GUÍA PARA ...

Padres, hijos, profesores, orientadores, monitores...

NAVEGA SIN MIEDO ... PERO CON CUIDADO

EL JUSTICIA DE ARAGÓN

GOBIERNO DE ARAGON
Departamento de Ciencia, Tecnología y Universidad

El importante desarrollo de la tecnología de la información y de la comunicación, y, particularmente, la enorme potencialidad de Internet para transmitir información, intercambiar contenidos y establecer contactos con otras personas, ha supuesto un enorme cambio en nuestro modelo social, al permitir a cualquier persona, el acceso a los contenidos de la Red.

Los menores, como parte activa de la sociedad, son también usuarios asiduos de Internet, a la que acuden, tanto para jugar y comunicarse con otras personas, como con la finalidad de obtener una fuente de conocimiento en su proceso de aprendizaje. Ello encierra la posibilidad de que los menores estén expuestos, de forma accidental o consciente, a materiales inadecuados, bien porque vulneren su dignidad, o porque supongan un ataque a los Derechos del Niño. La presencia de pornografía infantil en la Red, la violencia extrema o gratuita, la incitación al odio y la discriminación y los posibles contactos con personas que pueden engañar al menor entablando relaciones de abuso, han motivado la reacción de la sociedad para proteger los derechos de los menores.

Resulta prioritario el compromiso de todos los agentes sociales en la defensa de estos derechos, desde las familias, que deben enseñar buenas prácticas del uso de Internet a sus hijos, acompañándoles en su aprendizaje, hasta los poderes públicos y los Gobiernos, que vienen obligados a divulgar el conocimiento de esas buenas prácticas y deben eliminar las posibles perturbaciones que determinados contenidos de la Red pueden causar en los derechos y en la dignidad de los menores.

Sirva, para ello de ejemplo, la iniciativa que ahora presenta el Departamento de Ciencia, Tecnología y Universidad del Gobierno de Aragón.

Fernando García Vicente
JUSTICIA DE ARAGÓN

El Departamento de Ciencia, Tecnología y Universidad del Gobierno de Aragón tiene como uno de sus objetivos prioritarios la extensión del uso de las tecnologías en nuestro territorio para paliar los efectos de lo que se ha venido llamando “la brecha digital”.

Las tecnologías de la información y las comunicaciones han conseguido cambiar en poco tiempo nuestra manera de relacionarnos con los demás, de trabajar, de estudiar y de realizar transacciones varias. El segmento más joven de la población vive ya totalmente inmerso en este nuevo modelo de sociedad de la información y del conocimiento, aprovechando al máximo sus beneficios, y presentando también una mayor exposición a sus riesgos. Internet es, sin duda, una de las herramientas tecnológicas que más atractivo ofrece a los jóvenes, y también es la vía en la que se detectan mayores posibilidades de que se comprometa la formación en valores, tan necesaria en esas edades.

Desde la experiencia, los padres y tutores son capaces de percibir los riesgos potenciales de internet, aunque en muchos casos no sepan identificarlos exactamente, y tampoco cómo proteger a los menores bajo su tutela de esas amenazas. Este hecho genera desconfianza y, en algunos casos, un rechazo que creen justificado al uso de este tipo de herramientas tecnológicas.

A través de esta publicación el Departamento, con la inestimable colaboración del Justicia de Aragón, pretende transmitir un mensaje claro de que el uso de internet y, en general, de cualquier herramienta basada en las tecnologías de la información y la comunicación, es un elemento de progreso en nuestra sociedad, que aporta beneficios inmediatos en todos los aspectos de nuestra vida; pero, como ocurre con cualquier otra herramienta, hay que conocer los principios básicos para una utilización segura. Estas elementales normas de precaución son útiles tanto para la necesaria supervisión de padres, tutores y profesores, como para la tranquilidad de uso por parte de nuestros niños y jóvenes.

Siguiendo estas reglas básicas conseguiremos, como reza el título de la publicación, navegar sin miedo, pero con cuidado.

Ángela Abós Ballarín
CONSEJERA DE CIENCIA, TECNOLOGÍA Y UNIVERSIDAD
Gobierno de Aragón

NAVEGAR EN LOS MARES DE UN NUEVO UNIVERSO

Según los estudios del Observatorio Aragonés de la Sociedad de la Información, casi el 90% de los niños entre 11 y 14 años utilizan Internet, y de los jóvenes hasta 24 años el 98%. Internet se ha convertido en una herramienta básica para su formación, en un medio de entretenimiento y en un nuevo canal de comunicación y socialización. Por ello, tanto la familia como la escuela han de facilitarles el acceso pero, a la par deben educarlos para comportarse adecuadamente en este nuevo universo que, sin duda, será uno de los ámbitos donde se desarrolle su futuro.

Por su parte, los adultos pueden realizar infinidad de actividades en Internet, como conocer las noticias de actualidad, comprar multitud de productos y servicios, realizar trámites ante las administraciones, consultar información y, también, comunicarse con sus familiares y amigos e incluso hacer nuevos conocidos.

Pero, al igual que en el mundo real, toda prudencia es poca, ya que hay personas que pueden utilizar Internet para abusar de la curiosidad de los menores, engañar a los adultos o simplemente con el fin de crear dificultades en el equipamiento informático. En este folleto damos unos sencillos consejos para tratar de evitar los problemas que pueden encontrarse en la red, comenzando con los que tienen que ver con los menores y siguiendo por los que son comunes a todos los usuarios.

El primer consejo es muy sencillo: al navegar utilice, como en el mundo real, el **sentido común**. Desconfíe de **lugares** que le ofrezcan precios excesivamente baratos, relaciones que le parezcan extrañas, trabajos de ensueño y, en general, de todo aquello que esté fuera de lo normal en las relaciones personales y en las transacciones económicas. Si es adulto, traslade esta cautela general a niños y adolescentes, explicándoles pormenorizadamente los riesgos que conlleva el no ponerla en práctica siempre.

En chaval.red.es puede encontrar más consejos y links a lugares seguros para los niños.

Los deberes

A diferencia de lo que ocurre con las publicaciones tradicionales, no existe un control previo de los contenidos que se publican en Internet, donde, junto a publicaciones de gran calidad, pueden encontrarse sitios web con contenidos incorrectos o inexactos. Por ello enseñar a utilizar Internet en los estudios no es sólo enseñar a buscar en el *Google*, sino también a **identificar la fuente de la que proviene la información y a valorar su fiabilidad.**

Los juegos

Los expertos consideran que los juegos de ordenador contribuyen al desarrollo de numerosas facultades de los menores pero, como todo, deben utilizarse con medida. **Ponga un límite al tiempo de juego ante el ordenador y cúmplalo de forma estricta.** No permita que el ordenador se convierta en el único amigo de su hijo. **Compruebe si el juego indica la edad para la que es apropiado y, en todo caso, evite los de contenido violento.**

Las relaciones

Casi la mitad de los menores conversa por Internet *(chatea)* varias veces a la semana. Hay dos formas de hacerlo, una son los *chats*, "salones de conversación" en Internet donde cualquiera puede entrar identificándose únicamente con un apodo o *nick.* **Lo mejor es impedir que los niños entren a los chats, salvo que sean especiales para ellos y estén moderados por un adulto.** Otro medio para *chatear* son los programas de mensajería instantánea, como el *Messenger*, en los que los contactos se identifican con una dirección de correo electrónico y se les puede aceptar o rechazar. Este medio es mucho **más fiable, pero** los problemas surgen cuando la red de contactos se amplia mucho, de forma que **al final pueden introducirse en ella personas sobre las que el menor no tiene ninguna referencia.**

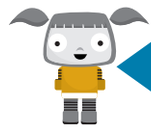
Reglas básicas

Para los menores

- No des nunca tus contraseñas, ni siquiera a tus amigos
- No des tus datos personales por Internet sin preguntar antes a tus padres o profesores
- No quedes nunca sólo con alguien que hayas conocido por Internet. Habla antes con tus padres y haz que te acompañen
- Cuando te encuentres en Internet con algo que te haga sentir incómodo o molesto, antes de seguir, consulta con tus padres o profesores
- Tapa el objetivo de la webcam cuando no la estés utilizando y no la uses **nunca** en conexiones con personas que no conozcas personalmente

Para los padres

- Instale el ordenador en una zona de uso común, **no en el dormitorio de los niños**
- No deje a mano de los niños las contraseñas, datos de las tarjetas de crédito y similares. No elija la opción de que el ordenador las recuerde
- La opción *Historial* de los navegadores le permite ver las páginas que se han visitado.
- Oriente al niño hacia lugares que sean de su interés y apropiados para su edad, hay muchos en Internet



Las herramientas de control parental son programas que impiden el acceso a contenidos pornográficos, violentos o racistas. Los navegadores más utilizados tienen una opción llamada Asesor de Contenido que permite filtrar los sitios a los que se accede. Y son muy aconsejables los programas específicos: gratuitos, como Naomi (http://www.radiance.m6.net/spanish.html), o de pago, como CiberPatrol, CiberSitter, Net Nanny, o el español Optenet.

Sea cuidadoso con su información personal

Algunos filtros antispam gratuitos:

G-Lock SpamCombat

www.glockksoft.com/sc

K9

www.keir.net/k9.html

Outlook Security Agent

www.outlooksecurityagent.com

SpamFighter

www.spamfighter.com

Spamihilator

www.spamihilator.com

SpamPal

www.spampal.org

Contraseñas

No dé nunca sus contraseñas. Todos los sistemas de banca y comercio electrónico están diseñados de forma que nunca hay que pedirle sus contraseñas o números de identificación, salvo para introducirlos en las pantallas correspondientes del web de la entidad. Por tanto en ningún caso le pedirán que las revele por correo, teléfono o ningún otro medio.

La estafa con más éxito en Internet es el phishing, que consiste en obtener las contraseñas mediante engaño, normalmente simulando ser un banco o una entidad oficial.

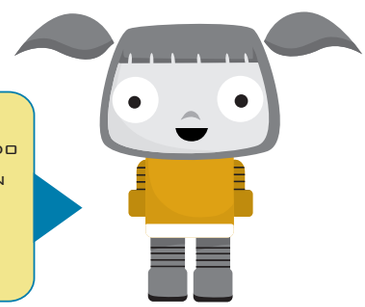
Dirección de correo

No de la dirección de correo a cualquiera, le ayudará a evitar el spam, que es el envío de correos no deseados y que se ha convertido en uno de los principales problemas de Internet. Si recibe uno de estos correos no lo abra, porque puede introducirle un virus, ni lo conteste, porque si contesta confirma al que lo envió que la dirección es correcta y está activa.

Datos personales

Sólo en algunos casos las autoridades pueden manejar sus datos personales sin su consentimiento. Tiene usted derecho a conocer la información que cualquiera tenga sobre su persona (derecho de acceso) y a obligar a que se deje de utilizar, si no hay una causa justa que lo impida (derecho de cancelación).

La Agencia de Protección de Datos es un organismo creado para proteger su información personal. Si quiere más información o presentar una denuncia visite: www.agpd.es



¿Con quién he conectado?

Verifique la seguridad de la conexión

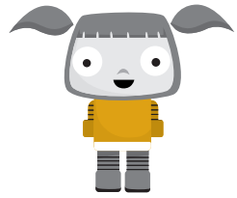
Los sitios web que le piden datos deben tener un certificado de servidor, que permite comprobar su identidad y hace que la conexión se cifre, de forma que no pueda ser leída por terceros. Busque un pequeño candado cerrado que aparecerá en el navegador y haga click sobre él, podrá ver los datos de identificación del sitio web.

Los comercios electrónicos

Los comercios electrónicos tienen que incluir en su web la denominación social, NIF, domicilio y dirección de correo electrónico de la empresa que los gestiona. También tienen que informar de los trámites que hay que seguir para contratar con ellas y de las condiciones generales de la contratación, así como confirmar la celebración del contrato enviando un acuse de recibo del pedido que se haya realizado.

Los conocidos virtuales

A través de Internet es posible hacer nuevos conocidos, pero también es muy fácil que estos nos engañen sobre quienes son realmente. Por tanto, no facilite información personal a quienes sólo conozca por Internet y, si decide concertar una cita, quede en un lugar público y, preferiblemente, vaya acompañado.



Aunque su uso no está aun muy extendido hay también certificados para las personas. Si alguien se identifica utilizando uno de estos certificados, por ejemplo firmando con él un correo electrónico, puede usted fiarse de su identidad. En España, los certificados personales más utilizados hasta la fecha han sido los emitidos por la FNMT y, recientemente, ha comenzado a expedirse el DNI electrónico, que incluye dos certificados, uno para firma y otro para identificación.

Utilice un antivirus

¿Qué son los virus?

Hablamos de *malware* para referirnos a los programas malintencionados. Entre ellos están los virus que tienen efectos perjudiciales y necesitan la intervención del usuario para reproducirse; los gusanos, que se reproducen solos; y los troyanos que bajo la apariencia de un programa "legal", esconden uno perjudicial.

¿Cómo entran los virus en mi ordenador?

Algunos aprovechan vulnerabilidades del sistema operativo. Para protegerse de ellos hay que instalar las actualizaciones que publica el fabricante. En el caso de *Windows* es aconsejable activar la opción de *Actualizaciones Automáticas*. Otros virus entran a través del correo electrónico, así que nunca abra correos de origen desconocido y elimínelos lo antes posible de su ordenador. Tenga en cuenta que suelen elegirse asuntos que despiertan la curiosidad del destinatario. Otro medio es la instalación del programa. Conteste NO cuando el sistema le diga, sin que se lo haya pedido, que se va a instalar un programa. También es muy útil navegar con una cuenta de usuario que no tenga permisos de administrador y desde la que, por tanto, no es posible instalar programas.

Hay también certificados que sirven para que los fabricantes firmen sus programas. Cuando instale un programa firmado el sistema le garantizarla la autenticidad e integridad del mismo.

Los antivirus

Son programas que identifican los virus y pueden buscarlos y eliminarlos escaneando los discos o, lo que aun es mas interesante, detectarlos cuando entran en nuestro ordenador. Es preciso actualizarlo con frecuencia para que pueda reconocer a los virus más recientes. Tener un antivirus actualizado es una medida básica de seguridad.

Algunos antivirus gratuitos:

BitDefender

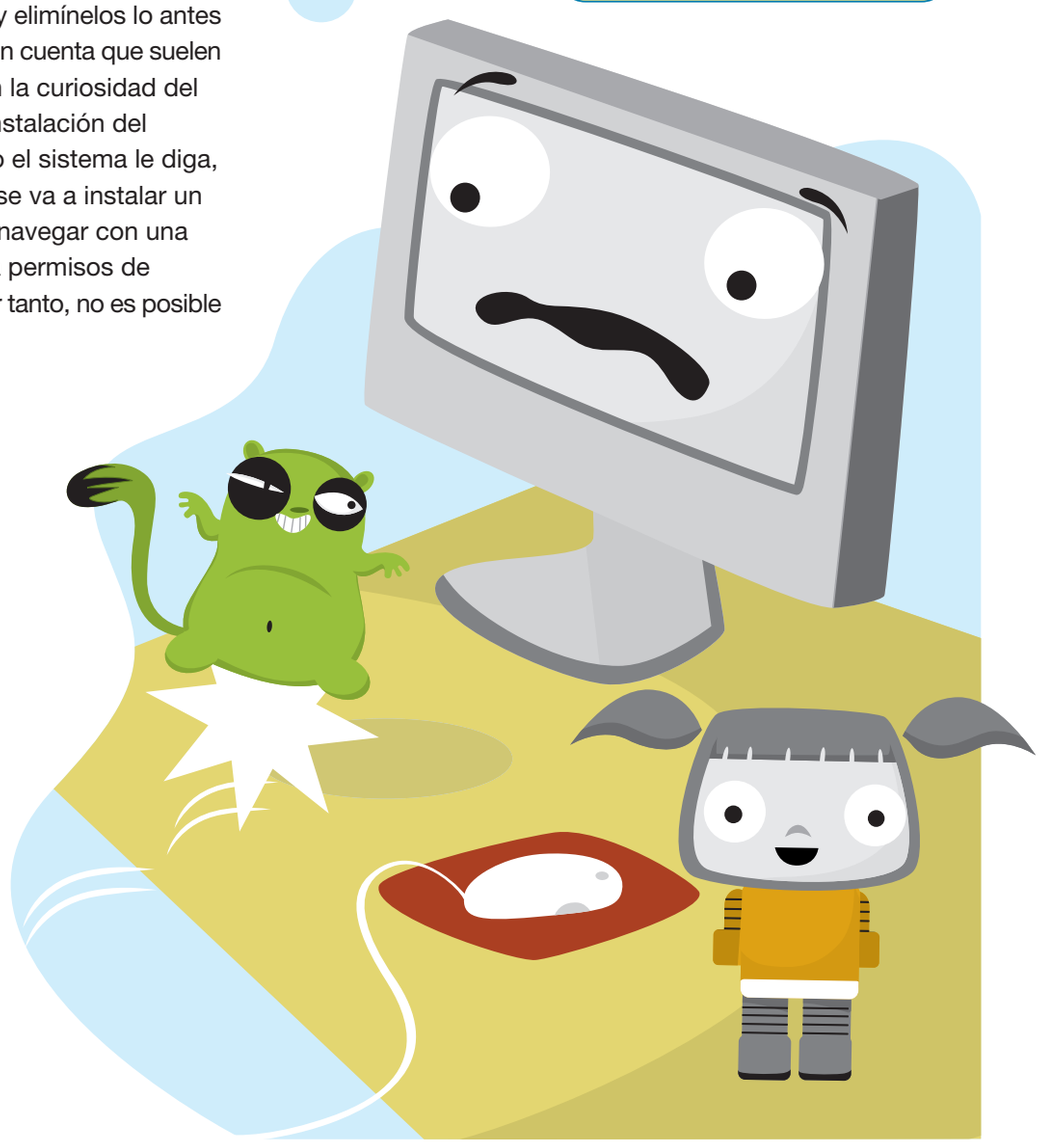
www.bitdefender-es.com

AntiVir

www.free-av.com

Free avast!

www.asw.cz



Controle lo que entra y sale de su ordenador

Los programas espía *(spyware)*

Hay espías "buenos", como la barra de búsqueda de *Google* a la que usted autoriza para que envíe a *Google* información sobre las búsquedas que realiza. Pero hay también programas que se instalan de forma oculta en su ordenador y pueden enviar sin que lo sepamos la información contenida en el mismo e incluso las contraseñas que tecleamos.

Algunos antispyware gratuitos:

Windows Defender
www.microsoft.com/spain/athome/security/spyware/software/default.mspx

AdAware
www.lavasoftusa.com

Evite que su ordenador se convierta en un zombie

Un ordenador *zombie* es aquel que, sin que su propietario lo sepa, está controlado por un usuario malicioso que, normalmente, lo emplea para fines como enviar spam, distribuir *malware* o como servidor para fraudes como el *phishing*. Son dianas fáciles los ordenadores que permanecen largos periodos encendidos para descargar música o videos, sin que su propietario adopte medidas de seguridad.

Los cortafuegos

Los cortafuegos son programas que analizan la información que entra y sale del ordenador. Evitan los ataques desde el exterior y, además, permiten detectar si el ordenador es un *zombie* o si tiene programas espía, ya que nos avisan de que hay programas desconocidos intentando enviar información a Internet. Junto con el antivirus son las medidas básicas de seguridad para un ordenador doméstico.

Algunos cortafuegos gratuitos:

Zonealarm
download.zonelabs.com comodo
www.personalfirewall.comodo.com

En el sitio
alerta-antivirus.red.es puede encontrar más antivirus y cortafuegos gratuitos.

Navegar sin temor ...

El Justicia de Aragón

GOBIERNO DE ARAGON
Departamento de Ciencia, Tecnología y Universidad