Recogidas del Libro Blanco para el uso educativo de las nuevas tecnologías e internet. **Junta de Personal Docente-Junta de Andalucía.**

1.Hable siempre con sus hijos e hijas sobre lo que hacen y encuentran en Internet.

2.Acuerde con sus hijos e hijas que nunca proporcionen información personal familiar: edad, dirección, DNI, teléfono, su propia imagen en fotografía o video, etc.

3.Tenga cuidado con el e-mail y los archivos adjuntos, cuando no conoce quién lo envía, ya que podrían contener virus o códigos maliciosos. Nunca abra correos sospechosos.

4.Muéstrese interesado por las amistades que sus hijos e hijas hacen en línea, especialmente en los sistemas de «chats», de mensajería instantánea (Messenger) y redes sociales (Tuenti, Facebook, ...).

5.Anime a sus hijos e hijas para que le informen de todo lo que les haga sentir incómodos, les desagrade u ofenda, o de aquello de lo que hayan tenido conocimiento en relación con los riesgos de Internet.

6. Hágales ver que acciones que para su hijo o hija puedan resultar de lo más normales, tienen su riesgo, como subir fotografías o videos propios a la red, que en cuanto a su difusión y por el número de personas que lo verían, podría ser algo similar a poner su foto pegada a todas las farolas de la ciudad o divulgar su video en todas las pantallas de publicidad.

7.Evite páginas con contenidos nocivos o falsos. No crea todo lo que encuentra, vea o lea en Internet. Circula por la Red mucha opinión o meros comentarios, más que verdadero conocimiento, por lo que se corre el riesgo de desinformarse más que de informarse.

8.Mantenga un contacto permanente con el Centro Educativo, en relación con el uso que sus hijos e hijas hacen de Internet.

9.No culpabilice a sus hijos e hijas sobre lo que ocurra en Internet, ni sea alarmista.

10.Acuerde un tiempo «generoso» para que sus hijos e hijas hagan uso de Internet, pero establezca un tiempo concreto de uso, así como un código familiar de uso de Internet. Es aconsejable que no se encierren en una habitación para navegar por Internet, sino que esto se haga en un lugar del hogar visible por todos. La manera más directa de evitar los riesgos en el uso de Internet es la prevención. Habría que tener siempre en cuenta estos dos principios básicos:

Las familias han de confiar en los centros y en el profesorado e informar a los tutores y tutoras de las incidencias que les parezcan sospechosas. Los padres y las madres han de confiar también en sus hijos e hijas, propiciando un ambiente familiar de comunicación confianza y libertad, utilizando conjuntamente Internet, hablando de ello, no culpabilizando siempre a los menores o no convirtiendo Internet en una nueva niñera, como la televisión, con la que tener a nuestros hijos e hijas ocupados.

11.La pérdida de la privacidad. Se produce cuando proporcionamos, a través de Internet, información sobre nuestra vida personal, o imagen personal, para poder entrar en determinados espacios comunes o para la utilización «gratuita» de servicios. Muchas páginas solicitan datos personales para un uso fraudulento de los mismos. ¿Qué medidas adoptar? No usar siempre el mismo nombre de usuario y contraseña en todos los servicios que utilice (si se desea conservar una misma contraseña, se le puede ir agregando algún número a la misma para que sea distinta según distintos servicios que se usen en Internet). No proporcionar, por principio, datos personales como nombre, dirección, número de DNI, número de teléfono o fotografías/vídeos suyas o de su familia.

12. El phishing Es el intento de adquirir fraudulentamente información de una persona, como la identidad y código secreto de una tarjeta electrónica o del acceso a los datos bancarios. Actúa a través de la recepción de un correo electrónico en el que en nombre de una entidad bancaria se pide al usuario esta información. El mensaje suele imitar conbastante exactitud la imagen habitual de la entidad. ¿Qué medidas adoptar? No proporcione nunca información sobre su cuenta bancaria, su identidad o el código de acceso. Informe a su entidad bancaria de la recepción de cualquier correo sospechoso.

13.El correo masivo (spam) y los virus El correo masivo consiste en la recepción de una gran cantidad de correo electrónico no solicitado, que invade y puede incluso bloquear las cuentas que utilizamos. Los virus - también los denominados «gusanos y troyanos»- causan serios problemas a nuestro ordenador: borrando información, tomando el control del mismo, adquiriendo información sensible, etc. ¿Qué medidas adoptar? Utilice algún programa de protección contra virus informáticos, y manténgalo actualizado. Utilice los sistemas anti-spam de su proveedor de Internet o del programa de correo electrónico. No abra nunca archivos adjuntos de un correo desconocido y borre el que no le parezca conocido.

14.Las compras por Internet Internet es, igual que sucede con otros medios de comunicación, un terreno dominado por la propaganda comercial igual que la T.V. Muchas

páginas que parecen orientadas a la «educación o el entretenimiento» contienen gran cantidad de anuncios de productos o servicios no siempre necesarios ni beneficiosos. Por otra parte es cierto que la compra «on-line» en algunas empresas es muy segura, pero comprar en Internet no es siempre seguro. Confíe en fórmulas de pago segura como "PayPal". Utilice tarjetas bancarias virtuales recargables (consulte con su banco estas opciones) que permiten realizar pagos como si de una tarjeta tradicional de plástico se tratase, pero cargándola sólo con la cantidad de dinero que se desee. ¿Qué medidas adoptar? Haga saber a sus hijos o hijas que no están autorizados a comprar por Internet, sin su permiso y consentimiento. Cuando vaya a comprar asegúrese que la empresa utiliza un «protocolo seguro» (compruebe que la dirección de Internet comienza con «https://» y que en la parte baja de la página web aparece un candado cerrado). No facilite sus datos personales y bancarios si no está seguro de la «fiabilidad» de la empresa en la que compra.

15.Los juegos de azar. Aunque no todos los proveedores son fraudulentos, conviene evitar el acceso a menores a dichas páginas. ¿Qué medidas adoptar? La mejor manera para evitar que sus hijos e hijas quieran utilizar juegos de azar es que usted no juegue a ellos ni en el mundo real ni en el virtual. Evite aquellas páginas en las que se anuncia un casino u otro juego de azar .

16.Acoso on-line, o a través del móvil (sms) Se produce cuando se acosa a un niño o niña a través de Internet, un programa de mensajería instantánea o por correo electrónico, o bien a través de mensajes a su teléfono móvil. Suele ser una continuación del acoso escolar, pero utilizando otros medios y no podemos subestimar los problemas que el acoso causa. ¿Qué medidas adoptar? No permita que sus hijos o hijas envíen mensajes o e-mails de acoso a otros niños o niñas; han de comprender que el acoso provoca muy serios perjuicios. Si sus hijos son objeto del acoso de compañeros y compañeras de la escuela, hable con el tutor o tutora. Recurra a informase e instalar en su ordenador soluciones de control parental.

17. Los contactos a través de Internet Existe el riesgo de que personas con intereses ocultos puedan establecer alguna vía de
contacto con sus hijos e hijas, generalmente por mediación de algún sistema chat, sin que el menor sea consciente de ello. ¿Qué medidas adoptar? Inscríbase y participe en los mismos chats que sus hijos para conocer qué se dice y de qué tratan.
Debería hacerles entender y aceptar a sus hijos e hijas que no pueden proporcionar información personal (fotografías, nombre, número de teléfono, dirección, etc.) a nadie en un chat o en Internet, sin su previo conocimiento. Nunca un menor puede encontrarse en persona con alguien que sólo conoce online, sin su conocimiento o presencia.

18.Los propios contenidos de Internet. Se trata de un riesgo que no suele ser tan conocido como los anteriores. Podemos encontrar páginas desde las que se incita a la anorexia y a la bulimia, otras que nos ofrecen contenidos racistas, xenófobos, pornográficos o aquellas otras en las que determinadas sectas pretender reclutar a nuevos miembros. ¿Qué medidas adoptar? Elabore un código de uso de Internet para toda la familia, con el tiempo de uso permitido y tipo de información a la que se puede acceder . Instale en el ordenador algún sistema de filtro que limite el acceso a páginas con información pornográfica. Utilice sistemas de búsqueda en Internet especialmente orientados a menores como por ejemplo: http://yahooligans.yahoo.com/ Si se accede a alguna página pornográfica, hable sobre la misma con el menor en lugar de ocultarla o culpabilizarle. Compruebe el historial del navegador de sus hijos y hable con ellos si encuentra páginas de estos tipos. Solicite información sobre sitios de Internet con contenidos interesantes para la formación y educación de sus hijos e hijas y visítelos con ellos. Si alguna vez encuentra sitios con contenidos como los mencionados, conviértalos en motivo de reflexión, discusión y debate con sus hijos e hijas.

Más información en:

• www.internetsegura.net • www.securytic.es •www.kiddia.org (portal familiar y para menores de 12 años) •www.37seis.org (para adolescentes de 12 a 17
años) • www.pantallasamigas.net •www.sexting.es El sexting, o envío de contenidos de tipo sexual (fotografías y/o videos) a otras personas que no los deseen recibir, por medio de teléfonos móviles o Internet. http://www.youtube.com/watch?v=xjRv3okyfww•Teléfono de información de la Consejería de Innovación, Ciencia y Empresa: **902 113 000** •10 claves para usar Internet con seguridad http://www.pantallasamigas.net/recursos- educativos-materiales-didacticos/cd-las- diez-claves/index.htm