ACTÚA
Proyecto Juvenil de
Conciencia Social Positiva

JÓVENES

3.- REGLAS BÁSICAS PARA UN USO SANO DE LAS RRSS

3.1- SEGURIDAD Y PROTECCIÓN EN LAS RRSS
3.2- MI PÚBLICO HA DE SER PRIVADO
3.3- RIESGOS: AGUJEROS DE LA RED
3.4- ALERTAS

Asociación Participa para la Inclusión Social

Fundación María José Jove

3.1- SEGURIDAD Y PROTECCIÓN EN LAS RRSS

Las Redes Sociales (RRSS) no son en sí mismas positivas ni negativas; el uso que se haga de ellas y las condiciones en las que se produzca determinará si es un uso sano o dañino. Por tanto, utilizar responsablemente las RRSS implica ser consciente de los potenciales riesgos para tomar medidas que te protejan. Las siguientes recomendaciones pretenden orientarte sobre las diferentes opciones para ayudarte a un uso más seguro.

- Conoce y configura las **opciones de privacidad** de las diferentes RRSS y Apps. Haz que tu perfil sea privado, accesible sólo para tus personas de confianza y sin datos que puedan comprometer tu privacidad.

Haz uso también de las diferentes opciones que te ofrecen las Redes como "bloquear" o "denunciar" para mantener siempre tu privacidad y seguridad; por ejemplo, eliminar una imagen, vídeo o comentario que no queramos que sea público.

Existen opciones que permiten conocer tu localización en cada momento. En algunos casos son de mucha utilidad (excursiones, viajes, salidas...) pero hazlo conscientemente y con el conocimiento de tu familia porque, en determinadas circunstancias, es un riesgo que todos tus contactos y otras personas con dispositivos de búsqueda puedan saber en todo momento donde estás.

- Infórmate y respeta las **condiciones de uso** de las diferentes Apps, RRSS etc. que utilices. Algunas de ellas son de gran importancia y afectan a cómo y dónde pueden usarse nuestros datos (edad recomendada, derechos y/o difusión de imágenes, condiciones de alta, difusión de comentarios, opciones de bloqueo, borrado de contenidos, condiciones de baja...). Estas indicaciones mejoran el uso y manejo que se hace de las Redes.

Respeta también las indicaciones y rangos de edad y uso de las diferentes webs, RRSS y Apps, y cuenta siempre con la autorización de tus padres/madres/tutores para darte de alta en cualquier sitio web. La mayorías de RRSS y Apps tienen recomendaciones respecto a la edad de sus usuari@s. Es muy conveniente tenerlas en cuenta.

- Protege siempre tus **datos personales** para favorecer tu privacidad y seguridad. No difundas ni publiques datos como dirección, teléfono etc. en tus RRSS, chats o sitios web, y por supuesto no compartas esta información con personas desconocidas. También es importante no introducir datos de carácter personal (datos bancarios, contraseñas etc.) cuando usamos una red abierta y pública o cuando usamos un ordenador o dispositivo que no sea el nuestro propio y personal (en bibliotecas, cafeterías etc.). Si utilizas uno de estos dispositivos para acceder a tu e-mail, Red Social etc., recuerda siempre cerrar sesión al finalizar.

- Utiliza **contraseñas seguras y secretas** y no publiques ni difundas las mismas. Para mejorar tu seguridad puedes modificarlas cada cierto tiempo.

- Utiliza la **Webcam** sólo con quienes conozcas personalmente y cúbrela cuando no la utilices usando una pegatina o similar.

Del mismo modo, no aceptes ni abras documentos, archivos, e-mails etc. de personas desconocidas. Podrías poner en riesgo tu dispositivo y lo que es más importante, a ti mism@.

- **No creas todo lo que lees** en Internet. No toda la información que aparece publicada en la Red es cierta y alguna puede ser muy perjudicial. Contrasta la información por otros medios o consultando a un familiar o educador@.

- Mide el **tiempo de uso** que dedicas a las RRSS, Apps y dispositivos móviles en general. El tiempo pasa rápido cuando hacemos uso de nuestros dispositivos y puede que le dediques más tiempo del que crees. Puedes establecer un límite y unos horarios. La recomendación de l@s expert@s es no dedicar más de 3 horas al día.

Puede ser útil también desconectar las diferentes notificaciones de redes, juegos etc. que distraen nuestra atención con llamadas y avisos constantes. No es preciso consultar cada minuto el móvil. Establece pausas o momentos para consultar tus RRSS.

- Recuerda que **Internet es eterno**. Todo lo que subas a la Red (fotos, vídeos, comentarios…) quedará ahí almacenado de forma permanente y podrá ser visto por casi todo el mundo. Además, en muchas ocasiones, dejas de ser el propietari@ de esas fotos, vídeos etc. para ceder los derechos a las diferentes webs y/o plataformas. Tus contenidos o informaciones serán públicos en cualquier momento; ahora o dentro de 5 ó 10 años.

- El **anonimato no existe**. No es posible permanecer desconocid@ ni anónim@ una vez que te registras en una Red Social. Cuida tu identidad y la información que proporcionas a los demás.

- Recuerda que **insultar, amenazar, robar** contraseñas y/o **suplantar** la identidad de otra persona son delitos castigados por Ley.

No seas partícipe de mensajes o cadenas de mal gusto sobre otras personas y comunica siempre a un adulto si sufres acoso, amenazas, insultos etc. a través de cualquier dispositivo electrónico o si conoces a alguien que se encuentre en esta situación. Recuerda: "No trates a los demás como no te gustaría que te trataran a ti".

En el caso de que seas víctima de mensajes amenazantes, ofensivos o hirientes de forma continuada, no respondas a ellos y sigue estos pasos:

-Guarda los mensajes como pruebas.
-Si conoces a la persona, pídele que lo retire.
-Contacta con el administrador de la web, plataforma etc. para denunciarlo.
-Pide ayuda a un adulto; padres/madres, tutores, profesores etc.

- No subas, facilites o difundas fotografías, vídeos o información de terceras personas sin su **consentimiento**. Aunque se trate de personas de tu confianza debes consultarles siempre primero. Recuerda también que cuando envíes e-mails a varias personas, debes respetar la privacidad de las mismas y no dejar a la vista sus direcciones. Utiliza para ello la opción "con copia oculta" (CCO).

- Vigila tus **contactos**. No añadas a personas o "amig@s" que no conozcas personalmente ni aceptes peticiones o conversaciones de desconocidos, ni en la Red ni cara a cara. Al igual que no aceptarías por la calle la invitación de un extraño, no lo

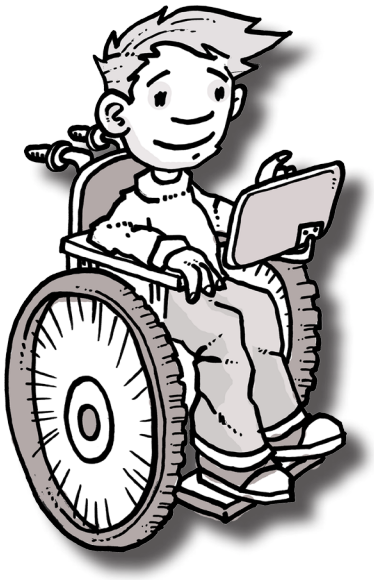
hagas de manera virtual.

Comenta también con tu red de amig@s o contactos que no deseas que se compartan fotos o información personal tuya de ningún modo, o al menos sin tu previo consentimiento. Haz que tus amig@s conozcan esta información.

- Ten especial precaución con las **personas desconocidas**. No difundas ni compartas información con estas personas ni aceptes documentos, e-mails o solicitudes por parte de las mismas. Por supuesto no utilices tampoco la Webcam ni quedes físicamente con ellas.

- Navega por **sitios web seguros** y evita el acceso a contenidos inadecuados. Debes mantener también siempre activo un programa antivirus en todos tus dispositivos.

- Protege siempre tu **identidad digital**; recuerda que ésta la construyes tú y que se mantiene de forma permanente y visible en la web. Mantén siempre una actitud proactiva en defensa de tu privacidad.



3.2- MI PÚBLICO HA DE SER PRIVADO

No publiques ni compartas en la Red **datos personales** como edad, teléfono, apellidos o DNI. Podrías ser víctima de un robo de identidad o poner en peligro tu seguridad.

Evita facilitar indiscriminadamente tu **dirección** y/o **ubicación**. Hay personas que pueden utilizarlo para robarte o acosarte.

Evita publicar **fotos comprometidas** que podrían buscarte un compromiso o situación no deseada (contenidos privados, íntimos...).

No compartas fotos de contenido **sexual**.

Evita publicar tus planes de **vacaciones** o salidas; a donde te marchas, con quien, cuánto tiempo etc. Facilitar esta información puede provocar que seas víctima de robos.

No difundas ni compartas nunca tus **datos bancarios**.

Evita poner tu número de **teléfono móvil** o fijo en la Red.

Las **contraseñas** no se deben compartir y han de ser seguras.

No compartas ni difundas **información de otras personas** sin su consentimiento (sean conocidas o no).

Presta atención a los **vídeos** que compartes o difundes, pueden convertirse en virales y ser vistos por cualquier persona.

3.3- RIESGOS: AGUJEROS EN LA RED

Cualquier Red Social precisa de la Tecnología de la Información y la Comunicación como aplicaciones que son. Por tanto utilizan Internet. Eso significa que, además de los riesgos específicos de cada Red Social, al convertirnos en usuari@s estamos expuestos también a los riesgos de navegar por Internet. Nuestra identidad, nuestros equipos, datos que tenemos almacenados, contraseñas e información de todo tipo puede verse comprometida. Enumeramos algunos de los principales.

Redes abiertas

Existen redes WiFi públicas (Redes gratuitas y que, en algunos casos, no nos solicitan contraseña) en diferentes espacios: centros comerciales, cafeterías, bibliotecas, aeropuertos. Cuando nos conectamos a esa Red no debemos facilitar datos importantes (contraseñas, datos bancarios…), ya que corremos el riesgo de que sean robados.

Webcam

Debemos tener precaución con el uso de nuestra Webcam del ordenador u otros dispositivos. Hay personas que pueden grabarte sin que lo sepas mediante diferentes softwares, programas etc., para después chantajearte o difundir esas imágenes. Para evitarlo, podemos tapar la Webcam con una simple pegatina o gomet.

Virus

Un virus informático es un programa que se instala en nuestro dispositivo y que puede llegar a través de diferentes medios: mensajes, descargas de sitios web no seguros, correos electrónicos, dispositivos USB, etc. Los virus pueden copiar nuestros archivos (fotos, documentos o contraseñas) y utilizarlos sin nuestro permiso y también infectar y/o inutilizar nuestro dispositivo.

Mensajes estafa

Los mensajes estafa nos llegan a través de diferentes medios (SMS, e-mail, WhatsApp…) proporcionando algún tipo de información falsa: premios variados, que hemos ganado un sorteo en el que no hemos participado, petición para que facilitemos algún dato personal como número de cuenta bancaria, etc. Nunca debemos hacer caso a estos mensajes y mucho menos facilitarles la información que nos solicitan.

Troyanos

Un troyano es un tipo de virus muy peligroso y que puede llegar a robar y destruir la información de nuestro dispositivo. Normalmente se caracterizan por engañar a los usuarios disfrazándose de programas o archivos benignos (archivos de música, fotos, archivos adjuntos de correo etc.), con el objeto de infectar y robar información personal.

Cookies

Cookie es el nombre que recibe un lugar de almacenamiento temporal de información que usan páginas de Internet. Por lo general, su función es guardar y recordar información relevante de los usuarios de una web o plataforma (preferencias, ubicación geográfica, lugares más visitados...). Un ejemplo sería cuando nos registramos por primera vez en una plataforma (compra online, correo electrónico etc.) e introducimos nuestros datos de acceso. Las posteriores visitas a esta plataforma nos encontraremos con que hemos sido "recordad@s" por el sitio web.

Chantaje digital

Se trata de un tipo de chantaje que se lleva a cabo a través de los diferentes medios que ofrece la Red, principalmente las RRSS. Para prevenirlo es fundamental estar alerta, no mostrar información personal de manera pública y no aceptar en nuestro círculo a personas desconocidas, porque pueden llegar a utilizar nuestra información para suplantar la identidad o chantajearnos de diferentes maneras.

Suplantación de identidad

El robo de identidad ocurre cuando una persona se hace pasar por otra utilizando sus datos personales con el fin de obtener algo a cambio, realizar algún acto ilegal o causar algún tipo de daño o perjuicio (pedir un préstamo bancario en nombre de otra persona, crear un perfil falso en una Red Social, proporcionar información falsa y perjudicial etc.).

Sexting

Es la difusión o publicación de contenidos de tipo sexual (principalmente fotografías o vídeos) producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico. No deben de compartir jamás fotos de contenido íntimo o sexual con otras personas, ya sean conocidas o no.

Ciberbullying

Es el uso de los medios telemáticos (Internet, telefonía móvil y Redes Sociales principalmente) para ejercer acoso psicológico entre iguales mediante diferentes acciones como insultos, amenazas etc. Es importante que sientan que pueden contar con vosotros, tanto si son víctimas de ciberbullying, como si conocen a alguien que lo sufra o ejerza.

3.4- ALERTAS

Como hemos referido en varias ocasiones a lo largo de estos materiales, el ámbito de las RRSS y las TICS son cambiantes; de modo que la forma más prudente de actuar es, sin alarmismos, "chequear" cada cierto tiempo cómo nos relacionamos con ellas. En concreto, enumeramos algunos comportamientos y actitudes que deben hacernos reflexionar sobre si nuestro uso es saludable.

Las alertas deben dispararse si nos ocurre en alguna ocasión que:

1. Quedamos menos con amig@s y/o familiares por pasar tiempo conectad@s a la Red o usando móviles, tabletas etc.

2. Nos sentimos nervios@s, inquiet@s o intranquil@s si no tenemos acceso a Internet, la Red Social no funciona o lo hace con lentitud.

3. Caminamos mientras utilizamos algún dispositivo electrónico.

4. Lo primero y lo último que hacemos al día es consultar las RRSS.

5. Nos sentimos desprotegid@s o frustrad@s si no disponemos de un smartphone u otro dispositivo.

6. Usamos las RRSS, jugamos con nuestro dispositivo etc. mientras realizamos otro tipo de actividad (comer, leer, estudiar…).

7. Preferimos comunicarnos con otras personas a través de las RRSS, aunque estén en el mismo espacio que nosotr@s.

8. Nos sentimos tristes o preocupad@s si los demás no interactúan con nosotr@s en la Red con comentarios, 'me gustas', retuits etc.

9. Sentimos la necesidad de compartir cualquier cosa del día a día mediante fotografías, textos o vídeos.

10. Creemos que la vida de los demás es mejor que la nuestra basándonos en lo que vemos en las RRSS.

11. Dejamos constancia de nuestra visita (también llamado "Check-in") en casi todos los lugares que visitamos.

12. Dejamos de hacer otras actividades por conectarnos a la Red o utilizar cualquier dispositivo.

13. Interrumpimos constantemente cualquier actividad que estábamos haciendo por consultar nuestro dispositivo.

14. No disfrutamos plenamente de algunas actividades o experiencias por el hecho de grabarlas o contarlas en las Redes continuamente.

15. Pasamos más tiempo del que pensamos o deberíamos dedicado a la Red y a los diferentes dispositivos (más de tres horas al día).

SI QUIERES SABER MÁS…

BIBLIOGRAFÍA

Asociación para la Investigación de Medios de Comunicación (2012) Acceso a Internet de los niños menores de 14 años en EGM. Acceso Disponible: http://www.aimc.es/-EGM-Ninos-en-Internet-.html

Calvo, S. (2012) Generando entornos personales de aprendizaje en red: relación y reflexión dialéctico–didáctica a partir de plataformas virtuales. Revista Iberoamericana de Educación n. º 60 (septiembre-diciembre). OEI. Madrid.

Garmendia, M. et Al (2012). Los Menores en Internet. Usos y seguridad desde una perspectiva Europea. Quaderns del CAC 38, vol. XV (1) (pp. 37-44).

Luengo, J.A. (2012): "Menores e intimidad en la red: Cuando los demás son objetos". Lázaro, I.; Mora, N. y Sorzano, C. (Coords.) "Menores y nuevas tecnologías", pp. 167-207. Madrid. Técnos y Universidad Pontificia de Comillas.

Luengo, J.A. (2013): "Promover valores y ética en las relaciones digitales: la necesidad de actuar cuanto antes". Avances en Supervisión Educativa. Nº 18. Asociación de Inspectores de Educación de España.

Morduchowicz, R. (2012): "Los Adolescentes y las Redes Sociales: La Construcción de la Identidad Juvenil en Internet". Edit. Fondo de Cultura Económica de España. Argentina.

Tsitsika, A., Tzavela E. y Mavromati, F. (2012). "Investigación sobre conductas adictivas a Internet entre los adolescentes europeos". Funded by the European Union Safer Internet plus.

RECURSOS WEB

Ciber Corresponsal: www.cibercorresponsal.org. Una red que funciona como un periódico digital hecho por l@s jóvenes donde comparten sus intereses, preocupaciones y reflexiones.

Club Penguin: www.clubpenguin.com. Página de Disney que ayuda a mejorar tu nivel de seguridad aportando consejos y herramientas. Cuenta con juegos y Apps.

Mi novio me controla lo normal: www.minoviomecontrola.com y también en www.minoviomecontrola.blogspot.com.es. Espacio web dirigido especialmente a jóvenes para informar y concienciar sobre ciberacoso, bullying, ciberbullying y violencia de género a través de las nuevas tecnologías.

Pantallas Amigas: www.pantallasamigas.net. Fomento de la ciudadanía digital responsable en la infancia y la adolescencia. Cuenta con material educativo audiovisual, programa para centros escolares, apoyo a padres y madres etc.

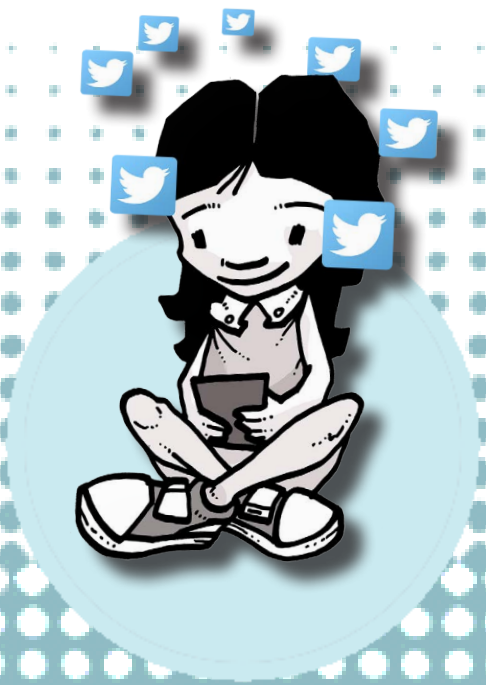
Protege tu información: www.protegetuinformacion.com. Ayuda a mejorar tu nivel de seguridad aportando consejos y herramientas.

Quérote Máis: www.xuventude.xunta.es/querote-mais.html. Servicio de asesoramiento e información juvenil de Galicia.

Suicide Machine: www.suicidemachine.org. Para borrar nuestro rastro al darnos de baja en una Red Social.

Tú decides: www.tudecideseninternet.es. Aspira a concienciar a l@s jóvenes sobre la importancia de preservar sus datos personales en Internet.

Violencia sexual digital: www.violenciasexualdigital.info. Web ligada a Pantallas Amigas y creada como recurso en línea para poner a disposición de la sociedad un conjunto de informaciones y recursos útiles para la prevención y la intervención en materia de violencia sexual que se produce en el medio digital.



ACTÚA
Proyecto Juvenil de
Conciencia Social Positiva