.2%	0.4%	16.4%	4.8%	9.7%	2.2%
March	6.7%	55.9%	2.4%	0.4%	17.6%	4.7%	9.5%	2.3%
February	5.7%	55.3%	2.4%	0.4%	19.1%	4.8%	9.6%	2.2%
January	4.8%	55.3%	2.6%	0.5%	19.9%	4.8%	9.3%	2.2%

http://www.w3schools.com – Estadísticas de plataforma de Sistema Operativo

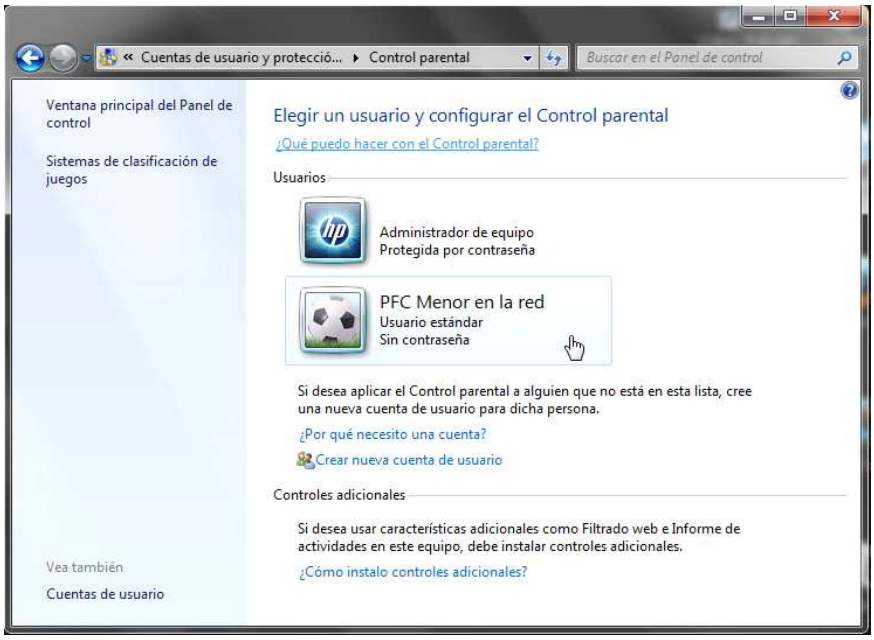
Por tanto, si somos usuarios del mismo podremos encontrar en nuestro propio PC una forma de controlar a los más pequeños de la casa de forma sencilla y gratuita.

Para empezar, si el menor no tiene su propio equipo y va a utilizar el mismo que nosotros, lo más apropiado sería crearle su propia cuenta de usuario. De esta manera, el administrador podrá controlar todos aquellos programas o aplicaciones al que el joven tendrá el acceso permitido o denegado, según nos parezcan apropiados para su edad.

Para ello accederemos a la sección de *Cuentas de Usuario y Protección Infantil* del *Panel de Control*.

Una vez dentro del configurador, seleccionaremos la opción *Agregar o quitar cuentas de usuario* para tener así acceso a la opción que finalmente nos dejará *Crear una nueva cuenta*. Así pues, definimos el nuevo perfil de usuario (no Administrador, pues de esta manera tendría los permisos suficientes para deshacer todos cambios que consideremos convenientes para su seguridad) y le asignamos un nombre.

Finalmente, relacionaremos el nuevo usuario creado con la opción Configurar Control Parental:



Con esta configuración que nos brinda el propio Sistema Operativo podremos controlar el tiempo que el menor utiliza el ordenador y los juegos o aplicaciones que el niño podrá utilizar. Sin embargo, por defecto no podremos revisar el contenido que consulta en Internet ni el uso que hace de él.

Para ello, Windows dispone de una herramienta adicional llamada ***Windows Live Protección Infantil*** que podremos descargar de Internet de manera gratuita en la página web del proveedor: http://www.microsoft.com/spain/windowslive/familysafety.aspx.

Para poder utilizarlo, únicamente necesitaremos iniciar sesión con nuestra cuenta Microsoft (que podremos crear de forma gratuita si aún no estamos registrados).

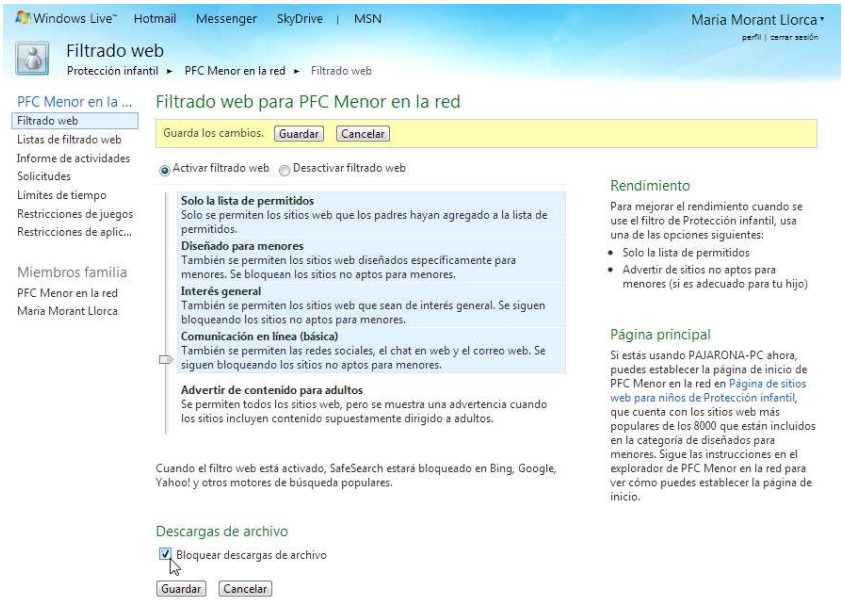
Tras esto, seleccionaremos la cuenta o cuentas de usuario del equipo sobre las que queremos aplicar el control parental y en *Configuraciones adicionales* seleccionaremos el nuevo proveedor de control que acabamos de descargar:

Tras esto, solo nos quedará ir al sitio web de *Windows Live Protección Infantil* (al seleccionar el usuario correspondiente al menor con el control activado nos redirigirá automáticamente a través del navegador establecido por defecto) y configurar las diferentes opciones que nos presenta según nuestras necesidades.

Como vemos en el menú de la izquierda, las opciones principales que se permiten son las siguientes:

- **Filtrado web**: En este subapartado nos permitirá definir el conjunto de páginas web que podrá visitar el menor: únicamente la lista definida por

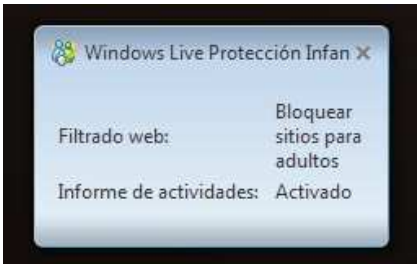
los padres, permitirles también el acceso a aquellos sitios web diseñados específicamente para menores, etc.



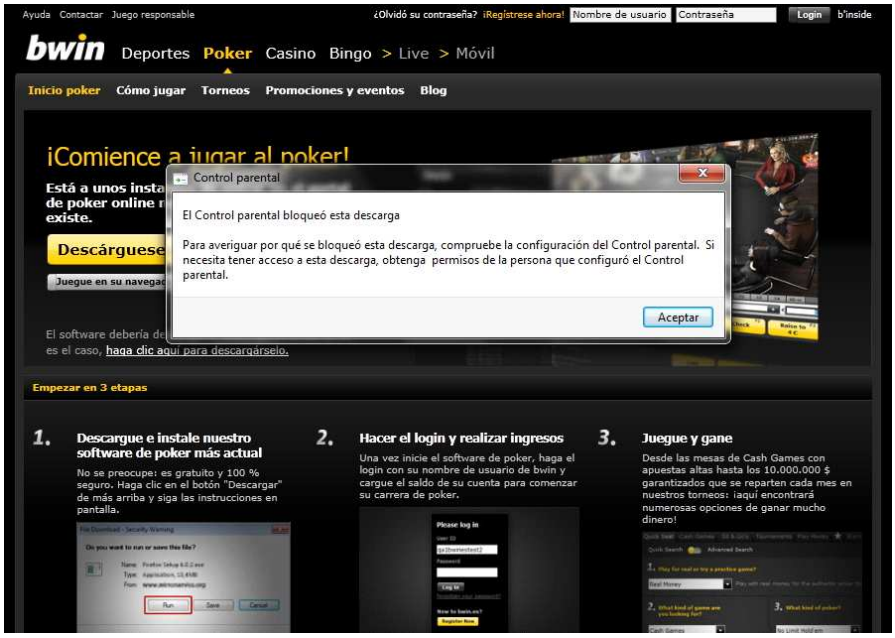
Además, como se observa en la captura hemos seleccionado la opción *Bloquear descargas de archivos*. De esta manera podremos impedir acciones peligrosas que no habíamos considerado de primeras.

Por ejemplo, el menor en cuestión inicia sesión con su usuario y se dirige a navegar por Internet.

Al entrar con su cuenta automáticamente se le anuncia que el sistema de protección infantil está activado:

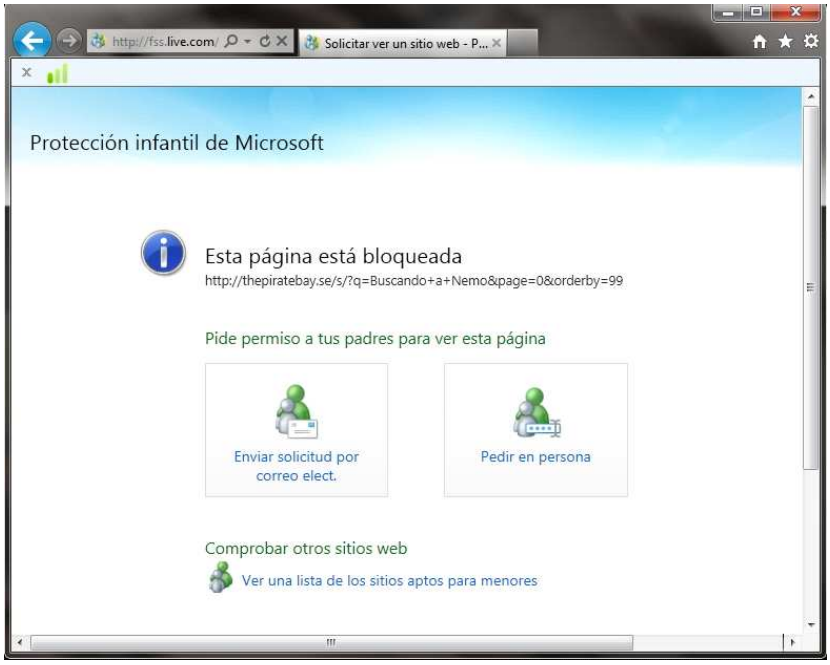


Una vez seleccionado el navegador el menor accede a un sitio online de apuestas que en principio no tiene bloqueado. Al menor le llama la atención la pestaña de partidas de Póker de las que tanto hablan sus primos mayores y decide probar fortuna. Al intentar obtener el programa para poder jugar, automáticamente le aparecerá un mensaje del control parental impidiéndole la descarga:



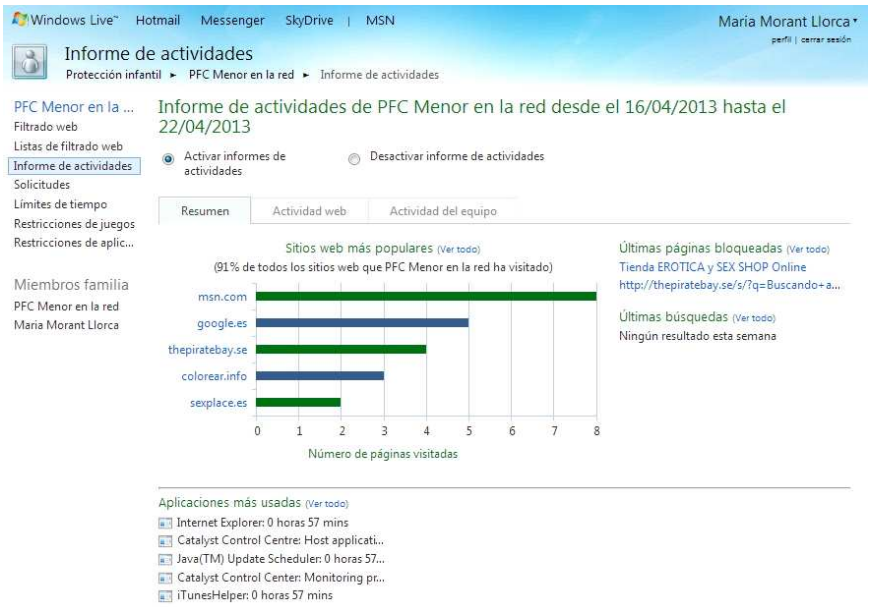
- **Listas de filtrado web:** Este apartado nos permite crear una lista blanca y otra negra sobre los sitos web que deseemos dar o privar explícitamente el acceso al menor:

Si por ejemplo el menor intentase acceder a cualquiera de los sitios bloqueados, automáticamente le saltaría la siguiente pantalla:



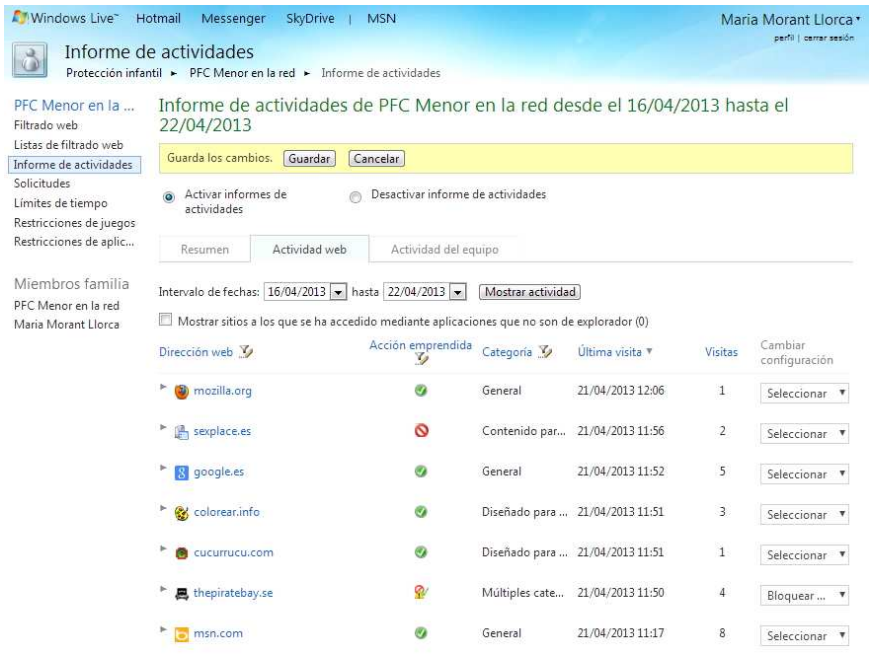
De esta forma, se le permitirá al menor enviar un aviso al padre para pedirle permiso para acceder a la página en cuestión. Éste lo recibirá en su correo electrónico y además podrá ver la petición en la sección *Solicitudes* de la que hablaremos más adelante.

- **Informe de actividades:** En esta sección obtendremos un resumen de la actividad del menor tanto en la web como en el propio equipo. Además, en la parte de la derecha nos detallará las páginas bloqueadas a las que ha intentado acceder el menor.



Además tendremos disponible la opción de recibir el mismo resumen de actividades en nuestro correo electrónico, de forma que nos evite tener que estar entrando constantemente al sitio web:

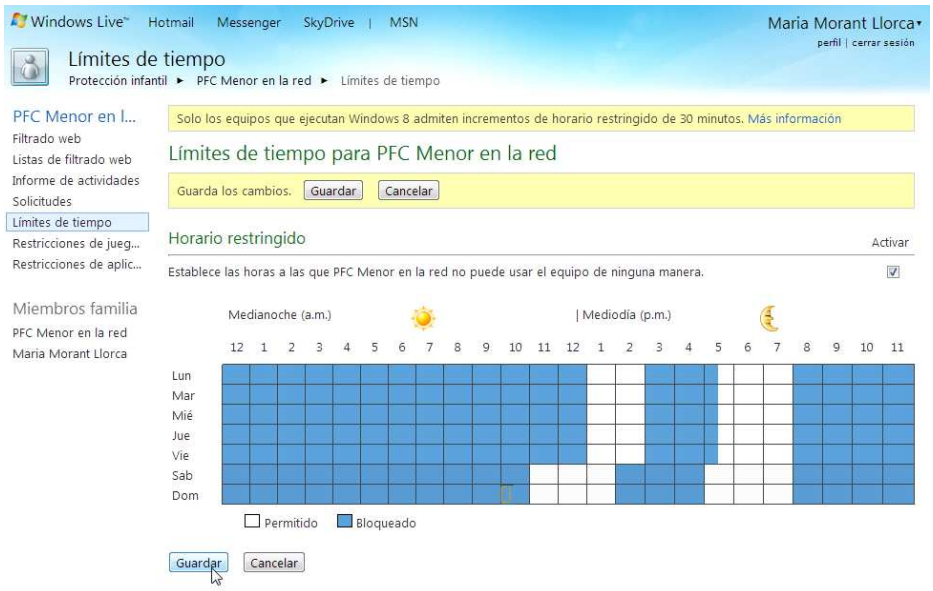
Además, podremos obtener información más detallada sobre la actividad del joven en las pestañas de Actividad web y Actividad del equipo:



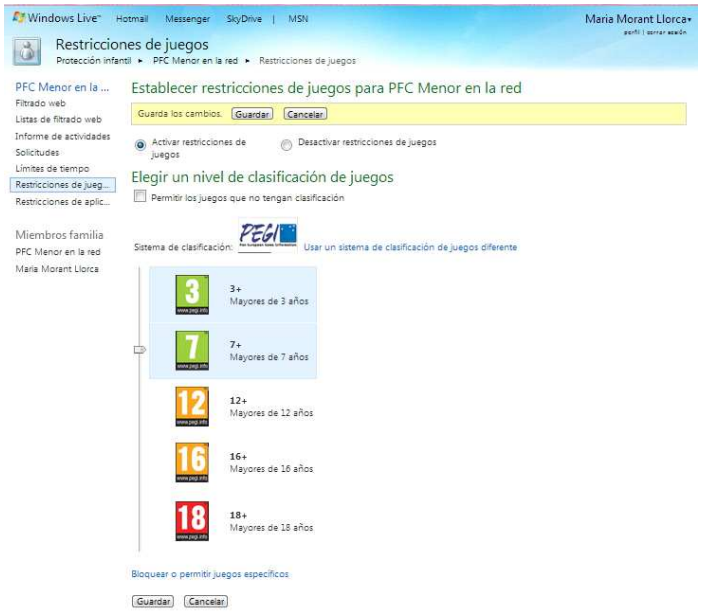
- **Solicitudes:** Como hemos comentado, aquí irán a parar todas las solicitudes que envía el menor para hacer saber a los padres que desea tener acceso a una página que tiene bloqueada.

Como vemos, en el combo de la derecha se nos permitirá seleccionar la opción más adecuada para cada una de las solicitudes.

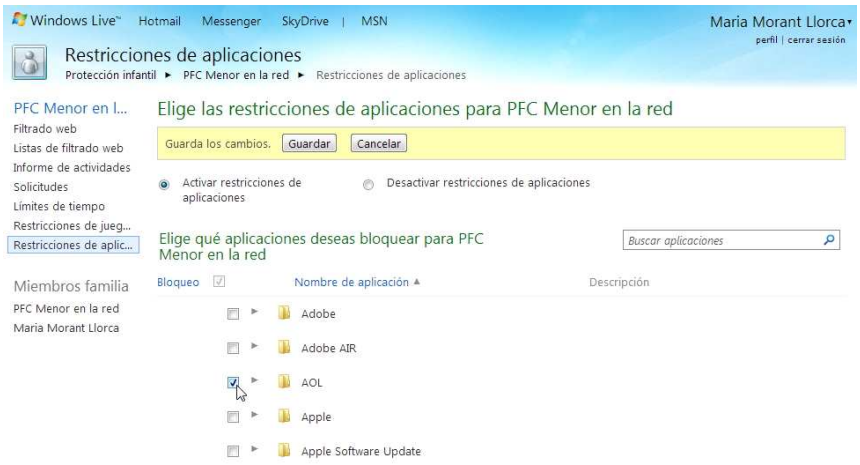
- **Límites de tiempo:** En este apartado podremos definir el horario en el que el menor tendrá permitido la utilización del equipo. Éstos se definen en intervalos de media hora:



- **Restricciones de juegos:** En esta sección podremos restringir el acceso a juegos no recomendados para el menor según su edad y el sistema de clasificación por edades PEGI.



- **Restricciones de aplicaciones:** Finalmente en esta última sección podremos otorgar o denegar el permiso pertinente al menor para la utilización de las aplicaciones instaladas en el ordenador. Tendremos disponible un buscador para filtrar y acceder directamente a las aplicaciones que queramos bloquear.



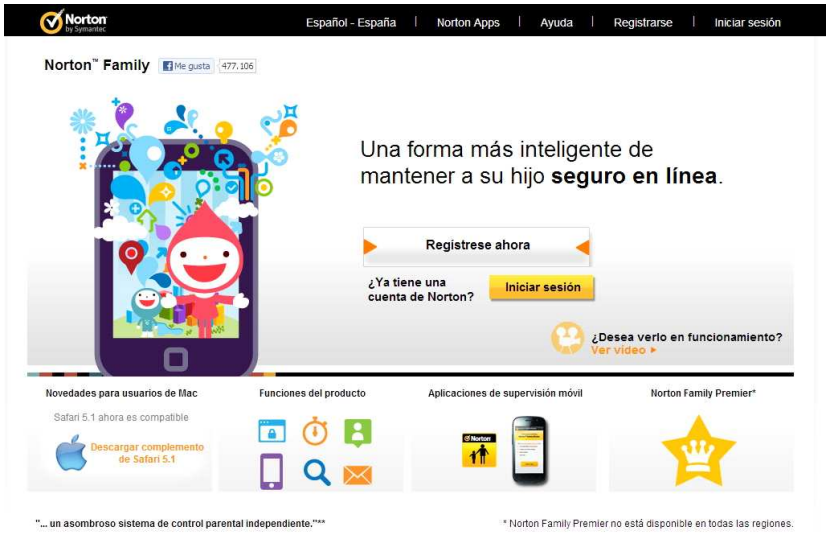
En conclusión, se trata de un sistema de protección bastante completo y sencillo y que además nos podemos descargar de forma gratuita.

Existen otros programas más flexibles a la hora de configurarlo y con distintos métodos de clasificación de contenidos, como la clasificación por palabras clave o categorías que podremos seleccionar nosotros mismos. Sin embargo, esta herramienta nos ofrece cierta comodidad, puesto que la parte básica de configuración nos viene por defecto instalada en el propio sistema operativo y únicamente nos faltará descargarnos el complemento.

4.3.2 Norton Online Family

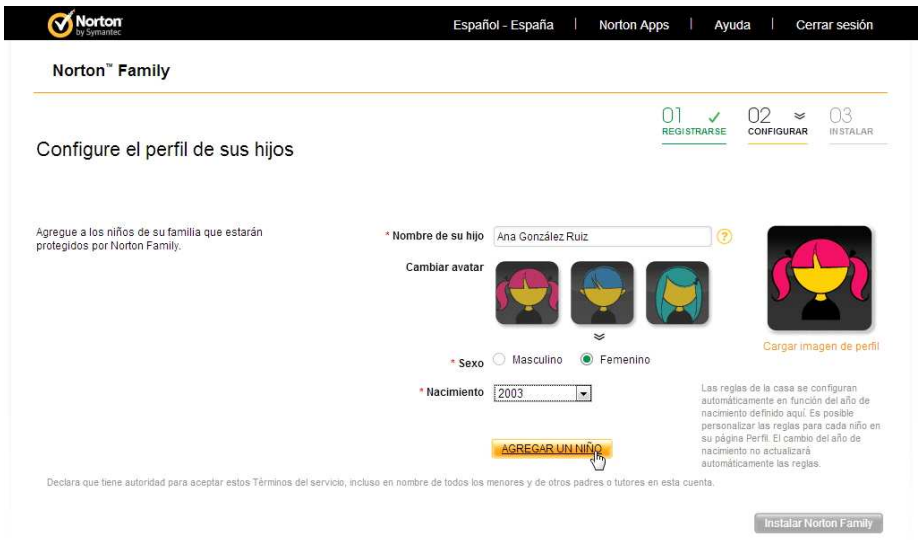
Una de las características más importantes de esta herramienta consiste en ser uno de los primeros programas de control parental que se apoyó en el sistema de la *Nube* para el control y administración de cada uno de los equipos de casa.

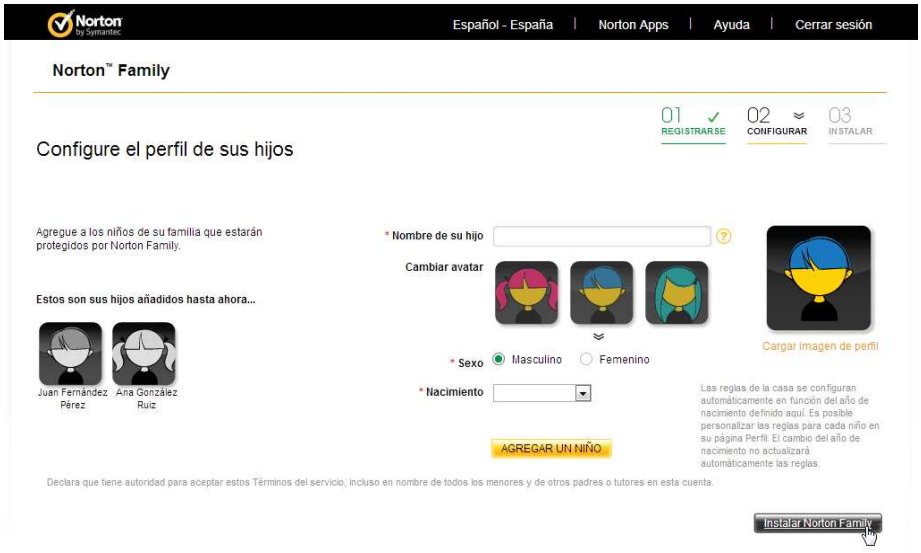
Se trata de una herramienta de pago, aunque presume de una versión gratuita bastante completa que podremos obtener entrando en el sitio web https://**onlinefamily.norton**.com.



Para empezar seleccionaremos la opción *Regístrese ahora*. Las primeras alternativas que nos ofrecerá será el obtener la versión completa que precisa de una cuota o por el contrario obtener una versión gratuita con opciones más limitadas.

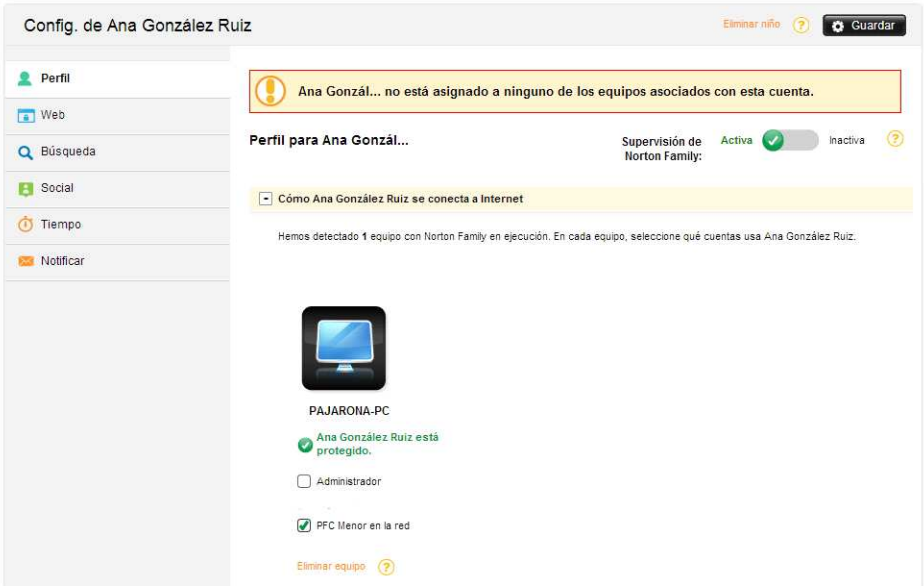
En este caso seleccionaremos la versión gratuita y pasaremos a la configuración de usuarios. En la primera pantalla editaremos nuestro perfil y a continuación haremos lo mismo con cada uno de los menores sobre los que queramos aplicar el control parental, de forma que podremos personalizar las limitaciones y grado de control para cada uno de ellos:





Por tratarse de una herramienta que se sirve del sistema de Nube para su administración, únicamente hará falta instalar el software en los equipos que vayan a utilizar los menores. Además, esta herramienta presenta versión para dispositivos Android.

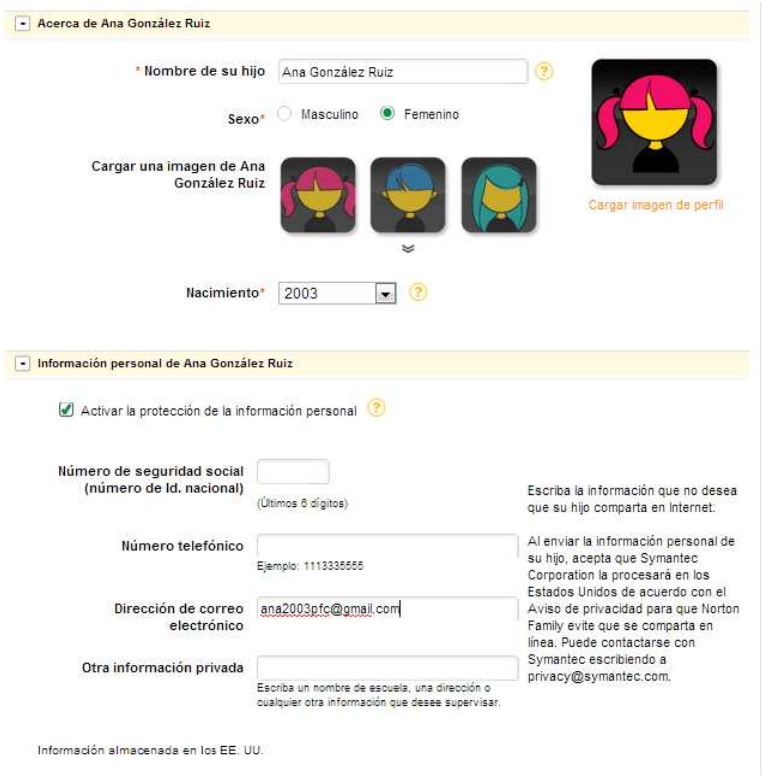
Finalmente instalaremos el producto y únicamente nos quedará configurar las diferentes opciones de filtrado para cada uno de los niños que hayamos dado de alta. Recordemos que podremos conectarnos al administrador desde cualquier dispositivo con acceso a Internet.



Veamos las opciones de configuración que nos presenta esta herramienta:

- **Perfil**: En este primer apartado definiremos el perfil de cada uno de los usuarios y les asignaremos las cuentas del equipo que puede utilizar y a las que se aplicará el control.

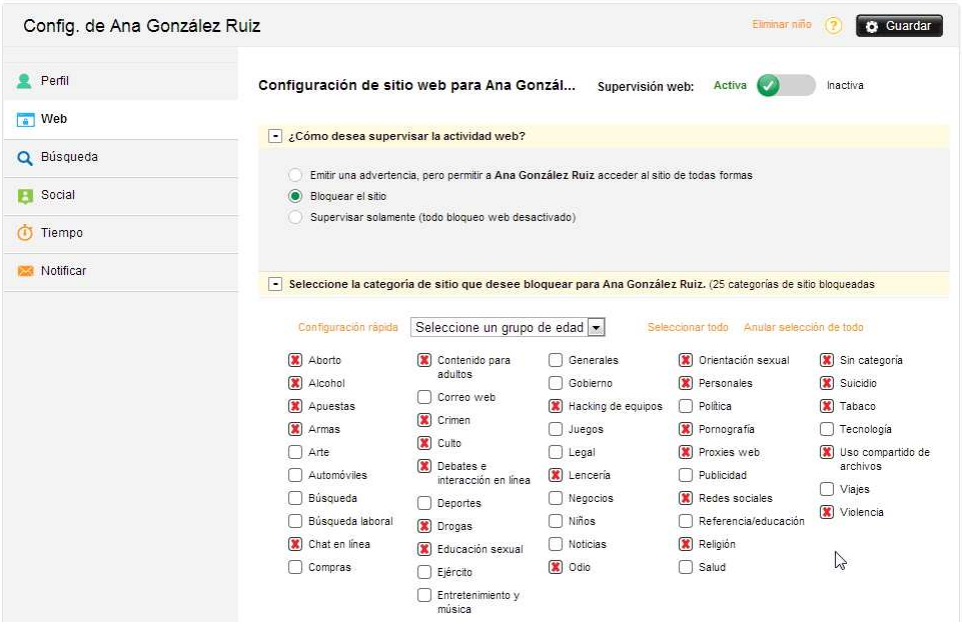
Para ello primer seleccionaremos el usuario en cuestión y a continuación editaremos su información principal:



En la parte inferior de la pantalla, nos permitirá editar información personal del menor que deseemos supervisar. De esta forma podremos controlar qué información comparte el menor en la red.

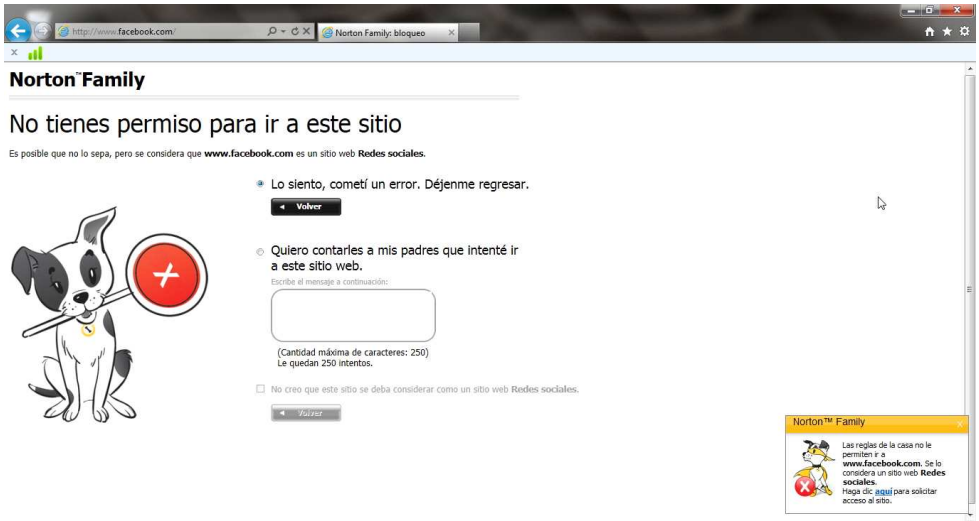
- **Web**: En esta sección configuraremos el conjunto de páginas web a las que el joven tendrá acceso. Para ello, utilizaremos un sistema de clasificación por categorías y una lista blanca y negra de sitios específicos a los que el menor tendrá acceso permitido o denegado.

  Además, podremos seleccionar el grado de severidad del control. Podremos escoger entre: avisar al usuario de que el sitio al que intenta acceder no es apropiado para él pero dejarlo entrar de todas maneras, bloquearle completamente el acceso o desactivar el bloqueo pero supervisar las visitas:



Como vemos en la captura, por defecto nos aparecerán unas categorías marcadas como *inadecuadas* para menores según el rango de edad que seleccionemos en el combo de la parte superior. Sin embargo, podremos marcar o desmarcar todas aquellas categorías que consideremos oportunas.

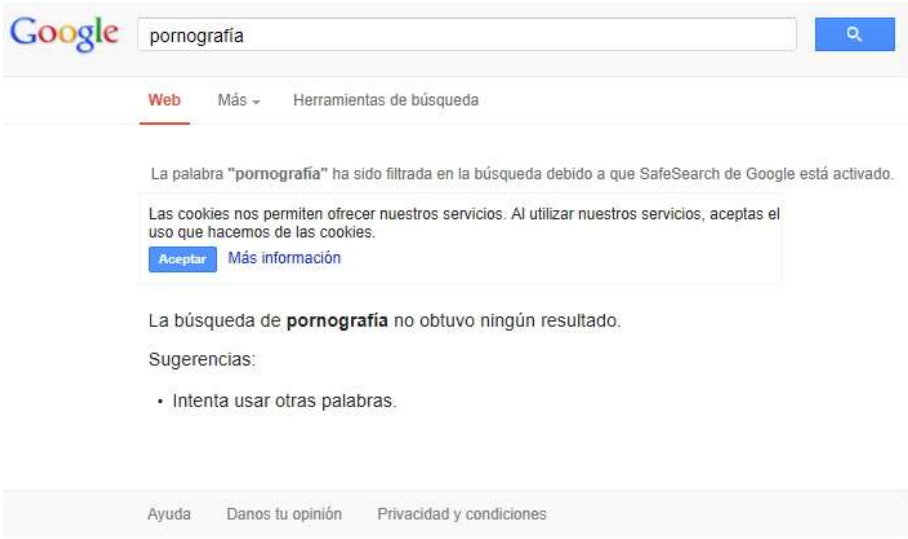
Si por ejemplo el menor intentase entrar en el sitio web de una red social, cuya categoría tiene bloqueada, el navegador le redirigirá a la siguiente pantalla:



En la parte inferior de esta sección definiremos las listas blancas y negras de los sitios que el menor tendrá el acceso explícitamente permitido o denegado independientemente de la categoría a la que pertenezcan:

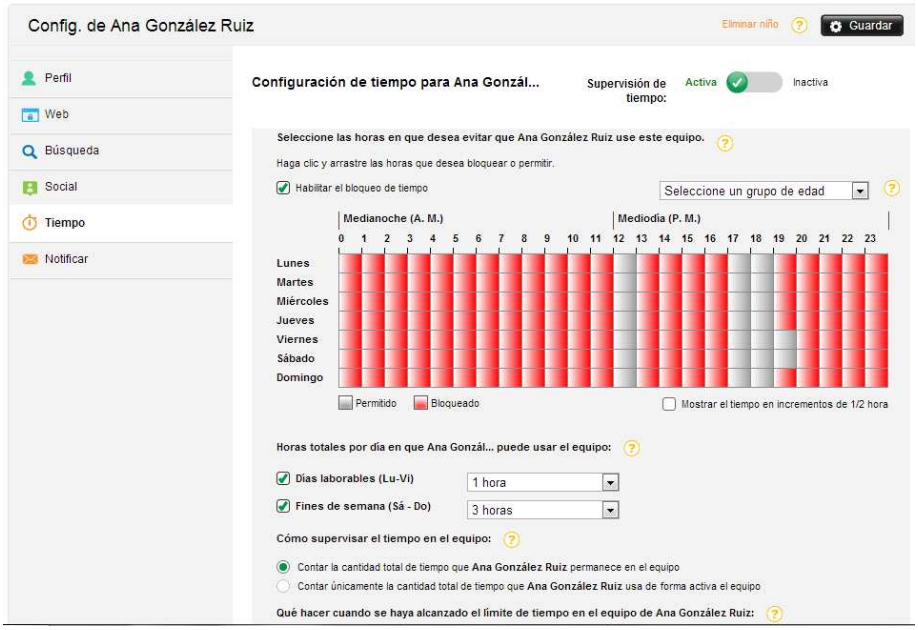
- **Búsqueda**: En este apartado únicamente nos dejará seleccionar la opción que activa el filtrado de contenido para adultos incluido en algunos motores de búsqueda:

Por tanto, si el menor intenta acceder a contenido poco apropiado para su edad, el buscador no le mostrará ningún resultado:



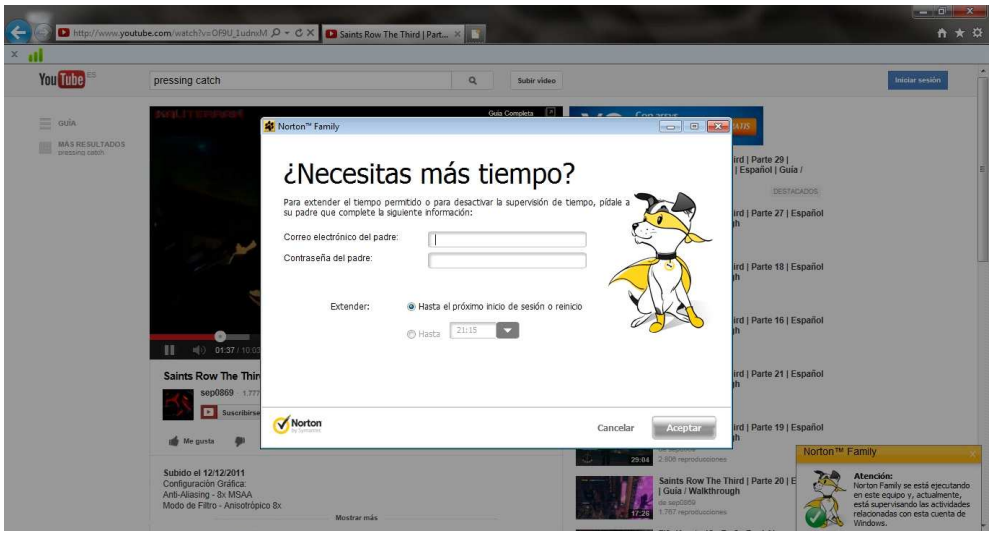
- **Social**: Se listan todas las redes sociales a las que pertenece el menor así como su información básica del perfil: nombre, edad y avatar o fotografía de perfil. De esta forma, podremos controlar qué hacen los menores en la red y podremos asesorarlo a la hora de tomar algunas decisiones.

- **Tiempo**: En esta sección podremos definir el rango de horas en las que el menor tendrá acceso a su cuenta de usuario:



Además, podremos definir el máximo de horas al día que el menor podrá pasar delante de la pantalla. Permite distinguir entre días laborables y fin de semana.

Si el menor sobrepasa el límite permitido, automáticamente le saltará el siguiente mensaje en la pantalla:



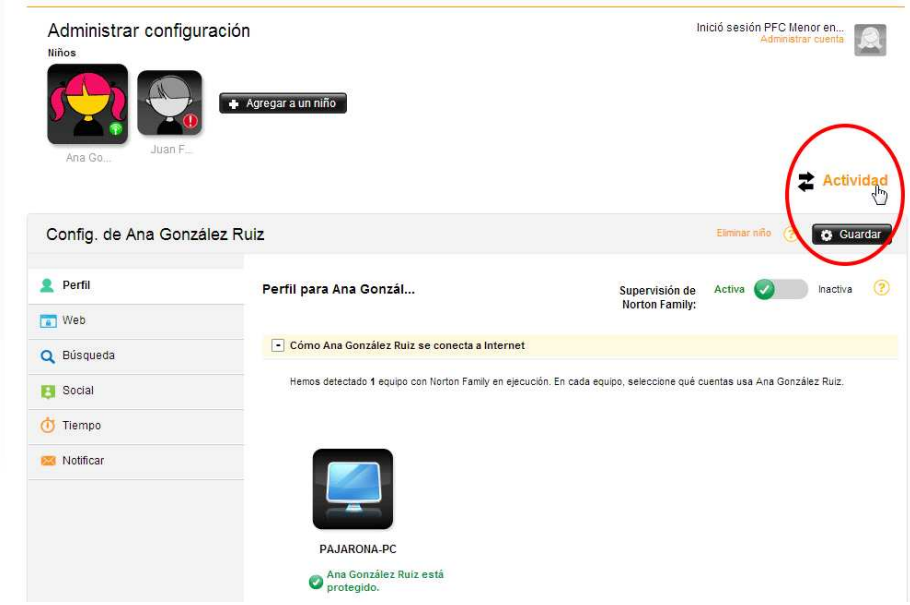
De esta manera, recaerá en manos del padre el decidir si le concede más tiempo para navegar o utilizar el equipo.

- **Notificar**: Permite seleccionar los casos en los que queremos que se nos envíe un aviso al correo electrónico. Por ejemplo, cuando el menor ignora una advertencia, visita un sitio bloqueado o se da de alta en alguna red social:

Si por ejemplo nuestro usuario accediese a una página web de una categoría que tiene específicamente bloqueada, como el de una red social, automáticamente recibiremos en la dirección de correo electrónico especificada un e-mail como el siguiente:

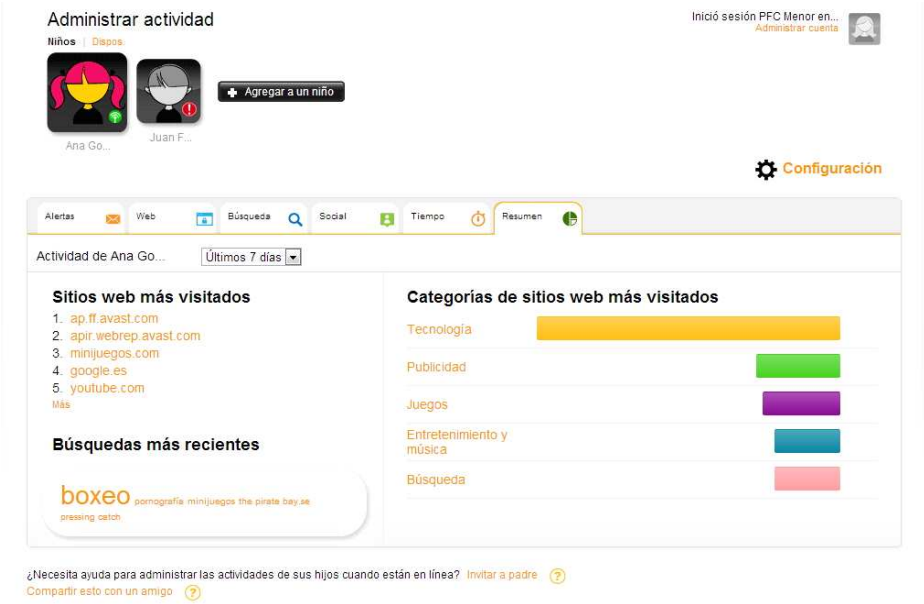
Ya tenemos definidas las reglas de navegación para cada uno de los menores de la casa.

Únicamente nos quedará revisar la actividad de los mismos en la pestaña correspondiente del administrador:



En esta sección volveremos a tener las mismas pestañas que nos aparecían en la parte de la derecha de la configuración de reglas de navegación. En este caso, al entrar en cada una de ellas nos aparecerá información detallada de la actividad del menor en la red. Esto es, sitios visitados, búsquedas realizas, alertas emitidas, etc.

En la última pestaña tendremos una visión genera más resumida de dicha actividad:



Por lo que hemos visto, la herramienta presenta una gran variedad de alternativas de configuración y flexibilidad a la hora de establecer unas normas de navegación para los más pequeños de la casa.

Al igual que ocurre con el resto de herramientas de control parental más importantes, éstas tienen unas opciones más discretas que la versión completa de pago, aunque la elección de una versión u otra dependerá del grado de control que queramos ejercer sobre los menores a nuestro cargo. Cabe recordar que ante todo se precisa de una buena educación y diálogo con los jóvenes para concienciarlos de los problemas y riesgos a los que se enfrentan por hacer un uso indebido de la red.

En este caso, la versión *Premium* permite, además de todo lo comentado en la versión gratuita:

- En *Smartphones* permite controlar los mensajes de texto y aplicaciones instaladas, además de la supervisión y el filtro web que también ofrece la versión gratuita.
- Supervisión de vídeos vistos.
- Resumen detallado del tiempo de actividad del menor en el equipo.
- Informes semanales o mensuales por correo electrónico.

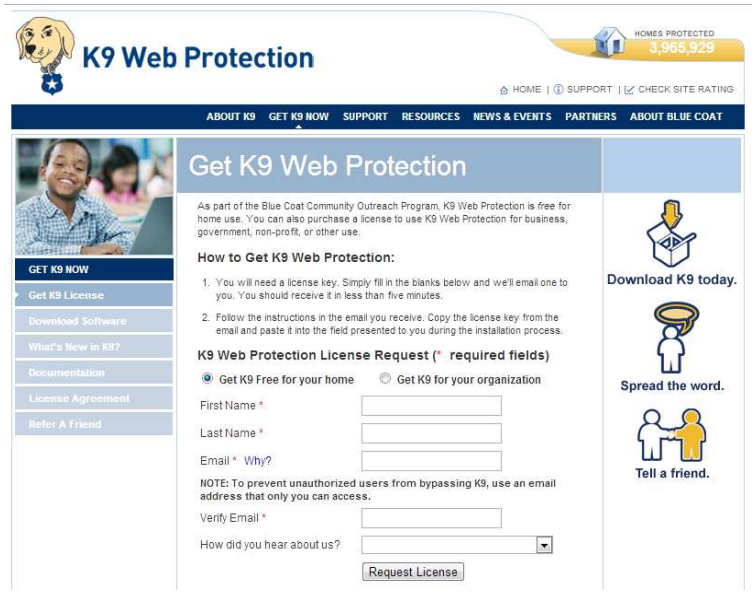
- Elaboración de informes detallada y consolidada.
- Historial extendido de actividad hasta 90 días.

4.3.3 K9 Web Protection

Probablemente estemos ante la herramienta de control parental gratuita más completa que podremos encontrar en la red, aunque a día de hoy únicamente está disponible en inglés.

Además, también tiene su versión para varios tipos de dispositivos, ya sea un ordenador, un Smartphone o una tableta.

Para conseguirlo, entraremos en la web del producto y rellenaremos el formulario pertinente para pedir nuestra licencia gratuita:



De esta manera, recibiremos en nuestro correo electrónico el código de instalación y las instrucciones a seguir para instalar el producto en nuestro equipo.

Así pues instalaremos la herramienta y proporcionaremos una contraseña de administrador para que el resto de usuarios que vayan a utilizar el equipo no puedan cambiar las normas de navegación que pretendemos establecer.

Una vez instalado, ejecutaremos el programa *Blue Coat K9 Web Protection Admin* desde el menú *Inicio* y automáticamente se abrirá el administrador del programa en nuestro navegador web predeterminado.

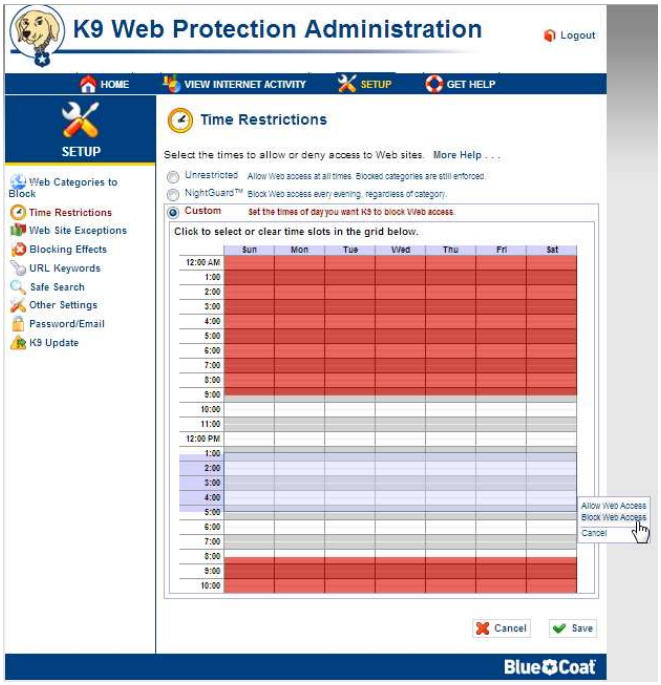
Tras insertar la contraseña, podremos empezar a configurar la herramienta según consideremos oportuno. Para ello, disponemos de las siguientes opciones:

- **Web categories to block:** Este primer apartado nos presenta un grupo de categorías en las que se clasificarían los sitios web y podremos decidir a cuáles el menor tendrá el acceso permitido o denegado.

  Por defecto la herramienta ya nos plantea algunas categorías bloqueadas dependiendo del grado de protección que queramos aplicar. Por ejemplo, seleccionando el nivel alto de protección (High) pasaríamos a bloquear todo contenido inadecuado, así como el acceso a redes sociales o a cualquier sitio web sin clasificación. De igual forma existen otros niveles de protección más moderados o incluso mínimos.

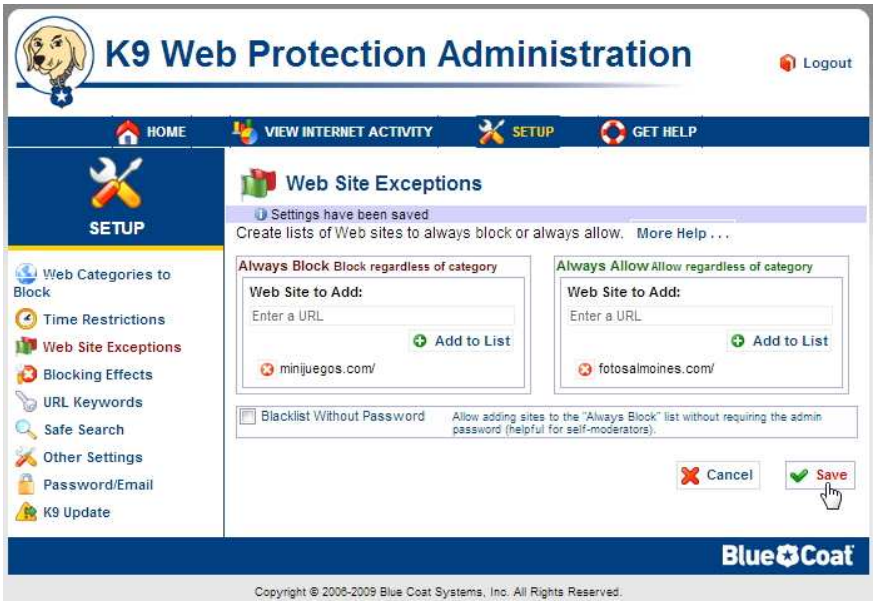
  Además, nos brinda la oportunidad de ser nosotros mismos quienes decidamos qué categorías podremos bloquear en la opción *Custom*.

- **Time restrictions:** Esta herramienta también nos permite establecer los límites de tiempo en los que el usuario tendrá acceso a la red.



Como vemos, podremos definir los intervalos en los que el menor podrá estar en Internet dependiendo del día de la semana y en periodos de media hora, a diferencia de otros software de control parental que divide estos intervalos en horas completas.

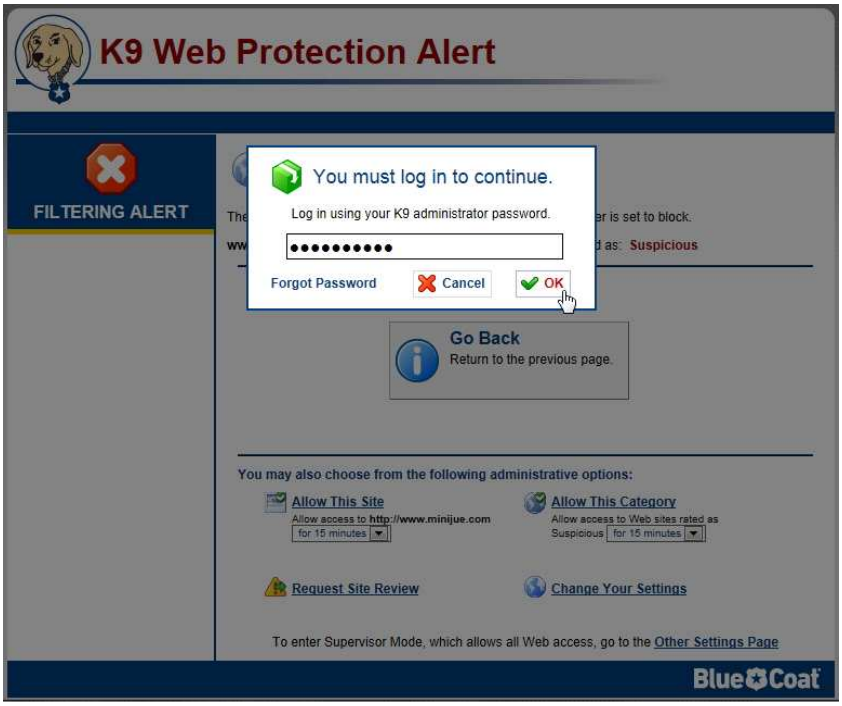
- **Web site exceptions:** En este apartado nos permitirá establecer las excepciones de aquellos sitios web en los que el menor tendrá el acceso permitido o denegado explícitamente independientemente de la categoría a la que pertenezcan. Esto se definirá a través de la creación de una lista blanca y otra negra:



- **Blocking effects:** En esta sección de la herramienta de configuración podremos establecer los efectos que se producirán al intentar acceder a un sitio al que el menor tenga el acceso denegado.

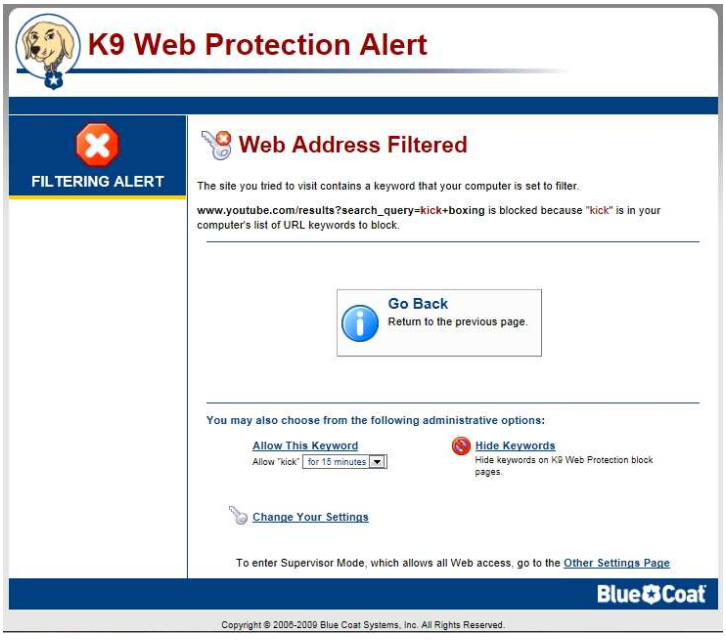
Entre ellos, se podrá escoger entre la emisión del sonido de un ladrido advirtiendo de que se trata de un sitio peligroso, o forzar la aparición de un formulario de acceso a la configuración en la que el administrador podrá anular o cambiar las restricciones establecidas tras insertar la contraseña correspondiente.

De esta forma, si el menor accede a una sitio considerado como sospechoso, automáticamente saltará el siguiente formulario:



- **URL Keywords:** Otra opción de filtrado que podremos configurar en esta herramienta se trata de la definición de unas pablaras clave. De esta manera, al intentar acceder a una URL que contenga alguna de ellas no obtendremos ningún resultado.

Por ejemplo, hemos considerado el *kick boxing* como una práctica peligrosa a los ojos de un menor y por ello hemos filtrado todo el contenido que contenga cualquiera de las palabras que la componen. De esta manera, si el menor intenta buscar algún vídeo sobre este deporte, automáticamente le saltará el siguiente mensaje en su pantalla:



Además, también hemos filtrado la pabla *foto*. De esta manera evitaremos que el menor entre en blogs o páginas web en las que consideremos que pueda enfrentarse a imágenes ofensivas o inadecuadas para su edad.

Recordemos que siempre podremos editar las excepciones a las que el menor tendrá siempre acceso independientemente del resto de filtros. Recordemos que habíamos definido en la lista blanca la siguiente URL: www.fotosalmoines.com

Si intentamos acceder al sitio (recordemos que contiene la palabra *foto* en su dirección), nos dejará entrar sin problemas:

- **Safe Search:** En este apartado podremos activar el filtrado avanzado de contenidos para adultos que incluyen los principales motores de búsqueda como Google, Ask o Yahoo!.
- **Other settings:** Finalmente en esta última sección podremos activar el filtro avanzado de contenido *no apto* para menores de cierta edad en YouTube, así como otras opciones de actualización y filtrado.

Ya hemos acabado de configurar todas estas reglas en la opción *Set Up*. Si lo que queremos es supervisar qué ha estado haciendo el menor en la red, seleccionaremos esta vez la opción *View Internet Activity* del menú principal del administrador.

Una vez dentro, podremos escoger entre un resumen general de la actividad del menor o por el contrario una información más detallada sobre las búsquedas, visitas a sitios web y la hora exacta de cada acceso.

- **View Activity Summary**: Resumen general de categorías visitadas y de eventos producidos (búsquedas y accesos web bloqueados):

- **View activity detail:** En esta sección podremos seleccionar y obtener información más detallada sobre la actividad del usuario. Además, podremos filtrar la información por categorías. Por ejemplo queremos supervisar si el menor ha accedido a sitios P2P para descargar contenido ilegal:

Como se observa, la herramienta ha captado tanto la URL como la hora exacta del intento de acceso.

Podremos hacer lo mismo para todas las categorías.

En conclusión, se trata de una herramienta completísima y muy flexible a la hora de establecer las reglas de navegación y los contenidos a los que el menor en cuestión tendrá acceso cuando acceda a Internet. Además, se trata de una herramienta completamente gratuita.

Sin embargo, en comparación con otras herramientas de control parental, cabría mencionar dos desventajas principales:

- **Instalación local.** A diferencia de otros productos de su misma categoría, únicamente tendremos acceso a la administración y supervisión de contenido en aquellas máquinas en las que tengamos el software instalado. Por tanto, no presenta el sistema de Nube que permite controlar la actividad del menor desde cualquier equipo con conexión a Internet.

- **No permite la creación de perfiles de usuario.** Otra desventaja importante, es que el software se aplica para todos los usuarios del equipo en el que está instalado. Por tanto, aunque tengamos varios usuarios creados en el sistema operativo las restricciones se aplicarán a todos y con el mismo grado de control y flitrado.

4.3.4 Qustodio

Estamos ante otra herramienta de control parental basada en la Nube, por lo que únicamente precisaremos de su instalación en aquellos equipos que utilice el menor cuya actividad queremos supervisar.

Se trata de un producto de pago, aunque dispone de una versión gratuita más discreta disponible en su página web.

Cabe destacar que se trata de un software de origen español.

Para empezar, entraremos en la web del producto y seleccionaremos la opción *Descargar*:

Una vez descargado, lo ejecutaremos y procederemos a su instalación y configuración.

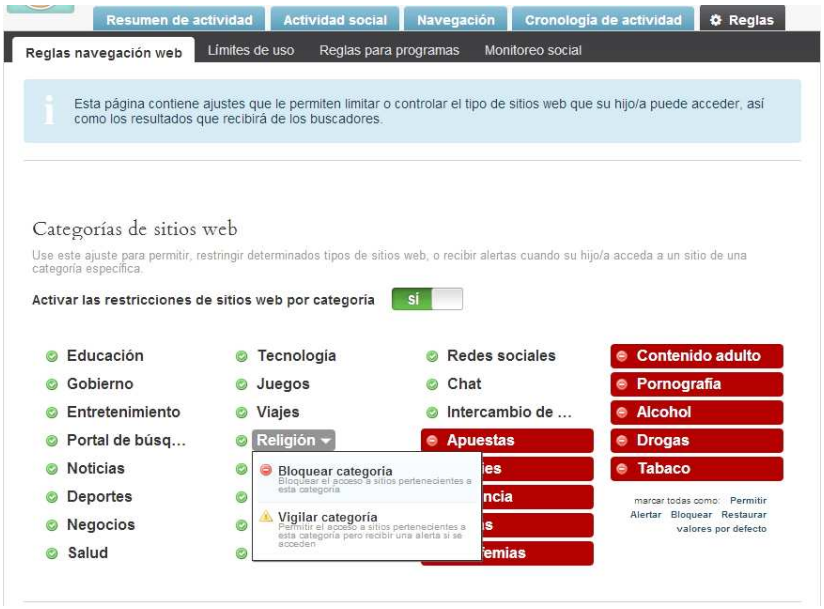
Una de las ventajas de este producto es la creación de varios perfiles de usuario y su asociación a cada una de las cuentas de nuestro equipo. De esta forma, podremos personalizar la configuración para cada uno ellos:

Como se trata de un sistema de control parental basado en la Nube, podremos acceder al administrador iniciando sesión en el **Portal Familiar de Qustodio** (https://family.qustodio.com/) a través de cualquier equipo con conexión a Internet.

Allí tendremos una distribución por pestañas de cada uno de los perfiles de usuario definidos en la instalación, de forma que podamos personalizar las reglas de navegación para cada uno de ellos.

Para empezar seleccionaremos el usuario que hemos creado y seleccionaremos la última subpestaña para definir las normas. Para ello, disponemos de varias herramientas de filtrado:

- **Reglas de navegación web**: La pantalla se divide en dos partes. En la parte superior se definen un grupo de categorías en las que se clasificarán el conjunto de sitios web. Por defecto, aparecerán bloqueadas aquellas que la herramienta considere más peligrosas o inadecuadas para los menores de edad. Sin embargo, podremos desbloquear algunas categorías o bloquear algunas que en principio no estén consideradas como dañinas.



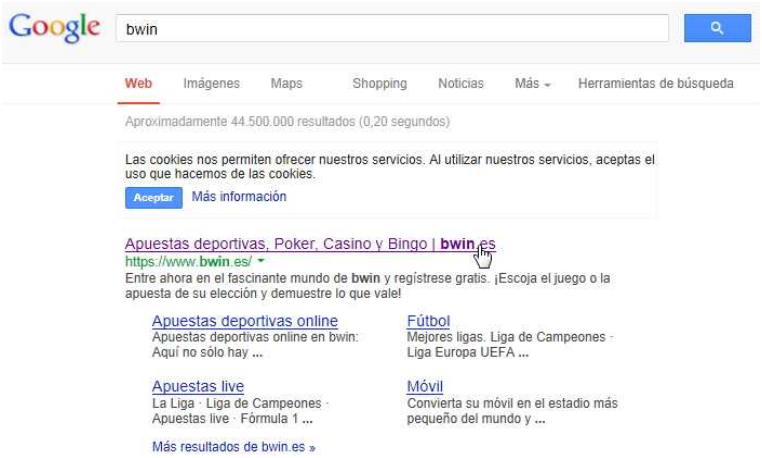
Como vemos en la captura, tendremos además tres grados de protección: bloquear directamente las páginas web pertenecientes a la categoría, permitir el acceso o simplemente supervisar el acceso sin llegar a bloquearlo.

En la parte inferior de la pantalla se permite, además, la definición de una lista de sitio web concretos en las que indicaremos específicamente si el usuario tendrá el acceso permitido, denegado o permitido pero con supervisión, independientemente de la categoría a la que pertenezcan.

Finalmente, en la parte derecha indicaremos el comportamiento de la herramienta a la hora de mostrar contenido no categorizado o a la hora de mostrar resultados de búsqueda.

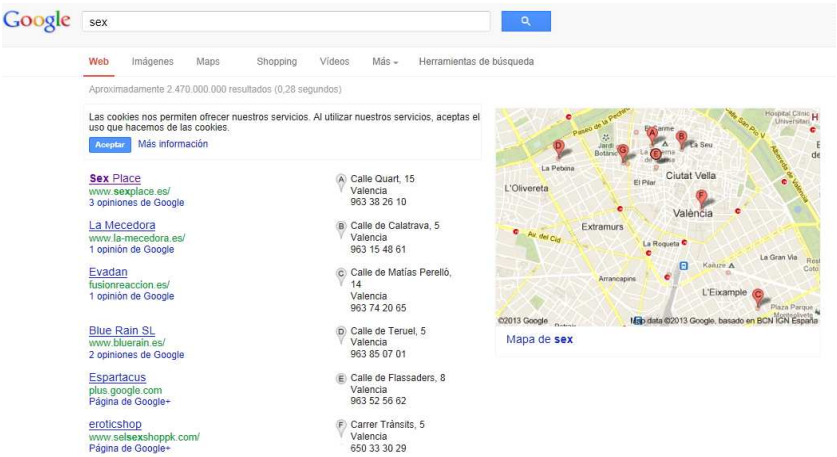
Comprobemos los límites de esta configuración. Intentaremos acceder a un sitio de apuestas al que menor tiene prohibido el acceso a través de un buscador.

Como vemos, el buscador nos muestra los resultados convenientes, pues no se considera contenido potencialmente inseguro:



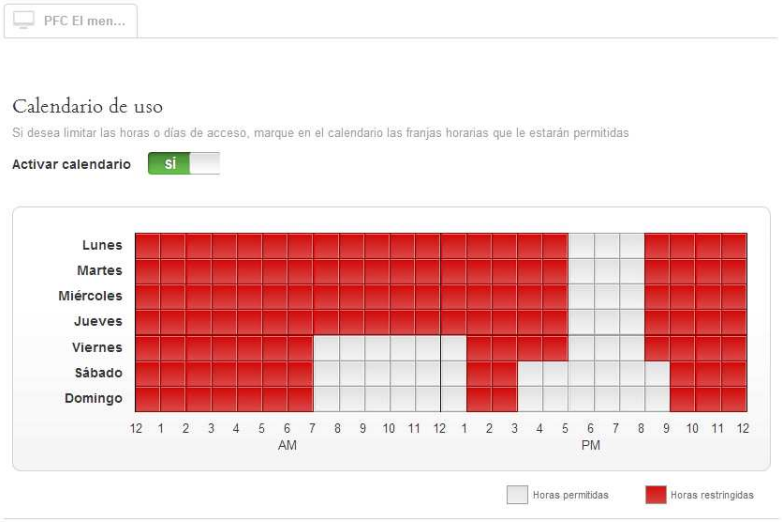
En cambio, a la hora de acceder al sitio web, el navegador nos redirigirá automáticamente a nuestra pantalla de inicio, pues la categoría *Apuestas* la tenemos marcada como *Bloqueada*.

Sin embargo, también habíamos bloqueado la categoría *Contenido Adulto* en la lista de categorías y si buscamos por la palabra *sex* nos aparecerá una lista de sitios web pertenecientes a varios negocios a lo que además tendremos acceso:



Por tanto, debemos ser muy cuidadosos a lo hora de filtrar el contenido y tomar las medidas oportunas cuando nos encontremos en estas situaciones.

- **Límites de uso:** En la siguiente sección podremos establecer los límites horarios en los que el menor tendrá acceso a la web. También está divida en dos partes. Primero definiremos el calendario de acceso:

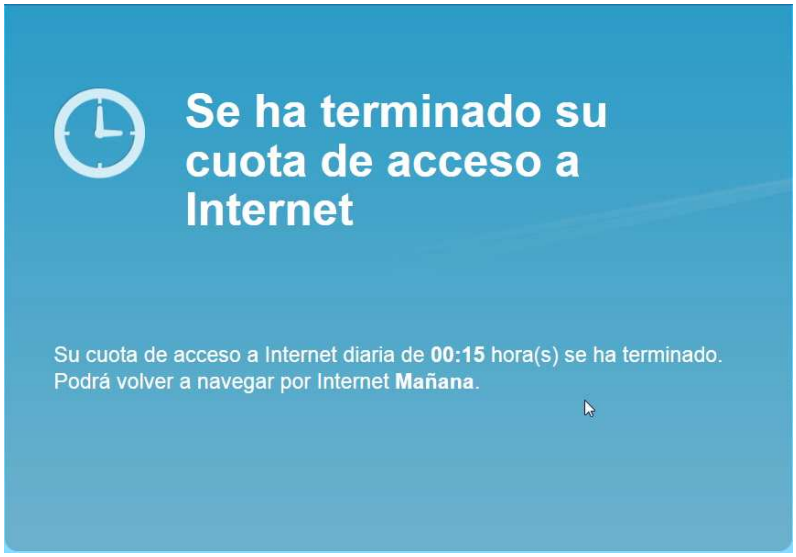


Como vemos también es configurable según el día de la semana y en periodos de una hora.

En la parte inferior de la pantalla, además, podremos definir un tiempo máximo diario en el que el menor podrá estar conectado a Internet, así como las medidas a tomar cuando éste sobrepase este tiempo:

Como se observa en la captura, tendremos la opción de bloquear el dispositivo cuando se alcance el límite establecido o bien bloquear únicamente la conexión a internet. Además, existe la posibilidad de alertar al padre sobre esta situación.

Así, si un menor excede el tiempo permitido, automáticamente le saldrá el siguiente mensaje en la pantalla:



Y si hemos seleccionado la opción de alerta al encargado del menor, éste recibirá el siguiente mensaje en su correo electrónico:


Alerta de Qustodio

Qustodio (no-reply@qustodio.com) Afegeix als contactes 28/04/2013

Estimado Maria,

José ha intentado visitar el siguiente sitio web desde el dispositivo PFC El menor en la red:

- google.es: Terminó la cuota de acceso a Internet.

Para más detalles, siga estas instrucciones:

1. Visite https://family.qustodio.com/user-activity/summary/user/65477/?utm_campaign=activity-alert-es&utm_medium=email&utm_source=v-1
2. Acceda, escribiendo su dirección de correo electrónico y contraseña, y pulsando *Acceder*.

Gracias,
El Equipo de Qustodio

Por favor no responda a este mensaje. Esta dirección de correo electrónico forma parte de un sistema automatizado y no podemos responder a los mensajes enviados a esta dirección.

¿Necesita ayuda? Póngase en contacto con nosotros en: support@qustodio.com

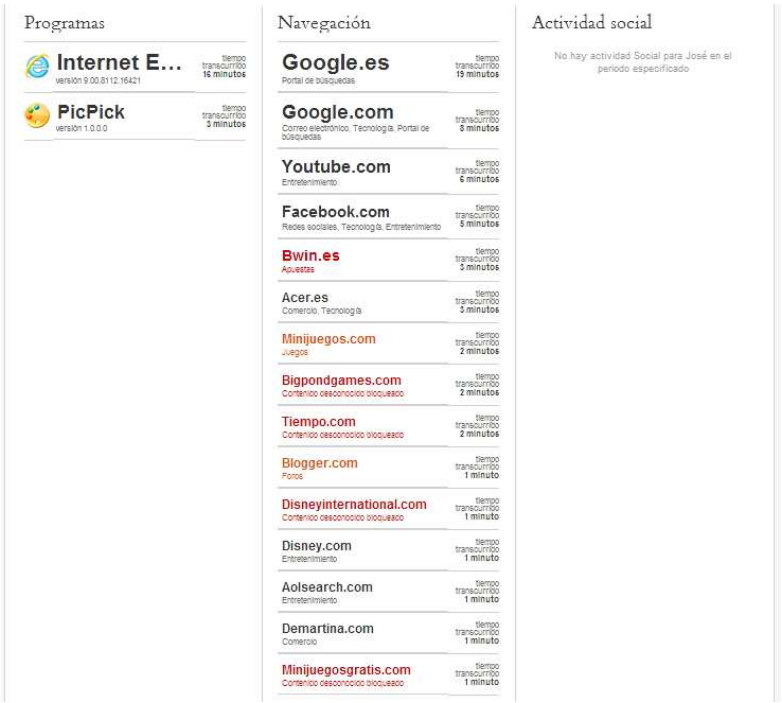
- **Reglas para programas:** Esta opción está únicamente disponible para la versión Premium. En ella se pueden controlar los programas y juegos a los que tendrá acceso el usuario:

- **Monitoreo social:** Esta opción tampoco la tendremos disponible en la versión gratuita. En ella podremos activar una monitorización avanzada de la actividad del menor en Facebook, de forma que podamos orientarle y aconsejarle a tomar las decisiones correctas en su uso de la red social.

Ya hemos terminado con la configuración de la herramienta y únicamente nos quedará comprobar los resultados de su instalación.

Para ello, accederemos a las pestañas principales de *Resumen de actividad*, *Actividad Social*, *Navegación* y *Cronología de actividad* para obtener unos informes muy vistosos y detallados sobre la actividad del menor en la red.

En la primera pestaña correspondiente al **Resumen de actividad**, podremos observar de forma gráfica y sintetizada las categorías de sitios web que ha estado visitando el menor así como el tiempo de uso en cada una de ellas.



Además podremos filtrar esta información y mostrar únicamente las búsquedas o visitas que hemos catalogada como inadecuadas para el joven. Para ello, seleccionaremos la opción *Actividad Cuestionable*:

Toda esta información también la podremos recibir en nuestro correo electrónico en forma de informes diarios de actividad.

La siguiente pestaña relativa a la **Actividad Social** nos ayudará a conocer qué hace el menor en las redes sociales aunque, como hemos comentado, esta opción la tendremos únicamente habilitada en la versión Premium de la herramienta.

En la pestaña de **Navegación** se mostrará de forma detallada todas aquellas páginas que ha estado visitando el menor en el periodo de tiempo especificado así como los datos de tiempo de uso y días de visita.

Además incorpora una pequeña clasificación del sitio web en cuanto a Popularidad, Integridad y Seguridad Infantil.

A todo esto, comentar que también podremos filtrar la información por aquellas que suponen una *Actividad Cuestionable*.

Finalmente en **Cronología de Actividad** mostrará todas las páginas web visitadas de forma cronológica.

En esta pestaña también tendremos la opción de filtrar por la información que más nos interese y a su vez nos permitirá seleccionar una nueva acción para cada una de las webs visitadas, ya sea añadirla en la lista blanca de sitios webs siempre permitidos, bloquear su acceso o simplemente vigilarlo.

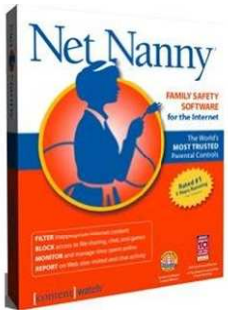
En definitiva, aquí tenemos otra alternativa bastante completa para controlar la actividad de los niños y adolescentes en la red, aunque se echa de menos el poder controlar el uso de las redes sociales. Recordemos que la opción avanzada de Facebook únicamente está disponible en la versión *Premium*.

4.4 Inventario software de Control Parental

En el apartado anterior hemos comprobado las posibilidades y limitaciones que nos brindan alguna de las herramientas gratuitas más relevantes de control parental.

Sin embargo, existe un gran número de productos también gratuitos y otros más completos de pago con esta misma finalidad. A continuación nombraremos algunos de ellos con sus características principales.

4.4.1 Net Nanny



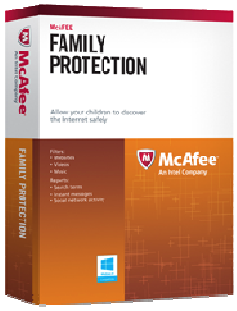
Se trata de una de las mejores herramientas de control parental de pago y destaca por ser fácil de configurar y con un gran número de opciones.

Veamos sus principales características:

- Filtrado en Internet: Permite bloquear pornografía, sitios de intolerancia, salas de chat cuestionables, juegos en línea y sitios de juegos, acceso a redes sociales, etc.
- Fotos, Foros y Blog: Restringir información personal que los menores publican online.
- Palabras clave de bloqueo: Creación de una lista "negra" personalizada de términos y frases que consideremos no aptas para el menor.
- Administración remota desde la Nube
- Monitoreo de navegación Web y mensajería instantánea
- Bloqueo de juegos de PC mediante el sistema de clasificación por edades de la ESRB(Entertainment Software Rating Board)

- IM Alerta y Análisis: Net Nanny Mensaje examina el contenido de los mensajes instantáneos (IM) y alerta a los padres a través de correo electrónico sobre posibles acosadores, intimidadores y otros comportamientos inapropiados online. Utiliza las aplicaciones y protocolos de mensajería instantánea basados en Web como Facebook, MySpace, MSN y Yahoo.
- Controles de Tiempo de Uso de Internet
- Integración con los principales motores de búsqueda

4.4.2 McAfee Family Protection



Se trata de otra de las herramientas de control parental más completas que podemos contratar hoy en día.

Al igual que Net Nanny no dispone de versión gratuita y la podremos obtener pagando una cuota anual de 36,95 euros. Principales características:

- Permite el bloqueo de hasta 35 categorías de sitios Web cuestionables y filtra el contenido inadecuado.
- Control de vídeos de YouTube mediante el filtrado por pablaras clave
- Establecer horario en la que los menores tendrán acceso a Internet
- Supervisión y registro de conversaciones de mensajería instantánea
- Registro del envío de información confidencial a través de las redes sociales
- Ayuda a mantener el equipo a salvo de las amenazas que se encuentran en los programas de uso compartido de archivos peer-to-peer
- Elaboración de informes de actividad completos
- Envío automatizado de alertas de correo electrónico cuando se intenta acceder a sitios web de contenido inadecuado
- Administración por categorías de la visualización de programas de televisión y películas por Internet

- Filtrado de música de iTunes que contenga lenguaje explícito en el título de la canción

4.4.3 PC Pandora

Esta herramienta se caracteriza por su constante monitorización de la actividad del usuario.

También es un software de control parental de pago, aunque podremos obtener una versión de prueba en la web del producto: http://www.pcpandora.es

Principales características:

- Monitoriza y registra todos los mensajes de correo electrónico mediante la realización de "fotografías virtuales".
- Monitoriza y registra todos los mensajes instantáneos en chats y programas de mensajería instantánea.
- Monitoriza y registra todas las teclas pulsadas.
- Monitoriza y regitra todos los sitios Web visitados.
- Envío de un reporte a cualquier ordenador con todos los mensajes de correo, chats, páginas web visitadas y en definitiva todo lo que hace el ordenador en el intervalo de tiempo que decidamos.
- Bloqueo de los sitios web no deseados.
- Posibilidad de ejecución en modo oculto
- Supervisa y ejecuta todos los programas de captura en el PC

4.4.4 bSecure

Nos encontramos ante otro software de control parental basado en la nube. También se trata de un producto de pago y, aunque está disponible la versión para varios dispositivos, precisa al menos de un PC con el sistema operativo Windows para

poder controlar el resto.

Principales características:

- Acceso a la consola de administración desde cualquier navegador. Se trata de un sistema basado en la nube.
- Filtrado de páginas web rápido y flexible.
- Monitorización de redes sociales como Facebook, Twitter, MySpace y otras 75.
- Filtración para todos los dispositivos de casa con acceso a Internet
- Filtrado de programas de televisión, películas y juegos por sistema de clasificación por edades
- Establecimiento de límites horarios en el que cada perfil de usuario de la cuenta tendrá acceso a Internet
- Filtrado integrado para dispositivos iPhone y iPad
- Alertas en tiempo real sobre actividad sospechosa

4.4.5 Cybersitter

Se trata de otra herramienta de control parental de pago, aunque no goza de la popularidad de las primeras de la lista. A continuación listaremos sus especificaciones:

- Monitorización remota: Se puede observar y grabar actividades en tiempo real de todos los pc conectados en la red local
- Control de chat de Facebook, posts en Facebook y Twitter y actividades de grupos
- Filtrado completo de conexiones HTTPS / SSL
- Creación de distintos perfiles de usuario con filtros personalizados
- Creación de horarios de conexión a sitios por categorías
- Bloqueo personalizado y opciones adicionales
- Bloqueo de cookies y otros métodos de seguimiento de nuestros hábitos de navegación

- Se integra con los servidores DNS gratuitos para asegurar una protección permanente contra *exploits* de redirecciones DNS
- Bloqueo del acceso a Internet por parte de aplicaciones específicas
- Excluir algunas aplicaciones del filtrado

4.4.6 Control Kids

Estamos ante otra alternativa de control parental gratuito.

Control Kids filtra todo contenido inadecuado de los sitios web : la pornografía, la violencia, la pedofilia, las sectas religiosas, los sitios de descargas ilícitas, etc.

Características principales:

- Filtra todo sitio web con contenido inapropiado
- Control paterno compatible con TODOS los navegadores: Internet Explorer, Firefox, Chrome, Safari, Opera, etc.
- Ninguna configuración morosa a realizar
- Compatible con Windows Me/2000/NT/XP/Vista/Seven
- Completamente transparente para el utilizador
- Protegido con una contraseña
- Filtra los contenidos de carácter pornográfico
- Bloquea automáticamente los sitios de phising / estafas

4.4.7 MintNanny

En esta ocasión hablamos de un sistema de control parental para Linux y completamente gratuito.

Desafortunadamente, únicamente permite el bloqueo de páginas no deseadas mediante la creación de una “lista negra”.

4.4.8 Gnome-Nanny

Aquí tenemos otra herramienta de control parental gratuita para Linux.

Como vemos, éstas ofrecen unas opciones más limitadas que el resto de herramientas estudiadas. Estas son sus características:

- Controlar lo sitios a los que tendrá el acceso permitido o denegado cada uno de los usuarios definidos
- Delimitar los horarios en los que el menor podrá:
    - Utilizar el ordenador
    - Navegar por la web
    - Mandar correos electrónicos
    - Utilizar un servicio de mensajería instantánea

4.4.9 Pure Sight

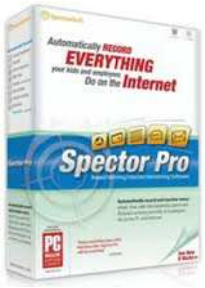
Herramienta de control parental para Windows de pago, aunque tenemos disponible una versión de prueba gratuita en la web: http://www.puresight.com/

Únicamente está en inglés.

Principales características:

- Configuración protegida con contraseña
- Protección contra el cyberbulling en mensajería instantánea, programas de chat y Facebook.
- Control de intercambio de archivos en redes peer-to-peer
- Filtrado de contenido web ofensivo o inapropiado
- Establecimiento de límites horarios para el uso específico de determinadas herramientas como la mensajería instantánea
- Alertas en tiempo real de acciones peligrosas y resúmenes de la actividad del menor en Internet

4.4.10 Spector Pro



El objetivo de este sistema de control es el de registrar absolutamente todo lo que ocurre en el pc. Por tanto, más que un sistema preventivo se trata de una herramienta de control.

Se trata de un software de pago con las siguientes características:

- Captura de todos los comandos y pulsaciones de teclas
- Captura de conversaciones de Chat y mensajería instantánea
- Lector de todos los correos electrónicos, tanto enviados como recibidos
- Revisión de todo el historial de navegación y las acciones realizadas en cada uno de los sitios web visitados
- Control de la actividad en Facebook
- Revisión remota de las grabaciones desde otro PC o Mac
- Control de las búsquedas realizadas
- Control de todos los programas ejecutados
- Alertas en cuanto alguien utuliza un lenguaje inapropiado o visitan un sitio web sospechoso
- Bloqueo de páginas web y chat
- Monitorización por capturas por orden de ejecución

4.4.11 Trend Micro Guardian

Trend Mictro Guardian presenta 3 niveles de control para Windows: a mayor nivel se incuyen más equipos y dispositivos móviles, aunque en la versión más económica podemos encontrar todo lo necesario para una navegación segura.

Aunque funciona principalmente como un antivirus,

también ofrece un apartado destinado al control parental en el que podremos:

- Monitorizar la actividad del menor en las redes sociales
- Monitorización de mensajería instantánea
- Monitorización de sitios de vídeos visitados, etc.
- Gestión desde la nube

4.4.12 Web Watcher

Al igual que ocurría con Spector Pro, este sistema de control parental está basado en el registro de acciones realizadas en el equipo más que en los bloqueos.

Características:

- Registro de teclas
- Monitorización de actividad en redes sociales como Facebook y MySpace
- Control de correo electrónico, tanto de e-mails enviados como recibidos
- Control de la actividad por programas
- Monitorización de mensajería instantánea, tanto de mensajes enviados como recibidos
- Captura de imágenes cada periodo de tiempo especificado
- Bloqueo de páginas web mediante una lista negra
- Notificaciones al utilizar algunas palabras clave establecidas en cualquier tipo de comunicación
- Control de búsquedas en Google y Bing
- Sistema basado en la Nube

4.4.13 OTROS – Navegadores y Complementos de navegador

Aunque las herramientas que vamos a comentar son mucho más rígidas y limitadas que los productos de Software de Control parental que acabamos de describir, éstas están especialmente diseñadas para niños de corta edad y presentan un diseño muy atractivo y llamativo.

KidZui

KidZui es un navegador web destinado a los más pequeños de la casa.

Es gratuito y también puede utilizarse como agregado del Mozilla Firefox.

En él podremos encontrar una selección de sitios web, imágenes, vídeos y juegos especialmente dedicados a los niños. Únicamente se podrá acceder a esta lista blanca elaborada por padres y maestros, por lo que los padres podrán estar tranquilos mientras el menor navega por la red.

Kido'Z

Nos encontramos ante otro navegador web especialmente dedicado a los niños.

Este incluye un buscador, juegos en línea, videos apropiados para los más pequeños, etc.

Además, se puede instalar en un PC, tableta o Smartphone.

A diferencia de KidZui, este navegador permite a los padres personalizar el contenido al que tendrá acceso el menor y, además, establecer los límites de tiempo en los que el pequeño podrá estar delante de la pantalla.

FoxFilter

Para los usuarios del navegador Mozilla Firefox, existe un complemento a descargar de forma sencilla y gratuita que nos ayudará a bloquear contenido inapropiado como podría ser la pornografía.

4.5 Conclusiones

En definitiva, tenemos un gran abanico de posibilidades a la hora de proteger a los jóvenes ante todas las amenazas y contenido inapropiado que nos ofrece la red.

Dependiendo de la madurez del menor, optaremos por unas herramientas más básicas y rígidas o por el contrario, podremos decantarnos por otras más personalizables que nos permita acoplar los filtros según nos convenga.

A modo de resumen, dependiendo del rango al que pertenezca la edad del menor podremos optar por:

Niños menores de 9 años:

- Herramientas rígidas en las que el niño únicamente tenga acceso al contenido que consideremos oportuno. Sin más.
- Como hemos visto, tenemos navegadores para niños dedicados a tal fin como KidZui y Zido'Z

Pre-adolescentes entre 9 y 13 años:

- Herramientas más flexibles en las que se permita la edición de listas blancas y negras o por categorías. De esta forma, podremos editar el contenido al que tendrá el acceso permitido o denegado.
- Además, muchos de los menores de esta edad ya posean su propio PC, por lo que convendría establecer unos límites de tiempo que limitara una excesiva conexión a la red.
- En este rango, entrarían la gran mayoría de herramientas estudiadas: Qustodio, K9 Web Protection, Norton Online Family, Net Nanny, etc.

Adolescentes menores de 18 años:

- Así como en los niños de corta edad podremos optar por software que únicamente permita el acceso a cierto contenido, en este caso nos encontramos en la situación opuesta; por la edad del joven, quizá únicamente sea necesario bloquear determinado contenido que podemos considerar ofensivo.
- Así pues, nos servirá cualquiera de las herramientas comentadas en el apartado anterior: Qustodio, Net Nanny, Norton Online Family, etc. que

nos permita bloquear páginas de contenido inadecuado mediante listas negras o categorías.

- Sin embargo, en estos casos se recomienda optar por una estrategia de supervisión más que de bloqueo, pues los menores de esta edad ya son más conscientes de los peligros a los que se enfrentan y probablemente sea más eficiente y constructivo una buena charla con ellos.

Por ello, como hemos estado comentando a lo largo de este apartado, una navegación segura por la red pasa principalmente y en primera instancia por una buena educación y concienciación sobre todos aquellos peligros que nos podemos encontrar y la forma de actuar ante estas situaciones. Debemos considerar el software únicamente como una herramienta complementaria que nos ayude a navegar más tranquilos.

5. Casos de estudio

5.1 Introducción

Como se expone en el primer punto de la presente memoria, la red ha sufrido una enorme evolución desde que naciera para fines educativos y de investigación hasta tal y como la conocemos hoy en día. Estos cambios y nuevas posibilidades la convierten actualmente en una herramienta casi indispensable de nuestro día a día y nos lleva a estar conectados de forma permanente a través de nuestros ordenadores, tabletas o smartphones.

Además, cada vez se tiende a empezar a utilizar las nuevas tecnologías a una edad más temprana y, de igual forma que nos beneficiamos de las innumerables ventajas que presentan, también nos sometemos a todos los peligros que conlleva el hacer un mal uso de ellas.

Por ello y, debido al grado de inmadurez y vulnerabilidad que presentan los jóvenes de corta edad, "la educación en aspectos de seguridad, privacidad, protección de los derechos de las personas, etc. es algo que se debe enseñar desde la infancia" (INTECO, 2012) tal y como se anuncia en la guía de actuación contra el ciberacoso desarrollada por el Instituto Nacional de Tecnologías de la Comunicación.

Podemos clasificar los diferentes riesgos a los que se exponen los menores al utilizar la red basándonos en diferentes criterios. Uno de ellos sería el diferenciar entre los ataques o acoso de menores entre iguales, es decir, de menor a menor, o el acoso a un menor por parte de un adulto.

Atendiendo a esta clasificación, existen tres peligros principales que siempre han estado presentes: el acoso escolar entre alumnos (entre iguales), el acoso a un menor por parte de un adulto con un fin sexual y la pornografía infantil (estos dos últimos pertenecerían a la segunda categoría). Con el avance de las nuevas tecnologías y el gran auge de las redes sociales, estos riegos cobran mayor importancia, pues la difusión del contenido ofensivo o comprometido se agiliza bastante de forma que se agrava la situación. En este contexto digital, el acoso entre menores se conoce por ciberacoso o *ciberbullying* y el acoso a un menor por parte de un adulto por *grooming*.

A continuación profundizaremos en cada uno de ellos y expondremos algunos consejos o recomendaciones para intentar evitar estas situaciones, citaremos algunos casos reales así como las sentencias dictadas en cada uno de ellos.

Sin embargo, no son los únicos peligros existentes hoy en día. Podremos encontrar otros como el robo de identidad, phishing, spam o actividades como el sexting, cuya práctica se está extendiendo hoy en día por el uso de los smartphones y las nuevas aplicaciones que permite compartir contenido multimedia de forma inmediata y en cualquier lugar.

Algunos de estos riesgos están directamente relacionados con el acoso a menores que acabamos de comentar, ya que algunas actividades como el robo de identidad o sexting son algunos de los medios que utilizan los atacantes para burlar o chantajear a sus víctimas y provocar así una situación de acoso.

Por ello, aunque únicamente profundizaremos en los casos de Ciberbullying y grooming, dedicaremos un subapartado a definir estos otros factores de riesgo que el menor también deberá tener en consideración al hacer uso de las nuevas tecnologías.

5.2 Ciberacoso o ciberbullying

5.2.1 Definición

Según el Diccionario de la Real Academia de la Lengua, se define acosar como:

(Del ant. cosso, carrera).

1. tr. Perseguir, sin darle tregua ni reposo, a un animal o a una persona.

2. tr. Hacer correr al caballo.

3. tr. Perseguir, apremiar, importunar a alguien con molestias o requerimientos.

En nuestro contexto, prestaremos atención únicamente a la primera y tercera definición. Por tanto, entenderemos por acoso toda aquella acción que involucre amenazas, chantaje, humillación, hostigamiento y todas aquellas acciones cuya finalidad sea la de molestar o dañar a una persona y que se ejecuta de forma repetida en el tiempo.

Este tipo de acoso ha existido siempre y ha sido un problema preocupante a tener en consideración.

Sin embargo, el gran cambio de la red desde sus comienzos y la aparición de las redes sociales hacen que este concepto evolucione

adaptándose a las nuevas tecnologías y nazca lo que hoy en día conocemos por **ciberbullying**.

Por tanto, definiremos ciberbullying como el tipo de acoso en el que los medios utilizados para atormentar a las víctimas sean de naturaleza tecnológica, es decir, vía mensaje de texto, correo electrónico, aplicaciones de mensajería instantánea o difusión a través de redes sociales, blogs, foros, etc.

Así pues, tal y como se expone en la *Guía legal sobre ciberbullying y grooming* publicada por el Instituto Nacional de Tecnologías de la Comunicación: "Recientemente, los expertos han venido elaborando un nuevo concepto de acoso que se vale de medios electrónicos y que recibe el nombre de ciberbullying o ciberacoso. Esta conducta se define como acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños. En una definición más exhaustiva, se puede decir que ciberbullying supone el uso y difusión de información lesiva o difamatoria en formato electrónico a través de medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de vídeos y fotografías en plataformas electrónicas de difusión de contenidos." (INTECO, 2009)

Reuniendo las citas de los psicólogos Jose María Avilés y Javier Urra transcritas en el documento *Guía de actuación contra el ciberacoso* (publicado por el Ministerio industria, energía y turismo de España), así como las características enumeradas en este mismo documento, en la *Guía legal sobre ciberbullying y grooming* y sitios web dedicados a orientar a padres y educadores sobre cómo abordar este problema y otros riesgos presentes al utilizar la red (tales como http://www.pantallasamigas.net/, www.segu-kids.org, www.emici.net o los centros de ayuda de las principales redes sociales), podemos enumerar las características principales que contempla el ciberbullying de la siguiente manera:

- **Acoso entre iguales.** El ciberbullying se caracteriza por ser un acoso entre personas de edades similares. En el estudio que nos ocupa, hablaremos del ciberbullying en el caso en que tanto la víctima como el acosador son menores de edad.

- **No contiene elementos de índole sexual.** Este tipo de acoso incluye acciones de humillación, burla, chantaje. etc., pero ninguna de estas

acciones tiene alguna finalidad sexual. En el caso de tenerla, estaríamos hablando de *grooming*, comportamiento que definiremos en el punto siguiente de este apartado.

- **La situación de acoso se dilata en el tiempo.** No se trata de una acción puntual sobre la víctima, independientemente de la gravedad de los hechos, sino un acoso continuo y repetido sobre la misma persona.

- **El medio utilizado para llevar a cabo el acoso sea tecnológico.** Esto es, que la víctima utilice cualquiera de los medios siguientes:

    - Envío de mensajes a través del móvil. Por ejemplo, enviando masivamente y de forma repetida mensajes intimidatorios, ofensivos e insultantes hacia el menor o que incluyan amenazas de daños.

    - Publicaciones en redes sociales. Por ejemplo, publicando secretos, rumores o cotilleos sobre alguien para dañar su reputación o haciéndose pasar por otra persona para difundir materiales e informaciones online que deja mal a esa persona en cuestión.

    - Publicaciones en blogs con el mismo objetivo.

    - Aplicaciones móviles que permiten la difusión de contenido multimedia.

    - Correo electrónico. Al igual que ocurre con los mensajes a través del móvil, el acosador utilizaría en este caso el correo electrónico para mandar e-mails con la finalidad de intimidar y humillar a la víctima.

    - Acoso a través de *chats online*

    - Acoso a través de *juegos online*

  Así pues, en general, el medio utilizado para llevar a cabo el acoso será Internet y todos aquellos servicios asociados al mismo.

- Generalmente los episodios de ciberbullying ocurren entre jóvenes que se conocen físicamente. Por ejemplo, pueden ser compañeros de clase o instituto, y este podría ser el escenario en el que empieza el acoso al menor. Sin embargo, pasará a considerarse ciberbullying en el momento en el que el acosador comienza a emplear cualquiera

de los medios tecnológicos que acabamos de comentar para atormentar a la víctima.

- Existen algunos casos en los que causar daño de forma explícita a la víctima no sea el objetivo de la acción agresora inicial. Sin embargo, el impacto de las redes sociales y en general los servicios de difusión de contenido digital multiplica y agrava los riesgos a los que se exponen los menores al publicar determinado contenido en la red. De esta forma, es difícil cuantificar la repercusión que tendrá cierto tipo de acciones cuya intención inicial sea simplemente la de gastar una broma a un compañero o difundir un rumor. En estos casos desconocemos en qué medida esta acción pueda llegar a derivar en una situación descontrolada.

Además, en el *Protocolo de actuación escolar ante el Ciberbullying* publicado por la EMICI (Equipo Multidisciplinar de Investigación del Ciberbullying: http://www.emici.net/), se diferencian tres tipos distintos de ciberacoso de la siguiente manera:

> El ciberbullying se identifica fundamentalmente como bullying indirecto que puede concretarse en tres formas de acoso: el hostigamiento, la exclusión y la manipulación.
>
> - **Hostigamiento**, cuando se envían imágenes o vídeos denigrantes sobre una persona, se realiza seguimiento a través de software espía, se envían virus informáticos, se elige en los videojuegos on-line siempre al jugador menos habilidoso para ganarle constantemente y humillarle, etc.
>
> - **Exclusión**, cuando se usan entornos públicos para acosar repetidamente o mandar comentarios despectivos o rumores difamatorios con el fin de provocar una respuesta expansiva, cuando se niega el acceso a fotos, chats o plataformas sociales de todo el grupo a la víctima, etc.
>
> - **Manipulación**, cuando se utiliza la información encontrada en las plataformas, como por ejemplo las redes sociales, para difundirla de modo no adecuado entre las y los miembros de las mismas, cuando se accede con la clave de otra persona y se realizan acciones que pueden perjudicarle en su nombre, etc. (EMICI, 2011)

En cuanto a los perfiles de los roles que participan en la acción de ciberacoso, podremos distinguir entre:

- **Acosador**: Comúnmente, son personas con problemas de autoestima que necesitan rebajar el ánimo de los demás para sentirse superiores. De esta forma, actúan de forma dominante para manifestar su fuerza. Además, según recopila el estudio *Análisis y*

abordaje del acoso entre iguales mediante el usa de las nuevas tecnologías realizado por el Centro de Estudios Jurídicos y de Formación Especializada del Departamento de Justicia de la Generalitat de Cataluña, los aspectos definitorios del menor acosadores son:

- Necesidad imperiosa de dominar a otros; les gusta valerse de la fuerza física
- Bajo rendimiento académico
- Impulsividad y baja tolerancia a la frustración
- Dificultades para asumir y cumplir la normativa
- Una actitud de mayor tendencia hacia la violencia y el uso de los medios violentos
- Poca empatía hacia las víctimas de agresiones y una opciones relativamente positiva de sí mismos
- Las relaciones con los adultos suelen darse de manera agresiva
- Son protagonistas tanto de agresiones *proactivas* (deliberadas con la finalidad de conseguir un objetivo) como *reactivas* (defensivas ante el hecho de ser provocados) (Bartrina, 2011)

Además, podemos añadir dos perfiles más asociados a este acosador:

- ***Reforzador de la agresión.*** El que estimula y anima la agresión.
- ***Ayudante del agresor.*** El que apoya y ayuda al que agrede.

- **Víctima:** Son las personas que sufren la agresión. En este caso existen varios perfiles, de entre los cuales podremos encontrar alguno de los siguientes:

  - El menor solitario con pocos amigos, inseguro, baja autoestima y escasa red social
  - Alumno brillante con el que terminan metiéndose los compañeros
  - El alumno irritante de la clase para sus compañeros que termina siendo el blanco de sus agresiones
  - El alumno que intenta encajar en el grupo ocupando cualquier rol con tal de ser aceptado, aunque como

contraposición se convierta en objeto de maltrato o humillación

- El menor con una característica distintiva que ridiculiza al menor (por ejemplo, “tener las orejas de soplillo”)

Además, al igual que ocurre para el caso del agresor, encontramos otro perfil involucrado en la acción relacionado con la víctima, que sería:

- ***Defensor de la víctima*.** Aquella persona que intenta ayudar a la víctima a salir de la victimización.

- **Espectadores.** Son las personas que observan la agresión desde fuera. Estos no participan en la acción a priori, aunque dependiendo de la actitud que adapten ante ella se pueden convertir en:

  - Cualquiera de los roles secundarios que acabos de comentar:
    - El *reforzador de la agresión*, que la estimula
    - El *ayudante del agresor*, que lo apoya
    - El *defensor de la víctima*, que lo ayuda
  - Consentidores de la agresión: Meros espectadores que tratan de no implicarse en la agresión y que, por tanto, la consienten.

Ahora que conocemos las principales características del ciberbullying y los elementos que lo componen, estudiaremos algunos datos sobre el problema en la actualidad y plantearemos algunos consejos para intentar evitarlo y solucionarlo.

5.2.2 Algunos datos

A finales de marzo de 2011 se publicaron los resultados del estudio realizado por la red europea de investigación **EU Kids Online,** en el que se encuestaron a más de 25.000 niños y niñas de 25 países europeos entre 9 y 16 años y a uno de sus padres sobre el uso que realizan en Internet y los riesgos experimentados en ese uso.

La encuesta preguntaba sobre los siguientes peligros que podemos encontrar en la red: pornografía, *bullying*, recepción de mensajes sexuales, contacto con personas que no conocemos cara a cara, citas con personas contactadas online, contenidos creados por los usuarios

que puedan ser potencialmente lesivos, y uso mal intencionado de datos personales.

En este apartado comentaremos los resultados relacionados con el ciberbullying al que han sido sometidos los encuestados o del que han sido testigos.

Una de las conclusiones clave que presenta el informe sobre el estudio, explica que:

- **Significativamente, el riesgo no ocasiona frecuentemente daño, según manifiestan los niños**. Ser acosado online por medio de mensajes desagradables o hirientes es el riesgo menos frecuente pero es el que más frecuentemente llega a disgustar a los niños. (EU Kids Online, 2011)

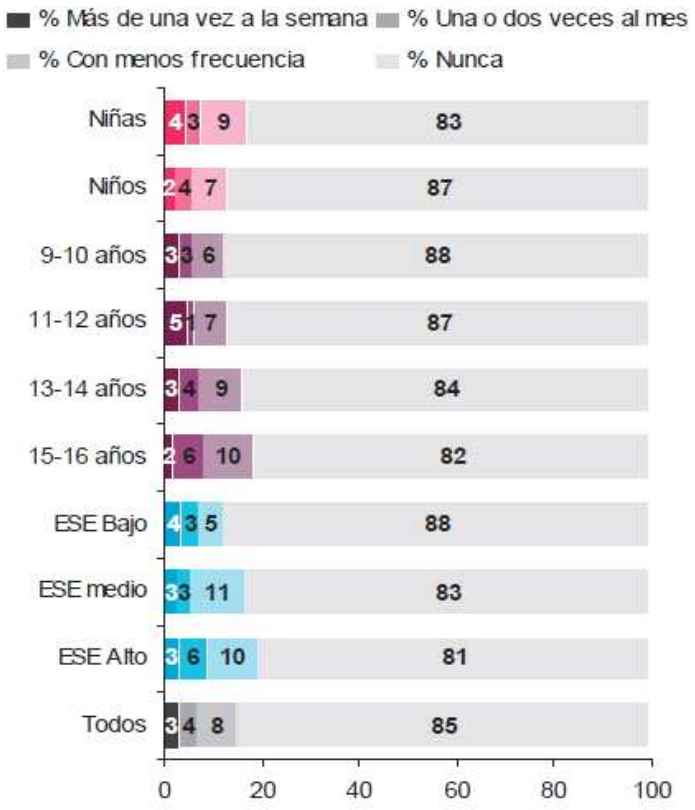
En cuanto a la frecuencia en la que los menores sufren bullying, encontramos los siguientes resultados y conclusiones:

- En España el 16% de los menores entre 9 y 16 años afirmaron haber sufrido este tipo de conducta tanto *online* como *offline*. La media en Europa se sitúa ligeramente por encima (21%). En cambio, el porcentaje es de un 5% cuando se trata de menores que han sufrido bullying online.

- El *bullying* es una experiencia frecuente en muy pocos casos —sólo el 3% de los encuestados que habían sufrido bullying *online* u *offline* en los últimos 12 meses en España afirmaron sufrir estas conductas más de una vez a la semana, y el 4% una o dos veces al mes (en Europa estos porcentajes son del 4% en ambos casos). (EU Kids Online, 2011)

En la siguiente tabla de resultados se muestran las diferencias en cuanto al género, edad y estatus socioeconómico de los entrevistados:

Gráfica 31. Menores que han sufrido *bullying online* u *offline* en los últimos doce meses



EU Kids Online (2011) – *Menores que ha sufrido bullying online u offline en los últimos 12 meses*

Como se observa, existe un porcentaje ligeramente mayor (17%) en cuanto a las chicas que afirman haber sufrido esta conducta frente al de los chicos (13%). Lo mismo ocurre en cuanto a la frecuencia, donde el 4% de las chicas gana al 2% de los chicos.

Además, el porcentaje de casos aumenta en los menores en plena adolescencia frente a los menores de edades más tempranas: 12% entre niños y niñas de 9 y 10 años y un 18% entre los de 15 y 16.

Finalmente observamos también una relación entre los casos de bullying entre los distintos niveles de estatus socioeconómico: a nivel más alto, mayor incidencia.

A continuación mostraremos una tabla comparativa de las formas de acoso de los menores, diferenciando por edad, género y si éste se realiza cara a cara o utilizando algún medio tecnológico (y que, por tanto, contaríamos como casos de ciberbullying):

Tabla 16. Cómo han sufrido *bullying* los menores en los últimos doce meses, por edad y género

%	9-12 años		13-16 años		Todos
	Niños	Niñas	Niños	Niñas	
Cara a cara	9	10	10	13	11
En internet	1	4	2	12	4
Por teléfono, mensajes o imágenes	1	1	1	5	2
Online o *offline*	11	15	16	22	16

EU Kids Online (2011) – *Cómo han sufrido bullying los menores en los últimos doce meses, por edad y género*

Como se observa, no existen grandes diferencias de edad entre los menores que sufren acoso cara a cara o en persona y, en cambio, sí que aumentan considerablemente los casos de ciberbullying a medida que aumenta la edad. Además, destaca la gran diferencia de casos de ciberacoso entre niños y niñas. Así, podemos ver cómo existe un 4% de casos de acoso a través de Internet entre niñas entre 9 y 12 años frente a un 1% de niños, y un 12% de casos entre las adolescentes de 13 a 16 años frente a un escaso 2% de los chicos.

En general, en el contexto temporal en el que se sitúa este estudio (recordemos que fue publicado en marzo de 2011) se reflejaba una realidad en la que los casos de acoso cara a cara entre menores suponían una mayoría frente a los realizados a través de Internet o del móvil, sobre todo en edades más tempranas.

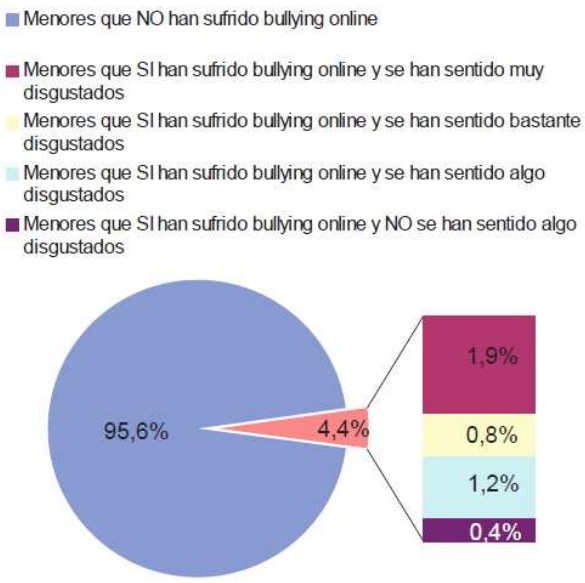
En cambio, el 19 de marzo de 2013 el periódico *El País* publicaba la noticia en la que se recogía información sobre el número de llamadas recibidas en la Línea de Atención sobre Ciberbullying durante el año 2012 (http://sociedad.elpais.com/sociedad/2013/03/19/actualidad/1363700296_848102.html). Estas fueron un total de 343 por parte de menores (casi una denuncia al día), incrementando así un 151% desde que se iniciara este servicio en 2008 y que por tanto pone de manifiesto el incremento de este tipo de acoso en los últimos años.

Volviendo al estudio realizado por *EU Kids Online*, en una de las preguntas de la entrevista se cuestionaba a los menores que habían

sufrido ciberbullying sobre la medida en la que se sintieron afectados por este tipo de acoso. Según publica el informe:

- Entre aquellos menores que han sufrido bullying online, el porcentaje de ellos que se han sentido en alguna medida afectados es el 90%. Es decir, en este caso la exposición al riesgo casi se convierte en un daño en sí mismo para el menor. Entre las víctimas de este acoso el 44% afirmaron sentirse muy disgustados por haber sufrido esa situación, 18% bastante disgustados y el 28% un poco disgustados:

Gráfica 33. Nivel de daño de los menores que afirman haber sufrido *bullying* online



EU Kids Online (2011) – *Nivel de daño de los menores que afirman haber sufrido bullying online*

En cuanto a las plataformas a través de las cuales han sufrido el acoso podemos observar los resultados en la siguiente tabla:

Tabla 17. Plataformas a través de las que el menor ha sufrido *bullying* en los últimos 12 meses, por edad

%	Edad				Todos
	9-10	11-12	13-14	15-16	
En una red social	0	1	5	5	3
Por mensajería instantánea	1	2	3	4	2
Por e-mail	0	0	0	0	0
En una web de juegos	0	0	0	0	0
En un chat	0	0	0	1	0
En algún otro lugar de internet	1	0	0	2	1
En general en internet	**1**	**3**	**6**	**7**	**5**

EU Kids Online (2011) – *Plataformas a través de las que el menor ha sufrido bullying en los últimos 12 meses, por edad*

- Aunque en general, la gran mayoría de los menores no ha sufrido bullying en internet, en los casos en los que se ha dado, este acoso ha provenido sobre todo de redes sociales o de mensajería instantánea. El bullying en internet a través de otras aplicaciones casi no tiene repercusión. Esta tendencia se da tanto los resultados de los menores en España como en Europa. (EU Kids Online, 2011)

Si concretamos en las formas en las que los menores se sintieron acosados, la respuesta de las chicas y chicos entre 11 y 16 años fueron las siguientes:

Tabla 18. ¿Qué forma de *bullying* sufrió el menor en los últimos doce meses? Por edad (+11años)

%	Edad				Todos
	9-10	11-12	13-14	15-16	
Me enviaron a través de internet mensajes desagradables o hirientes	n.r.	2	4	2	3
Se enviaron o postearon en internet mensajes desagradables o hirientes sobre mí	n.r.	0	1	1	1
Sucedieron otras cosas desagradables o hirientes	n.r.	0	2	2	1
Fui amenazado en internet	n.r.	0	1	1	1
Fui expulsado o excluido de un grupo o actividad en internet	n.r.	0	1	0	0
Otras cosas	n.r.	1	0	2	1
En general en internet		**3**	**6**	**7**	**5**

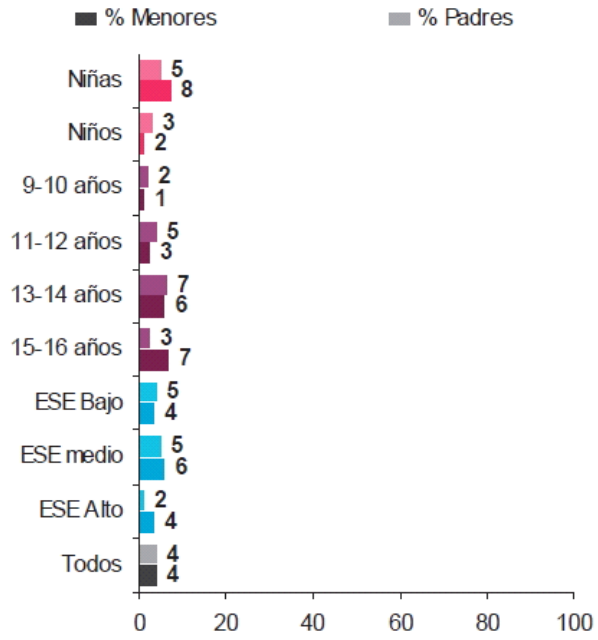
EU Kids Online (2011) – *¿Qué forma de bullying sufrió el menor en los últimos doce meses? Por edad (+11 años)*

A modo de resumen, el informe publica:

- El envío de mensajes desagradables en la red en general con imágenes desagradables o hirientes referidas a la víctima es la forma más habitual de acoso (reportada por el 3% de los menores en España en ambos casos). Mientras que otras formas de acoso apenas tienen presencia. (EU Kids Online, 2011)

Finalmente, en este estudio se preguntaba también a los padres sobre la incidencia de los riesgos de Internet y, a modo de comparativa entre sus respuestas y las proporcionadas por sus hijos, podemos observar los resultados en la siguiente tabla:

Gráfica 35. Percepción de los padres de las experiencias de *bullying online* experimentadas por los menores

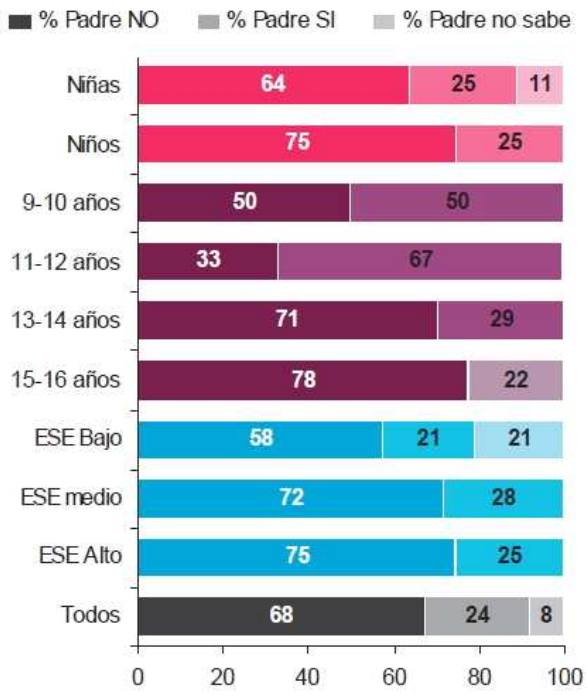


EU Kids Online (2011) – *Percepción de los padres de las experiencias de bullying online experimentadas por los menores*

- En general, tanto el 4% de los menores como el 4% de los padres afirman que ellos mismos o sus hijos han sido víctimas de este acoso
- Hay un porcentaje ligeramente mayor entre las niñas que dice haber sufrido bullying (8% frente a 5%) y se observa también una mayor incidencia con la edad.
- Hay un nivel de acuerdo bastante alto entre las afirmaciones de los menores y las percepciones de los padres. Este acuerdo se centra fundamentalmente en la idea de los padres de que su hijo no ha sufrido este tipo de acoso. (EU Kids Online, 2011)

En la siguiente tabla se muestran los resultados centrándose esta vez en aquellos menores que han sufrido *bullying online* incorporando la opinión de sus padres:

Gráfica 36. Percepción de los padres de las experiencias de *bullying* online sufridas por los menores (solo menores que han sufrido *bullying* online)



EU Kids Online (2011) – *Percepción de los padres de las experiencias de bullying online sufridas por los menores (solo menores que han sufrido bullying online)*

- Entre el 4% de los menores españoles que afirman haber sufrido bullying en internet, únicamente el 24% (29% en Europa) de su padres parece estar al corriente de esta situación. En el 68% de los casos el padre afirma que su hijo no ha recibido mensajes de este tipo, y en un 9% no lo sabe.

- En función de la edad se observa un mayor conocimiento de estas situaciones en los padres de los menores más pequeños y un menor conocimiento en el caso de los padres de hogares de estatus socioeconómico más bajo. (EU Kids Online, 2011)

Como se ha venido comentando a lo largo de la presente memoria, la exposición al peligro que presenta la red hoy en día por el gran auge de las redes sociales se incrementa por el uso de **smartphones**. La utilización de estos dispositivos nos permite estar permanentemente conectado a Internet y recibir contenido multimedia en cualquier momento. Por ello, el peligro de ataque en este caso es constante.

En 2011, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) presentó el "Estudio sobre hábitos seguros en el uso de

smartphones por los niños y adolescentes españoles" que realizó conjuntamente con Orange.

En la web www.ciberbullying.com se recogen los datos destacados del informe sobre el estudio:

- El 2,5% de los menores ha sido objeto de ciberacoso a través del smartphone por parte de otros menores.
- La edad media de inicio en la telefonía móvil por parte de los menores españoles se sitúa entre los 10 y los 12 años.
- España es uno de los países donde los menores (de 10 a 16 años) afirman ver menos imágenes sexuales online: 11% frente a media europea del 14%
- También es uno de los países con menor incidencia del ciberbullying: 4%.
- El 31% de usuarios de más de 13 años usan smartphones (teléfonos inteligentes).
- El 82,3% de los menores usan su móvil para hacer y enviar fotografías.
- El 4,8% de los menores encuestados reconoce que su imagen ha sido difundida por otros sin haber prestado consentimiento.
- El 4,3% de los menores ha recibido imágenes sugerentes de personas de su entorno (sexting pasivo), y un 1,5% reconoce haberse hecho a sí misma/o fotografías de carácter sexy (sexting activo).
- El sexting activo es más practicado por chicas (2,2%) al contrario que sexting pasivo, más practicado por los chicos (5,1%).
- Un 3,8% de los menores afirma que ha recibido llamadas o SMS de adultos desconocidos que querían conocerles
- El 17,8% de los menores dice haber sido objeto de perjuicio económico (estafas, fraudes, etc.) con su smartphone. (Ciberbullying, 2011)

El informe destaca el espectacular avance en el uso intensivo de los servicios avanzados que ofrecen este tipo de teléfonos:

- acceso a redes sociales: del 7,1% en 2010 se ha pasado al 54,3% en 2011
- mensajería instantánea: del 12,4% al 48,3%
- juegos: del 51,6% al 65% (INTECO, 2011)

Como vemos, el informe recoge información sobre otras prácticas en la red como el sexting o el grooming, que comentaremos en su apartado correspondiente del presente punto de la memoria.

5.2.3 Cómo detectarlo

Una de las situaciones principales que nos hace alertarnos sobre el posible caso en el que un menor esté padeciendo algún tipo de acoso, se trata del evidente cambio de comportamiento del propio menor en los hábitos y costumbres de su conducta respecto a su comportamiento anterior.

En el caso concreto del ciberbullying, este cambio se hará especialmente patente en las variaciones bruscas de uso por exceso o defecto respecto al uso de dispositivitos que nos permiten tener acceso a la red y a las aplicaciones de mensajería instantánea o de difusión de contenidos.

De esta forma, la *Guía de actuación contra el ciberacoso* recoge las siguientes manifestaciones en niños y adolescentes:

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

- Por variabilidad de grupos de referencia

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

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

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

- Cambios somáticos
  - Aumento o pérdida de peso rápido derivados de cambios en el comportamiento ante la comida: falta de apetito o comidas compulsivas
  - Mareos frecuentes con síntomas no comunes

- Dolor de cabeza o estómago que no ocasionan despertares nocturnos pero que impiden realizar actividades normales como ir al colegio
- Diarreas frecuentes sin ir acompañadas de vómitos o fiebres (INTECO, 2012)

Además de la lista con los síntomas o manifestaciones que acabamos de comentar, la guía recoge la cita del psicólogo Jose María Avilés en la que afirma que "en casa se suelen producir reacciones bruscas o silencios significativos ante preguntas o requerimientos de sus padres por asuntos relacionados con sus contactos en las redes sociales o reacciones bruscas o cambios de humor después de una conexión. Más allá de la tendencia de los chicos a preservar el contenido de sus contactos a través de la Red, los padres deben diferenciar esto de un rechazo frontal y/o enfado palpable a mantener conversaciones, aceptar preguntas, realizar comentarios, etc. sobre sus relaciones y contactos a través de los soportes virtuales. Cuando se producen estas barreras comunicativas y de intercambio de información por parte de los chicos, en ocasiones es porque hay situaciones que desean ocultar y que piensan que ellos mismos pueden manejar" (INTECO, 2012).

Por tanto, tanto los padres como educadores deben estar atentos a estos posibles comportamientos y, atendiendo al perfil de acosadores y víctimas descritos en el correspondiente apartado de este punto, pensar si los menores a su cargo están realmente en una situación delicada que requiera especial atención.

5.2.4 Consejos y recomendaciones

Como hemos venido comentando, la acción fundamental para evitar estas situaciones pasa por una buena educación a los menores sobre la utilización de Internet y los peligros a los que se puede enfrentar al utilizar la red.

De esta manera, cabría alertar a los menores sobre los escenarios en los que se puede encontrar, sobre todo al utilizar las redes sociales, y se les intenta orientar sobre qué contenido puede resultar dañino u ofensivo tanto para él como cualquier otra persona a la hora de compartirlo y difundirlo en la red. Así, evitaríamos las situaciones que parten de una simple broma a un compañero y que por la rápida difusión y repercusión

de las redes sociales acaba en una situación de ciberacoso para algún menor.

Por ello, hay que concienciar a los jóvenes de las consecuencias de toda la información que comparten e intentar ponerlos en el lugar de la otra persona a la que hace referencia la publicación. De igual forma, cuando un menor se encuentra ante una imagen o comentario ofensivo o atacante sobre él mismo, hay que intentar convencerlo para que no responda a la provocación y que intente buscar apoyo de otros compañeros o familiares. Más adelante se indicarán algunos consejos sobre cómo actuar en estos casos.

Pero no solamente hay que educar a los menores. También las familias de los mismos deben saber los peligros a los que se exponen sus hijos al utilizar Internet de forma que puedan comprender y ayudar a los jóvenes a desenvolverse de una forma "sana" y fuera de peligro en la red. Además, se aconseja controlar hasta cierto punto y siempre respetando la intimidad del menor, lo que éste hace y comparte en la red o el tiempo que pasa conectado, de forma que se pueda percibir algún cambio de comportamiento que nos indique o nos alerte que éste se encuentre en una situación de peligro.

Para conseguir este objetivo, se recomienda mantener siempre unos niveles adecuados de comunicación intrafamiliar, de forma que los niños se sientan cómodos compartiendo con sus padres sus ideas y pensamientos en todo momento y sientan que puedan confiar en ellos. De esta forma, será el propio menor el que busque la comprensión y los consejos de los mismos cuando sientan que se encuentran ante una situación provocadora o peligrosa.

Dado que no siempre podremos conseguir estas situaciones y que en algunos casos son los propios menores los que se niegan a compartir esta información con sus familiares, existen unas herramientas que nos permiten controlar el contenido al que tendrá acceso el menor en la red, establecer los horarios de conexión y en algunas de ellas podremos hasta monitorizar incluso todo lo que comparten en las redes sociales. Además, estas herramientas son configurables según la edad del menor y los contenidos que los padres consideren adecuados para ellos. Hay que tener en cuenta que alguna de estas prácticas podrían ser extremas y que atentan directamente sobre la privacidad del menor, por lo que hay que intentar dialogar con ellos y únicamente utilizar las posibilidades de monitorización en casos en los que lo consideremos estrictamente necesario. En la presente memoria se dedica un apartado

a las principales herramientas de control parental que podemos encontrar hoy en día.

Finalmente, otro colectivo que debe estar al tanto de todos estos peligros y que debe conocer cómo actuar para evitar estas situaciones o cómo responder ante ellas es el propio colegio y sus maestros o profesores. Muchas de las situaciones que se suceden de esta índole entre menores suelen tener su origen en las relaciones que mantienen los menores en la escuela. Además, se trata del lugar donde los alumnos pasan una gran cantidad de tiempo y que, por tanto, puede resultar más evidente cierto cambio de actitud de uno de los niños a ojos de sus compañeros o profesores.

Por ello, será su responsabilidad el avisar a los padres o tutores legales de los implicados en el momento en que perciban que pueden estar ante un caso de acoso a un menor, y colaborar con ellos para intentar solventar la situación. Podemos encontrar información ampliada y detallada sobre el protocolo de actuación de los centros escolares ante una situación de ciberacoso en el siguiente enlace: http://www.emici.net/prot/Protocolo%20Ciberbullying.html

Además, convendría concienciar a los alumnos sobre esta problemática e intentar elaborar algunos talleres o charlas sobre cómo abordar el problema y cómo ayudar a un compañero del que conozcan que se encuentra en esta situación.

Cuando todas las medidas de prevención fracasan y menor acaba sometido a este tipo de acoso, la única solución que nos queda es actuar.

Lo primero que hay que hacer es "abordar al menor a través de la comunicación y la transmisión de confianza desde los adultos que están a su alrededor" (Avilés, 2012), según comenta el profesor José María Avilés, cuyas ideas recoge la *Guía de actuación contra el ciberacoso* y quien además, resume que "la **comunicación**, **evitación de la culpabilización** y transmisión de **confianza** son los primeros pasos a dar con él" (Avilés, 2012). Además, según propone:

> Se deben separar y argumentar con él primero las ineficaces:
>
> - Parálisis
> - Dejar pasar el tiempo
> - Miedo

- Confrontación virtual
- Sumisión
- Indiferencia

Y, después, buscas las que se consideran que pueden ser eficaces:

- Documentación del caso
- Búsqueda y apoyo de iguales y adultos
- Aserción de respuestas
- Evitación de situaciones problemáticas
- Bloqueo de las vías de comunicación
- Actuación coordinada escuela-familia. (Avilés, 2012)

Tras hablar con un adulto de confianza y contarle todo lo sucedido para que pueda ayudar al menor a analizar la situación, podemos encontrar algunos consejos para intentar mermar el acoso en las diferentes guías a las que venimos haciendo referencia en el presente un punto de la memoria y que podemos encontrar en el apartado de *Enlaces de interés*. Recogiendo las ideas principales de cada una de ellas, encontramos las siguientes recomendaciones:

- No responder nunca a las provocaciones, pues lo único que podemos conseguir es estimular más al acosador para que siga con su propósito.
- Intentar evitar las situaciones y lugares en las que se suele producir el acoso hasta que la situación se normalice.
- En caso de sufrir acoso por parte de amistades de las redes sociales, denunciar socialmente y eliminar el contacto siguiendo las indicaciones que se encuentran en el centro de seguridad de cada una de ellas. Hay que ser especialmente cuidadoso con la información que compartimos y con quién lo hacemos así como el material que nuestros amigos comparten sobre nosotros.
- Únicamente contar lo sucedido a personas en las que realmente confíe la víctima, pues las apariencias engañan y puede que las personas implicadas en el acoso no sean como aparentan.
- Guardar las pruebas del acoso para poderlo demostrar.

- Intentar asegurarse de la identidad del acosador o acosadores, sin llegar a invadir derechos de ninguna persona.

- Tratar de dialogar con el acosador, haciéndole saber que su actitud y acciones molestan a la víctima y pedirles sin agresividad ni amenazas que dejen de hacerlo.

Por tanto, hay que intentar siempre acabar con la situación dialogando entre las partes implicadas del acoso intentando evitar que el problema se nos vaya de las manos y que se normalice en el menor tiempo posible.

Si aun siguiendo estos consejos básicos el acoso persiste, habría que concienciar al acosador que lo que está haciendo es perseguible por la ley y que únicamente intentamos frenar la situación antes de llegar a las autoridades.

Finalmente, si con estas últimas amenazas el acosador continúa con su actividad, únicamente nos quedará la opción de tomar medidas legales y dejar la resolución del problema en manos de las autoridades pertinentes.

5.2.5 Estudio de casos

Como hemos visto en el punto *Algunos datos* de este mismo apartado, cada vez son más los menores afectados por casos de ciberacoso y actualmente se puede ver en las noticas algunos sucesos escalofriantes con un final fatal para las víctimas.

En este apartado recogeremos alguno de los casos más llamativos y que más repercusión han tenido a nivel mundial.

Casos nacionales

Afortunadamente en España no se conoce ningún caso de ciberacoso en el que la víctima haya querido acabar con el problema atentando contra su propia vida, aunque el número de denuncias por este tipo de acoso ha ido aumentando año tras año.

Sin embargo, sí que se han hecho públicos algunos casos en los que se han visto involucrado varios menores y que expondremos a continuación:

Detienen a 3 chicos de 14 años por amenazar a otra menor a través de una red social (Europapress, 2011)

Noticia publicada por el periódico El Mundo el 12 de enero de 2011: http://www.elmundo.es/elmundo/2011/01/12/madrid/1294826167.html

En el municipio madrileño de Mejorada del Campo, un menor interpuso una denuncia en la que afirmaba que habían publicado información difamatoria en una red social en la que se le acusaba de un delito que no había cometido y en la que además recibía amenazas de muerte.

Tras una investigación por parte de la Guardia Civil de la localidad, se localizaron a 3 menores implicados en el acoso cuyas edades se comprendía entre 14 y 15 años. Éstos fueron detenidos y se les imputó el delito de amenazas e injurias.

Condenado a pagar 100 euros por reírse en 'Tuenti' de un compañero (EFE, 2009)

Noticia publicada por el periódico El País el 23 de mayo de 2009: http://sociedad.elpais.com/sociedad/2009/05/23/actualidad/1243029602_850215.html

La noticia cuenta la historia de un joven sevillano que publicó en su foto de perfil de la red social **Tuenti** una imagen trucada de un compañero de clase en la que aparecía tocando el violín en el blanco de una diana. A raíz de esta publicación, la víctima recibió una gran cantidad de comentarios despectivos por parte de éste mismo y otros compañeros.

Como consecuencia, el joven que publicó la imagen, ya mayor de edad, fue multado con 100 euros y tanto él como sus compañeros fueron condenados a realizar trabajos en favor de la comunidad en un comedor de caridad próximo al colegio.

Detenidos siete adolescentes de un centro de menores por acosar y humillar a otro y difundirlo (Ollés, 2009)

Noticia publicada por el periódico Diario de Mallorca el 27 de febrero de 2009: http://www.diariodemallorca.es/sucesos/2009/02/27/sucesos-detenidos-siete-adolescentes-centro-menores-acosar-humillar-difundirlo/439877.html

Siete adolescentes, seis chicos y una chica entre 15 y 16 años, fueron detenidos en Mallorca por difundir un vídeo grabado con el móvil en el que golpeaban y vejaban a la víctima. Los agresores, que junto a la víctima atendían a un centro de reinserción de menores, difundieron el vídeo entre otros adolescentes y lo subieron al portal Youtube, lo que provocó que la difusión fuese mayor.

Todos fueron detenidos y acusados del delito contra la integridad moral.

Casos Internacionales

A nivel internacional sí que se conocen más casos de ciberacoso con un final trágico en el que la víctima acaba con su martirio quitándose la vida. Debido a la gravedad de la situación, estas noticias se difunden por todo el mundo y de alguna forma intentan concienciar a las personas sobre el grave problema que supone el hacer un uso inadecuado de la red.

Veamos los casos más relevantes.

Un caso de ciberacoso conmociona a la sociedad canadiense (Monge, 2012)

Noticia publicada por el periódico El País el 17 de octubre de 2012: http://sociedad.elpais.com/sociedad/2012/10/17/actualidad/1350506605_509352.html

Uno de los casos que tuvieron más repercusión en los medios fue el de Amanda Todd, la joven canadiense de 15 años que acabó suicidándose en octubre de 2012 tras sufrir daños de ciberbullying a raíz de una sextorsión.

Todo empezó cuando un desconocido se puso en contacto con la joven a través de la red y le pidió que le mostrase los pechos por la webcam. Amanda accedió y, un año más tarde este desconocido comenzó a acosarla a través de mensajes por la red social Facebook. El acosador la amenazaba con publicar la imagen en la que aparecía con el pecho descubierto si no se desnudaba frente a la cámara. El acosador cumplió su amenaza, y al poco tiempo la imagen de la joven ya estaba en los ordenadores de sus compañeros, familia y profesores.

La víctima se cambió de ciudad y colegio, pero las imágenes la perseguían y poco a poco volvió a estar sometida al mismo ciberacoso una y otra vez hasta que acabó quedándose sin amigos.

La joven intentó hacerse daño varias veces, mutilándose y haciéndose cortes en los brazos.

Un mes antes de suicidarse, grabó y compartió un vídeo a través de la plataforma Youtube en el que contaba toda su historia a través de cartulinas y pedía auxilio, pues tras la difusión de sus imágenes la gente la insultaba y la juzgaba y había perdido a todos sus amigos y el respeto de la gente.

Vídeo:
http://www.youtube.com/watch?feature=player_embedded&v=vOHXGNx-E7E

Desgraciadamente, Amanda no soportó la presión del constante acoso y acabó quitándose la vida.

Tras la difusión de la notica, el vídeo fue visitado por millones de personas y sirvió para hacer más evidente el grave problema del ciberacoso que en algunos casos puede tener consecuencias fatales como el de la joven canadiense.

Procesada una mujer que usó MySpace para engañar a una adolescente que se suicidó (EFE, 2008)

Noticia publicada por el periódico El País el 16 de mayo de 2008: http://sociedad.elpais.com/sociedad/2008/05/16/actualidad/1210888802_850215.html

Megan Meier era una joven estadounidense con tendencia a la depresión desde que era muy pequeña.

En 2006 Lori Drew, la madre de una antigua amiga de Megan, creó una cuenta falsa en MySpace para obtener información sobre ella y luego humillarla, en represalia por una supuesta difusión de rumores que Megan hizo contra su propia hija.

Para ello, se hizo pasar un por un joven de 16 años llamado Josh Evans. Josh y Megan se hicieron amigos en línea, aunque nunca llegaron a conocerse en persona. En octubre de 2006, "Josh" cambió el tono de los mensajes y le llegó a decirle comentarios como "No sé si quiero ser tu amigo más porque he oído que no eres muy agradable para tus amigos" o "Todo el mundo en O'Fallon sabe quién eres. Tú eres una mala persona y todo el mundo te odia.. El mundo sería un lugar mejor sin ti.".

Al poco tiempo de estos comentarios encontraron a la joven en su armario ahorcada.

Según informa el New York times en el ejemplar publicado el 27 de noviembre de 2008 http://www.nytimes.com/2008/11/27/us/27myspace.html?_r=2&hp&), Lori Drew fue condenada hasta 3 años de prisión y una multa de 300.000 dólares por carecer de antecedentes. Fue declarada culpable por acceder a ordenadores protegidos para obtener información con ánimo de infligir dolor emocional con mensajes fraudulentos a través de Internet, con el nombre de "Josh Evans".

Tras este suceso, la madre de la víctima creó la Fundación Megan Meier (http://www.meganmeierfoundation.org/), con la finalidad de "aportar conciencia, educación y promover un cambio positivo para los niños, padres y educadores en respuesta a la continua intimidación y el acoso cibernético a la que se exponen en su día a día".

Este caso en concreto demuestra que los jóvenes no son los únicos que precisan de una buena educación y concienciación sobre los peligros que suponen un simple comentario en la red ya que, como hemos visto, es impredecible la magnitud de las consecuencias que se pueden derivar de nuestros comentarios o publicaciones. En este caso, fue la madre de una antigua amiga de la víctima la que se hizo pasar por un menor y, tras algunos comentarios crueles y desafortunados acabaron psicológicamente con la menor llevándola a una gran depresión y suicidio.

Acoso escolar: En manos de las Chicas Malas (Alandete, 2010)

Reportaje publicado por el periódico El País el 11 de abril de 2010 (http://elpais.com/diario/2010/04/11/domingo/1270957957_850215.html)

Phoebe Prince era una joven irlandesa de 15 años quien, en verano de 2009, se mudó con su madre y sus hermanas a un pueblo de Massachusetts.

Pronto levantaría envidias entre algunos compañeros de instituto tras salir un tiempo con uno de los chicos populares. Los compañeros empezaron a acosarla, insultarla y humillarla en público en varios recintos del instituto. Tras terminar su relación con el joven, éste mismo se unió a los insultos.

El 14 de enero de 2010 y tras una emboscada en la biblioteca en la que sus compañeros le coreaban insultos, la joven decidió acabar con su vida ahorcándose en su casa. Su cuerpo fue encontrado por su hermana pequeña de 12 años.

Por tanto, se trata de un tipo de acoso principalmente escolar y que se dio principalmente en las aulas del instituto.

Sin embargo, lo curioso de este caso, es que el bullying continuó incluso tras la muerte de la joven a través de **Facebook**. Los padres de la víctima abrieron una página memorial en la red social en la que sus compañeros continuaban publicando una gran cantidad de mensajes crudos y crueles que acabaron siendo eliminados.

Como publica la noticia, se presentaron cargos criminales contra nueve compañeros de instituto: "Siete de ellos, mujeres de entre 16 y 17 años, por acoso. Y dos hombres, Austin Renaud, de 18 años, acusado de tener sexo con Phoebe, menor, y Sean Mulveyhill, de 17 años, también por sexo con una menor y por acoso."

La historia de Ryan Halligan (RyanPatrickHalligan, 2010)

Fuente: http://www.ryanpatrickhalligan.org/ y *Wikipedia* (http://es.wikipedia.org/wiki/Ryan_Halligan)

Al igual que ocurre con la mayoría de casos que hemos visto de ciberacoso entre menores, éstas suelen tener sus inicios a raíz de algunas relaciones entre compañeros en el instituto.

Ryan Halligan fue un joven adolescente que se suicidó a los 13 años tras sufrir acoso y ciberacoso por parte de algunos compañeros de secundaria.

Vivía en Essex Junction, Vermont, y a los 10 años empezó a sufrir acoso moral a causa del trastorno del aprendizaje que padecía. A raíz de una pelea en febrero de 2003, que fue disuelta por el subdirector del instituto, el acoso cesó durante un tiempo y acosador y víctima se acabaron convirtiendo en amigos.

Sin embargo, tras una visita al hospital, Ryan informó a su nuevo amigo sobre el examen vergonzoso al que le habían sometido y éste aprovechó dicha información para difundir el rumor de que Ryan era gay.

A causa de estos comentarios Ryan fue ciberacosado por sus compañeros, que se burlaban de él, a través de programas de mensajería instantánea como AIM. Muchas de estas conversaciones fueron encontradas archivadas en una carpeta del disco duro de la víctima en las que, además de encontrar burlas y humillaciones, su

padre descubrió que Ryan había estado hablando sobre muerte y suicidio con otro *ciberamigo* semanas antes de acabar con su propia vida.

Una mañana de octubre de 2003, la hermana de la víctima encontró el cuerpo sin vida del joven Ryan. Éste se había ahorcado animado por los consejos de su *ciberamigo*.

Tras lo sucedido, el padre de la víctima presionó para que se aprobaran leyes en Vermont para mejorar la forma en que las escuelas afrontan el acoso escolar y la prevención del suicidio. Además, este caso ha sido citado por los legisladores en diversos estados para proponer textos legislativos para frenar el ciberacoso.

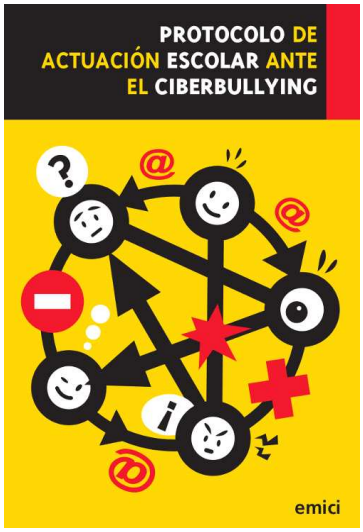
5.2.6 Enlaces de interés

A continuación citaremos algunos enlaces de interés y guías sobre el tema que nos ocupa:

- www.ciberbullying.com
- www.pantallasamigas.net
- http://www.protegeles.com/
- www.segu-kids.org
- www.inteco.es (Instituto Nacional de Tecnologías de la Comunicación)
- *Guía de actuación contra el ciberacoso* para padres y educadores, publicado por INTECO y el ministerio de Industria, Energía y Turismo de España:

http://menores.osi.es/sites/default/files/Guia_lucha_ciberacoso_menores_osi.pdf

- www.protocolo-ciberbullying.com



- www.emici.net (Equipo Multidisciplinar de Investigación del Ciberbullying)

- *Guía legal sobre ciberbullying y grooming*, publicado por el Observatorio de la Seguridad de la Información de INTECO

  https://www.inteco.es/guias/guiaManual_groming_ciberbullying

- EU Kids Online

  http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/WebsitesInNationalLanguage/spain.aspx
  http://www.sociologia.ehu.es/s0018-eukidshm/es/

- *Ciberbullying: Guía de recursos para centros educativos en caso de ciberacoso*, editada por el Defensor de Menor de la Comunidad de Madrid

  http://menores.osi.es/educadores/recursos-pedagogicos/ciberbullying-guia-de-recursos-para-centros-educativos-en-casos-de-c

- Centro de seguridad de las principales redes sociales:
    - Facebook:
        - https://www.facebook.com/safety
    - Twitter:
        - https://support.twitter.com/groups/57-safety-security
    - Youtube:
        - http://www.youtube.com/yt/policyandsafety/es/safety.html
    - Habbo Hotel:
        - http://www.habbo.es/safety/safety_tips
    - Instagram:
        - https://www.facebook.com/help/instagram
    - Google+:
        - https://www.google.com/intl/es/+/safety/

5.3 Grooming

5.3.1 Definición

Ya hemos visto en la definición de ciberacoso, que éste únicamente incluía intimidaciones y humillaciones hacia la víctima sin ningún objetivo sexual.

Cuando el acoso hacia el menor contiene elementos de índole sexual, éste pasa a ser lo que hoy en día se conoce como **grooming**.

En resumen, y tal como se define en la *Guía legal sobre ciberbullying y grooming* publicada por INTECO, grooming es un término anglosajón que se define como "un acoso ejercido por un adulto y se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor. Se podría decir que son situaciones de acoso con un contenido sexual explícito o implícito" (INTECO, 2009).

Las características principales de este tipo de ciberacoso son las siguientes:

- **Adultos contra menores.** Esto ocurre en la gran mayoría de los casos, en la que el acosador es un adulto que se aprovecha de la vulnerabilidad de un menor de edad.

- **Contiene elementos de índole sexual.** En caso contrario, estaríamos hablando del ciberacoso que hemos estudiado en el punto anterior.

- **El medio utilizado para llevar a cabo el caso sea tecnológico.** Al igual que ocurría en el ciberacoso, los acosadores utilizan cualquiera de los medios siguientes para extorsionar a la víctima:

    - Conversaciones a través de chats y programas de mensajería instantánea

    - Compartición de contenido multimedia, como imágenes o fotos comprometedoras. Por ejemplo, fotos del menor en una pose sexy o desnudos que más tarde podrá utilizar el acosador para chantajear y extorsionar al menor.

    - Publicaciones en redes sociales

    - Videoconferencias a través de una **webcam**. Suelen ser bastante comunes en estos casos, en los que el acosador convence a la víctima que se desnude para él delante de la cámara o realice actos de tipo sexual.

- En algunos casos, los acosadores consiguen o roban datos privados de sus víctimas, tienen acceso a sus contactos y extorsionan a los

menores, amenazándolos con distribuir alguna imagen comprometedora de ellos, para conseguir más de ellos y mantener la relación de abuso.

- Otra de las acciones que toman los acosadores son actos de seguimiento, envío de regalos u objetos o pequeños actos de sabotaje sobre sus propiedades.

- Puede llegar a ser una de las consecuencias del denominado sexting o tendencia de algunos menores a realizarse fotografías íntimas y colgarlas en determinados lugares en Internet, bien sean públicos o supuestamente privados, en el caso que llegasen a manos inadecuadas.

- Este tipo de acoso lo suele afectar principalmente a las **chicas**.

Además, en el cuaderno de criminología titulado *El ciber-acoso con intención sexual y el child-grooming* (http://dialnet.unirioja.es/servlet/articulo?codigo=3795512) se distinguen cuatro fases principales por las que el adulto consigue hacerse con la confianza del menor y consumar el abuso:

- **Contacto y acercamiento**: el ciberacosador contacta con un menor a través de internet (Messenger, chat o redes sociales frecuentadas por menores). Finge ser alguien atractivo para el menor (otro menor de edad similar, buen parecido físico, gustos similares...), enviándole incluso imágenes de un menor que haya conseguido en la Red que responda a dichas características; es decir, lleva a cabo una estrategia preconcebida con el fin de ganarse su confianza poco a poco.

- **Sexo virtual**: consigue, en el transcurso de dicha relación, que el menor le envíe alguna fotografía comprometida, logrando que encienda la web-cam, pose denudo...

- **Ciberacoso**: si el menor no accede a sus pretensiones sexuales, el ciberacosador le amenaza con difundir la imagen que le haya capturado con mayor carga sexual a través de internet (YouTube...) y/o enviarla a los contactos personales del menor.

- **Abuso-agresiones sexuales**: ante las amenazas del ciberacosador, el menor accede a todos sus caprichos sexuales, llegando incluso, en algún caso, a contactar físicamente con el menor y abusar sexualmente de él. (Panizo, 2011)

Por tanto y partiendo de esta información, podríamos definir los perfiles de los roles que participan en esta acción:

- **Acosador**. En el caso concreto del grooming, los acosadores son principalmente gente adulta. Según explican desde el Grupo de

Delitos Telemáticos de la Guardia Civil, en uno de los últimos estudios realizados con la colaboración de la Universidad de Jaén (y cuya referencia podremos encontrar en la *Guía de actuación contra el ciberacoso*), apuntaba a "gente de mediana edad, de entre los 30 y 40 años, de familias desestructuradas y que vivían solos. Es un estudio basado en una muestra pequeña y, por el contrario, nosotros en el Grupo de Delitos Telemáticos hemos encontrado cosas de todo tipo, chicos de 16-17 años que están intentando acosar sexualmente a niñas de 10 años o de 14, e incluso hemos visto mujeres, que es bastante sorprendente, que se dedican a acosar a menores" (Lorenzana, 2012).

Además, la página web http://www.quenoteladen.es/, dedicada a la lucha para la prevención del grooming y acoso sexual, distingue entre tres tipos distintos de acosadores:

- **Acosador directo.** Son aquellos que frecuentan foros, chats, redes sociales o páginas con el objetivo de identificar menores. Tras esto, suelen presionar a las víctimas para conseguir unas primeras imágenes comprometedoras, por ejemplo, a través de la webcam. No es raro que estos acosadores sean del entorno y acosen también a otros adultos.

- **Acosador oportunista. "**Se trata de aquellos individuos que encuentran en Internet imágenes íntimas de menores, no necesariamente pornográficas, y las convierten en objeto de su acoso." A través de ellas, intentarán chantajear a la víctima amenazándola con difundir a nivel global las fotos o vídeos que ha encontrado, o incluso enviarlos directamente a los conocidos, familiares, etc, del/la menor.

- **Acosador específico**. "Se trata de pedófilos con un objetivo muy claro: obtener del menor imágenes pornográficas y, si las distancias lo permiten, establecer contacto sexual con el menor. Normalmente se trata de individuos que dedican tiempo al acercamiento, que pretenden ganarse primero la confianza del/la menor y que intentan pasar desapercibidos. Son los más difíciles de identificar y los que más información e imágenes suelen obtener."

- **Víctima**. En este caso no existe ningún perfil específico, cualquier persona podría ser la víctima. Principalmente este tipo de acoso

afecta a las chicas, aunque también existen casos en los que las víctimas son jóvenes varones

En este caso y, a diferencia de lo que ocurría en el ciberacoso que hemos estudiado, únicamente dos personas participan en la acción. Además, no suele haber espectadores ni reforzadores o apoyadores de cualquiera de los dos roles. En estos casos, la víctima suele sentirse avergonzada de sus acciones y le cuesta más compartir con alguien su situación. Del mismo modo ocurre con el acosador, que suele ser una persona adulta y, por tanto, es bastante más madura y consciente de que sus acciones son perseguidas por la ley.

Una vez conocidas las principales características de este tipo de acoso, comentaremos algunos datos sobre la relevancia de este problema en nuestro país y expondremos algunas recomendaciones.

5.3.2 Algunos datos

El estudio "Hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza en sus padres" (http://www.pantallasamigas.net/estudios-realizados/inteco-estudio-habitos-seguros-uso-tic-menores-econfianza-padres-pantallasamigas.shtm) en su edición de marzo de 2009 y realizado por el Instituto Nacional de Tecnologías de la Comunicación, más conocido como INTECO, recoge a modo de resumen las siguientes conclusiones: "…el acoso sexual se posiciona como el riesgo que más preocupa a los padres, de todos los analizados (6 de cada 10 lo considera grave o muy grave). La alta preocupación que los padres muestran hacia la situación no se traduce en una elevada incidencia. Más bien al contrario, con un 1% de casos declarados por los menores, el riesgo de grooming es, de todos los analizados, uno de los que presenta menores tasas de incidencia reconocida." (INTECO, 2009)

En el siguiente gráfico de barras se observa el grado de conocimiento entre padres e hijos españoles sobre el problema del acoso sexual:

Gráfico 80: Conocimiento del riesgo de acoso sexual (%)

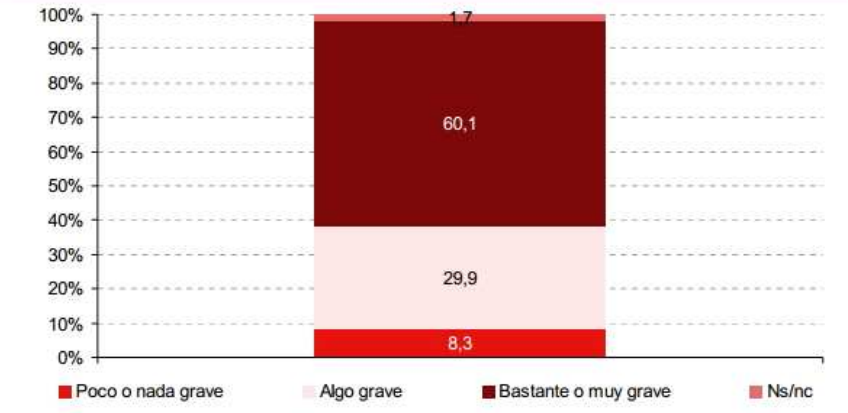
Fuente: INTECO

Por tanto, más del 50% de los entrevistados son conscientes de esta amenaza a la que se exponen al hacer uso de las TIC. Aunque los datos están bastante igualados entre padres e hijos, los padres son quienes más manifiestan conocer este riesgo.

En el caso de los menores entrevistados, el estudio concluye que existe un conocimiento significativamente más alto entre las niñas (62,2%) que entre los niños (39,7%).

También se preguntó a los padres sobre la clasificación que harían al riesgo del acoso sexual en cuanto a la consideración de la gravedad del problema. Los resultados se muestran en la siguiente imagen:

Gráfico 81: Gravedad adscrita por los padres al riesgo de acoso sexual (%)

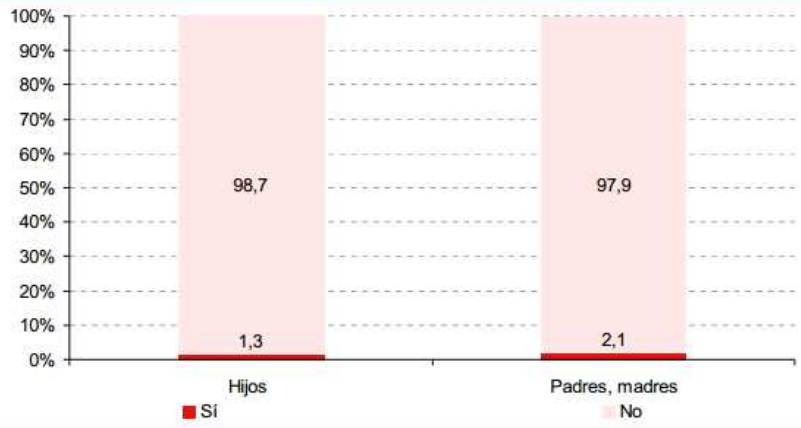


Fuente: INTECO

Por tanto, más de la mitad de los padres (60,1%) lo consideran un riesgo muy grave, frente a casi un 30% que lo considera algo grave.

Partiendo de la muestra de entrevistados que se sometió al estudio, únicamente un 2,1% de los padres y un 1,3% de los hijos afirman que los menores han estado expuestos a situaciones que identifican como grooming o acoso sexual:

Gráfico 82: Incidencia directa de acoso sexual (%)

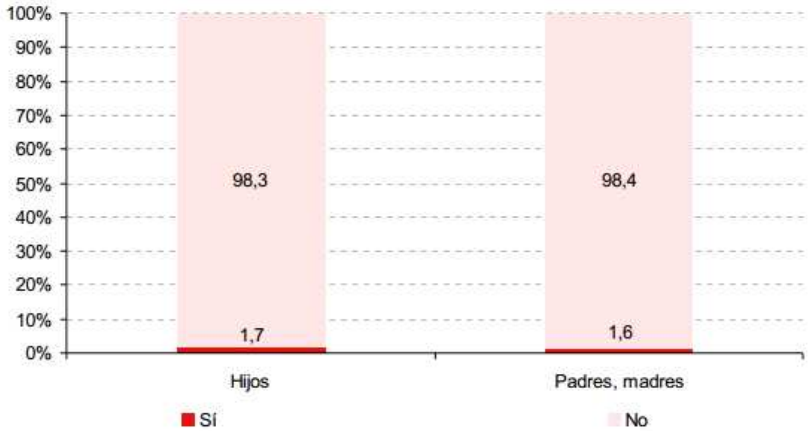


Fuente: INTECO

Como se observa en el gráfico, se presenta una desviación en un punto en cuanto a las respuestas de padres e hijos. En este caso, los padres parecen tener una percepción más estricta sobre la consideración de qué se considera acoso sexual.

Finalmente se preguntó sobre la incidencia del acoso sexual no directamente sobre el menor, sino sobre alguien de su entorno:

Gráfico 83: Incidencia indirecta de acoso sexual (%)



Fuente: INTECO

En este caso las percepciones son aún más bajas y no existe apenas diferenciación entre la percepción de padres e hijos.

Finalmente, con los datos recogidos en las últimas oleadas de estudios realizados por el INTECO sobre las situaciones de riesgo para menores conocidas por los padres, podemos observar las conclusiones en la siguiente tabla comparativa:

Situaciones de riesgo para menores conocidas por los padres

	may-ago'11	sep-dic'11	ene-abr'12
Haber sido objeto de acoso sexual	1,5%	1,9%	0,6%
Citarse a solas con adultos o desconocidos	3,7%	2,0%	1,1%
Tratar con adultos que se hacen pasar por niños	5,6%	3,3%	3,1%

Fuente: Observatorio INTECO

Observando los datos mostrados en la tabla, vemos cómo el número de situaciones de riesgo para menores conocidas por los padres ha disminuido entre el segundo cuatrimestre de 2011 y el primero de 2012. Hay que tener en cuenta siempre que el estudio se realizó sobre una muestra representativa (3.646 usuarios en el caso de la 18ª oleada del primer cuatrimestre de 2012) y que, por tanto, hay que tomar estas cifras con cautela.

Por otra parte, recordemos el estudio realizado por la red europea de investigación EU Kids Online del que habíamos hablado en el punto anterior sobre ciberacoso.

Cuando se les preguntó a los niños sobre los tipos de mensajes sexuales que éste había encontrado online en los últimos meses, las respuestas fueron las mostradas en la siguiente tabla resumen:

Tabla 21. Tipos de mensajes sexuales que el menor ha encontrado online en los últimos doce meses, por edad (+11 años)

%	Edad				Todos
	9-10	11-12	13-14	15-16	
Me han enviado un mensaje de contenido sexual en internet	n.r.	1	3	8	4
He visto un mensaje de contenido sexual que había sido colgado en Internet y que también podían ver otras personas	n.r.	1	3	5	3
He visto a otras personas practicando actividades sexuales	n.r.		5	3	3
Alguien me ha pedido que hable sobre practicar actividades sexuales en internet	n.r.	1	1	2	1
Me han pedido una foto o video mostrando mis órganos sexuales en internet	n.r.	1	0	0	0
Ha visto o recibido de cualquier tipo	**n.r.**	**3**	**10**	**13**	**9**

QC169: Durante los ÚLTIMOS 12 MESES, ¿has hecho alguna de estas cosas en internet…?

Base: Todos los menores que usan internet en España entre 11 y 16 años.

EU Kids Online (2011) – *Tipos de mensajes sexuales que el menor ha encontrado online en los últimos 12 meses, por edad (+11 años)*

Si nos fijamos en los dos últimos puntos de la tabla, éstos hacen referencia a lo que podría llegar a convertirse en una de las primeras fases del grooming en las que el acosador intenta conseguir una primera imagen comprometida del menor.

Según resume el informe:

- El porcentaje de menores a los que alguien (a través de internet) les ha pedido hablar de sexo o enviar una fotografía o video suyo mostrando sus órganos sexuales es muy bajo. Alrededor del uno por ciento en España y del 2% en Europa. En el caso de los menores de 15 y 16 años también se observa un aumento pero dentro de una incidencia muy baja. (EU Kids Online, 2011)

Para más información sobre los resultados del estudio, consultar el informe que se puede obtener a través del enlace: http://www.sociologia.ehu.es/s0018-eukidshm/es/

5.3.3 Cómo detectarlo

Como hemos comentado a lo largo de este punto, el grooming no es más que un tipo concreto de ciberacoso en el que entran en juego elementos de tipo sexual.

Por tanto, los síntomas que presentan las víctimas de este tipo de extorsión suelen ser los mismos que se han expuesto en el apartado correspondiente al ciberacoso.

Sin embargo, algunas de las manifestaciones descritas en el apartado al que hacemos referencia, en algunos casos podrían verse acentuadas, debido al miedo o chantaje que pueda estar sufriendo el menor.

5.3.4 Consejos y recomendaciones

Partiendo de las recomendaciones enumeradas en el apartado de ciberacoso, destacamos y añadimos los siguientes consejos que ha de tener en cuenta el menor y que se han recopilado consultando las diferentes guías y páginas web que se listan en el apartado *Enlaces de interés* del presente punto de la memoria:

- Rechazar los mensajes de tipo sexual o pornográfico. El menor debe exigir, ante todo, respeto.
- Que el menor evite publicar fotos suyas o de sus amigos en sitios públicos.
- Utilizar perfiles privados en las redes sociales.
- Analizar las fotos que se van a subir a las redes sociales y asegurarse de que no tienen un componente sexual. Hay que pensar en las consecuencias a la hora de compartir estas imágenes y pensar en quién puede llegar a verlas.
- Filtrar las amistades que se agregan en las redes sociales. No aceptar a personas que no hayamos visto físicamente y a quienes no conozcamos bien.

- Que el menor respete tanto sus propios derechos como los de sus amigos/as. Hay que guardarse el derecho a la privacidad de sus datos personales y de su imagen.

- Utilizar contraseñas privadas y complejas.

- Evitar incluir información personal como la edad en los *nicknames*

- Si se ha producido una situación de acoso guardar todas las pruebas que se pueda: conversaciones, mensajes, capturas de pantalla, etc.

- Ante estas situaciones, no ceder al chantaje. La víctima deberá animarse a hablar con sus padres o alguna persona adulta de confianza. Ante cualquier duda, consultar páginas de ayuda contra el acoso como http://www.protegeles.com/

En cuanto a los padres, volver a recordar que cualquier acción preventiva pasa por una buena educación de los hijos en cuanto a los peligros que se pueden encontrar en Internet y sus consecuencias. Además, sería recomendable que siguieran los siguientes consejos:

- Involucrarse y aprender a manejar las nuevas tecnologías. Le ayudará a saber qué hace su hijo cuando está conectado y los posibles riesgos a los que se enfrenta.

- Enseñar a los hijos a ignorar el spam y a no abrir archivos que procedan de personas que no conozca personalmente o sean de su confianza. Explicarles que existen programas capaces de descifrar nuestras claves de acceso al correo electrónico.

- Situar el ordenador de la casa en una habitación de uso común, donde pueda tenerlo controlado. Evitar, en lo posible, colocarlo en el dormitorio de los hijos.

- Limitar la conexión de los menores a los momentos en los que se encuentren acompañados por los padres o cualquier otro adulto.

- Intentar controlar el uso inadecuado de la webcam. Además, siempre se puede restringir su uso mediante una clave de seguridad que sólo los padres conozcan.

- Controlar las fotos publicadas por ellos mismos y por el menor en la red. No se trata de prohibir, sino de conocer las fotos publicadas.

- Alimentar la confianza de los hijos, para que en caso de verse envueltos en cualquier acción sospechosa, puedan confiar en ellos y

se sientan impulsados a contarles la situación en la que se encuentran.

- Cuando los padres o responsables legales del menor tienen conocimiento expreso de la situación, denunciarlo antes las autoridades pertinentes. Desde el Grupo de delitos Telemáticos de la Guardia Civil avisan que "No se trata únicamente de poner fin a estas situaciones, cosa prioritaria, sino de localizar al responsable para evitar que se repitan en el futuro o con otras víctimas potenciales. En muchas ocasiones, los acosadores no actúan contar una sola víctima, sino que disponen de varios "contactos" a los que regularmente acosan." (GDT de la Guardia Civil, 2011)

Además de forma preventiva existen también, como hemos comentado en las recomendaciones ante el ciberacoso, los software de control parental que permiten limitar las horas que el menor pasa delante de la pantalla e incluso monitorizar la actividad del menor en la red en los casos en que los padres crean conveniente para su seguridad.

5.3.5 Estudio de casos

A continuación comentaremos algunos casos reales de *grooming* que se han conocido tanto en nuestro país como en otros países del mundo.

Casos nacionales

Mi 'ciberamigo' me chantajea (Espinosa, 2009)

Noticia publicada por el periódico El País el 15 de junio de 2009: http://elpais.com/diario/2009/06/15/sociedad/1245016805_850215.html

Un joven estudiante en Sevilla de 24 años fue arrestado y encarcelado por acosar y extorsionar hasta 250 jóvenes, la mayoría chicas menores de edad de toda España e incluso alguna extranjera.

Como hemos comentado en las fases de este tipo de acoso, el acosador se había inventado hasta 12 personalidades distintas para ganarse la confianza de sus víctimas y conseguir así más información e imágenes de ellas. Cuando la amistad se consolidaba y reunía material suficiente, el acosador desvelaba su verdadero rostro.

En 2008 hubo una investigación inicial partiendo de una denuncia registrada en Madrid, en la que una joven contaba cómo estaba siendo víctima de un chantaje a través de Internet. Esta denuncia permitió seguirle la pista al acosador y en octubre de 2008 el acosador fue localizado y detenido, aunque finalmente quedó en libertad. Sin embargo, se le intervinieron dos ordenadores portátiles y dos discos duros y tras analizar el material que contenían se constató la existencia de más víctimas. Esto abrió una segunda investigación que permitió cifrar el número total de víctimas que conocemos. Además de imágenes de éstas, se conoce que el acosador utilizó programas de control remoto para acceder a contenido de cuentas y archivos personales de sus víctimas y así tener más material con el que chantajearlas.

En Junio de 2009 se volvió a detener al acosador y esta vez fue enviado a prisión.

Un detenido en Gandia por acosar a 300 niñas en Internet (Almenar, 2013)

Noticia publicada por el periódico El País el 1 de abril de 2013: http://ccaa.elpais.com/ccaa/2013/04/01/valencia/1364808608_611228.html

El pasado mes de marzo se detuvo en la localidad valenciana de Gandia a un hombre de 27 años por acosar supuestamente a 300 niñas a través de Internet.

Al igual que ocurre con la mayoría de acosadores, se hacía pasar por un menor para ganarse la confianza de las víctimas a través de la web y redes sociales y, tras conseguir su amistad, les hacía propuestas de índole sexual. Además, habitualmente les mostraba imágenes de contenido pornográfico e incluso llegó a captar fotografías de las víctimas mostrando sus cuerpos desnudos. También intentó quedar personalmente con ellas, pero afortunadamente no lo consiguió.

El acosador está actualmente en libertad con cargos, aunque la investigación continúa abierta para determinar el grado de ejecución de los delitos.

Detenido un presunto acosador de adolescentes a través de Facebook (EFE, 2011)

Noticia publicada por el periódico El País el 5 de mayo de 2011: http://elpais.com/elpais/2011/05/05/actualidad/1304583471_850215.html

En mayo de 2011 fue detenido un hombre de 30 años de la localidad catalana de Sant Pere de Ribes por acosar presuntamente hasta una docena de jóvenes entre 12 y 13 años de edad.

El acosador duplicó el perfil de Facebook de una joven de 12 años y, aprovechándose de su perfil, se hacía pasar por ella para contactar con sus amigas y conseguir así información. Cuando ya había recogido suficiente, la utilizaba para presionar y amenazar a la víctima con llamadas y mensajes con la intención de quedar para tener relaciones sexuales. Afortunadamente se estima que el detenido no tuvo tiempo de encontrarse con ninguna de ellas.

Finalmente el acosador fue puesto en libertad con cargos.

Tras este incidente, los centros escolares se animaron a repetir campañas de sensibilización a los jóvenes sobre los riesgos que conlleva la red tal y como la conocemos hoy en día.

LUCIA13. Diario de un acoso en la Red (Abril y Pérez-Lanzac, 2007)

Reportaje publicado por el periódico El País el 25 de noviembre de 2007: http://elpais.com/diario/2007/11/25/eps/1195975611_850215.html

Aunque no se trate realmente de un caso de grooming en todo el sentido de la palabra, hacia la mitad del reportaje se transcribe la conversación de messenger mantenida entre acosador y víctima que presentó un padre a la policía y que permitió detener a uno de los pedófilos más activos en la red.

Se trata de un relato muy interesante, pues las intenciones del acosador y el chantaje quedan patentes enseguida.

El acosador entraba en contacto con las menores en algún chat fingiendo ser una chica de 14 años. Les pedía su cuenta de Messenger, las agregaba como contacto y les enviaba un virus a través del cual podría obtener la clave de acceso a su correo electrónico para obtener más información.

La conversación publicada y que presentó el padre de una joven catalana de 14 años fue la siguiente:

LucySoto. Ola perdona si te he agregado.

Bea. Ola.

LucySoto. Es q tengo algo importante q decirte.

Bea. A mi? k?

LucySoto. Te he cambiado tu contraseña y pregunta secreta [necesarias para activar la cuenta de Messenger] si cierras tu msn no podras abrirlo.

LucySoto. Te he robado tu msn te lo devolvere.

LucySoto. Solo quiero q me hagas un favor.

LucySoto. Contesta o me meto en tu msn.

Bea. Oyeee komo sabes mi clave?

LucySoto. Tu pregunta secreta era muy facil.

LucySoto. Me podrias hacer el favor que te pedi?

Bea. K favor era?

LucySoto. Conoces a una Rosita?

Bea. Si k la conozco

LucySoto. A ella tambien le hice lo mismo hace 2 semanas y le devolvi su msn porque ella me hiso un favor.

Bea. K favor era?

LucySoto. Primero quiero conocer con quien hablo.

LucySoto. Me llamo lucy y tengo 14 años tu?

LucySoto. Date prisa q me meto en tu msn y no hables con nadie.

Bea. Bea.

LucySoto. Soy de argentina tu?

Bea. España.

Bea. X favor me puedes devolver el msn.

LucySoto. Primero ponte la cam pa conocerte ok?

Bea. Ok.

LucySoto. No te veo bien.

LucySoto. Acomodala.

Bea. Aora?

LucySoto. Ok te pedire lo mismo q a tu amiga.

LucySoto. Primero quiero q sepas q soy les [lesbiana] no te molesta?

Bea. Yo soy bi.

LucySoto. Preguntale a tu amiga lo q le pedi y luego me dices si puedes hacerlo ok.

LucySoto. Pero date prisa.

[…]

Bea. Me vas a devolver el msn?

LucySoto. Si.

Bea. Seguro.

LucySoto. A tu amiga se lo devolvi.

LucySoto. Tengo un minuto date prisa.

Bea. Tengo k ensenyarte las tetas no?

LucySoto. Si.

LucySoto. Las dos.

[…]

Bea. Ya ta no?

LucySoto. Ok.

Bea. Me devuelves el msn xfavor?

(Abril y Pérez-Lanzac, 2007)

En mayo de 2007, la persona tras el *nick* LucySoto fue detenida gracias a la denuncia de "Bea" (el nombre real nunca fue revelado) y otras de sus víctimas. Resultó ser un peruano de 32 años al que se acusó de robo de contraseñas, coacciones y abusos sexuales.

Además, el reportaje publica otros casos y unos consejos básicos a tener en cuenta para evitar estos tipos de riesgos.

Casos internacionales

La policía alerta del chantaje con fotos íntimas de menores (Duva, 2008)

Noticia publicada por el periódico El País el 25 de marzo de 2008: http://elpais.com/diario/2008/03/25/sociedad/1206399608_850215.html

A principios de 2008 fue detenido un joven peruano de 29 años por extorsionar a dos niñas.

El acosador, Ricardo Javier Mendoza Navarro, empezó su táctica haciéndose pasar por una niña y así lograr ganarse la confianza de la mayor de dos hermanas (de 16 años). Tras esto, logró seducirla para obtener fotos y vídeos de índole sexual. Una vez prevenido de este contenido, amenazó a la joven con difundir esas imágenes entre sus amigas y conocidos.

Más tarde consiguió hacer lo mismo con la hermana pequeña de 12 años. Tras obtener tanto material, el acosador empezó a exigir dinero a la familia de las niñas a cambio de no difundir el contenido por Internet, llegando a ganar casi 5000 euros.

A finales de 2007 el padre de las víctimas se animó a denunciar el caso a la Policía, y el acosador fue finalmente detenido en Perú y acusado de distribución de pornografía infantil a través de Internet, extorsión de menores y exhibicionismo sexual a menores.

Tras la investigación, se comprobó que las dos hermanas no habían sido las únicas víctimas de este acosador.

Declaran culpable a imputado en primer juicio por "grooming" y ***Tribunal condena a 5 y medio años de presidio efectivo a autor de "grooming" (El Mercurio Online, 2008)***

Noticias publicada el 12 y el 17 de noviembre de 2008:

http://www.emol.com/noticias/nacional/2008/11/12/330490/declaran-culpable-a-imputado-en-primer-juicio-por-grooming.html

http://www.emol.com/noticias/nacional/2008/11/17/331231/tribunal-condena-a-5-y-medio-anos-de-presidio-efectivo-a-autor-de-grooming.html

Las noticias relatan el primer condenado en Chile por *grooming*. Se trata de José Duarte Caroca, quien por entonces era un joven universitario de 26 años de edad.

Éste fingió ser un adolescente para ser aceptado dentro de los contactos de chat de una menor de 12 años. Tras ganarse su confianza, le propuso que posara desnuda frente a la cámara web, exhibiendo sus pechos y

genitales. Con estas imágenes obligó a la menor a repetir las sesiones bajo la amenaza de hacer llegar las fotografías a su madre y amigos.

Finalmente, la madre de la menor denunció el acoso y el joven fue condenado a 5 años y medio de cárcel por los delitos de abuso sexual infantil, producción y almacenamiento de material pornográfico infantil e infracción a la ley informática.

5.3.6 Enlaces de interés

A continuación se listarán un conjunto de enlaces a páginas web de interés y algunas campañas o manuales de actuación ante el *grooming*. También se pueden consultar las citadas en el mismo apartado del punto anterior, pues el ciberacoso y el grooming están íntimamente relacionados y las webs dedicadas a la lucha contra los riesgos de internet suelen abordar ambos problemas.

- www.internet-grooming.net
- El ciber-acoso con intención sexual y el child-grooming, Quadernos de Criminología, número 15, 2011 (http://dialnet.unirioja.es/servlet/articulo?codigo=3795512)
- Web http://www.quenoteladen.es. Helpline para la prevención del grooming o acoso sexual.
- Web www.segu-kids.org
- *Guía legal sobre ciberbullying y grooming*, publicado por el Observatorio de la Seguridad de la Información de INTECO

  https://www.inteco.es/guias/guiaManual_groming_ciberbullying

- EU Kids Online

http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/WebsitesInNationalLanguage/spain.aspx
http://www.sociologia.ehu.es/s0018-eukidshm/es/

- http://www.protegeles.com/

- Página web del Grupo de delitos Telemáticos de la Guardia Civil: https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

5.4 Otros

Acabamos de describir los dos problemas principales que afectan directamente a los menores de edad y que más preocupan a padres y educadores. Sin embargo, existen otros riesgos conocidos y, aunque no dejan de ser importantes, algunos de ellos son riesgos directamente relacionados con los problemas de ciberbullying y grooming que acabamos de desarrollar y que, por tanto, únicamente definiremos y comentaremos algunos datos relevantes.

Así por ejemplo, existe la práctica hoy en día conocida como sexting, en la que dos personas intercambian mensajes e imágenes de índole sexual a través de sus smartphones. Lo que de primeras parece un simple intercambio de mensajes subidos de tono puede acabar creando una situación de extorsión por parte del receptor de las imágenes al emisor y acabar así desencadenando un caso de grooming.

De la misma manera, el receptor de estos mensajes podría ser un pederasta potencial coleccionista de imágenes que pueda llegar a difundirlas reforzando así el problema de la pornografía infantil.

Igualmente ocurre con el Happy Slapping, una práctica moderna consistente en la filmación de palizas proporcionadas a las víctimas de forma repentina y sin aviso para después subirla a la red consiguiendo humillarlas e intimidarlas. En este caso se trataría de uno de los recursos de los ciberacosadores.

Finalmente hablaremos de las estafas que se pueden cometer en Internet a través del spam o phising que, aunque afectan a todos los usuarios por igual, los menores quizá sean, por inmadurez, los más vulnerables a caer en las trampas de estos estafadores.

Veamos pues algunos de estos riesgos a los que nos exponemos hoy en día al utilizar las nuevas tecnologías.

5.4.1 Pornografía Infantil

Se denomina **pornografía infantil** a la reproducción y difusión sexualmente explícita de la imagen de un menor a través de fotografías o vídeos.

La distribución de este tipo concreto de pornografía está íntimamente relacionada con los términos pedófilo y pederasta, aunque cabría diferenciar el significado de cada uno de ellos:

- Se llama **pedófilo** a aquél individuo que siente atracción sexual exclusivamente por menores, aunque no necesariamente lleve a cabo sus fantasías sexuales.

- En cambio, se considera **pederasta** a aquél individuo que, no siendo esta su única opción sexual, sí que mantiene relaciones sexuales con menores.

Por tanto, y teniendo en cuenta ambas definiciones, podríamos estar ante el caso de un pederasta que no sea un pedófilo, de la misma manera que un pedófilo podría no ser un pederasta. Sin embargo, aquél individuo que siente atracción sexual exclusivamente por menores y lleva a cabo sus fantasías sexuales sería considerado ambos, un pedófilo y pederasta.

Estimular, engañar o presionar a los niños a participar en sesiones fotográficas o vídeos pornográficos o con actitud sexual implica una forma de explotación a los menores y que atenta directamente contra la dignidad de los niños. Es por ello que se considera una práctica completamente **ilegal** y está recogida en las leyes vigentes de cada país. En el apartado *Legislación* de esta memoria encontraremos todas las leyes referentes a este tema existentes en España en la actualidad.

Además, es muy común que el adulto intente ganarse la confianza y el cariño del menor para conseguir llevar a cabo sus objetivos. Como hemos explicado en el apartado de *grooming*, muchos agresores de esta índole utilizan las nuevas tecnologías para ganarse la confianza del menor a través de chats, fotoblogs o foros, hasta que consiguen que el propio menor acceda a enviar una primera imagen con algún contenido sexual. De esta manera, acaba siendo el propio menor el que se ve envuelto en el proceso de difusión de estos contenidos. Tras esto, el agresor puede valerse del chantaje, ya sea con la promesa de regalos o

con la amenaza de difundir las imágenes que ya posee del menor, para conseguir más y más imágenes de éste o para lograr encuentros físicos con él.

Como ocurre con el tema del acoso entre menores u otros riesgos como el robo de identidad, se trata de problemas que han existido siempre, incluso antes de la aparición de Internet y los nuevos medios digitales. Sin embargo, el avance de las nuevas tecnologías ha derivado en un incremento masivo de la disponibilidad, accesibilidad y volumen de pornografía infantil. Tanto las redes sociales como las redes P2P han ayudado a incrementar esta cantidad de material pornográfico, haciéndolo accesible a cualquier tipo de usuario, compartiendo de forma gratuita y en toda la red ficheros etiquetados de una forma determinada. Por ello, a menudo se ha criminalizado el canal de comunicación por su uso indebido.

El lado positivo de todo esto, es que la llegada de Internet no ha favorecido únicamente la difusión de este tipo de contenidos, sino que también ha facilitado el descubrimiento de redes de pornografía tanto nacionales como internacionales. Las autoridades han desarrollado nuevas herramientas online para ayudar a esta causa beneficiándose de la carencia de anonimato absoluta en la redes informáticas, de forma que han conseguido desbaratar en muchas ocasiones redes de pornografía infantil gracias al rastreo de comunicaciones.

Las pruebas son el gran número de titulares relacionados con este tema que podemos encontrar hoy en día en los periódicos o en las noticias:

Detenidas 41 personas por compartir pornografía infantil el Internet Almenar, 2013)

Noticias publicada por el periódico El País el 29 de abril de 2013 (http://ccaa.elpais.com/ccaa/2013/04/29/valencia/1367232921_594526.html)

"*La Policía Nacional ha detenido e imputado a 41 personas en 18 provincias por tenencia y distribución de vídeos que mostraban abusos sexuales a niños de hasta ocho años, según ha informado este lunes la Policía Nacional en rueda de prensa. Los arrestados compartían archivos P2P a través de Internet en los que se veía abusos sexuales a menores…*" (Almenar, 2013)

Detenido un pederasta que contactó en la red con 380 chicos fingiendo ser modelo infantil (EFE, 2011)

Noticia publicada por el periódico El País el 8 de abril de 2011 (http://elpais.com/elpais/2011/04/08/actualidad/1302250635_850215.html)

"*Los Mossos d'Esquadra han detenido a un hombre de 33 años, que ya ha sido encarcelado por orden judicial, acusado de crearse una falsa identidad en Internet, donde se hacía pasar por modelo infantil para contactar con menores con fines sexuales…"* (EFE, 2011)

Detenidas 65 personas por el intercambio de imágenes de pederastia en Internet (Agencias, 2002)

Noticia publicada por el periódico El País el 18 de junio de 2002 (http://sociedad.elpais.com/sociedad/2002/06/18/actualidad/1024351202_850215.html)

"*Un total de 65 personas han sido detenidas hoy en Francia en una investigación sobre la posesión e intercambio de fotografías de carácter pederasta por Internet, han informado las autoridades francesas…"* (Agencias, 2002)

Una operación en 141 países identifica a cientos de pederastas en Internet (Agencias, 2012)

Noticia publicada por el periódico El País el 4 de julio de 2012 (http://sociedad.elpais.com/sociedad/2012/07/04/actualidad/1341388585_915148.html)

"*Una operación policial en 141 países ha permitido identificar a cientos de pederastas en Internet, según acaba de anunciar la policía austriaca. Este organismo ha conseguido localizar a 272 personas solo en Austria siguiendo el rastro de vídeos con contenidos pornográficos infantiles..."* (Agencias, 2012)

Pederastas españoles invaden la Red (El País, 2000)

Noticia publicada por el periódico El País el 20 de agosto de 2000 (http://elpais.com/diario/2000/08/20/sociedad/966722401_850215.html)

"*Los pederastas han encontrado en Internet el medio idóneo para comerciar con la pornografía infantil. Además, han hallado en el ciberespacio un refugio seguro donde insuflarse ánimos para luchar contra los remordimientos. La avalancha de pornografía infantil en la Red es tal que los ciudadanos han convertido este delito en el que mayor número de denuncias suscita en la página de la Guardia Civil instalada en la Red (www.guardiacivil.org)...*" (El País, 2000)

Tras las detenciones realizadas y la información obtenida a través de varios estudios sobre la problemática, desde la Asociación Contra la Pornografía Infantil se han llegado a definir las características que forman el perfil del pederasta de la siguiente manera:

- En el 90% de los casos se trata de varones.
- Suelen ser varones de mediana edad, entre los 30 y 45 años. Sin embargo, hoy en día el 20% de las agresiones sexuales son cometidas por menores de edad.
- Se encuentran integrados en la sociedad y con frecuencia están casados.
- En el 85% de los casos conocen a su víctima.
- En el 68% de los casos son padres o familiares, por lo que, además, se considera incesto.
- En el 80% de los casos no tienen antecedentes penales.
- En el 98% de los casos actúan solos.
- En más del 50% de las ocasiones sufrieron carencia de afecto durante sus años de infancia y adolescencia.
- En muchos casos, abusan del alcohol y presentan falta de empatía y baja autoestima.
- En la mayoría de las ocasiones no padecen trastornos psiquiátricos, sólo en ocasiones trastornos de la personalidad y algunas veces trastornos psicopáticos.
- Presentan un elevado índice de reincidencia.

Tras haber listado las características que definen al agresor, únicamente nos queda presentar unos consejos básicos a seguir para evitar que un menor se vea envuelto en esta circunstancia:

- Mantener círculos de confianza en las redes sociales y no agregar o conversar con extraños o personas que no conozcamos bien.
- En caso de contactar y *chatear* con un desconocido, evitar delatar información sensible, privada y/o personal.
- Tener siempre en cuenta que algunas personas, sobre todo en Internet, pueden llegar a aparentar lo que no son. Por tanto hay que ser cauteloso en estos casos y especialmente con personas que no conocemos o acabamos de conocer.
- No enviar fotografías íntimas a desconocidos ni publicar fotos personales y/o privadas en Internet y las redes sociales.
- En caso de encontrar algún sitio que distribuya pornografía infantil, informar a un adulto y tomar las medidas pertinentes. Habrá que informar inmediatamente a las autoridades.

5.4.2 Sexting

El **sexting** se define como la práctica en la que una persona, principalmente adolescentes, envía a través de mensajes multimedia contenidos de índole sexual producidos generalmente por el propio remitente a través de su teléfono móvil. Se trata de contenidos muy íntimos, entre los que podemos encontrar grabaciones de sonidos, fotos eróticas o vídeos propios en actitudes sexuales, desnudos o semidesnudos.

Los destinatarios de estos mensajes suelen ser las parejas de los remitentes aunque, en algunas ocasiones, estos mensajes se envían a otros amigos como un simple juego o incluso a desconocidos que los adolescentes encuentran a través de salas de chat o redes sociales.

El portal *Connect Safely* (http://www.connectsafely.org), destinado a informar sobre el impacto de la web social y ayudar a padres y adolescentes en la educación sobre una navegación segura en las

nuevas tecnologías, identifican a los principales destinatarios de este tipo de mensajes como:

1. alguien que les gusta (21%);
2. el novio o novia (20%);
3. el ex novio/a (19%);
4. amigos en general (18%);
5. su mejor amigo/a (14%);
6. desconocidos (11%)
7. compañeros de clase (4%) (Connect Safely, 2011)

Además, el objetivo principal que persigue esta práctica es la de tener un encuentro sexual con el destinatario; "inicialmente intrascendente, más tarde se convierte en algo sugerente y finalmente explícito", según comenta el *Urban Dictionary*.

Lo que mucho desconocen, es que enviando este tipo de contenido se están exponiendo a graves riesgos, pues al utilizar las nuevas tecnologías nos podría resultar muy fácil encontrar este material distribuido de forma masiva e incontrolada a través de la red. Además, cabe recordar que muchos acosadores utilizan este tipo de contenido para extorsionar a sus víctimas y acabar creando así una situación de *grooming* que hemos desarrollado en el apartado correspondiente de esta memoria.

Es por ello que hoy en día existen un gran número de campañas de concienciación sobre este peligro y que van dirigidas especialmente a los jóvenes, pues son los más vulnerables y los que, además, más tiempo dedican a esta actividad. El sitio web de Pantallas Amigas, por ejemplo, presenta una serie de videos llamativos en los que intenta ilustrar las consecuencias a las que nos exponemos al enviar este tipo de contenido:

www.sexting.es – *Vídeo campaña antisexting*

Según esta web, algunos de los factores que podrían llevar a los adolescentes a realizar esta práctica podrían ser:

- Creen que una imagen en un terminal móvil está segura y no son capaces de proyectar, de imaginar, las variadas formas en que esa imagen puede salir del dispositivo. Un robo, un error, una broma, un extravío... o la voluntad de su propietario.

- Confían plenamente en la discreción —cuando no en el amor eterno profesado— por parte del destinatario del envío. Carecen de experiencia vital suficiente que les invite a pensar en que las cosas, en la vida, cambian por muy diversos factores.

- Sienten cierta presión de grupo que les lleva a ganar notoriedad y aceptación en este contexto, el digital, tan importante para ellos. Este factor, añadido a la plenitud hormonal, puede generar combinaciones poco recomendables.

- Las influencias y modelos sociales distan del recato. La exhibición de relaciones sexuales o desnudos por personas no profesionales, comunes, abundan en la Red. Si pueden ver a cualquier persona anónima en su intimidad a través de la Red, no parece tan grave que uno aparezca de esta guisa. El desnudeo es algo común, hasta cierto punto normalizado.

- Desconocen las consecuencias que para su vida puede llegar a tener el hecho de que esa imagen comprometida sea de dominio público.

- La natural falta de percepción del riesgo que acompaña a la adolescencia y el espíritu transgresor desencadenan ciertos desafíos. En algunos casos resulta simplemente divertido, en otros, sirve para coquetear o dar otro contenido a una relación. (Sexting, 2009-2013)

Conscientes pues de los peligros a los que se exponen los menores al compartir estas imágenes tan íntimas, recopilaremos un conjunto de consejos o recomendaciones a tener en cuenta para evitar acabar envuelto en una situación comprometida a raíz de esta práctica cada vez más común entre los jóvenes:

- Normalmente el término *sexting* hace referencia al tráfico de imágenes y vídeos de índole sexual en mensajes enviados a través del móvil. Sin embargo, éste puede ocurrir también a través de otros dispositivos o en la web. Por tanto, hay que ser cautelosos con todo lo que enviamos, pues realizar este tipo de práctica puede tener serias consecuencias psicológicas e incluso legales, sobre todo en los casos en los que se vean envueltos menores de edad.

- Es **ilegal** difundir imágenes sexuales de un menor. Para una mayor seguridad, no compartir fotos íntimas propias o de cualquier otra persona.

- Pensar en las consecuencias emocionales a las que nos podemos someter si enviamos las fotos a alguien que creemos ser nuestro amigo y éste lo reenvía o lo distribuye entre otras personas, violando nuestra confianza. Además, hay que pensar en la huella digital de estas imágenes. Una vez alguien las comparte en la web es muy difícil asegurarnos que éstas se eliminan de forma permanente.

- Como hemos comentado, algunos acosadores pueden utilizar este material para presionar a la víctima, ya sea en forma de acoso sexual o cualquier otro tipo de acoso, como el ejercido por alguna expareja para reclamar algún tipo de venganza tras una ruptura. Por tanto, siempre es una mala idea compartir este tipo de contenido.

- Deberemos ser cautos al utilizar el medio digital. No todo el mundo es como aparenta y algunas veces la gente cambia y puede llegar a hacernos daño.

- Si recibimos alguna foto o vídeo de esta índole, no debemos reenviarla a nadie más, sobre todo si las imágenes involucran a un menor de edad. Recordemos que podría considerarse como distribución de pornografía infantil.

- Además, si recibimos este tipo de imágenes ofensivas deberemos eliminarlas y, en caso de ser víctima de algún tipo de acoso, hablar con un adulto de confianza y contarle la situación.

- Si la imagen involucra a algún amigo o persona conocida, la persona en cuestión a la que hace referencia el contenido deberá percatarse de la situación y tomar las medidas oportunas. Recordemos que se trata de una práctica ilegal.

- Si la recepción de estas imágenes continúa, la víctima y los padres deberán tomar las medidas oportunas y, en los casos más graves, acudir a las autoridades pertinentes y reportar la situación.

En cuanto a los padres, se recomienda también seguir los siguientes consejos:

- Lo más importante es mantener una buena charla con el menor. Mantener la calma, y explicarles lo más claramente posible el tema de la intimidad y privacidad de las personas y las consecuencias a las que se enfrentan al enviar este tipo de contenidos. Para ello, es necesario que los padres aprendan la mayor cantidad de información posible sobre el problema.

- Intentar controlar el uso inadecuado de la cámara del teléfono móvil del menor y el contenido que comparten a través de las aplicaciones de mensajería.

- Controlar tanto las fotos publicadas o enviadas por los padres como por el menor en la red y entre sus contactos.

- Intentar ganarse la confianza del menor, de forma que ante la menor duda o problema confíen en ellos y les cuenten la situación.

- Controlar hasta cierto punto los tiempos que dedica el menor a navegar por la red y su comportamiento en la vida real. De esta manera, se podría detectar algún cambio de comportamiento que podría delatar un abuso por parte de un tercero.

- Si el menor ya ha enviado alguna foto semidesnudo o desnudo completamente, asegurarse que para de inmediato

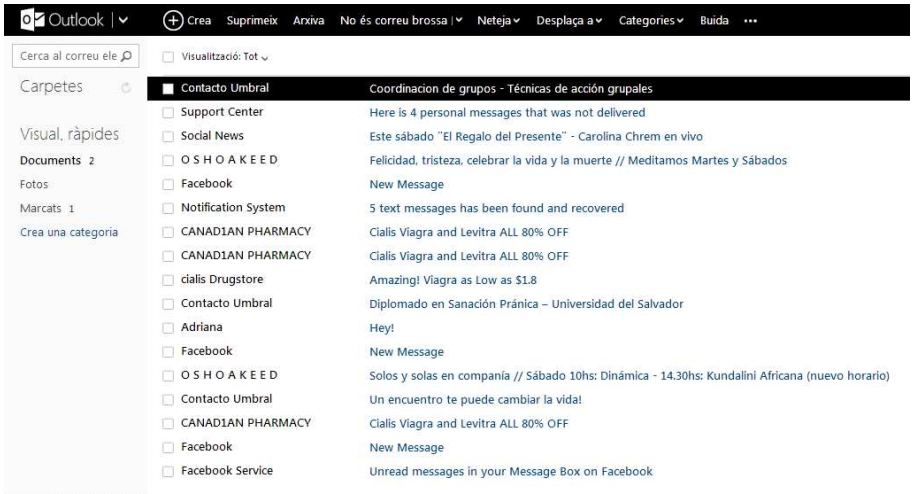
y elimina las foto, explicándoles las consecuencias psicológicas y legales que se podrían desarrollar si continúa mandando este tipo de contenido.

Para obtener una información más ampliada sobre esta problemática y conocer algunos datos, visitar las webs www.sexting.es y http://www.connectsafely.org, esta última únicamente disponible en inglés.

5.4.3 Spam

No siempre los contenidos inapropiados surgen de las páginas web que visitamos o las búsquedas que realizamos. En algunas ocasiones, esta información o contenido lo recibimos nosotros mismos sin haberla solicitado.

Así pues, definimos **spam** o correo basura a los mensajes no solicitados que recibimos de forma masiva en nuestra dirección de correo electrónico. Habitualmente tiene fines publicitarios, aunque en algunas ocasiones también es enviado por proveedores de contenidos para adultos o con fines ilícitos.



Desafortunadamente, se trata de un fenómeno que crece día a día y que a día de hoy representa un elevado porcentaje del tráfico de correo electrónico total. Además, aunque existen varios mecanismos de filtrado que nos permiten clasificar este tipo de correos y tecnologías más efectivas para luchar contra el spam, los *spammers* (o encargados de difundir este tipo de correo no deseado) se vuelven más sofisticados y modifican sus técnicas con objeto de violar y evitar todas las medidas tomadas por los usuarios.

Uno de los objetivos de estos *spammers* consiste en conseguir el mayor número de direcciones de correo electrónico válidas posibles. Para ello, se valen de distintas fuentes para la obtención de este tipo de datos como las que listamos a continuación:

- **Lista de correo:** El *spammer* se da de alta en la lista de correo y anota las direcciones del resto de contactos.
- **Los propios sitios web:** que con frecuencia contienen la dirección de su creador o de sus visitantes.
- **Uso de programas automáticos:** Recorren Internet en busca de direcciones en estos sitios web (grupos de noticias, weblogs, etc.)
- **Entrada ilegal en servidores**
- **Comprar bases de datos de usuarios a particulares o empresas.** Se trata también de un tipo de actividad ilegal, aunque en la práctica se realiza.
- **Técnicas de DHA (Directory Harvest Attack).** Esta técnica consiste en la generación de direcciones de correo electrónico pertenecientes a un dominio específico y envío de mensaje a las mismas. De esta forma, el servidor de correo del domino responderá con un error a las no existentes revelando así las válidas.
- **Correos electrónicos correspondientes a "cadenas".** Son correos que los propios usuarios reenvían masivamente revelando las direcciones de correo electrónico de todos los destinatarios, y que pueden llegar a acumular decenas de direcciones en el cuerpo del mensaje. Estas direcciones pueden llegar a ser captadas por algún troyano o por algún usuario malicioso.

Actualmente en España este tipo de práctica está prohibida por la Ley de Servicios de la Sociedad de la Información y Comercio electrónico que hemos comentado en el apartado Legislación de la presente memoria. Más concretamente, encontramos referencias en el artículo 19.2. que dispone que a todo lo referente al envío de comunicaciones electrónicas será aplicable la LOPD y el artículo 21 de la Ley 34/2002, de 11 de Julio de Servicios de la Sociedad de Información y Comercio Electrónico (LSSI) que dispone:

Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija. (LSSICE, 2002)

Para poder evitar este riesgo, expondremos las peculiaridades que caracterizan este tipo de mensajes de forma que los podamos reconocer de la forma más clara posible:

- Desconocemos el remitente del mensaje. Es habitual que esta dirección de correo esté falseada.
- El mensaje no suele tener dirección de respuesta.
- El asunto del correo presenta un mensaje que nos llama la atención o que podamos considerar interesante.
- Principalmente, el contenido es publicitario, como podrían ser:
    - Fórmulas para ganar dinero de forma rápida
    - Anuncios de sitios web
    - Ofertas inmobiliarias
    - Productos en promoción
    - Ayudas en temas humanitarios
- Aunque los correos de spam en español cada vez son más frecuentes, principalmente se trata de mensajes escritos en inglés

Además, existen otras variantes de este tipo de mensajes no deseados que recibimos a través de otros medios tecnológicos. Entre ellos encontramos:

- Spim: Mensajes publicitarios no deseados específicos para aplicaciones de mensajería instantánea.
- Spit: Spam sobre telefonía IP.
- Spam SMS: Mensajes no deseados recibidos en teléfonos móviles a través de SMS.

A continuación listaremos un conjunto de recomendaciones a seguir para evitar en la medida de lo posible el spam en nuestra bandeja de entrada del correo electrónico:

- Evitar en la medida de lo posible reenviar mensajes en cadena. Éstos suelen ser generalmente algún tipo de engaño.
- En caso de enviar algún mensaje de forma masiva a varios destinatarios, escribir las direcciones de email de los mismos en el apartado de Copia Oculta (CCO o CCC). De esta forma se evita que los *spammers* accedan y roben esta información.
- Nunca responder este tipo de mensajes. Al hacerlo estamos confirmando nuestra dirección de correo y sólo lograremos recibir más spam. Además, una de las técnicas más comunes de los remitentes de spam es incluir en el mensaje un enlace del tipo "si no quiere seguir recibiendo este tipo de mensajes, respóndanos a la dirección..."; de esa forma consiguen confirmar qué cuentas de correo están activas para poder seguir enviándoles mensajes indiscriminadamente.
- Al igual que hacemos con nuestro número de teléfono personal, evitar publicar nuestra dirección de correo privada en sitios webs, foros, redes sociales, chats, etc. ya que así únicamente conseguimos facilitar la obtención de las mismas a los *spammers*.
- Se aconseja tener varias cuentas de correo electrónico, de forma que asignaremos cada una de ellas para un fin. Así por ejemplo, podríamos tener una para nuestro correo personal, otra cuenta laboral y otra destinada al correo de contacto público o de distribución masiva.

- Algunos servidores de correo disponen ya de esta funcionalidad: nos permiten gestionar varias direcciones de email desde un mismo lugar. Por tanto, podremos aprovechar esta ventaja para publicar una cuenta alternativa a nuestra dirección de correo personal destinada al registro en sitios de baja confianza o para recibir *newsletters*.

- Cuando nos registremos o nos suscribamos a servicios o boletines de noticias en sitios web, hay que asegurarse de leer la letra pequeña para saber exactamente el uso que harán de nuestra información.

- Utilizar las técnicas de filtrado antispam que disponen la mayoría de servidores de correo electrónico. Éstas nos permiten clasificar los mensajes no deseados de forma eficiente. Sin embargo, hay que ter cautos a la hora de definir dichos patrones de filtrado, pues puede darse el caso de estar filtrando correo normal.

- Bloquear los mensajes de remitentes que te envíen spam utilizando los filtros que acabamos de comentar. De esta forma, los mensajes enviados a través de este destinatario irán a parar a la carpeta de correo no deseado o directamente a la papelera.

- La mayoría de proveedores de servicio de correo electrónico ofrecen formas de denunciar a los *spammers*, para así impedir que sus mensajes lleguen a otros usuarios.

- Se recomienda no abrir nunca los mensajes que identifiquemos como spam o, si lo hacemos, no hacer clic en ninguna URL o imagen que figure en el mensaje. Los remitentes de spam tienen formas de saber si hemos hecho clic en direcciones, imágenes o partes y, en definitiva, confirmar que nuestra dirección está activa.

- Tener cuidado con los documentos adjuntos. No debemos abrir ni reenviar documentos adjuntos que lleguen con mensajes de remitentes desconocidos, o que no estemos esperando. Además, habrá que tener especial cuidado con las extensiones de los archivos, especialmente con los ejecutables. Si decidimos abrir uno de estos archivos, convendrá analizarlo previamente con nuestro antivirus.

5.4.4 Phishing

Se denomina phishing a la actividad que consiste en atraer al usuario a cometer un delito de fraude informático a través de la colocación de un "anzuelo" que capte su atención. Por tanto, esta práctica estaría clasificada dentro del ámbito de las estafas cibernéticas.

Está relacionado con el término spam que acabamos de desarrollar, pues el método más común a través del que recibimos estas trampas es el correo electrónico y ambos tipos de mensajes nos llegan a nuestro buzón de correo sin haberlo solicitado. La diferencia fundamental radica en que el spam tiene un objetivo principalmente publicitario y, en cambio, la finalidad del phising es la de obtener y robar información personal y/o financiera del usuario.

Para ello, los *phishers* (los estafadores en este caso) utilizan un tipo de la denominada ingeniería social (práctica de obtener información confidencial a través de la manipulación de usuarios legítimos) para conseguir información confidencial de forma fraudulenta. Esta información podrías ser una contraseña, información detallada sobre tarjetas de crédito o cualquier otro tipo de información bancaria.

Alguno de los métodos más conocidos por los *phisers* para captar la atención del usuario, consiste en hacerse pasar por una persona o una empresa o entidad conocida en una aparente comunicación oficial electrónica, como podría ser un e-mail, algún mensaje a través de un sistema de mensajería instantánea o a través de llamadas telefónicas. Para ello, los phishers intentan clonar la identidad simulada de la forma más realista posible para hacer más creíble el engaño y lograr atraer al mayor número de usuarios posibles que caigan en la trampa.

Los casos más comunes son aquellos en los que los phishers se hacen pasar por una entidad bancaria conocida. El procedimiento consiste en enviar un correo electrónico a varios usuarios a los que invita a hacer clic en un enlace que los llevará a un sitio web que imita ser el original.

https://www.osi.es/ ***(Oficina de Seguridad del Internauta)*** - *Ej. Phishing Bankia*

De esta forma, el usuario ingresará información personal creyendo que la está otorgando a alguien de confianza. Una vez introducidos los datos, los *phisers* la podrán utilizar para realizar algún acto delictivo con ellos, del que podemos resultar gravemente dañados.

Por todo esto, debemos ser cautelosos sobre la información que compartimos a través de la red y estar atentos a este tipo de mensajes fraudulentos. De igual forma que hemos hecho con el spam, vamos a comentar las características principales de este tipo de fraude que nos permitirán distinguirlo y evitar de esta manera caer en la trampa de estos estafadores:

- El remitente del mensaje se trata de una empresa o entidad reconocida por el usuario.
- Hay que tener en cuenta que los *phishers* intentan clonar al máximo la apariencia de estas entidades copiando los colores y logotipos corporativos de la empresa, de forma que resulten más realistas y conseguir que más usuarios caigan en el engaño. Recordemos que con las nuevas tecnologías es muy fácil imitar a la perfección un sitio web conocido.

- El mensaje invita a ingresar (o re-ingresar) algún tipo de información personal que supuestamente la entidad ya debería conocer y que, por tanto, no nos debería pedir por ninguno de los medios que hemos comentado.

- El mensaje recibido suele contener algún enlace, dirección o cualquier otro tipo de dato de referencia en el cuerpo del correo electrónico.

Una vez reconocidos estos tipos de mensajes fraudulentos, deberemos seguir las siguientes recomendaciones para evitar caer en el engaño:

- Verificar siempre el remitente del correo que nos invite a introducir información personal y/o financiera.

- No volver a entregar información personal a una entidad si ya lo hemos hecho anteriormente. Ésta no debería pedirnos información que supuestamente ya conoce. Además, las empresas serias y de confianza nunca solicitan este tipo de información sensible a través de correos electrónicos.

- Ante la duda, verificar siempre el contenido del correo a través de una llamada telefónica a un número de información conocido previamente o bien indagando por la página web oficial de la entidad. Nunca llamar al número de teléfono que aparece en el correo, ya que éste podría formar parte del engaño.

- Como hemos comentado, esta amenaza está íntimamente relacionado con el spam. Por tanto, no hay que prestarle atención a este tipo de mensajes y deberemos eliminar el correo sospechoso sin realizar ninguna otra acción.

- No hay que clicar sobre los enlaces de los correos electrónicos. Ante la duda, siempre tendremos la posibilidad de teclear la dirección web directamente en nuestro navegador. Muchas veces los *phisers* utilizan los mismos nombres de dominio real de la entidad pero alternando algunas letras o la extensión del país de origen, de forma que a simple vista parezca que estemos accediendo al sitio original.

- Tras probar lo anterior, otra forma de verificar que estamos accediendo al sitio original de la entidad será asegurarnos

que la dirección web que se muestra en la barra del navegador empieza por https y no http. Además, en la barra de estado deberá aparecer el símbolo de un candado que indica que nos encontramos ante una página web segura.

- Utilizar antivirus y firewall. Aunque estas aplicaciones no se hacen cargo directamente del problema, pueden ayudarnos a detectar correos con troyanos o conexiones entrantes/salientes no autorizadas o sospechosas.

- Para finalizar, si conocemos algún tipo de amenaza como las citadas, deberemos informar a las autoridades pertinentes.

5.4.5 Happy Slapping

Se denomina **Happy Slapping** a la práctica en la que un grupo de gente, comúnmente adolescentes, abordan a una víctima y, sin motivo alguno, le propinan una paliza mientras filman la agresión a través de sus *smartphones*.

Generalmente el vídeo suele acabar colgado en internet en las redes sociales o en algún portal de difusión de vídeos como Youtube para que todo el mundo lo vea.

La mayoría de las veces la agresión se limita a un par de puñetazos, aunque en otros casos más graves la víctima es atada y sometida a varias sesiones de golpes. En diciembre de 2005 se dio a conocer la noticia en la que un hombre perdía la vida en una estación del metro de Londres tras recibir una paliza a manos de una joven de 15 años y sus amigos.

Fue en esta ciudad precisamente en la que nació esta moda peligrosa, en la que los agresores atacaban a sus víctimas en autobuses, metros o en los parques. Además, cabe destacar que una de sus características que lo hace aún más peligroso es que el ataque ocurre sin advertencia alguna y que, por tanto, cualquiera puede ser la víctima y en cualquier momento.

Además, el agresor o agresores no sólo se divierten con la violencia, sino que multiplican ese gusto al difundir los videos que, aunque suelen ser de baja calidad, tiene un gran impacto y les orgullecen.

En España llego el fenómeno en verano de 2005 y fue noticia el caso de dos jóvenes de 26 y 27 años que fueron detenidos en Barcelona por los Mossos d'Esquadra por agredir a peatones al azar y grabar los ataques en sus teléfonos móviles para posteriormente difundirlos a través de Internet (fuente periódico El País: http://elpais.com/diario/2006/01/19/espana/1137625218_850215.html)

Desgraciadamente, los jóvenes no tardaron en utilizar este mecanismo en las aulas para intimidar y humillar a sus compañeros por medio de redes sociales, blogs y servicios de mensajería instantánea. Como vemos, se trata de una de las prácticas que utilizan los jóvenes para ejercer ciberbullying a sus compañeros.

En algunos centros incluso los directores han optado por confiscar los teléfonos móviles con videocámara para evitar estas filmaciones y posteriormente alardear de ellas difundiéndolas entre sus compañeros. Se trata probablemente de uno de los pocos medios de prevención de estos actos, pues fuera de las aulas la responsabilidad de lo que pueda pasar recae directamente sobre los agresores.

5.4.6 Robo de identidad

El robo de identidad es un delito que tiene lugar cuando una persona, el ladrón o delincuente, suplanta la identidad de otra persona haciéndose pasar por ella y utiliza su información personal de índole financiera para solicitar préstamos, tarjetas de crédito, tramitar distintos servicios o incluso llegar a comprar propiedades de pequeño y gran valor.

Este problema siempre ha existido, desde mucho antes de la aparición de las nuevas tecnologías. El ladrón se valían de métodos tradicionales para acceder a estar información personal de la víctima, como podría ser robando su cartera, su buzón de correo físico o valerse del número PIN de la tarjeta de crédito observando las transacciones de las víctimas en los cajeros automáticos.

Sin embargo, tras la aparición de Internet, se ha incrementado considerablemente el riesgo de sufrir este tipo de crimen debido a la gran cantidad de flujo de información electrónica que circula día a día en la red.

No por ello deberíamos de dejar de aprovecharnos de la infinidad de ventajas que nos presenta la red hoy en día, como hacer transferencia a

través de los portales web de nuestros bancos, comprar productos por Internet o los billetes de avión de nuestro próximo viaje. Al igual que ocurre con el mundo real, podemos realizar estas transacciones siempre y cuando lo hagamos tomando ciertas medidas básicas de prevención y seguridad. Entre ellos, destacamos las siguientes recomendaciones principales:

- **Controlar el correo electrónico que abrimos.** Como hemos visto en otros de los riesgos a los que nos exponemos al utilizar Internet, existen algunos métodos como el spam o el *phishing* a través de los cuales los ladrones de identidad intentan obtener información confidencial del usuario. Consultar las recomendaciones para evitar estos riesgos en el apartado correspondiente.

- **Escribir manualmente la dirección URL de las entidades bancarias.** Nunca seguir un enlace que aparezca en un correo electrónico, ya que existe la posibilidad que éste sea fraudulento.

- **Utilizar contraseñas fuertes difíciles de descifrar por los hackers.** Alguno de los errores más comunes que cometen los usuarios es el de utilizar información personal como contraseñas de sus cuentas, utilizar una única contraseña predeterminada o que ésta contenga pocos caracteres. Sin embargo se recomienda que intentemos alargarlas, que las combinemos con números y caracteres y que, aunque tengan un significado para nosotros, no represente información personal que puedan averiguar otras personas con facilidad.

- **Evitar utilizar ordenadores de uso público para acceder a cuentas bancarias o tarjetas de crédito.** Esta información podría quedarse almacenada en las cookies del navegador, las cuales son una fuente de información utilizada por los hackers para obtener información confidencial. En caso de urgirnos acceder a Internet en cualquier lugar público, asegurarnos de cerrar todas las sesiones abiertas y eliminar el historial de navegación e información temporal.

- **Realizar compras seguras en Internet.** Para ello, deberemos asegurarnos que estamos accediendo a un sitio seguro. Una forma será comprobando que la URL del sitio web en el que pretendemos comprar empieza por *https* en lugar de *http* y,

en algunos navegadores, que aparezca una especie de candado que nos indique que el sitio es seguro. Además deberemos evitar proporcionar contraseñas o información confidencial por Internet y, en la medida de lo posible, investigar sobre el comerciante al que vamos a comprar, consultando comentarios de otros usuarios y compradores.

- **Nunca enviar información personal por correo electrónico.** Bajo ninguna circunstancia enviar contraseñas por Internet, ya sea a través del correo electrónico o por aplicaciones de mensajería instantánea.

Si tras seguir estas indicaciones básicas intuimos que estamos siendo víctimas de este delito, deberemos seguir los siguientes pasos:

- Llamar a las entidades con las que realizamos transacciones y denunciar la situación inmediatamente.
- Comunicarse con las emisoras de documentación, licencias u otros documentos de identidad para cancelar estos documentos y obtener uno de reemplazo.
- Mantenerse alerta de las cuentas que gestionamos de forma que podamos llegar a sospechar si alguien está utilizando nuestra información indebidamente.
- Si encontramos información fraudulenta, pedir que la quiten de nuestro registro.
- Y, fundamentalmente, avisar a las autoridades pertinentes y contar la situación. Habrá que denunciarlo lo antes posible, pues se trata de un crimen y podemos vernos envueltos en una situación comprometida.

6. Bibliografía

La bibliografía citada se ha consultado entre los meses de diciembre de 2012 a mayo de 2013, y todos los recursos se pueden encontrar en línea.

ABRIL, G. y PÉREZ-LANZAC, C. (25/11/2007), "*LUCIA13. Diario de un acoso en la Red*", EL PAÍS, http://elpais.com/diario/2007/11/25/eps/1195975611_850215.html

ACOSO EN LAS AULAS (2012), http://www.acosoenlasaulas.com/ciberbullying/casos-del-ciberbullying-en-espa%C3%B1a/

AGENCIAS (18/06/2002), "*Detenidas 65 personas por el intercambio de imágenes de pederastia en Internet*", EL PAÍS, París, http://sociedad.elpais.com/sociedad/2002/06/18/actualidad/1024351202_850215.html

AGENCIAS (04/07/2012), "*Una operación en 141 países identifica a cientos de pederastas en Internet*", EL PAÍS, Madrid, http://sociedad.elpais.com/sociedad/2012/07/04/actualidad/1341388585_915148.html

AGPD - Agencia Española de Protección de Datos (2013), www.agpd.es

AGUDO, A. y MONGE, Y. (19/10/2012), "*Humillada en la red, humillada en la calle*", EL PAÍS, Madrid y Washington, http://sociedad.elpais.com/sociedad/2012/10/18/actualidad/1350587479_648426.html

AGUDO, A. (19/03/2013), "*Un menor al día denuncia haber sido ciberacosado en España*", EL PAÍS, Madrid, http://sociedad.elpais.com/sociedad/2013/03/19/actualidad/1363700296_848102.html

ÁGUILA, F. (12/11/2008), "*Declaran culpable a imputado en primer juicio por "grooming"*", EL MERCURIO ONLINE, Santiago (Chile), http://www.emol.com/noticias/nacional/2008/11/12/330490/declaran-culpable-a-imputado-en-primer-juicio-por-grooming.html

AIMC - Asociación para la investigación de medios de comunicación (2013), "*15ª Encuesta Navegantes en la red*", http://www.aimc.es/-Navegantes-en-la-Red-.html

ALANDETE, D. (11/04/2010), "*Acoso escolar: En manos de las Chicas Malas*", EL PAÍS, http://elpais.com/diario/2010/04/11/domingo/1270957957_850215.html

ALMENAR VARA, P. (01/04/2013), "*Un detenido en Gandia por acosar a 300 niñas en Internet*", EL PAÍS, València, http://ccaa.elpais.com/ccaa/2013/04/01/valencia/1364808608_611228.html

ALMENAR VARA, P. (29/04/2013), "*Detenidas 41 personas por compartir pornografía infantil el Internet*", EL PAÍS, València, http://ccaa.elpais.com/ccaa/2013/04/29/valencia/1367232921_594526.html

ARGOL (05/12/2012), "*De Web 1.0 a Web 3.0*", http://www.koala-soft.com/de-web-10-a-web-30

BARTRINA ANDRÉS, M.J. (2012), "Análisis y abordaje del acoso entre iguales mediante el uso de las nuevas tecnologías", Barcelona, http://www20.gencat.cat/docs/Justicia/Home/%C3%80mbits/Formaci%C3%B3,%20recerca%20i%20docum/Recerca/Cat%C3%A0leg%20d%27investigacions/Per%20ordre%20cronol%C3%B2gic/2012/An%C3%A0lisi%20i%20abordatge%20de%20l%E2%80%99assetjament%20entre%20iguals/ciberdelicte_cast.pdf

BLOG CIBERBULLYING (2013), http://ciberbullyingcetis49.blogspot.com.es/2012_01_01_archive.html

BOE, nº 275 - Agencia estatal Boletín Oficial del Estado (1987), "*Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual*", http://www.boe.es/buscar/doc.php?id=BOE-A-1987-25628

BOE, nº 298 - Agencia estatal Boletín Oficial del Estado (1999), "*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*", http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

BOE, nº 166 - Agencia estatal Boletín Oficial del Estado (2002), "*Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*", http://www.boe.es/buscar/doc.php?id=BOE-A-2002-13758

BOE, nº 226 - Agencia estatal Boletín Oficial del Estado (2010), "*Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001*", http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

BSECURE (2013), http://www.bsecure.com/

CASADO, M.A., GARITAONANDIA, C., GARMENDIA, M. y MARTÍNEZ, G. CON OTROS MIEMBROS DE LA RED EU KIDS ONLINE (Marzo 2011), "*Riesgos y seguridad en internet: Los menores españoles en el contexto europeo*",

http://www.sociologia.ehu.es/s0018-eukidsct/es/contenidos/informacion/gi0404_informes2/es_00404_in/adjuntos/informe%20EU%20KIDS%20ONLINE%2015-2-2011.pdf

CASTRO, L., "*Qué es el robo de identidad y cómo prevenirlo. Consejos básicos de cómo evitar el robo de identidad en la era de Internet*", http://aprenderinternet.about.com/od/SeguridadPrivacidad/a/Robo-De-Identidad.htm

CIBERBULLYING (2013), "*Casos de Ciberbullying*", http://www.ciberbullying.com/cyberbullying/casos-de-ciberbullying/

CYBERSITTER (2013), http://www.cybersitter.com/

CÓDIGO PENAL, Artículos 189.1, 189.2, 189.3, 189.4, 189.7, 181, 186, 187.1

CONNECT SAFELY (2013), http://www.connectsafely.org

CONTROL KIDS (2013), http://www.controlkids.com/es/

DE HARO, J.J. (24/02/2009), "*Privacidad de menores y servicios de Internet*", http://jjdeharo.blogspot.com.es/2009/02/privacidad-de-menores-y-servicios-de.html

DELITOS INFORMÁTICOS (2013), www.delitosinformaticos.org

DETENLOS (2006-2008), "*Pedofilia*", http://www.detenlos.org/pedofilia.html

DUVA, J. (25/03/2008), "*La policía alerta del chantaje con fotos íntimas de menores*", EL PAÍS, Madrid, http://elpais.com/diario/2008/03/25/sociedad/1206399608_850215.html

EFE (16/05/2008), "*Procesada una mujer que usó MySpace para engañar a una adolescente que se suicidó*", EL PAÍS, Los Ángeles, http://sociedad.elpais.com/sociedad/2008/05/16/actualidad/1210888802_850215.html

EFE (23/05/2009), "*Condenado a pagar 100 euros por reírse en 'Tuenti' de un compañero*", EL PAÍS, Sevilla, http://sociedad.elpais.com/sociedad/2009/05/23/actualidad/1243029602_850215.html

EFE (08/04/2011), "*Detenido un pederasta que contactó en la red con 380 chicos fingiendo ser modelo infantil*", EL PAÍS, Barcelona, http://elpais.com/elpais/2011/04/08/actualidad/1302250635_850215.html

EFE (05/05/2011), "*Detenido un presunto acosador de adolescentes a través de Facebook*", EL PAÍS, Mollet del Vallès (Barcelona), http://elpais.com/elpais/2011/05/05/actualidad/1304583471_850215.html

EL MERCURIO ONLINE (17/11/2008), "*Tribunal condena a 5 y medio años de presidio efectivo a autor de "grooming"*", EL MERCURIO ONLINE, Santiago (Chile), http://www.emol.com/noticias/nacional/2008/11/17/331231/tribunal-condena-a-5-y-medio-anos-de-presidio-efectivo-a-autor-de-grooming.html

EL PAÍS (20/08/2000), "*Pederastas españoles invaden la Red*", EL PAÍS, Madrid, http://elpais.com/diario/2000/08/20/sociedad/966722401_850215.html

EMICI - Equipo Multidisciplinar de Investigación del Ciberbullying (2011), "*Protocolo de actuación escolar ante el ciberbullying*", ISBN: 978-84-9726-614-7, DL: BI-198-2011, http://www.emici.net/prot/Protocolo%20Ciberbullying.html

ESPINOSA, P. (15/06/2009), "*Mi 'ciberamigo' me chantajea*", EL PAÍS, Cádiz, http://elpais.com/diario/2009/06/15/sociedad/1245016805_850215.html

EU KIDS ONLINE (2011), "*Conclusiones clave encuesta EU Kids Online*", Universidad del País Vasco, http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsExecSummary/SpainExecSum.pdf

EUROPAPRESS (12/01/2011), "*Detienen a 3 chicos de 14 años por amenazar a otra menor a través de una red social*", EL MUNDO, Madrid, www.elmundo.es/elmundo/2011/01/12/madrid/1294826167.html

FACEBOOK - Centro de seguridad (2013), https://www.facebook.com/safety

GDT - Grupo de delitos Telemáticos de la Guardia Civil (2013), https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

GOOGLE+ - Centro de seguridad de Google+ (2013), https://www.google.com/intl/es/+/safety/

HABBO HOTEL - Consejos de seguridad (2013), http://www.habbo.es/safety/safety_tips

INFOSPYWARE (03/11/2008), "*¿Qué es el Phishing?*", http://www.infospyware.com/articulos/que-es-el-phishing/

INSTAGRAM - Servicio de ayuda de Instagram (2013), https://www.facebook.com/help/instagram

INTECO – Instituto Nacional de Tecnologías de la comunicación (Octubre 2008), "*Guía legal sobre las redes sociales, menores de edad y privacidad en la Red*", http://www.inteco.es/guias/guiaManual_redes_menores

INTECO - Instituto Nacional de Tecnologías de la comunicación (Marzo 2009), "*Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres*", https://www.inteco.es/Estudios/Estudio_ninos

INTECO - Instituto Nacional de Tecnologías de la comunicación (Mayo 2009), "*Guía legal sobre ciberbullying y grooming*", http://www.inteco.es/guias/guiaManual_groming_ciberbullying

INTECO - OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN y PANTALLAS AMIGAS (Febrero 2011), "*Guía sobre adolescencia y sexting: qué es y cómo prevenirlo*", https://www.inteco.es/guias/Guia_sexting

INTECO - Instituto Nacional de Tecnologías de la comunicación (Junio 2012), "*Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles Informe anual 2011 (17ª oleada)",* https://www.inteco.es/Estudios/Estudio_hogares_3C2011

INTECO - Instituto Nacional de Tecnologías de la comunicación (Octubre 2012), "*Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles 1er cuatrimestre de 2012 (18ª oleada)",* http://www.inteco.es/Estudios/Estudio_hogares_1C2012

INTECO - Instituto Nacional de Tecnologías de la comunicación (Octubre 2012), "*Guía de actuación contra el ciberacoso (Padres y Educadores)*", http://menores.osi.es/educadores/destacados/inteco-presenta-la-%C2%ABguia-de-actuacion-contra-el-ciberacoso%C2%BB-para-padres-y-educ

INTERNET GROOMING (2013), www.internet-grooming.net

K9 WEB PROTECTION (2013), http://www1.k9webprotection.com/

LORENZANA, C. (2012), (Capitán miembro del Grupo de Delitos Telemáticos de la Guardia Civil). Entrevista con el autor (Septiembre 2012)

LUENGO LATORRE, J.A. Y OTROS COLABORADORES (2011), "*Ciberbullying: Guía de recursos para centros educativos en caso de ciberacoso*", Defensor del Menor en la Comunidad de Madrid, Madrid, http://www.madrid.org/dat_norte/WEBDATMARCOS/supe/convivencia/guia_ciberbullying_def_menor_madrid1.pdf

LUQUE GUERRERO, J.M., "*Qué es el phishing y cómo protegerse*", http://seguridad.internautas.org/html/451.html

MCAFEE FAMILY PROTECTION (2013), http://home.mcafee.com/store/family-protection

MIEMBROS CONSEJO EUROPA (23/11/2001), "*Convenio sobre la Ciberdelincuencia*", http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF

MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE (2013), "*Definición de Propiedad Intelectual*", http://www.mcu.es/propiedadInt/CE/PropiedadIntelectual/Definicion.html

MONGE, Y. (17/10/2012), "*Un caso de ciberacoso conmociona a la sociedad canadiense*", EL PAÍS, Washington, http://sociedad.elpais.com/sociedad/2012/10/17/actualidad/1350506605_509352.html

MONOGRAFÍA PEDOFILIA (2013), http://www.monografias.com/trabajos11/pedofil/pedofil.shtml

MONTANE LOZOYA, J. (23/03/2010), "*Perfil del pedófilo, definición psicológica*", http://suite101.net/article/pedofilia-a13199

NET NANNY (2013), http://www.netnanny.es/

NORTON ONLINE FAMILY (2013), https://onlinefamily.norton.com

OLLÉS, M. (27/02/2009), "*Detenidos siete adolescentes de un centro de menores por acosar y humillar a otro y difundirlo*", DIARIO DE MALLORCA, http://www.diariodemallorca.es/sucesos/2009/02/27/sucesos-detenidos-siete-adolescentes-centro-menores-acosar-humillar-difundirlo/439877.html

O'Reilly, T (2005), "*Design Patterns and Business Models for the Next Generation of Software*", http://www.pcnet.com.es/internet/web20.html, http://es.wikipedia.org/wiki/Web_2.0

OSI - Oficina de Seguridad del Internauta (2013), http://menores.osi.es

PANIZO GALENDE, V., "*El Ciberacoso con intención Sexual y el childgrooming*", Quadernos de criminología: Revista de criminología y ciencias forenses, ISSN 1888-0665, Nº. 15, 2011 , págs. 22-33, http://dialnet.unirioja.es/servlet/articulo?codigo=3795512

PANTALLAS AMIGAS (2013), www.pantallasamigas.net

PANTALLAS AMIGAS, "*Sexting, un práctica de riesgo*", http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/sexting-una-practica-de-riesgo.shtm

PC PANDORA (2013), http://www.pcpandora.es/

PIENS@, "*Riesgos en Internet*" (2013), http://www.piensa.edu.sv/index.php/riesgos-en-internet

PISANI, F. (27/10/2005), "*Los 'nativos' del mundo digital y el futuro de las TIC*", EL PAÍS, http://elpais.com/diario/2005/10/27/ciberpais/1130377882_850215.html

POLO, C. (06/03/2013), "*Las mejores aplicaciones de control parental*", PC ACTUAL, http://www.pcactual.com/articulo/laboratorio/especiales/12591/las_mejores_aplicaciones_control_parental.html

PROTÉGELES (2013), http://www.protegeles.com/

PROTÉGETE, "*Menores y la protección de datos*", http://protegete.jccm.es/protegete/opencms/Ciudadanos/Proteccion_datos/menores.html

PURE SIGHT (2013), http://www.puresight.com/

QUE NO TE LA DEN - Helpline para la prevención del grooming o acoso sexual (2013), http://www.quenoteladen.es

QUSTODIO (2013), http://www.qustodio.com/es/

RAE (2013), http://www.rae.es

RED SEGURIDAD (2005), "*Los menores ante la ley orgánica de protección de datos*", Borrmart nº16, http://www.borrmart.es/articulo_redseguridad.php?id=393&numero=16

RYAN'S STORY PRESENTATION (2010), http://www.ryanpatrickhalligan.org/

SALA i GINER, G. y VALERO IGLESIAS, L.F. (Agosto 2006), "*Reflexiones a partir del fenómeno del "happy slapping"*", El Catoblepas, número 54, pág 14, http://nodulo.org/ec/2006/n054p14.htm

SEGU KIDS - Juntos en la red - Seguridad para menores, padres y docentes (2013), www.segu-kids.org

SEXTING (2013), http://www.sexting.es/

STOP SEXTING (2013), http://www.stop-sexting.info/noticias-news/

TREND MICRO GUARDIAN (2013), http://www.trendmicro.com/us/home/products/internet-safety/online-guardian/index.html

TUENTI (2013), https://www.tuenti.com

TWITTER - Twitter help center (2013), https://support.twitter.com/groups/57-safety-security

USEROS, C. (20/05/2011), "*FORMACIÓN: De la Web 1.0 a la Web 3.0 y la Web Semántica*", http://www.inforedsocial.es/index.php/formacion/393-de-la-web-10-a-la-web-30-y-la-web-semantica

WEB WATCHER (2013), http://www.webwatcher.com/ww/where/where-you-see.html?gclid=CMDLyM_DgrgCFVMetAod2EcAXA

WIKIPEDIA (2013), http://es.wikipedia.org

WINDOWS LIVE PROTECCIÓN INFANTIL (2013), http://www.microsoft.com/spain/windowslive/familysafety.aspx

YOUTUBE - Centro de seguridad (2013), http://www.youtube.com/yt/policyandsafety/es/safety.html