Instituto Nacional
de Tecnologías
de la Comunicación

Los controles parentales: cómo vigilar a qué contenidos de Internet acceden nuestros hijos.

Las nuevas tecnologías están a la orden del día entre los más pequeños. Tal es así, que no nos sorprendemos al ver a niños[1] enseñando a sus mayores a utilizar el DVD, la cámara digital, su nuevo móvil o incluso a navegar por la Red sin que aparentemente nadie les haya enseñado previamente. Nuestros niños y adolescentes son la generación de las nuevas tecnologías. Son la generación de Internet.

Internet se ha convertido en un medio para informarse, para aprender, para comunicarse, para jugar, para acceder a casi una infinitud de archivos, programas, etc. y satisfacer nuestras necesidades de conocimiento y ocio. No obstante, del mismo modo que son innegables los beneficios que nos brinda Internet, existen aspectos menos favorables que debemos conocer y prevenir, y en especial, cuando éstos afectan a los menores.

En este sentido, tanto los padres como los educadores están preocupados por la facilidad con la que los menores pueden acceder a contenidos poco apropiados[2]. Frente a este *todo vale*, se puede y se debe actuar desde una doble vertiente. Por una parte, luchar desde las instituciones del Estado contra los contenidos ilícitos (que no inapropiados) y los comportamientos delictivos que pululan por la Red. En segundo lugar, desde la educación y concienciación a nuestros menores sobre las claves para una navegación segura y responsable.

Según el estudio *Seguridad infantil y costumbres de los menores en Internet*[3], el 54% de los menores no ha recibido formación alguna sobre las normas básicas de seguridad frente a un 45% que afirma conocer dichas reglas. Además, el informe señala que el 86% de los menores usuarios accede a la Red desde ordenadores que no cuentan con ningún sistema de filtrado de contenidos y que entre el 28% y el 38% de los menores, accede a contenidos inconvenientes o nocivos (destacar que el porcentaje aumenta con la edad).

---

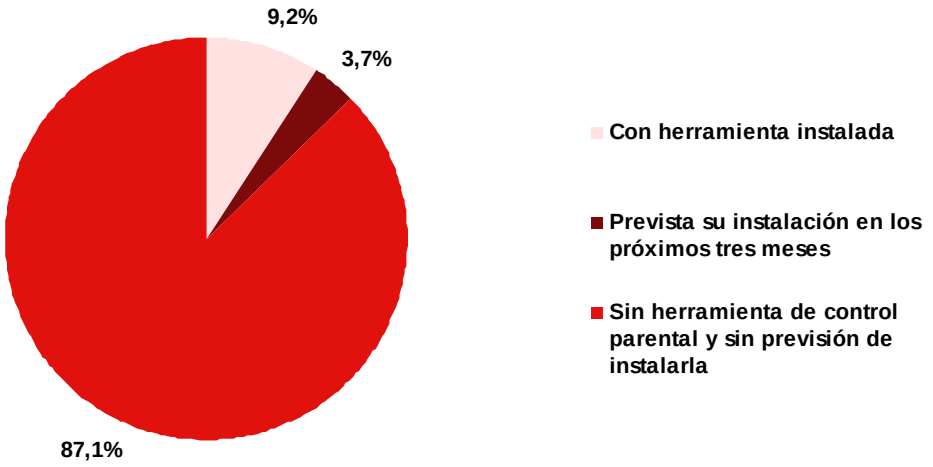
[1] A lo largo del artículo, nos referiremos a los destinatarios de estos controles utilizando términos como niños, adolescentes y menores, sin que con ello estemos realizando una clasificación determinada en las edades de los mismos.

[2] Más adelante haremos una referencia a la diferencia entre contenidos *apropiados, ilícitos* e *inapropiados.*

[3] Estudio realizado a 4.000 menores de entre 10 y 17 años de ambos sexos para el Defensor del Menor por las organizaciones de protección de la infancia ACPI (Acción Contra la Pornografía Infantil) y PROTÉGELES. Noviembre 2002.

Estos porcentajes no difieren de los resultados obtenidos en la 1ª Oleada del *Estudio sobre la Seguridad de la Información y e-Confianza de los hogares españoles* realizado por el Observatorio de la Seguridad de la Información de INTECO[4]. En él, se muestra que en enero de 2007, tan solo en 9,2% de los hogares encuestados está equipado con algún programa de control parental; si bien, el 12,9% tiene prevista su instalación en los tres meses siguientes.

Utilización de herramientas informáticas de control parental en ordenadores domésticos



Fuente: INTECO (enero 2007)

¿A qué tipo de contenidos podrían acceder nuestros hijos?

Hablar con menores de ciertos temas no siempre es una tarea fácil, y todavía menos si tenemos en cuenta que los adolescentes suelen ser muy recelosos cuando se abordan asuntos que, en su foro interno, consideran un ataque contra su intimidad. En particular aquellos que hacen referencia a sus amigos, a qué contenidos acceden, al número de horas que pasan ante el ordenador, con quién se mandan innumerables mensajes, etc.

[4] INTECO: *Estudio sobre la Seguridad de la Información y e-Confianza de los hogares españoles* (1ª Oleada: Dic-Ene 07)- www.inteco.es

El pasado mes de octubre se publicó el libro *Cómo controlar lo que hacen tus hijos con el ordenador: Técnicas de hacker para padres*[5], de la autora valenciana Mar Monsoriu, según la cual, *"cuando la comunicación falla, la alternativa que le queda a los padres es convertirse en un verdadero espía informático"*. Pero convertirse en espía no es la única solución frente a los contenidos nocivos y/o inapropiados que los menores pueden encontrarse; del mismo modo que tampoco es solución vetarles el acceso.

Pero, ¿a qué tipo de contenidos podrían acceder nuestros hijos? Los ***contenidos ilícitos*** son aquellos contenidos que vulneran la norma penal, es decir, que su publicación en la Red puede llevar (y de hecho lleva) asociado un delito. Como ejemplo de este tipo de contenidos podemos nombrar la pornografía infantil, pederastia, estafa informática, racismo, xenofobia. Todos ellos son contenidos perseguidos por la ley y que por tanto si tenemos noticia de ellos se deben denunciar inmediatamente ante los cuerpos y fuerzas de seguridad del Estado que trabajan en la persecución de este tipo de delincuentes y en la eliminación de la Red de dichos contenidos. No obstante, la acción contra los mismos es complicada pues en numerosas ocasiones, se encuentran alojados en otros países y cada país tiene su propia definición de ilegalidad de contenidos.

Cuando se hace referencia a los ***contenidos inapropiados*** la definición es mucho más sencilla. Si entendemos como contenidos apropiados aquellos comúnmente denominados como "para todos los públicos", por exclusión, los contenidos inapropiados hacen alusión a contenidos que, si bien no vulneran la ley, pueden resultar ofensivos o nocivos para determinadas personas, en este caso menores. Así, son contenidos *no aptos*[6] (pornografía, drogas, violencia, juegos de azar, etc). En cualquier caso son *per se* difícilmente objetivables ya que ante un mismo caso, lo que para unos padres resulta que no es apropiado para su hijo, otros pueden pensar que su hijo "ya tiene edad para ver ciertas cosas". Es por ello que éstos son los contenidos de los que se ocupan las técnicas de filtrado que más adelante se exponen.

[5] Monsoriu Flor, M: (2007): Cómo Controlar lo que hacen tus hijos con el ordenador: Técnicas de hacker para padres; Madrid, ed: Creaciones Copyright.

[6] De acuerdo a la vigente Ley Orgánica para la Protección del Niño y del Adolescente, se considera contenidos no aptos, aquellos que promuevan, hagan apología o inciten a la violencia, a la guerra, a la comisión de hechos punibles, al racismo, a la desigualdad entre el hombre y la mujer; a la intolerancia religiosa y cualquier otro tipo de discriminación; al uso y consumo de cigarrillos y derivados del tabaco, de bebidas alcohólicas y demás especies previstas en la legislación sobre la materia y de sustancias estupefacientes y psicotrópicas, así como aquellos de carácter pornográfico, que atenten contra la seguridad de la Nación o que sean contrarios a los principios de una sociedad democrática.

Filtrado de contenidos

Para solventar estos problemas, han salido al mercado diferentes sistemas de control parental de los contenidos. Así, sistemas operativos como *Windows Vista* y *Mac OS X 0.5 Leopard* ya cuentan con controles parentales incorporados; ambos, con sus ventajas y con sus limitaciones. Los dos sistemas incorporan, dentro de su ***control parental***, diferentes opciones como son: límites de tiempo y contenidos, determinación de juegos y programas ejecutables,…Además, los diferentes proveedores de Internet, por una pequeña cuota adicional, ofrecen también algún tipo de filtrado de contenidos.

Pero los controles parentales no sólo aparecen en los diferentes sistemas operativos, sino que hay multitud de programas (tanto gratuitos como bajo licencia de pago) que permiten diferentes **técnicas de filtrado**[7].

1. Control del tiempo: se ofrece la posibilidad de determinar el tiempo que el menor puede estar conectado a Internet; la limitación podemos realizarla por horas y días por semana. Resulta muy útil cuando no queremos que el niño se pase *las horas muertas* delante del ordenador y también ayuda a determinar el tiempo de conexión de los niños que están solos en casa.

2. Bloqueo de palabras clave: Consiste en bloquear las páginas que contengan aquellas palabras que creamos que llevan asociadas contenidos inapropiados (sexo, apuestas, drogas, casino,…). Tiene una pega y es que con ésta técnica se pueden producir numerosos "falsos positivos", es decir, corremos el peligro de bloquear contenidos que pueden no ser nocivos para los menores ya que se bloquean las palabras aisladamente, sin tener en cuenta el contexto en el que se hayan integradas.

3. Registros: Realiza un recuento de las páginas que han sido visitadas o a las que se ha intentado visitar. Sirve para revisar y comprobar los hábitos de navegación de los menores.

   Esta técnica no precisa que el menor sea consciente de que los contenidos están siendo limitados, pero como ya hemos comentado con anterioridad, la base de una navegación segura es el diálogo entre padres/educadores y niños. Además, esta falta de confianza puede derivar en inseguridades y descrédito por parte de los niños hacia sus padres.

[7] Los diferentes proveedores de Internet (Telefónica, Orange, Ono,…), por una pequeña cuota adicional, ofrecen también algún tipo filtrado de contenidos.

4. Bloqueo de programas: Bloqueo de determinada información de servicios del tipo mensajería instantánea, correo electrónico, descarga de programas, etc.

   Con el bloqueo de estas páginas, es evidente que se bloquea también un uso incorrecto de las mismas. Algunas herramientas permiten además, el bloquear la salida de determinada información, ya sea de manera voluntaria o por accidente (nombre, dirección, datos bancarios,…).

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

   Las *listas negras* consisten en determinar las páginas a las que se restringe el acceso; lo cual lleva un peligro asociado, y es la rapidez con la que se añaden cada día contenidos y páginas a la Red y por tanto es prácticamente imposibles tenerlas actualizadas.

   Las *listas blancas* son más restrictivas pero aseguran le denegación de acceso a determinados contenidos. Se trata de listas de páginas a las que se permite el acceso por considerarlas apropiadas.

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

   La Plataforma para la Selección de Contenidos de Internet (PICS), desarrollada por el World Wide Web Consortium (W3C), proporciona un medio más eficiente para controlar el acceso a los contenidos. El sistema de etiquetado fue diseñado originalmente para ayudar a los padres y maestros en el control de acceso de los menores a la Red.

   Este sistema tiene sus partes positivas y las negativas. Como positivo, señalar que es independiente del idioma, lo que posibilita la restricción de un mayor número de contenidos, y el hecho de que es el propio padre/educador quien bloquea lo que cree oportuno. Lo negativo es que no siempre existe dicha clasificación en ciertas páginas porque no existe un estándar común que sigan los generadores de contenidos y de páginas web.

Pero no sólo existe la posibilidad de establecer un control en Internet, también los móviles y las consolas empiezan a introducir una serie de restricciones en su uso.

Bien es cierto que el uso de Internet, el móvil y los videojuegos muchas veces se solapa. Los menores juegan en línea, se descargan tonos, juegos para la videoconsola o el móvil y, a todo ello hay que sumarle el resto de actividades que ofertan los móviles.

Una de las videoconsolas más populares entre los adolescentes, la X-Box 360, entre sus características en su última versión, incluye la posibilidad de establecer un control parental. Además, tiene la posibilidad de establecer diferentes tipos de control según el menor esté jugando en línea o sin conexión. En el caso en que el menor esté jugando sin conexión, el control parental se puede configurar para licitar o negar el acceso a juegos en función de la clasificación PEGI[8]. Si el menor juega conectado a la Red, se puede determinar el acceso a determinados contenidos así como los contactos que establece el menor.

No se puede olvidar el hecho de las adicciones tecnológicas[9]. Es difícil determinar el porcentaje de menores que está o puede estar desarrollando una adicción a los videojuegos en Red[10], pero es una problemática que está ahí y no puede, ni debe, pasar inadvertida.

En lo que respecta a la utilización del móvil, los padres suelen ser más restrictivos; o al menos creen serlo. Y se hace hincapié en el *creen* porque la mayor parte de las veces se auto-convencen de que el hecho de controlar el dinero que invierten en el mismo es suficiente. Pero no lo es. Ya no solo por el hecho de que la tecnología avance de tal forma que ahora podamos conectarnos a la Red desde el móvil, si no porque los peligros a los que los menores se enfrentan desde sus móviles se empiezan a parecer cada vez más a los que se encuentran en la Red.

Cuando nuestros hijos deciden bajarse melodías o conectarse a Internet desde su móvil, la exposición a virus y códigos maliciosos es casi la misma que cuando lo hacen desde el ordenador. Pero ¿con quién hablan?, ¿a quién mandan y de quién reciben los mensajes?, ¿sólo a/de sus compañeros de colegio o hay alguien más? En el correo electrónico se

[8] PEGI es la abreviatura de *Pan European Game Information* que establece una clasificación por edades para videojuegos y juegos de ordenador, proporcionando a padres, compradores y consumidores online una mayor confianza al saber que el contenido del juego es apropiado para una determinada edad. Esta clasificación es simplemente una recomendación sobre el contenido del juego, no es determinante.

[9] La Asociación alicantina de afectados por la ludopatía y otras adicciones, Vida Libre, ha atendido en lo que va de año a diez personas, en su mayoría jóvenes veinteañeros, con un problema de adicción tecnológica.
http://actualidad.terra.es/provincias/alicante/articulo/vida_libre_internet_1968593.htm

[10] Según el estudio de ACPI-PROTÉGELES para el Defensor del Menor, el 23% de los encuestados afirma que juega en cada conexión que realiza, lo cual puede resultar significativo y determinante como grupo de riesgo a desarrollar una adicción a los videojuegos

reciben mensajes de personas desconocidas (*spam*), en el móvil sucede lo mismo, pudiéndose recibir mensajes y llamadas de supuestas ofertas, premios, sorteos a los que el usuario no para a preguntarse si sus hijos los omiten o por el contrario, responden.

Desde hace ya algún tiempo, las diferentes compañías ponen a disposición de los padres una serie de controles parentales en los móviles. Con ellos pueden, no sólo de controlar el gasto, sino la restricción de llamadas y mensajes tanto por número como por destinatario (a los contactos de la agenda o a una serie de números determinados), limitar los contenidos a los que acceden (en la Red), o el acceso al servicio *localízame.*

Herramientas gratuitas de control parental

A continuación se referencian algunas herramientas gratuitas que permiten a los padres conocer y controlar los contenidos a los que sus hijos acceden en la Red:

1. **Asesor de contenidos de Internet Explorer:**

   http://www.microsoft.com/spain/windows/ie/using/howto/contentadv/config.mspx

   Idioma: Español

   Características:

   - Es una opción en el navegador Internet Explorer.
   - Puede configurarse de tal forma que active diferentes filtros y detecte los contenidos según haya sido etiquetada la página.
   - Da la posibilidad de crear listas de páginas “permitidas” para incluir los sitios que consideras adecuados para tus hijos (listas blancas).
   - Permite agregar “filtros adicionales” más complejos que simplemente las etiquetas en la página.

2. **Parental control bar:**

   http://www.aboutus.org/ParentalControlBar.org

   Idioma: Inglés

   Características:

   - La instalación se hace de la misma forma que una “barra de herramientas” en los navegadores Internet Explorer, Firefox y Safari en computadoras con sistema operativo Windows 98/ME/2000/XP.

- Cuando se activa el Child Mode, automáticamente se bloquean las páginas etiquetadas con contenidos no aptos, las que no estén clasificadas (esto es configurable) y las que se agreguen a la lista negra.
- Permite la creación de listas de páginas blancas para incluir los sitios que consideras adecuados para tus hijos.
- Permite colocar páginas que estén etiquetadas como aptas dentro de las listas negras si contienen información inadecuada.
- Da la opción de saber en qué páginas ha entrado tu hijo.

3. **Naomi:**

   http://www.naomifilter.org/spanish.html

   Idioma: Varios (incluye español)

   Características:

   - Se instala como una aplicación independiente en Windows NT/ME/2000/XP
   - Si detecta un contenido inadecuado, automáticamente cierra el navegador. La detección se realiza por medio de técnicas inteligentes que van más allá del simple etiquetado.
   - No se puede configurar. Para dejar pasar páginas aptas que, por defecto han sido bloqueadas, es preciso desactivar el programa.
   - Además de bloquear el navegador, bloquea también programas de tipo chat, compartir archivos, etc.

4. **Leopard:**

   http://www.faq-mac.com/noticias/node/26785

   Idioma: Español

   Características:

   - Permite la configuración de cuentas de usuario específicas para los niños.
   - Permite la restricción de contenidos de tres formas diferentes: acceso ilimitado, limitación selectiva y aprobación selectiva.
   - Control del acceso a mail e iChat (aplicaciones de mensajería instantánea relacionadas con MSN aparecerán como otras aplicaciones.)
   - Permite un control del tiempo de uso.
   - Da la opción de saber en qué páginas ha entrado su hijo.

Recomendaciones de INTECO a los usuarios

Actualmente, por parte del **Observatorio de la Seguridad de la Información** de INTECO se están llevando a cabo diferentes estudios relacionados con la seguridad de los menores en Internet:

a) ***Estudio sobre los hábitos de seguridad en el uso de las TIC y acceso a contenidos por niños y adolescentes y e-confianza de padres y tutores:*** este estudio abordará dos frentes:

- La realización de los trabajos de estudio y análisis de los usos, hábitos, acceso a contenidos, conocimientos y percepción de seguridad de los menores respecto a las TIC, en especial Internet, así como los conocimientos, consciencia, percepción, implicación sobre la seguridad y e-confianza de los padres respecto del uso de las tecnologías de la información y la comunicación por parte de sus hijos.

- La elaboración de una guía práctica con consejos para un uso seguro y adecuado de las nuevas tecnologías y sus servicios (Internet, telefonía, videojuegos, etc).

b) ***Estudio sobre la seguridad de las plataformas educativas:*** en dicho estudio, se realizarán trabajos de análisis, investigación, diseño y desarrollo de un informe sobre la seguridad de los contenidos y servicios integrados en las plataformas educativas, a partir del análisis de información disponible en la materia, análisis de casos de éxito a nivel nacional e internacional y entrevistas a expertos en la materia, con el objetivo de definir qué estándares de seguridad son necesarios de cara al desarrollo de las mismas.

Por otro lado, tal y como se ha presentado anteriormente, resulta necesario poner al servicio de los usuarios una serie de recomendaciones para evitar que los menores sean víctimas o accedan a contenidos ilícitos e inapropiados. En esa línea, desde INTECO se ofrece a todos los usuarios las siguientes recomendaciones:

1. **Eduque al menor** sobre los posibles peligros que puede encontrar en la Red.

2. **Acompañe al menor en la navegación** cuando sea posible, sin invadir su intimidad.

3. **Advierta al menor de los problemas de facilitar información personal** (nombre, dirección, teléfono, contraseñas, fotografías, etc.) a través de cualquier canal.

4. **Aconséjele no participar en charlas radicales** (provocadoras, racistas, humillantes, extremistas, etc.) ya que pueden hacerle sentir incómodo.

5. **Infórmele de que no todo lo que sale en Internet tiene que ser cierto,** ya que pueden ser llevados a engaño con facilidad.

6. **Preste atención a sus "ciber-amistades"** en la misma media que lo hace con sus amistades en la vida real.

7. **Pídale que le informe** de cualquier conducta o contacto que le resulte incómodo o sospechoso.

8. **Vigile el tiempo de conexión** del menor a Internet para evitar que desatienda otras actividades.

9. **Utilice herramientas de control parental** que le ayudan en el filtrado de los contenidos accesibles por los menores.

10. **Cree una cuenta de usuario limitado** para el acceso del menor al sistema.