



USO
SEGURO
DE LAS
NUEVAS
TECNOLOGÍAS



EDITA:

Servicio de la Mujer.

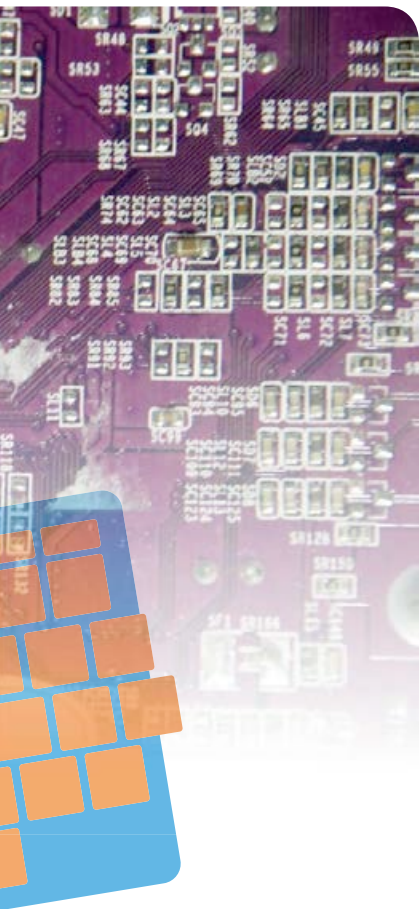
Dirección General de Familia y Salud.

Área de Familia, Asuntos Sociales y Zonas de Especial Actuación.

Ayuntamiento de Sevilla



Para empezar:



Las oportunidades que ofrecen las Nuevas Tecnologías de la Información y la Comunicación son incuestionables: el acceso instantáneo a la información, las relaciones sociales en la Red y el llamado ocio digital nos muestran que las Nuevas Tecnologías forman parte de nuestro proceso de socialización. Sin embargo, las TICs vienen acompañadas de nuevos desafíos: la posibilidad de acceder a contenidos inadecuados, el robo de datos personales, la suplantación de identidad o el ciberacoso hacen que sea necesario establecer estrategias de prevención y actuación conjunta para promover el uso responsable y seguro de las tecnologías digitales.

Para muchas personas jóvenes: Internet, los videojuegos o los teléfonos móviles, son un medio y un espacio para relacionarse, comunicarse, navegar, buscar información, jugar, estudiar, descargar música, etc. Sin embargo, por muy divertido que sea, no son un juguete, encierran riesgos potenciales y reales para menores y jóvenes. Por eso es necesario enseñarles a utilizar las tecnologías digitales de un modo adecuado, estando con ellos y ellas en todo momento hasta que aprendan un modo seguro y responsable de navegar por las mismas.

Algunos datos...

- El 84,6% de jóvenes de 15 a 29 años accede varias veces al día a Internet.
- Más del 87% de chicos y chicas utilizan Internet en primer lugar, para acceder a las redes sociales, seguido del uso de correo electrónico y la búsqueda de información o documentación.
- Los chicos y las chicas de 15 a 19 años son quienes tienen más personas agregadas en sus redes sociales siendo la media de 393 personas.
- El 28% de jóvenes entre 15 y 29 años considera probable quedar con alguien que ha conocido a través de Internet.





- El 51,5% de jóvenes usa las redes sociales para compartir fotos, videos, etc., cerca del 20% para hacer nuevos amigos y amigas y para ligar algo más del 9%.
- El 30% de chicos y chicas de 15 a 24 años (siendo este porcentaje algo superior en el caso de las chicas) ha tenido que pedir ayuda a su padre y/o su madre por contactos on line con personas extrañas.
- El 10,3% de adolescentes de 15 a 19 años ha encontrado contenidos explícitamente violentos o sexuales.
- El 7,4% de las chicas de 15 a 29 años reconoce haber sido objeto de acoso on line, reduciéndose este porcentaje en el caso de los chicos hasta un 2,1%.

Datos INJUVE (2011/2012)

CONOCIENDO CONCEPTOS BÁSICOS DE SEGURIDAD (conocer para prevenir)...

Qué son las actualizaciones del sistema operativo??

Son modificaciones en el sistema operativo del ordenador sugeridas por el propio fabricante con intención de solucionar problemas aparecidos o prevenir inconvenientes en el futuro. Es fundamental para la seguridad y confiabilidad del equipo.

Qué es un malware??

Es una aplicación informática que tiene como objetivo infiltrarse en el sistema operativo de un ordenador sin el conocimiento de su dueño/a y que puede comprometer la seguridad del mismo. Incluye virus informáticos, gusanos, troyanos y spyware (sistema espía).

Qué es un firewall (cortafuegos)??

Es una aplicación informática cuya función es proteger nuestro ordenador de intrusiones externas no deseadas. Permite o limita el tráfico de información entre el ordenador y la Red.

Qué es un antivirus??

Es una aplicación informática diseñada para detectar, bloquear, eliminar y, si es posible, prevenir las operaciones malintencionadas (malware) en un ordenador. Es el complemento obligado de un firewall (cortafuegos).

Qué es un hacking??

Es la entrada directa de una persona en un sistema informático sin el conocimiento de su dueño/a, ayudándose de alguna “vulnerabilidad” del equipo que lo permita.

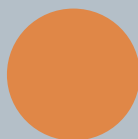
Qué es el spam??

También llamado “correo electrónico no deseado” o “correo basura” es el conjunto de mensajes no solicitados que, enviados masivamente, están en condiciones de perjudicar el equipo informático que los reciba.



Para evitar estas situaciones se deben adoptar, al menos, estas MEDIDAS DE SEGURIDAD:

1. Proteger el ordenador con un buen sistema antivirus y “cortafuego” (firewall) y mantenerlos actualizado.
2. Utilizar los sistemas antispam del proveedor de Internet o del programa de correo electrónico.
3. Instalar en el ordenador algún sistema de filtro que limite el acceso a páginas de contenido inapropiado.
4. Utilizar contraseñas fuertes que son aquellas que reuniendo algunas características (longitud mínima, uso de mayúsculas y minúsculas, inclusión de números,...) tienen menos probabilidad de que alguien las averigüe, cambiarla cada cierto tiempo, además de que no sea siempre la misma.



Los RIESGOS en la Red más relevantes para menores y adolescentes son...

1. Acceso a contenidos inapropiados.

La información en Internet viene acompañada de una problemática que es la posibilidad de que menores y adolescentes puedan encontrar imágenes o información de contenidos inapropiados: violentos, discriminatorios, sexistas, racistas,... Estos contenidos pueden llegarles al acceder a determinadas páginas, blogs, foros o a través de SPAM (correo electrónico "basura"). También pueden encontrarse con la publicidad emergente o "pops up", (pequeñas ventanas que se abren en el navegador encima de la página web que se está viendo), que en muchas ocasiones vienen referidas a contenidos, servicios y/o informaciones inapropiadas para ellos y ellas. Para evitar esto, es importante instalar un buen filtro parental/marental, que es una herramienta para impedir el acceso a este tipo de contenidos, para ello se puede visitar la página www.archivospc.com, que ofrece programas gratuitos de filtrado. Estos filtros, no obstante no sustituyen la necesaria labor de supervisión que deben realizar las personas adultas.



2. Conductas de acoso.

Hay quienes aprovechando el anonimato que permite la Red manifiestan comportamientos abusivos y/o violentos en la misma, especialmente con niñas y chicas jóvenes. Pueden desarrollar las siguientes conductas:

Ciberacoso o cyberbullying

Menores y adolescentes pueden ser víctimas de **ciberbullying** cuando a través de Internet, teléfonos móviles, consolas de juegos u otras tecnologías telemáticas son objeto de amenazas, humillaciones, hostigamiento, etc., por otra persona que también es menor de edad y que conocen en su vida “real”.

Acoso sexual o grooming

También pueden ser objeto de acoso sexual o **grooming** cuando una persona mayor de edad intenta ganarse su confianza a través de la Red para conseguir que le faciliten datos personales y de contacto, imágenes en las que aparezcan en ropa interior, de baño o semidesnudo/a, que posen ante la webcam con posturas “provocativas” o “eróticas” o en definitiva para concertar encuentros sexuales en la vida “real”.

Sextorsión o ciberchantaje

Cuando una persona utiliza los contenidos sexuales a los que ya tiene acceso y amenaza con publicarlos si la persona a la que chantajea no le envía nuevas imágenes o vídeos, no consiente tener contactos sexuales, no continúa con la relación de pareja, etc.

Existen **indicadores** de que el/la menor o adolescente puede estar siendo víctima de alguna de estas conductas: cuando pasa más tiempo del habitual delante del ordenador o por el contrario, apenas se conecta; que esté muy triste o con nervios después de consultar su correo o navegar por la Red; cuando no quiere ir al colegio o instituto sin motivos aparentes; tiene problemas para dormir o está más retraído/a,...

3. Amenazas a la privacidad.

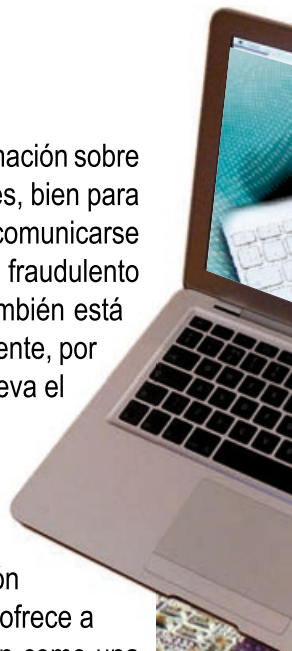
Puede producirse cuando proporcionan a través de Internet información sobre su vida o imágenes, bien para poder acceder a espacios comunes, bien para utilización gratuita de servicios o como forma de relacionarse y comunicarse con sus amigos/as. Muchas páginas solicitan datos para un uso fraudulento de los mismos. Esta exposición de la vida privada en la Red también está muy relacionada con las conductas de acoso descritas anteriormente, por ello es importante explicar e informar sobre los riesgos que conlleva el “colgar” información y/o imágenes en la Red.

4. Uso problemático y abusivo.

Internet, por características tales como la inmediatez, la posibilidad de adoptar nuevas identidades, el anonimato, la sensación de gratificación, la facilidad de acceso o el control en el manejo, ofrece a sus usuarios y usuarias una serie de recompensas que la sitúan como una herramienta con potencial adictivo. En este sentido, hay que estar atentos/as en el uso que nuestros/as menores y adolescentes hacen de las TICs.

Algunos **indicadores** de encontrarse en esta situación pueden ser: la pérdida de control y la dependencia en el uso de las tecnologías digitales, la ocultación tanto del tiempo de uso como del objetivo del mismo, el abandono de otras actividades y su sustitución por el uso de las nuevas tecnologías y/o los cambios de comportamiento.

En este sentido, sería importante elaborar un **CÓDIGO DE USO** de Internet **CONSENSUADO** para toda la familia donde se establezca **cómo** (herramientas de uso: ordenador, móvil, tablet, videojuegos,...), **cuándo** (horarios y tiempos), **dónde** (lugares: en casa, en el cole, en casa de amigos o amigas, zonas wifi,...) y **para qué** (objetivos, finalidad) usar la Red. Plasmarlas **POR ESCRITO** y fijarlas en un **SITIO VISIBLE**. Además puede visitarse la página www.tecnoadicciones.com (línea de ayuda sobre usos problemáticos asociados a las nuevas tecnologías).





5. Información abundante y de fácil acceso.

Internet es una fuente inmensa de información, pero ésta puede ser errónea o incompleta. Existen muchas páginas que sólo ofrecen el conocimiento parcial sobre algún aspecto concreto que dista mucho del conocimiento real y científico. Hay que buscar fuentes que nos ofrezcan credibilidad en sus informaciones u opiniones y contrastar cualquier noticia que encontremos en la Red. No quedarnos con la primera versión.

6. Spam, virus y otros.

Cuando nuestros/as niños/as y adolescentes tienen cuentas de correo electrónico se exponen a la posibilidad de recepción de spam que invaden el ordenador e incluso pueden bloquear sus cuentas. Además pueden ir acompañados de virus, también “gusanos y troyanos”, que causan problemas en los ordenadores: borrando información, tomando el control del mismo, adquiriendo información sensible, etc. Esta posibilidad de que los ordenadores adquieran virus está muy relacionado también con las descargas de archivos que se realizan. Para evitar esto es importante tener en cuenta lo dicho más arriba sobre las medidas de seguridad que se deben adoptar para proteger nuestras herramientas digitales que cuentan con conexión a la Red (ordenador, tablet, móviles, etc.).

En estos casos **CONSEJOS QUE PODEMOS OFRECER...**

- Enseñarles que nunca deben enviar datos personales que los/las identifiquen (nombre, apellidos, edad, teléfono, dirección de casa o del cole, contraseñas,...) y que sean iguales de cuidadosos/as con la información personal de sus familiares, amistades y conocidos/as.
- Explicarles que eviten publicar fotos o conectar la webcam con desconocidos/as, además de taparla cuando no se utilice, incluso aunque el ordenador esté apagado.(www.cuidadoconlawebcam.com).
- Decirles que no concierten citas con personas que hayan conocido a través de la Red.
- Pedirles que cierren inmediatamente cualquier página, chat o mensaje que les haga sentirse incómodos/as.
- Animarles a saber buscar y a seleccionar los contenidos.
- Invitarles a certificar la credibilidad y el rigor de las fuentes de cada web.
- Informales de la existencia de infracciones legales asociadas al uso de Internet (amenazas a través de la Red, intimidación/acoso sexual, delitos contra la propiedad intelectual, etc.) y de las consecuencias de su trasgresión.

TODO ESTO DEBE IR SIEMPRE ACOMPAÑADO DE LA NECESARIA Y PRECISA SUPERVISIÓN QUE DEBEN REALIZAR LAS PERSONAS ADULTAS.

La MEDIDA más IDÓNEA de evitar los riesgos en el uso de las Nuevas Tecnologías es la PREVENCIÓN

QUÉ PODEMOS HACER LAS PERSONAS ADULTAS??

1. Solicitar información y/o formación para acercarnos a las tecnologías digitales.
2. Actuar como referentes y modelos para nuestros/as menores y adolescentes en relación a las TICs. Sé tu mismo o tú misma buen ejemplo de su uso.
3. Fomentar la confianza y la buena relación con los y las menores y adolescentes a nuestro cargo para que tengan libertad para contarnos cualquier contratiempo que hayan tenido en el uso de las Nuevas Tecnologías.
4. Comentar con naturalidad y regularidad los riesgos que tiene la Red.
5. Navegar y chatear de vez en cuando con ellos y ellas y así conocer sus hábitos y preferencias y crear un clima de mayor confianza.
6. Supervisar activamente el uso que hacen los y las menores y adolescentes de las Nuevas Tecnologías.
7. Procurar que el ordenador se conciba como una herramienta de uso familiar: que se utilice con unas normas, con un objetivo concreto y con supervisión.
8. Colocar el ordenador en el salón o zona de uso común.

Para terminar enlaces de Internet:

www.protegeles.com

www.micueva.com

www.exprimelared.com

www.pantallasamigas.net

www.osi.es

www.kiddia.org

Policía Nacional (Brigada de Investigación Tecnológica):

<http://policia.es/colabora.php> *(para denuncias y consultas)*

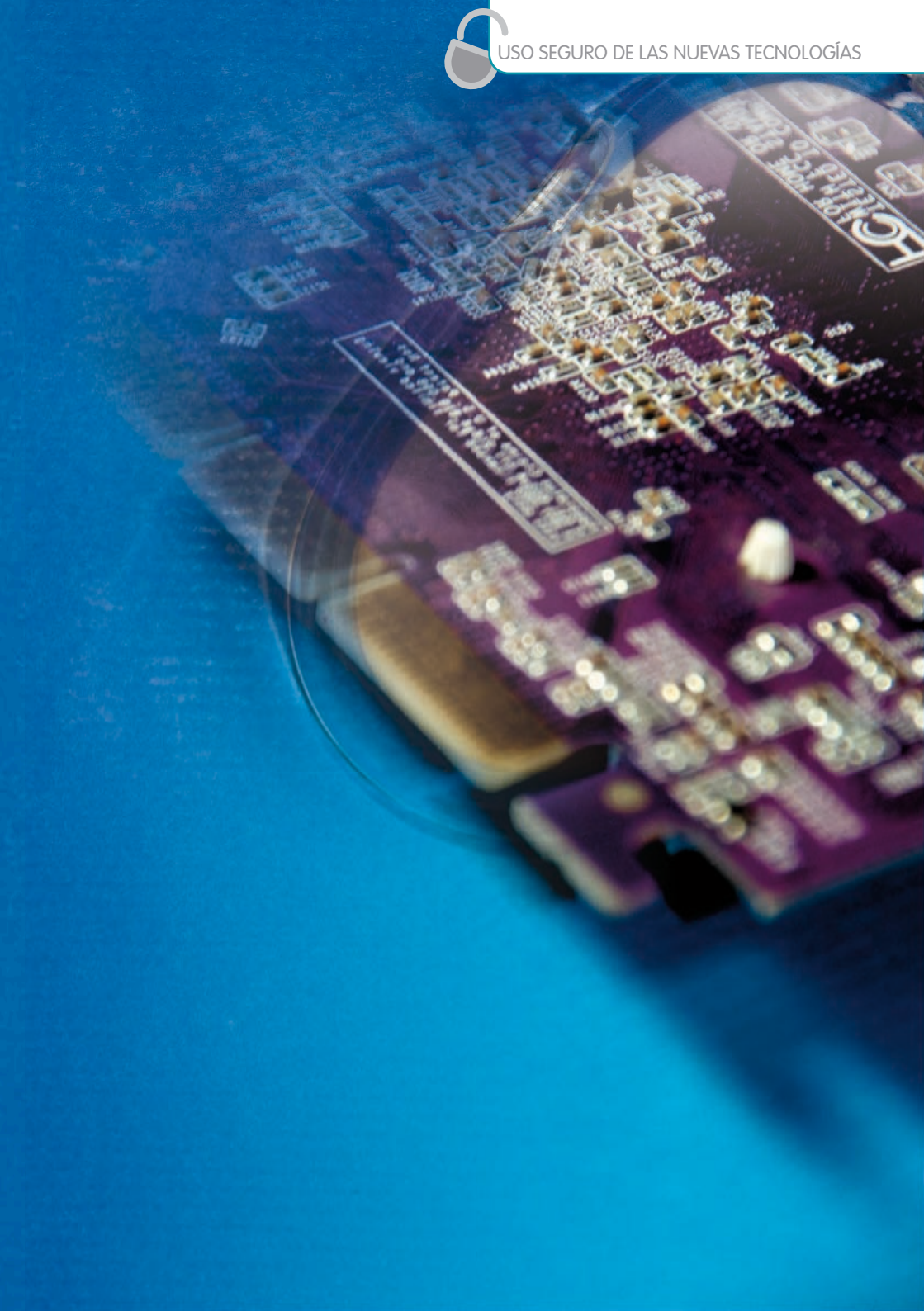
www.policia.es/bit/ *(web informativa)*

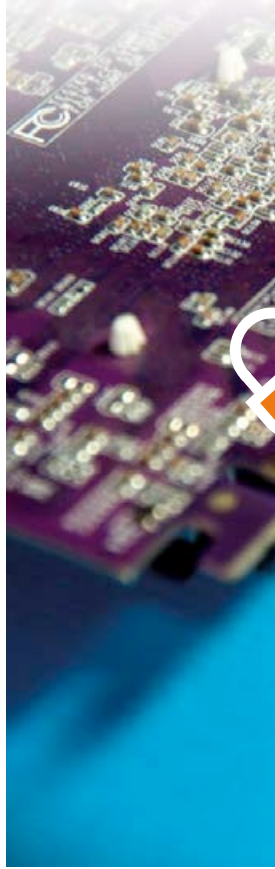
Email: delitos.tecnologicos@policia.es

Guardia Civil (Grupo de Delitos Telemáticos):

www.gdt.guardiacivil.es *(para información, denuncias, consultas, etc.)*

Tél: 900 101 062





NO8DO

AYUNTAMIENTO DE SEVILLA

Familia, Asuntos Sociales
y Zonas de Especial Actuación
Dirección General de Familia y Salud

www.sevilla.org