

# **INTERNET SEGURA PARA A INFANCIA**

# Programa

1	Aplicacións en Internet.....	2
1.1	Web.....	2
1.2	Correo electrónico.....	2
1.3	Chats, mensaxería instantánea. Teclado, micrófono e webcams.....	2
1.4	Compartimento de contido.....	2
1.5	Redes sociais.....	3
1.5.1	Tecnoloxía.....	3
1.5.2	A identidade dixital.....	3
1.5.3	Usos.....	3
1.5.4	Exemplos.....	3
1.5.4.1	Facebook.....	3
1.5.4.2	Tuenti.....	3
1.5.4.3	Twitter.....	3
1.5.4.4	Outras.....	4
1.6	Intercambio e descargas directas de arquivos.....	4
1.6.1	Uso.....	4
1.6.2	Tecnoloxía.....	4
1.6.2.1	Descarga directa.....	4
1.6.2.2	Programas “Peer to Peer”.....	4
1.7	O teléfono móbil.....	4
2	Riscos e ameazas.....	4
2.1	Virus, vermes, cabalos de troia.....	4
2.1.1	Métodos de contaxio.....	4
2.2	Correo non desexado.....	5
2.3	Timos e fraudes.....	5
2.4	Roubo de identidade.....	5
2.4.1	Métodos.....	5
2.4.1.1	Adiviñar o contrasinal.....	5
2.4.1.2	Virus.....	6
2.4.1.3	“Phising”.....	6
2.5	Comercio electrónico e poxas.....	6
2.6	Privacidade e intimidade.....	6
2.7	Ciberdelincuencia dirixida ó Menor.....	6
2.7.1	Condutas delictivas.....	6
2.7.1.1	Desencadeantes.....	7
2.7.1.2	Estadísticas.....	7
2.7.2	A vítima.....	8
2.7.3	O Autor.....	8
2.7.4	Marco Legal.....	9
2.7.4.1	Rol da Xustiza.....	9
2.7.4.2	Rol dos Corpos e Forzas de Seguridade do Estado.....	9
2.8	Plans de acción.....	10
2.8.1.1	Tarefas a desenvolver polos pais e fillos.....	10
3	Boas prácticas.....	11
3.1	Uso do ordenador.....	11
3.2	Comunicación entre pais e fillos.....	11
4	Ferramentas básicas.....	12
4.1	Precaucións básicas: Antivirus.....	12
4.1.1	Antivirus de utilización gratuíta para o fogar.....	13
4.1.2	Antivirus de pago.....	13
4.2	Configuración segura dos navegadores máis utilizados.....	13

4.2.1 Firefox 3.5.....	14
4.2.1.1 Instalación de extensións para unha navegación segura.....	15
4.2.2 Internet Explorer 8.0.....	16
4.2.3 Outros navegadores: Google Chrome, Opera, Safari (Apple).....	19
4.3 Ferramentas de control parental .....	19
4.3.1 Ferramentas de control parental no Sistema Operativo.....	19
4.3.2 Ferramentas de control parental integradas no Antivirus.....	20
4.3.3 Ferramentas de control parental no router ADSL.....	20
4.3.4 Programas comerciais de control parental.....	20
4.4 Exame periódico dos rexistros históricos de navegación.....	21
4.5 Exame das 'cookies'.....	21
5 Técnicas máis avanzadas .....	21
5.1 Filtros de contidos.....	21
5.1.1 Diversas técnicas de filtrado.....	21
5.2 Importancia de utilizar versións actualizadas do software.....	22
5.3 Banners con contido explícito.....	22
5.4 Procuras seguras en Internet.....	22
6 Referencias.....	23
6.1 Aplicacións.....	23
6.2 Ciberdelincuencia dirixida o menor.....	23
6.3 Ferramentas .....	24
7 Autores.....	24

# Aplicacións en Internet

## **Web**

A Web é un sistema de documentos dispoñibles en Internet que están conectados entre si a través de ligazóns. Estes documentos poden conter textos, fotografías, vídeos, etc. Podemos acceder a estes documentos dende un navegador de diversos modos, por exemplo indicando a súa dirección realizando unha procura nalgún buscador ou seguindo unha ligazón dende outro documento.

## **Correo electrónico**

O correo electrónico tamén coñecido como mail ou email é un método para enviar e recibir mensaxes a través de Internet. A través do correo electrónico tamén podemos intercambiar fotografías, vídeos, etc.

## **Chats, mensaxería instantánea. Teclado, micrófono e webcams.**

A mensaxería instantánea é un sistema de conversa en liña que permite que varias persoas conversen en tempo real. Inicialmente a conversa realizábase escribindo as mensaxes, hoxe en día xa son habituais os chats de voz e de vídeo de forma que se dispoñemos de micrófono e altosfalantes podemos falar con unha persoa de forma similar a se estivésemos a manter unha conversa telefónica é incluso vela se dispón de webcam.

## **Compartimento de contido**

Hai diversos servizos en Internet que permite aos usuarios **colgar información** para ser **libremente accedida** por outros. **Textos** e reflexións a través de blogs ou cadernos de bitácora como Blogger. As **fotografías** e imaxes son compartidas en servizos coma Flickr ou Google Picasa. Os **vídeos** sóbense en servizos coma Youtube, actualmente a terceira web máis consultada no mundo.

## **Redes sociais**

Chámase servizos de rede social a aplicacións de Internet que teñen coma característica fundamental a interacción entre os membros conectados da devandita rede.

## **Tecnoloxía**

Estas aplicacións úsanse **directamente co navegador**, non é necesario un programa especial. Permiten un grao de interactividade moi elevado empregando novas técnicas de programación e incluso se fála dunha nova versión da “World Wide Web”, a **Web 2.0**.

## **A identidade dixital**

Así pois, unha rede social está formada por nodos que son cada un dos individuos. O individuo está representado por unha **identidade dixital** que se crea no momento de rexistrarse (darse de alta) no servizo.

Cada nodo está conectado con outros por unha relación normalmente de amizade. O conxunto dos nodos interconectados é a **rede de amigos** ou contactos.

## Usos

O uso fundamental é a **comunicación** cos membros da rede, mais entendendo comunicación nun sentido amplo. Non só é **intercambio de mensaxes** coma ocorre co correo electrónico o cos sistemas de conversa. O repertorio amplíase a intercambio de **contidos** coma **fotografías, vídeos**, enlaces de páxinas, enquisas, xogos, frases célebres, listas de afeccións... tanto persoais coma doutros pero cos membros da rede. Unha rede social pode satisfacer case que tódalas necesidades de comunicación sen utilizar nengún outro servizo de Internet.

## Exemplos

### **Facebook**

Este servizo de rede social é quizais o de uso **máis estendido no mundo**. Segundo algunhas fontes é a segunda páxina web máis visitada (despois de Google) e conta con **300 millóns de usuarios** activos. Está claro que non a usan só menores.

Ademais da capacidade de mensaxería e de compartido de contidos, empresas ou programadores fan **aplicacións extras** que dan a Facebook moitas outras funcionalidades coma xogos de estratexia, cadeas de mensaxes, recordatorio de aniversarios e miles máis.

### **Tuenti**

Tuenti é una rede social desenrolada por un empresa de capital español e é moi popular aquí. Está moi estendida entre adolescentes. Era usada por tantos menores que dende abril de 2009 cambiou as condicións de uso e os niveis de privacidade por defecto. Agora o acceso está prohibido a menores de 14 anos.

### **Twitter**

Twitter é una rede social que está especializada no intercambio de mensaxes curtas coma os dos SMS dos teléfonos móbiles. Trátase de responder á pregunta “¿Que estás a facer?” e compartila cos teus contactos.

### **Outras**

Pero hai máis: MySpace (orientada a grupos musicais), Hi5 (popular en América Latina), Orkut (Brasil)...

## **Intercambio e descargas directas de arquivos**

### **Uso**

Otro dos usos máis populares de Internet e “baixarse” contidos como música, películas ou xogos.

### **Tecnoloxía**

Para a descarga de contidos que “pesan moito” (gran tamaño) utilízanse principalmente 2 tipos de tecnoloxía.

#### **Descarga directa**

Co mesmo **navegador** descárgase o arquivo que está aloxado nun **servidor central**. Este servizo pode ser gratuíto aínda que tamén hai versións de pago que garanten a velocidade de descarga.

Exemplos de estes servizos son RapidShare ou MegaUpload.

### ***Programas “Peer to Peer”***

Para o emprego da tecnoloxía “peer to peer”, P2P ou “entre iguais” é necesario contar con programas específicos. Os arquivos están aloxados entre moitos ordenadores, non nun ordenador central. Mentres se baixan os datos que faltan, tamén se están a compartir (subir).

Hai varios sistemas cos seus programas correspondentes. Os máis populares son eMule e Bittorrent.

### ***O teléfono móbil***

Os móbiles actuais que teñen acceso a Internet son coma ordenadores pequenos. Pódense usar tódalas posibilidades de Internet aínda que o uso principal é para o envío de mensaxes e o compartimento de contidos en redes sociais xa que nestes usos é cando se aproveita máis a inmediatez e ubicidade do teléfono.

## **Riscos e ameazas**

### ***Virus, vermes, cabalos de troia...***

O “malware” son **programas informáticos** creados para facer **dano**. Pódense clasificar de moitas formas segundo as técnicas que empregan: **virus** polo seu método de contaxio, **vermes** pola súa capacidade de reproducirse a si mesmos ou **cabalos de troia** por camuflarse dentro de programas lexítimos.

### **Métodos de contaxio**

Un ordenador pode ser contaxiado a través de varios puntos vulnerables.

O método máis habitual é a **execución dun programa que inxecta o virus**. Este programa pode estar **adxunto nunha mensaxe** de correo electrónico as veces enviado por unha persoa coñecida que xa é vítima do virus. Outras veces o virus viaxa en **disquetes, CD/DVD ou nas memorias USB** que ao introducires no ordenador se executan automaticamente. Tamén poden estar en arquivos descargados de Internet (descargas directas ou P2P).

Existe outro método de contaxio que saca proveito do mal funcionamento ou **vulnerabilidades** dalgúns programas coma o navegador ou incluso o mesmo sistema operativo para infectar o ordenador. Ao visitar unha páxina web programada especificamente para aproveitar este faio de seguridade o ordenador queda infectado. Incluso, cando o problema afecta ao sistema operativo, simplemente a conexión con Internet pode provocala infección.

### ***Correo non desexado***

O correo non desexado ou “spam” son mensaxes enviados indiscriminadamente con intencións propagandísticas ou criminais. O “spam” pódese utilizarse para tratar de difundir virus, obter outras direccións de correo para facer máis “spam”, estender información falsa (bulos) e servir de vehículo para distintos tipos de fraudes.

### ***Timos e fraudes***

As cadeas de correos poden servir para a propagación de **información falsa** por parte de grupos interesados. Tamén coma método de facerse con **direccións de correo para facer máis “spam”**. Un exemplo pode ser unha mensaxe que pide visitar unha páxina ou enviar mensaxes a unha

dirección dunha organización humanitaria que resulta ser falsa.

Noutras ocasión prometen **ofertas de emprego falsas** que resultan ser trampas para facer de intermediarios en operacións ilegais. Por exemplo, piden os teus datos bancarios para ingresar cartos procedentes de operacións ilegais que piden que transfiras ao estranxeiro cometendo un delito de evasión de capital.

Tamén é común o **timo nixeriano**: ofrecen algo de moito valor a cambio dun pequeno adianto de cartos.

## ***Roubo de identidade***

O roubo de identidade consiste en facerse pasar ou **suplantar a unha persoa** accedendo a un servizo, principalmente banca por Internet, contas de correo electrónico ou redes sociais.

No caso da banca por Internet a intención é **transferilos cartos** ou facerse cos **datos das tarxetas de crédito**.

A suplantación en contas de correo electrónico ou redes sociais ten coma obxectivo o roubo de información privada na busca de aspectos que podan ser obxecto de chantaxe ou de contactos para empregalos en outros timos ou fraudes.

## **Métodos**

Hai varios métodos para o roubo de identidade.

### ***Adiviñar o contrasinal***

Trátase de adiviñar os datos de acceso do usuario **probando** con combinacións aleatorias, utilizando listas de contrasinais máis comúns (“123456”, “qwerty”, “password” ...) ou incluso empregando datos da vítima (data de nacemento, DNI...) obtidos de páxinas públicas, mensaxes de correo ou porque o suplantador coñece á vítima.

### ***Virus***

Moitos virus están preparados para obter os datos de acceso persoais. Así, cando se accede a unha páxina dende un ordenador que está infectado por un virus de este tipo, esta información é reenviada á organización criminal para o seu uso.

### ***“Phising”***

Outro método é o “phising” que se refire ás prácticas que tratan de enganar ao usuario facéndolle pensar que está enviando os datos de acceso no sitio correcto sendo este fraudulento. O máis habitual é a falsificación da aparencia dunha páxinas web: a través dun enlace dun correo electrónico falso chégase a unha páxina falsa que captura, que aparenta ser a do banco.

## ***Comercio electrónico e poxas***

Coma no real, o comercio electrónico pode ser unha fonte de riscos: vendas de obxectos falsos ou defectuosos, cobros incorrectos, reutilización dos datos para outros cargos. O risco acrecéntase nas tendas no estranxeiro e nas vendas de materiais non permitidos en España coma fármacos ou armas.

## ***Privacidade e intimidade***

Tanto por roubo de identidade, por mal uso dos controis de privacidade ou por terceiros que distribúan información persoal, o dereito á privacidade e a intimidade pódese comprometer en

Internet.

Calquera persoa pode distribuír ditos contidos por correo electrónico, en páxinas persoais ou blogs e en redes sociais.

É importante salientar que non fai falla ser usuario de Internet para ser vítima deste problema.

## ***Ciberdelincuencia dirixida ó Menor***

A diario asistimos preocupados ante os datos que sobre acoso, sexual ou de outra índole, e pornografía infantil están a verter con fins informativos e disuasorios todos os medios de difusión. Son datos preocupantes, e que requiren da nosa máxima atención. Sería desexable unha pronta, enérxica e eficaz solución a este problema, nembargantes de difícil enfoque no eido globalizado de Internet.

O desenrolo das **TIC (Tecnoloxías da Información e Comunicaci3ns)**, e a idea de **aldea global**, que tantos **aspectos positivos** trouxeron a nosa sociedade actual, xeraron indirectamente un incremento exponencial dun tipo de delincuencia, a dirixida os menores no eido das TIC.

## **Condutas delictivas**

Existen dúas razóns principais que dan orixe a este tipo de ciberdelincuencia e que hai que saber diferenciar. Por unha banda, a crecente demanda de pornografía infantil e por outra, o tamén crecente acoso do que son obxecto os menores por parte doutros menores cuxos fins non sempre teñen un enfoque sexual.

O acoso sexual, a diferenza doutros tipos de acoso non menos importantes, derivan en primeira instancia nun negocio que move elevadas cantidades de diñeiro a diario. Os maioristas que manexan este tipo de negocio albérganse en “**paraísos legais**”, onde a prostitución infantil é algo habitual e os menores encóntranse legalmente desamparados. A conexión con estas redes, serve de motor ós pedófilos e pederastas que actúan dende outros lugares do mundo xerando e compartindo material para “disfrute persoal” o como parte de tal deleznable negocio.

## ***Desencadeantes***

A continuación descríbense tódalas condutas reprobadas pola nosa sociedade e tipificadas como **delito** polo Código Penal.

### **•Chantaxe**

Neste contexto denomínase ó acto de ameaza de difamación pública, ou outro tipo de danos, baseada normalmente en procesos de difamación e/ou difusión de imaxes e datos capturados do Menor sen o coñecemento deste. O fin normalmente é o de conseguir que a vítima actúe segundo os intereses da parte actora. Normalmente este comportamento buscado na vítima persegue fins de carácter sexual, aínda que nun menor número de casos a ameaza pretende obter algún proveito pecuniario transformándose en delito de extorsión no eido xurídico.

### **•Exhibicionismo**

Definido xeralmente como o acto por parte dun individuo de exporse publicamente de xeito espontáneo e axeo ás normas sociais, adquire neste contexto un carácter de exhibición obscena castigado pola Lei, de maior gravidade no caso de ser dirixido a menores de idade. No contexto cibernético, o autor tratará de exhibirse ante o Menor, mediante envío de fotos nu, ou mediante o uso dunha Webcam.

### **•Grooming**

Término aparecido no eido de Internet, e referido ó conxunto de accións deliberadas levadas a cabo por un adulto e dirixido a un menor con fines sexuais. Parte do establecemento de lazos de confianza, e incluso amizade, ó longo do tempo co Menor. Persegue obter imaxes eróticas ou pornográficas deste, e nun alto número de casos a consumación dun encontro sexual.

#### •Ciberbullying

No contexto telemático, fai referencia ó uso de distintos medios dende os que se exerce acoso psicolóxico entre iguais, e dicir, entre menores de idade. Diferénciase do grooming principalmente en que o acosador é un Menor e o tipo de acoso non é de índole sexual . Os medios habituais son Internet, xogos online, foros, e telefonía móbil.

#### •Captura e difusión de imaxes/conversacións

Acción levada a cabo por parte dun adulto ou outro Menor, con distintos fins, e xeralmente co descoñecemento deste. Aparte dos casos de grooming e ciberbullying, estes datos intercámbianse en foros de contido ilegal, ou perseguen outro tipo de fins dos catalogados como delitos informáticos e descritos anteriormente neste dossier.

#### •Falsidade documental

Neste contexto, fai referencia ó acto de atribuír accións falsas a un Menor mediante atribución documental, xeración, almacenamento e difusión de información susceptible de prexudicar o seu honor. En moitos casos, este tipo de acción lévase a cabo no eido dos delitos informáticos descritos o longo deste documento.

### **Estadísticas**

Tal como mencionamos anteriormente, hai que facer diferenza entre os delitos cometidos por adultos a menores, e os cometidos entre menores. Referente a este último, só no ano 2008 rexistráronse entorno a 400 denuncias de **bullying**, casi todas na franxa de idade das vítimas de 12-13 anos, das cales un 20 % correspondéronse con **ciberbullying**.

#### •Fonte das denuncias

- Pais (63 %)
- Vítima (12%)
- Terceiros (7%)
- Familiares do autor (4%)
- Docentes (2%)
- Amigos ou coñecidos da vítima (1%)
- Outros (11%)

#### •Sexo da vítima

- Rapazas (55 %)
- Rapaces (45%)

No caso do **Grooming**, o número de casos multiplicouse por 15 nos últimos 4 anos, sendo significativos os seguintes datos:

#### •Comportamento da vítima

- Menores ciberacosados algunha vez (44%)

- Citas por Internet con descoñecidos (14,5%)
- Menores que acudiron ao encontro (10%)
- Menores que non avisaron a alguén antes de acudir á cita (7%)
  - Facilitación do número do móbil algunha vez (30%), dos cales o 17% afirma que o fixera a miúdo.
  - Facilitación da ubicación algunha vez (16%), dos cales o 9% afirma que o fixera a miúdo.

## **A vítima**

Este tipo de cyberdelincuencia ten como vítima a rapaces cunha idade por debaixo dos 18 anos. Mentres a franxa máis afectada polo cyberbullying (e polo bullying en xeral) sitúase a partires dos 12 anos, o grooming non diferencia a idade se temos en conta que o único que a limita por abaixo é a capacidade do Menor para poder establecer unha conversación por Internet. Evidénciase polo tanto a importancia dunha vixilancia tecnolóxica (mediante ferramentas informáticas) e paterna, se queremos poder educar aos nosos fillos en un ambiente seguro.

## **O Autor**

O autor do cyberbullying (e bullying en xeral), é un Menor no que recaen unha o varias das seguintes circunstancias: pais separados, fracaso escolar, desarraigo social, problemas cas drogas, problemas co alcohol, delincuencia. Na maior parte dos casos o autor basea as súas accións no anonimato, e non as interpreta como un acoso, e/ou abuso, senón coma un xogo, polo que a súa errada perspectiva do acto cometido lévalle a concluír que se trata dunha mala interpretación do “xogo” por parte da vítima.

O autor do Grooming, aínda que pode compartir algunha das características anteriores, non ten por que. Máis ben correspóndese cunha persoa que leva unha dobre vida, cuxa atracción pedófila lle leva a frecuentar o círculo do Menor, cuxo *modus operandi* comenza pola recabación de información dende perfís públicos. Unha vez elixida e identificada a vítima, pasa a unha segunda fase na que tratará de entra en contacto con ela, utilizando nesta ocasión outras ferramentas como son a mensaxería instantánea e o correo electrónico. Tras unha terceira fase, na que trata de gañarse a confianza do Menor, ven o envío de material pornográfico e conversacións de alto contido sexual. Na seguinte etapa fai uso da inxenuidade do Menor e do descoñecemento sexual, propio da súa idade, para invitalle a conectar a súa webcam, onde será gravado en escenas que atentarán contra a súa persoa e que o autor do grooming usará para comezar a coaccionar e chantaxear á vítima. Chegados a este punto, o menor en case todos os casos gardará silencio sobre o pesadelo que está vivindo e seguirá a vivir, exposto a importantes danos psicolóxicos e risco físico para súa persoa.

## **Marco Legal**

Existen diferentes aspectos legais de actualidade que se están a tratar entorno o marco do Convenio sobre Ciberdelincuencia do Consello de Europa. Neste senso hai que dicir que son moitos os aspectos a integrar e varios os axentes intervintes que teñen que traballar a diario neste ámbito cheo aínda de lagoas legais.

## **Rol da Xustiza**

### **•Amparo e protección do Menor**

Faise necesario dar amparo ás vítimas, ao mesmo tempo que se legisla para castigalos feitos en menores de 14 anos, onde actualmente os seus actos resultan inimputables.

### •Código Penal

Reformar e actualizar o Código Penal no referente a delitos informáticos, cubrindo as lagoas existentes actualmente.

### •Lei do Menor

Reformar a Lei do Menor (L.O. Do 12 de Xaneiro do ano 2000), para actualizalos contidos á realidade dos rapaces e rapazas comprendidos na franxa de idade entre 14 e 18 anos.

## ***Rol dos Corpos e Forzas de Seguridade do Estado***

### •Grupos estatais especializados

- Brigada de Investigación Tecnolóxica da Policía Nacional
- Grupo de Delitos Telemáticos da Garda Civil

### •Grupos autonómicos especializados

- Ertzaintza
- Mossos d'Esquadra

### •Fase de Instrución

- Denuncia
- Análises de indicios
- Fase probatoria
- Seguimento de tráfico e análise de datos
- Identificación e localización dos presuntos Actores
- Orden de rexistro
- Incautación de material
- Análise forense do material incautado
- Imputación de delitos

## ***Plans de acción***

Os pais están na obriga de participar das novas tecnoloxías de xeito activo, co gallo de coñecer mellor o que está a facer o Menor neste entorno e os riscos que lle rodean. Ó final deste documento relaciónanse direccións de interese onde informarse adecuadamente.

Por outra banda, cabe dicir que unha das tarefas que levamos a cabo os profesionais das TIC, dende hai tempo e de xeito constante, recae na **información** e na **formación** á Sociedade no ámbito das TIC. Neste senso, tanto a nivel nacional como autonómico, o Colexio Oficial de Enxeñeiros de Telecomunicación organiza charlas e cursos en coordinación cas distintas Administracións.

## ***Tarefas a desenvolver polos pais e fillos***

- Ensine ó seu fillo a ignorar o **spam** e correos de **descoñecidos**.
- Explíquelles que existen moreas de programas circulando na Rede, capaces de obter as súas claves de acceso.
- Sen que sinta atentada a súa intimidade**, sitúe nun lugar común o computador que utilizan os

rapaces para acceder a Internet. O ordenador con conexión a Internet no debería estar no cuarto do menor para evitar que se conecte a Internet pola noite sen a supervisión dun adulto. Un bo lugar para ubicar o ordenador sería no salón, de modo que a pantalla sexa sempre visible para calquera persoa que se atope no salón.

•Se por motivos de espazo o ordenador ten que estar no cuarto do menor é aconsellable tomar unha serie de medidas:

- Colocalo de modo que calquera que entre no cuarto poida ver a pantalla.
- Sempre que o menor use o ordenador debe manter a porta do cuarto aberta.

•Restrinxa (**ou de selo caso, evite**) o uso da webcam, mediante unha clave de acceso manexada por vostede.

•Fale de xeito natural co seu fillo deste tema. Fágase coa súa confianza para coñecer que fai cando accede a Internet.

•Incúlquelle que **non debe facilitar datos persoais** a través do computador a ninguén que coñecera por Internet. É moi importante que o menor saiba que non debe pedir ni dar información que poida identificalo como poden ser direccións, teléfonos, contrasinais. Tampouco debe compartir información relativa aos hábitos da familia como por exemplo a que escola vai, onde xoga, onde traballan seus pais, os seus horarios, etc. Se alguén insiste en pedirlle ese tipo de información a un menor, este debe alertar aos pais.

•O menor ten que saber que **non pode quedar só con xente descoñecida** e no caso de quedar debe ir sempre acompañado por un adulto.

•Do mesmo xeito, explíquelle que **nunca envíe material audiovisual a descoñecidos**, nin de el nin de outros.

•Razoe co Menor, que o feito de colocar una imaxe persoal en perfíles públicos pode dar lugar a un **uso ilegal** da mesma por terceiras persoas.

•Non cometa o erro de pensar que ten a situación baixo total control, xa que os rapaces móvense fora do seu fogar e poden acceder a Internet dende fora da casa. No caso de detectar contactos engadidos a programas de mensaxería, redes sociais, ou á súa dirección de correo electrónico, pregúntelle sobre eles e como se coñeceron.

•Fágalle entender o erro de concibir Internet como un “mundo virtual”, xa que os efectos nocivos, a miúdo e por desgracia, desenvólvense no mundo real.

•**Analice o comportamento do seu fillo.** Se amosa un comportamento ausente e preocupado, e detecta que está moitas horas diante do computador, pode estar vivindo un caso de cyberbullying o grooming.

## Boas prácticas

Non imos negar que existen riscos a hora de usar Internet, por moitas precaucións que tomemos, é inevitable que nalgún momento o menor se vexa exposto a contidos inadecuados ou a situacións conflitivas.

O feito de que hoxe en día a maioría dos rapaces teñen un maior dominio do ordenador que os seus pais, o que tampouco axuda moito nestes casos.

Pero a prohibición de dispoñer de conexión a Internet no fogar non é a solución, xa que o menor podería acceder a Internet na casa dalgún amigo ou en cibercafés sen a supervisión dun adulto.

Se establecemos unha serie de pautas co menor, será máis doado que saiba como actuar cando se atope ante algunha situación incómoda. Estas pautas non requiren ningún coñecemento informático previo. Aparte das comentadas anteriormente, daremos unhas recomendacións adicionais.

## ***Uso do ordenador***

- O menor non debería usar o ordenador que algún membro da familia use para temas laborais xa que corremos o risco de que accidentalmente entre un virus e destrúa información importante ou alguén acceda a información protexida.
- Limitar as horas que o menor adica a navegar por Internet. O menor tamén debe adicar tempo aos deberes, a xogar cos seus amigos a conversar cos seus pais.
- Non é recomendable que o menor se conecte a Internet antes de ir a durmir. Se o menor está a chatear antes de ir a durmir isto pode provocar alteracións no sono, pois os rapaces ao ir a deitarse seguirán pensando na actividade que estaban a realizar.
- Se hai varios nenos na casa establecer quendas para compartir o ordenador de forma que non sexa sempre o mesmo usuario o que monopolice o seu uso.

## ***Comunicación entre pais e fillos***

- Fomentar a comunicación entre pais e fillos. Animar ao menor a que informe a un adulto cando atope algún tipo de información ou se atope ante unha situación que o faga sentirse incómodo, lle desagrade ou o ofenda.
- O menor debería compartir as contrasinais do correo, Messenger, etc cos pais. É moi importante que se estableza un clima de confianza de forma que sexa o neno o que voluntariamente comparta esta información cos pais xa que se se sente espiado probablemente acabará creando contas de correo que os pais descoñezan.
- Ensinarlle aos rapaces que aínda que non se atopen cara a cara con unha persoa deben gardar as mesmas condutas de educación e respecto a hora de chatear, enviar correos, participar en foros, etc.
- Compartir experiencias co neno. É aconsellable que de cando en vez naveguemos ou chateemos co neno. Como se dixo anteriormente, tamén é aconsellable manter conversas casuais con eles para saber que fan cando están conectados a Internet, que páxinas visitan, con quen chatean, a quen coñeceron, etc.
- Debemos de ter en conta que se o ordenador con conexión a Internet é usado por varios membros da familia, o menor pode acceder ao historial de navegación e ver as páxinas que anteriormente visitou outro usuario. No caso que anteriormente alguén visitase páxinas con contido para adultos quedaría un rexistro no historial facilitándolle o acceso ao menor.
- O menor debe saber que se chega a unha páxina na que se indica que o acceso a menores de idade non está permitido debe abandonar a páxina.

## **Ferramentas básicas**

### ***Precaucións básicas: Antivirus***

Constitúen a primeira barreira de entrada contra calquera ameaza, sexa esta:

- Ataque dende Internet
- Memoria ou lapis USB contaminado

- Outro computador na mesma rede WIFI ou cableada
- Un virus que entrou a través dun E-Mail
- Un virus introducido dentro dun documento de Word

Hai que resaltar que se non se dispón de antivirus, aínda que soamente esteamos conectados a Internet de forma pasiva e sen navegar, estamos igualmente expostos a estas ameazas. Isto é debido a que hai programas que realizan procuras automatizadas a través da Internet, buscando vulnerabilidades en equipos conectados, que tamén se chaman portas ou portos abertos. Polo tanto, a seguridade por adoptar unha actitude pasiva non existe.

Unha vez instalado, o antivirus vaise a encargar de actualizarse el só de forma automática para ter ao día a súa base de datos de ameazas. Isto vaille a permitir estar constantemente ao día dos últimos virus que circulan por Internet. Deste xeito vains a poder recoñecer e neutralizar.

A función do antivirus é monitorizar constantemente todas as vías de acceso polas que pode entrar un virus, detectalo e neutralizalo. Isto inclúe monitorizar todos os correos, todos os documentos, memorias USB, discos externos, conexión a Internet, etc

Ademais do termo xenérico de virus que se aplica a calquera elemento daniño que nos pode entrar no ordenador, hai toda unha serie de termos máis especializados, que se poden enumerar neste pequeno glosario de ameazas:

•**Vermes ou gusanos:** Son programas moi similares aos virus, xa que tamén se autoreplican e teñen efectos daniños para os computadores, pero se diferencian en que non necesitan infectar outros ficheiros para reproducirse.

•**Troianos:** Un troiano ou cabalo de Troia é un programa que se diferencian dos virus en que non se reproduce infectando outros ficheiros. Tampouco se propaga facendo copias de si mesmo como fan os vermes.

•**Portas traseiras:** É un programa que se introduce no computador de xeito encuberto, aparentando ser inofensivo. Unha vez é executado, establece unha "porta traseira" a través da cal é posible controlar o computador afectado. Isto permite realizar no mesmo accións que poden comprometer a confidencialidade do usuario ou dificultar o seu traballo.

•**Spyware:** O spyware é un software que recompila información dun computador e despois transmite esta información a unha entidade externa sen o coñecemento ou o consentimento do propietario do computador. O termo spyware tamén se utiliza máis amplamente para referirse a outros produtos que non son estritamente spyware. Estes produtos, realizan diferentes funcións, como mostrar anuncios non solicitados (pop-up), recompilar información privada ou redirixir solicitudes de páxinas.

Hai programas, un pouco máis lixeiros que os antivirus, que ofrecen unha protección específica contra algunha destas ameazas en particular como os programas antispysware.

## Antivirus de utilización gratuíta para o fogar

Son a solución máis simple para o fogar. Un dos máis amplamente utilizados é o **AVAST na súa versión HOME** <http://www.avast.com/esp/download-avast-home.html>. Este fabricante de Antivirus pon a disposición dos usuarios, unicamente para a súa utilización nos fogares, unha versión gratuíta de libre distribución. Só é necesario descargala da súa web, executala e posteriormente, unha vez reiniciado o ordenador rexístrala. Todo o proceso é gratis.

Para evitar problemas é sempre importante descargar os programas do fabricante orixinal xa que existen un montón de webs de intermediarios que ofrecen en teoría a descarga gratuíta do programa pero á hora de utilizalo reclaman o pago por envío dun SMS ou calquera outra artimaña.

## **Antivirus de pago**

Existen unha gran cantidade de antivirus comerciais:

- Panda Antivirus: <http://www.pandasecurity.com>
- Norton Antivirus: <http://www.symantec.com/region/é/>
- Kaspersky: <http://www.kaspersky.com/sp/>
- ESET NOD32: <http://www.eset.es/>

Mentres que o nivel de protección é equiparable, o importante é dispor dun, non importa cal, xa sexa libre ou comercial.

Un aspecto importante a ter en conta é a renovación das licenzas. Un Antivirus coa licenza caducada é na maioría dos casos equivalente a non ter ningún tipo de protección. Isto é aínda máis importante no caso dos equipos de nova adquisición nos que un antivirus vén incorporado pero cunha licenza promocional, que normalmente caduca ao cabo de 3 meses co cal o equipo queda completamente desprotexido se non se fai nada para evitalo.

Outro aspecto a ter en conta é que mentres que normalmente os antivirus son intercambiabes no sentido de que é indiferente dispor dun ou outro a condición de que se dispoña dalgún, non son acumulables. Isto quere dicir que en ningún caso o nivel de protección aumenta por instalar 2 antivirus superpostos. É máis, normalmente a instalación dun antivirus sobre outro xa instalado non é recomendable e sempre é aconsellable desinstalar primeiro a versión de pago da que dispomos por exemplo, para instalar un de libre distribución.

## ***Configuración segura dos navegadores máis utilizados***

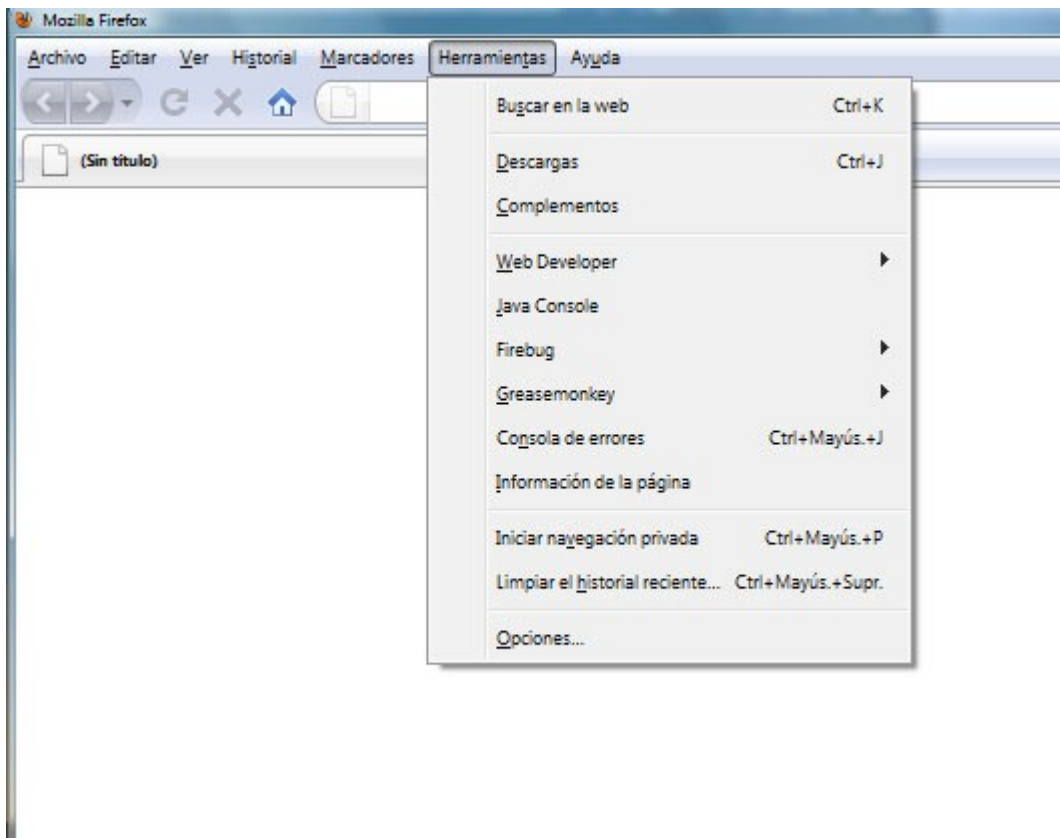
Aínda que adoita vir activado por defecto, é importante ter activo o bloqueo de elementos emerxentes ou pop-ups. Os pop-ups son as ventaniñas molestas con información comercial omnipresentes en moitas páxinas e que se non as bloqueamos rapidamente nos van a saturar a pantalla. Ademais esas fiestras poden redirxir o navegador a outra dirección co perigo que isto conleva.

Os navegadores máis utilizados hoxe en día son o Internet Explorer de Microsoft e o Mozilla Firefox. Mentres que o Explorer ven instalado con Windows, o Mozilla Firefox hai que descargalo de Internet aínda que de forma gratuíta da páxina <http://www.mozilla-europe.org/es/firefox/>

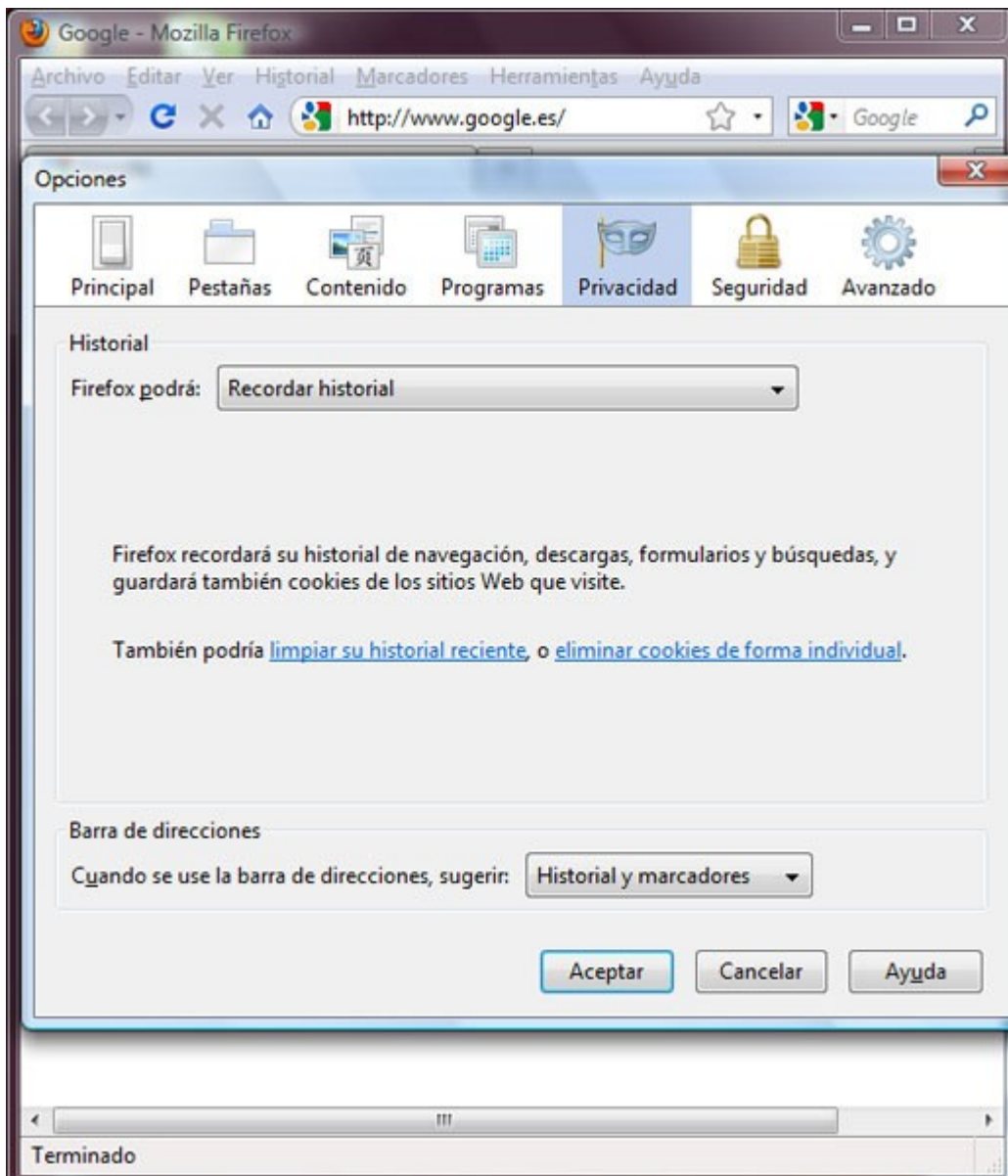
En xeral Mozilla Firefox é máis seguro e está exposto a moitas menos vulnerabilidades que Internet Explorer. Desgraciadamente a día de hoxe aínda que Firefox cumpre moito máis a raxatabla os estándares de navegación en Internet, hai páxinas que aínda funcionan ben soamente con Internet Explorer.

## **Firefox 3.5**

Para unha configuración segura do navegador Firefox, debemos acceder ás opcións de configuración.

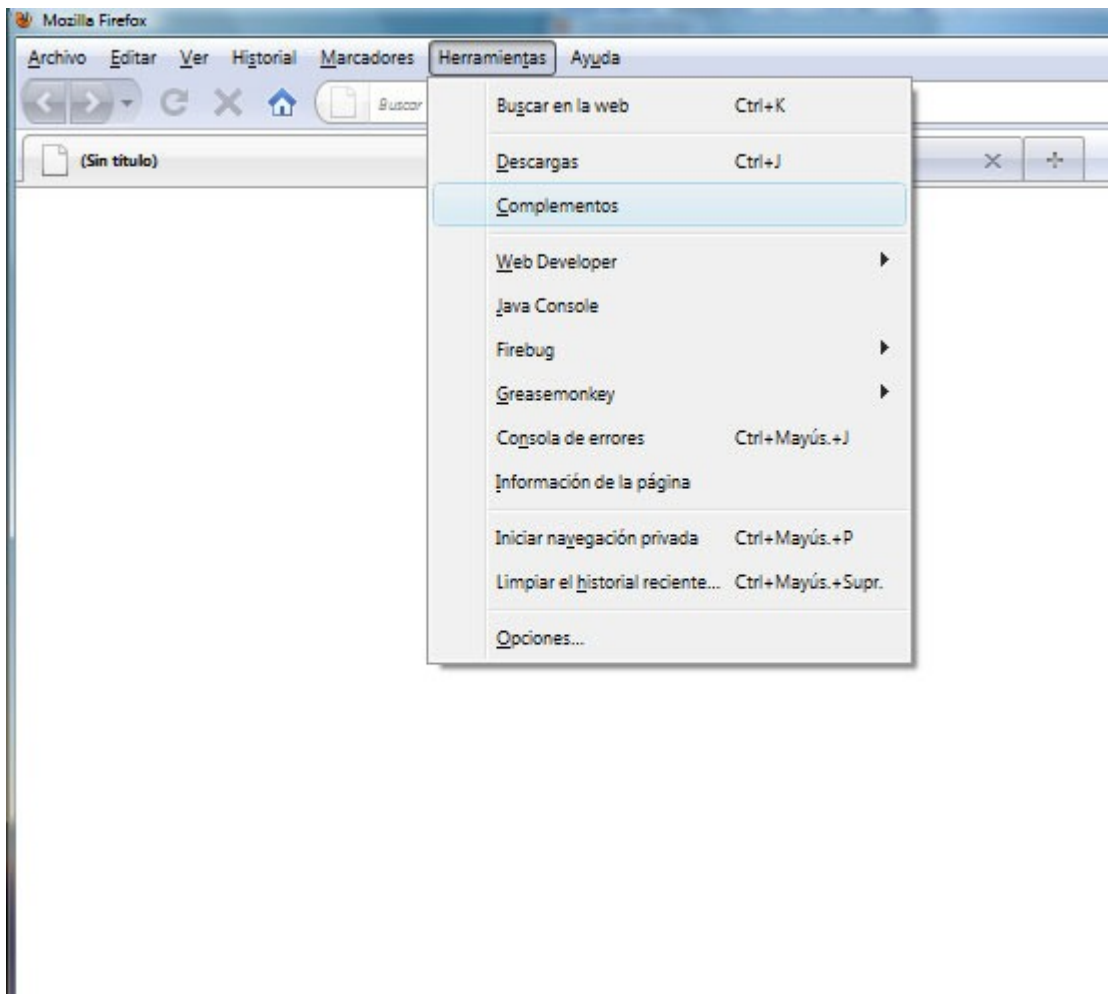


Dentro das opcións temos varias pestanas. Se seleccionamos a opción de Privacidade, dános acceso á limpeza do histórico así como a configurar de que xeito e con que periodicidade se pode borrar de xeito automático.



### ***Instalación de extensiones para unha navegación segura***

Mozilla Firefox permítenos instalar unha gran cantidade de complementos mediante os que se configuran funcionalidades adicionais que abarcan multitude de temáticas, desde procuras temáticas, instalación de barras de ferramentas modificadas a plugins para unha navegación segura. O acceso a instalación e configuración de complementos de Mozilla Firefox atópase indicado na seguinte imaxe.

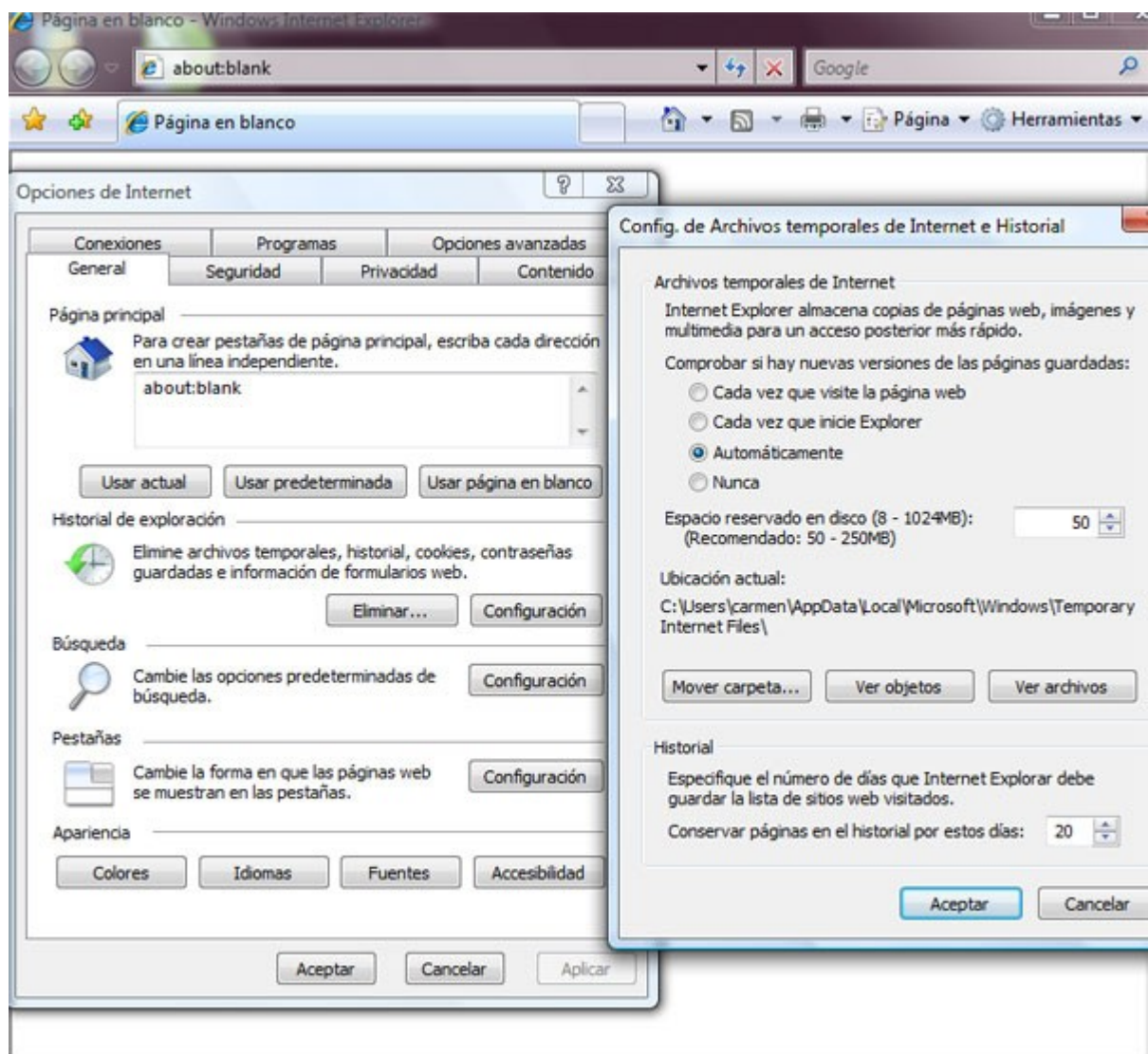


A páxina de acceso aos complementos de Mozilla Firefox é <https://addons.mozilla.org/é-É/firefox/>. Facendo unha procura polo termo kids vainos a aparecer unha lista cos complementos máis utilizados para filtrar contidos inapropiados para a infancia

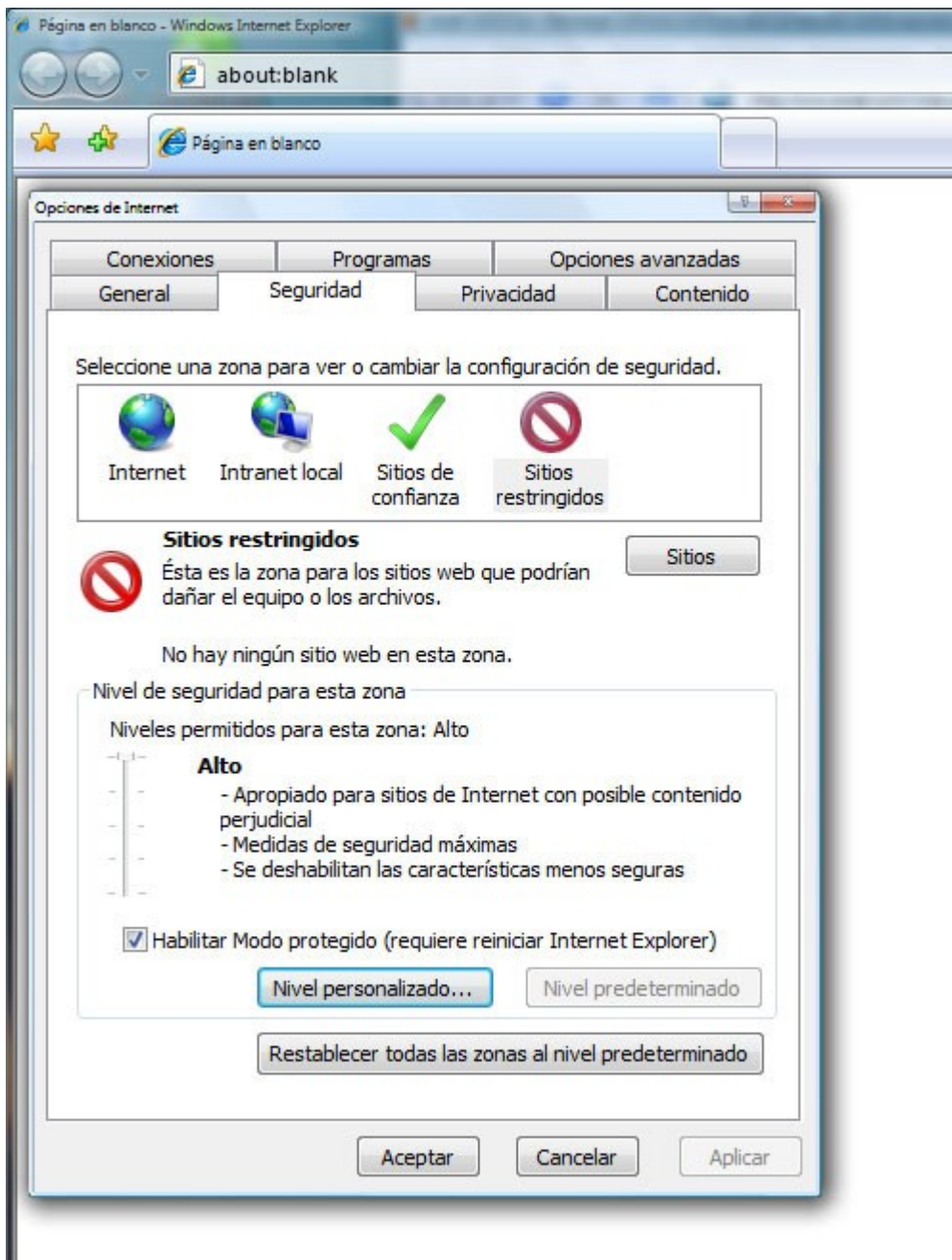
## Internet Explorer 8.0

O acceso ás opcións de configuración de Internet en Internet Explorer atópase ao igual que en Firefox, baixo Ferramentas -> Opcións de Internet.

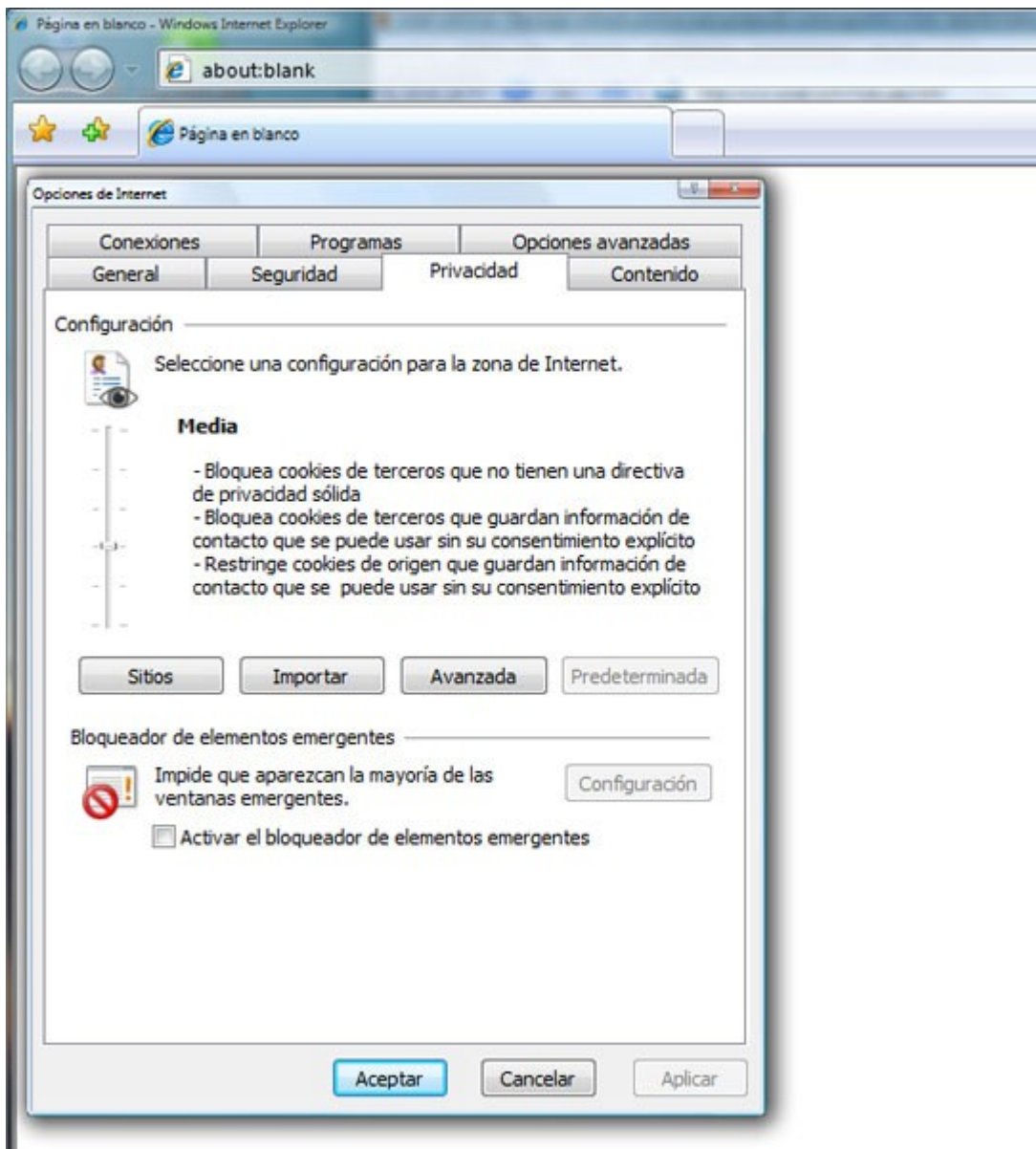
Dentro das opcións de configuración de Internet, podemos movernos por un sistema de pestanas a través de diferentes áreas temáticas. Se seleccionamos a pestana Xeral, dámos acceso á zona de borrado de arquivos temporais e configuración do borrado automático de históricos.



Seleccionando a pestana Seguridad podemos acceder á configuración de acceso restrinxido a determinados sitios.



Dentro da pestana de Privacidade podemos configurar diferentes niveis de protección no acceso a Internet.



## **Outros navegadores: Google Chrome, Opera, Safari (Apple)**

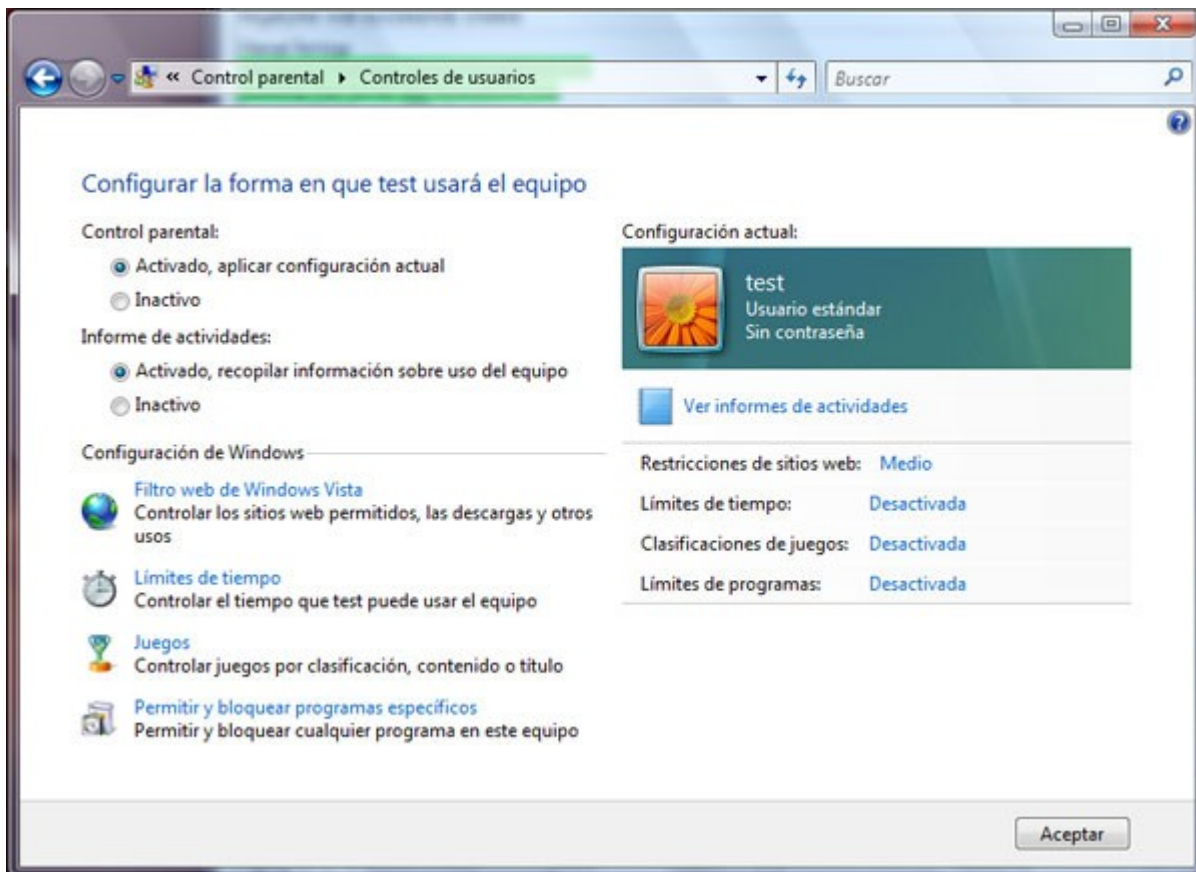
En xeral ofrecen un nivel de protección comparable ao de Mozilla Firefox e a súa utilización é xeralmente unha cuestión de gustos persoais e nivel de adaptación que se queira das propiedades do navegador. En todo caso a súa configuración é similar á de Firefox.

## ***Ferramentas de control parental***

Son unha axuda xa que non hai ningunha que sexa é 100% segura ou completa, todas presentan lagoas. Isto lévanos a resaltar a importancia do labor educativo e formativa que sempre debe estar presente se queremos un control parental eficaz e responsable.

## **Ferramentas de control parental no Sistema Operativo**

Nos casos dos últimos sistemas operativos de Microsoft, Vista e Windows 7, ven incorporada una ferramenta de control parental a que se accede dende o panel de control.



Nela pódense configurar dende as páxinas web que queremos filtrar, o tempo máximo de conexión, o tipo de xogos o que poden ter acceso oua lista de programas do computador que queremos permitir que se utilicen, podendo bloquear os programas de chat por exemplo.

## Ferramentas de control parental integradas no Antivirus

Os Antivirus comerciais inclúen habitualmente un filtro de control parental, pero a súa configuración pode ser un pouco laboriosa a non ser que se utilicen configuracións predefinidas nas que simplemente hai que contestar a preguntas do tipo si se teñen rapaces e si se quere protexelos.

## Ferramentas de control parental no router ADSL

O operador que nos prové o acceso ADSL a Internet xunto co router fornécenos un CD de instalación no que como unha das opcións de configuración está a posibilidade de bloquear contidos inadecuados.

Hai que resaltar que esta opción de configuración do router non está sempre dispoñible para os fogares e vai depender do operador: Así por exemplo R-cable non dá a priori a clave de acceso ao router e é necesario solicitala. R ten un produto de control parental de pago integrado nun kit de seguridade baixo o nome comercial de Seguridade R.

Por outro lado, Telefónica por exemplo, deixa sempre por defecto como clave 1234.

## Programas comerciais de control parental

Outra opción interesante é a posibilidade de adquirir unha ferramenta mellorada de control parental. Existen varios programas específicos para esta labora coñecidos como **Nanny's**, coma por exemplo

**Net Nanny 6.0** <http://www.netnanny.com/>. Neste caso esta ferramenta atópase tamén nunha versión demo gratuita durante 14 días.

### ***Exame periódico dos rexistros históricos de navegación***

Un exame simple e rápido dos rexistros de navegación máis recente consiste en facer click sobre a caixa despregable na que se introduce a dirección de navegación ou URL.

Apareceranos unha lista coas direccións web visitadas recentemente. Non entanto, é moi fácil borrar este histórico xa que non hai máis que elixir xeralmente en Ferramentas -> Opcións/Propiedades do navegador e seleccionar Borrar ou Limpiar histórico. Como consecuencia, se o histórico nos aparece baleiro, hai que pensar que o menor pode borrar o rastro voluntariamente.

### ***Exame das 'cookies'***

O seguinte nivel no exame de históricos serían as cookies. As cookies son uns pequenos ficheiros que as páxinas web ás que nos conectamos almacenan no noso computador. A súa función é que a próxima vez que nos conectemos, non teñamos que volver a introducir a mesma información que xa introducimos a primeira vez. Dende a opción do menú Ferramentas -> Opcións/Propiedades, na pestana Privacidade podemos examinalas facendo click en Mostrar cookies. Cada unha vai ter o nome do sitio web que a creou polo que en xeral serán da forma adopt.euroclick.com ou accesories.skype.com. O feito de que estean aí non quere dicir necesariamente que voluntariamente visitemos esa páxina pero o que debemos buscar aquí, e o tipo de información que debe alertar aos pais, é un exceso de cookies con nomes de contido dubidoso ou inapropiado.

## **Técnicas máis avanzadas**

### ***Filtros de contidos***

A función básica dun filtro de contidos é cortar o acceso, a través de Internet, a contidos ilícitos e inapropiados. Antes de pasar a comentar as diferentes técnicas de filtrado de contido que existen, imos intentar explicar que entendemos por contidos ilícitos e contidos inapropiados.

Son contidos ilícitos aqueles que van contra a norma penal e a súa publicación en Internet pode considerarse como delito. Por exemplo, material relacionado coa pederastia, a pornografía infantil, apoloxía do terrorismo, estafa, etc. Estes contidos non deberían estar dispoñibles en Internet e a nosa responsabilidade como cidadáns é notificalo á Policía para que faga as comprobacións oportunas e tome as medidas que correspondan en cada caso.

Son contidos inapropiados aqueles que, aínda que non van contra a lei, son nocivos para os menores pola súa natureza e/ou finalidade xa que pode interferir no seu normal proceso de educación/formación. Por exemplo, contidos pornográficos, relacionados coas drogas, violencia escolar e acoso, xogos de azar, incitación á anorexia, elaboración de explosivos, etc. O problema é que este tipo de contidos ten un matiz subxectivo moi elevado en función da persoa que os valore. Podemos atopar imaxes que para nós son altamente prexudiciais para os nosos fillos e, con todo, outros pais poden considerar que son educativas porque os seus fillos deben coñecer todo o que hai fóra.

Para calquera de ambos os tipos de contidos existen ferramentas que nos axudan a facer un filtrado previo e non cheguen a aparecer nas pantallas dos nosos computadores.

### **Diversas técnicas de filtrado**

Existen moitas técnicas de filtrado de contido. As máis usuais son:

- Filtrado por contido, que consta dunhas listas de recursos non apropiados aos que se impide o acceso e que se actualizan continuamente.
- Filtrado semántico, cuxo obxectivo é comparar as palabras dun texto cunha serie de palabras clave que están asociadas a contidos non apropiados. Pero presenta o problema dos 'falsos positivos', é dicir, as palabras con varios significados non todos nocivos, que son sistematicamente vetadas sen estudar o contexto no que están incluídas por exemplo a palabra sexo que excluiría tamén calquera referencia a educación sexual.
- Filtrado de imaxes, que analiza a imaxe analizando tecnicamente a imaxe e buscando características típicas das imaxes pornográficas.
- Filtrado por catalogación, que consiste en asociar a cada páxina web unha información relativa ao tipo de contido da páxina. É como unha etiquetaxe da páxina, transparente para o usuario. Con esta técnica facilítase o bloqueo de determinadas páxinas dende o navegador e ferramentas pero ten o problema de que é o propio provedor da páxina o que ten que autoclasificarse de forma voluntaria, xa que non existe unha lexislación respecto diso que obrigue a iso.

### ***Importancia de utilizar versións actualizadas do software***

É importante utilizar as últimas versións tanto dos programas dos que dispomos no computador como do sistema operativo. Isto permite que estes programas implementen os últimos parches de seguridade. A maioría dos programas hoxe en día permiten a opción de actualizacións automatizadas que nos permiten despreocuparnos deste proceso e debemos configurar simplemente a periodicidade coa que queremos que se actualicen.

### ***Banners con contido explícito***

Os Banners son anuncios ou publicidade en formato gráfico que aparece nas páxinas web. Moitas veces estas banners teñen contidos explícitos. Aínda que existen filtros para filtrar estas imaxes están moito menos difundidos e son máis complexos que as técnicas de filtrado tradicionais.

Hai que ter en conta que estes banners poden aparecer en páxinas completamente lexítimas como poden ser xornais ou portais de contido xenérico. Simplemente ter a precaución de non facer click sobre eles xa que nos poden redirixir o navegador a direccións completamente indesexadas.

En todo caso a maneira de actuar non debería ser diferente do que se fai na calle cando se ve unha valla ou cartel cun contido publicitario agresivo ou inapropiado, salvo por dúas diferencias fundamentais: na calle os contidos publicitarios están un pouco máis regulamentados pola visibilidade social que teñen e por outro lado o menor en Internet solo fronte a estes banners está moito máis desprotexido e pode sentirse máis confuso que nun espacio público.

### ***Procuras seguras en Internet***

Cando realizamos unha procura en Internet a través de Google, utilizando calquera termo común vaimos a saír un gran número de páxinas que fan referencia a ese termo. Aínda que os motores de buscas como google tratan de optimizar este proceso e facelo tan neutral como sexa posible, existen unhas técnicas coñecidas como SEO (Search Engine Optimization) que permiten que os provedores máis agresivos comercialmente figuren sempre nos primeiros postos desas procuras. Isto ocorre sistematicamente para case todas as buscas de produtos con valor comercial.

Os riscos de ir directamente aos primeiros resultados da procura van ser que descarguemos ou ben un programa fraudulento ou tipicamente que nos pidan diñeiro para completar a descarga. Estes servizos nas webs lexítimas van ser gratuítos, de aí a importancia de evitar no posible estes intermediarios.

A estratexia para evitar este tipo de agresións é moi simple: simplemente ignorar os primeiros 3 ou 6 resultados da procura e centrarse naqueles resultados que nos levan directamente á web do provedor, fabricante, etc con nomes de dominio curtos e terminados en .es ou .com.

## Referencias

### *Aplicacións*

- Facebook. <http://www.facebook.com>
- Tuenti. <http://www.tuenti.com>
- “Tuenti deja fuera a los menores de 14 años”.  
[http://www.elpais.com/articulo/tecnologia/Tuenti/deja/fuera/menores/anos/elpeputec/20090706elpeputec\\_5/Tes](http://www.elpais.com/articulo/tecnologia/Tuenti/deja/fuera/menores/anos/elpeputec/20090706elpeputec_5/Tes). Recuperado 1 de novembro de 2009.
- Termos de uso de Tuenti. [http://www.tuenti.com/#m=Corporate&func=view\\_terms\\_of\\_use](http://www.tuenti.com/#m=Corporate&func=view_terms_of_use)  
Recuperado 30 de outubro de 2009
- RapidShare. <http://www.rapidshare.com>
- MegaUpload. <http://www.megaupload.com>
- eMule. <http://www.emule-project.net>
- BitTorrent. <http://www.bittorrent.com/>

### ***Ciberdelincuencia dirixida o menor***

Poderá ampliar información sobre este tema nos seguintes enlaces:

[www.internautas.org](http://www.internautas.org)

[www.protegeles.com](http://www.protegeles.com)

[www.seguridadenlared.org](http://www.seguridadenlared.org)

[www.portaldelmenor.es](http://www.portaldelmenor.es)

Se sospeita que o seu fill@ está sendo vítima de grooming o cyberbullying:

- Póñao en coñecemento das autoridades policiais o antes posible. Pode poñerse en contacto coa Policía ou Garda Civil da súa Localidade ou ben directamente cos grupos especializados:

#### **Brigada de Investigación Tecnolóxica da Policía Nacional**

[www.policia.es/bit/index.htm](http://www.policia.es/bit/index.htm)

#### **Grupo de Delitos Telemáticos da Garda Civil**

[www.gdt.guardiacivil.es/](http://www.gdt.guardiacivil.es/)

- Ata recibir a axuda dos Corpos e Forzas de Seguridade do Estado, recabe toda a información posible que lle sea útil ós grupos especializados da Policía e Garda Civil: Información enviada e/ou recibida (mensaxes de correo, fotos, vídeos,...), nick do autor, correo electrónico do autor, sitios que ha frecuentado co menor (salóns de chat, redes sociais, programas de mensaxería, ...)
- Co total seguridade, os grupos especiais da Policía e da Garda Civil necesitarán da súa colaboración activa na fase de instrución. Colabore con eles o máis que lle sexa posible, na medida dos seus coñecementos informáticos.
- En calquera caso, recorde que para calquera dúbida pode poñerse en contacto con profesionáís que

Ile poden axudar nestas tarefas:

**Colexio Oficial de Enxeñeiros de Telecomunicación de Galicia / Asociación de Enxeñeiros de Telecomunicación de Galicia**

[www.aetg.org](http://www.aetg.org)

**Colegio Oficial de Ingenieros de Telecomunicación**

[www.coit.es](http://www.coit.es)

## **Ferramentas**

•Canguro Net de Telefónica

[http://www.telefonicaonline.com/qx/faq/faqscanguro\\_generales.htm](http://www.telefonicaonline.com/qx/faq/faqscanguro_generales.htm)

•mundo-R: Filtrado de contenidos para Internet y televisión digital

<http://respuestas.mundo-r.com/>

•Seguridad R: Pack de seguridad de pago en R que incluye Control Parental

<http://seguridade.mundo-r.com>

•Control parental de Jazztel

<http://www.jazztel.com/hogar/>

•Información sobre como configurar el Control Parental en los diferentes modelos de routers

<http://www.adslzone.net/>

•Configuración segura red Wifi

[http://cert.inteco.es/Proteccion/Configuraciones\\_seguras/WiFi/wifi\\_medidas\\_basicas/](http://cert.inteco.es/Proteccion/Configuraciones_seguras/WiFi/wifi_medidas_basicas/)

•Decálogo para que su hijo tenga problemas en Internet

<http://menoresenlastic.fundacionctic.org/2009/10/06/decalogo-para-que-su-hijo-tenga-problemas-relacionados-con-internet/>

## **Autores**

*Fernando José Mato Méndez, Natalia Alonso Fontela, Miguel Gonzalez Alvarez, Jose Monteagudo Limeres*