ACTÚA
Proyecto Juvenil de
Conciencia Social Positiva

PADRES Y FAMILIA

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

Asociación Participa para la Inclusión Social

Fundación María José Jove

3.1. RIESGOS: AGUJEROS DE LA RED

Para que los menores puedan hacer un uso sano de las RRSS (un uso seguro, útil, gratificante, que no interfiera negativamente en su cotidianeidad y que facilite el el desarrollo personal y social), habrán de ser conscientes de los riesgos inherentes de las RRSS y de las estrategias de protección frente a ellos. Algunos de estos riesgos, agujeros de la red, son:

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 se deben facilitar datos importantes (contraseñas, datos bancarios, datos personales...), ya que se corre el riesgo de que sean robados.

Webcam

La mayoría de dispositivos incorporan una cámara, es indispensable tener precaución con el uso de la cámara o Webcam. Debemos comentar siempre esto con nuestros hij@s; y recordarles que hay personas que pueden grabarles sin que lo sepan mediante diferentes softwares o aplicaciones activados de forma remota. Para después chantajearles o difundir esas imágenes. Para evitarlo, pueden tapar la Webcam con una simple pegatina o gomet. Y en el caso de las aplicaciones para móviles, configurar opciones que bloqueen el acceso a la cámara.

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. Debemos informarles y enseñarles a identificar y preveer los posibles riesgos.

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 deben hacer caso a estos mensajes, y mucho menos facilitarles la información que nos solicitan.

Troyanos

Un troyano es un tipo de virus muy peligroso; 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...).

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 Redes Sociales. Para prevenirlo es fundamental informar a los menores para que estén alerta, que no muestren información personal de manera pública y que no acepten en su círculo a personas desconocidas porque pueden llegar a utilizar su información para suplantar la identidad o chantajearles de diferentes maneras.

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.

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.). Es importante informar a nuestros hij@s de que esto puede pasar para que sepan prevenirlo.

Estos riesgos que nombramos y aquellos otros derivados de un uso inadecuado de las RRSS, pueden provocar algún cambio en los menores. De modo que la forma más prudente de actuar es, sin alarmismos, "chequear" cada cierto tiempo cómo se relacionan nuestros hij@s con ellas. En concreto, enumeramos algunos comportamientos y actitudes que deben hacernos reflexionar sobre si el uso que hacen de las RRSS es saludable.

Si percibimos que en alguna ocasión nuestros hij@s o familiares menores de edad:

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

Se sienten nervios@s, inquiet@s o intranquil@s si no tienen acceso a Internet, la Red Social no funciona o lo hace con lentitud.

Caminan mientras utilizan algún dispositivo electrónico.

Lo primero y lo último que hacen al día es consultar las Redes Sociales.

Se sienten desprotegid@s o frustrad@s si no disponen de su smartphone u otro dispositivo.

Consultan las Redes Sociales,envían mensajes, juegan con su dispositivo etc. mientras realizan otro tipo de actividad (comer, leer, estudiar…).

Prefieren comunicarse con otras personas a través de las Redes Sociales, aunque estén en el mismo espacio que ell@s.

Se sienten tristes o preocupad@s si los demás no interactúan con ell@s en la Red con comentarios, 'me gustas', retuits etc.

Comparten cualquier cosa del día a día mediante fotografías, textos o vídeos.

Comparan continuamente su vida con la de otras personas a través de lo que perciben en las RRSS.

Dejan constancia de su visita (también llamado "Check-in") en casi todos los lugares que visitan.

Interrumpen constantemente cualquier actividad que estaban haciendo por consultar su dispositivo.

No disfrutan plenamente de algunas actividades o experiencias por el hecho de grabarlas o contarlas en las Redes de forma continua.

Pasan más tiempo del que piensan o deberían dedicado a la Red y a los diferentes dispositivos.

3.2. ALGUNAS RECOMENDACIONES PARA AUMENTAR LA SEGURIDAD Y PROTECCIÓN DE LOS MENORES EN LAS REDES SOCIALES

Las 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 protejan a los menores. Las siguientes recomendaciones pretenden orientar sobre las diferentes opciones para favorecer un uso más seguro de las mismas.

- Es importante que conozcan y configuren las **opciones de privacidad** de las distintas Redes Sociales y aplicaciones que utilicen; debéis ayudarles a la hora de revisar y configurar las mismas. Es importante que sus perfiles sean privados, sólo accesibles para sus personas de confianza, conocidas personalmente y sin datos que puedan comprometer su privacidad y seguridad.

- Asegúrate de que conocen las diferentes opciones que ofrecen las Redes como "bloquear" o "denunciar" para mantener siempre su privacidad y seguridad; por ejemplo, eliminar una imagen, vídeo o comentario que no quieran que sea público.

Existen también opciones que permiten conocer su localización en cada momento. En algunos casos, son de mucha utilidad (excursiones, viajes, salidas...) pero debe ser algo que acordéis y configuréis de manera conjunta porque, en determinadas circunstancias, es un riesgo que todos sus contactos y otras personas con dispositivos de búsqueda puedan saber en todo momento donde están.

- Es fundamental que os mantengáis informados acerca de las **condiciones de uso** de las diferentes Apps, juegos, Redes etc. que utilicen. Algunas de ellas son de gran importancia, como las recomendaciones de uso y edad, y otras afectan a cómo y dónde pueden usarse los datos (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, por lo que es muy importante que las reviséis conjuntamente antes de hacer uso de cualquier App o Red Social.

- Debemos fomentar siempre la protección de sus **datos personales** y hacerlos conscientes y partícipes de lo importante que resulta esto para favorecer su privacidad y seguridad. No deben difundir ni publicar datos como dirección, teléfono etc. en sus Redes Sociales, chats o sitios web, y por supuesto no compartir esta información con personas desconocidas. También es importante que no introduzcan datos de carácter personal (datos bancarios, contraseñas, datos privados etc.) cuando usan una Red abierta y pública o cuando usan un ordenador o dispositivo que no sea el suyo propio (en bibliotecas, cafeterías, espacios habilitados etc.). Si utilizan uno de estos dispositivos para acceder a su e-mail o Red Social etc., recuérdales siempre que deben cerrar sesión al finalizar.

- Las **contraseñas** que utilicen han de ser seguras, y no deben publicar ni difundir las mismas. Para mejorar su seguridad podéis modificarlas cada cierto tiempo.

- La **Webcam** sólo deben utilizarla con quienes conozcan personalmente. Además

deben cubrir la misma cuando no la utilicen.

Del mismo modo, debéis concienciarles sobre la importancia de no aceptar ni abrir documentos, archivos, e-mails etc. de personas desconocidas. Podrían poner en riesgo su dispositivo y lo que es más importante, a ell@s mism@s.

- Que **no crean todo lo que leen** en Internet. No toda la información que aparece publicada en la Red es cierta, y alguna puede ser muy perjudicial. Deben contrastar la información por otros medios o consultándoos a vosotros o a un educador. Es importante que sepan que pueden recurrir a vosotros para cualquier incidente de este tipo.

- Medir el **tiempo de uso** que dedican a las Redes Sociales, Apps y dispositivos móviles en general. El tiempo pasa rápido cuando se hace uso de los dispositivos electrónicos, y puede que le dediquen más tiempo del que creen o del que deberían. Debéis establecer un límite y unos horarios en el que ellos puedan utilizarlos. La recomendación de los expertos es no dedicar más de 3 horas al día.

Puede ser útil también que desconecten las diferentes notificaciones de Redes, juegos etc. que distraen su atención con llamadas y avisos constantes. No es preciso consultar cada minuto el móvil. Establecer unas pausas o momentos para que consulten sus RRSS y dispositivos.

- Recordarles siempre que **Internet es eterno**. Todo lo que suban 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, dejan de ser los propietarios de esas fotos o vídeos para ceder los derechos a las diferentes webs y/o plataformas. Sus contenidos o informaciones serán públicos en cualquier momento; ahora o dentro de 5 o 10 años. Es importante que les hagáis conscientes de esta información.

- El **anonimato no existe**. No es posible permanecer desconocid@ ni anónim@ una vez que te registras en una Red Social. Debemos enseñarles a cuidar y valorar su identidad y la información que proporcionan a los demás. Tener presente siempre que **insultar, amenazar, robar** contraseñas y/o **suplantar** la identidad de otra persona, son delitos castigados por Ley. No deben utilizar la tecnología para realizar acciones que no harían en persona.

- Es importante concienciarles para que no sean partícipes de **cadenas con mensajes** de mal gusto sobre otras personas, así como de la gravedad de no actuar si son testigos de estas acciones. Debemos transmitirles confianza para que se sientan seguros a la hora de comunicar siempre a un adulto si sufren acoso, amenazas, insultos etc. a través de cualquier dispositivo electrónico o si conocen a alguien que se encuentre en esa situación. Recuérdales siempre: "No trates a los demás como no te gustaría que te trataran a ti".

En el caso de que sean víctimas de mensajes amenazantes, ofensivos o hirientes de forma continuada, es importante apoyarles y tomar medidas al respecto.

- Que no contesten nunca a los mensajes.
- Guardar los mensajes como pruebas.
- Contactar con el administrador de la Web, plataforma, portal etc. para denunciarlo.
- Ponerlo en conocimiento de las autoridades si es necesario.

- Debemos fomentar también el respeto por la privacidad ajena, por lo que no deben subir, facilitar o difundir fotografías, videos o información de terceras personas sin su **consentimiento**. Aunque se trate de personas de su confianza deben consultarles siempre primero. Recordarles también que cuando envíen e-e-mails a varias personas, deben respetar la privacidad de las mismas y no dejar a la vista sus direcciones. Para ello pueden utilizar la opción "con copia oculta" (CCO).

- Vigila sus **contactos**. No deben añadir a personas o "amig@s" que no conozcan personalmente ni aceptar peticiones o conversaciones de desconocidos, ni en la red ni cara a cara. Al igual que no deben aceptar por la calle la invitación de un extraño, no deben hacerlo tampoco de manera virtual.
Deben comentar también con su red de amig@s o contactos que no desean que se compartan fotos o información personal suya de ningún modo, o al menos sin su previo consentimiento.

- Insistir en que tengan especial precaución con las **personas desconocidas**. Que no difundan ni compartan información con estas personas ni acepten documentos, e-e-mails o solicitudes por parte de las mismas. Por supuesto, no deben utilizar la Webcam ni quedar físicamente con ellas.

- Supervisa e insiste en que han de navegan por **sitios Web seguros** y evitar el acceso a contenidos inadecuados. Es importante mantener también siempre activo un programa antivirus en todos sus dispositivos y activar un control parental de limitación de acceso a contenidos perjudiciales en caso de que sea necesario.

- Fomenta y trabaja siempre la protección de su **identidad digital**; recuérdales que ésta la construyen ell@s y que se mantiene de forma permanente y visible en la web. Deben mantener siempre una actitud activa en defensa de su privacidad.

En definitiva, adaptemos las medidas de seguridad y control para contrarrestar la vulnerabilidades de nuestros hij@s, dándoles más autonomía a cambio de responsabilidad. Procuremos que los menores acepten como natural cierto grado de control. Por ello, es adecuado acordar con los menores, una serie de condiciones para el uso de las RRSS (horarios, tiempo de dedicación, contenidos, controles de seguridad, respeto a recomendaciones de uso, reglas de seguridad y protección...), tanto en el uso de ordenadores como de teléfonos móviles. Manejar por escrito unas normas aceptadas por tod@s, incluso firmar simbólicamente un "contrato" de uso de los dispositivos puede ser una buena forma de regular el uso.

La mayoría de los expertos coinciden en que un móvil debe ir acompañado de instrucciones de uso, pero no sólo en el acto de entrega, sino también en su proceso de autonomía. Combinando instrucciones de uso, cierto control y confianza.

3.3. APPS Y HERRAMIENTAS PARA REGULAR EL USO EN LAS REDES SOCIALES

Existe un número importante de diferentes aplicaciones para control parental. Han surgido como respuesta directa a la rapidísima implantación del uso de dispositivos entre los más jóvenes. Dadas las múltiples posibilidades que ofrece la tecnología, que se creen herramientas para conocer el uso y prevenir el mal uso o abuso entre los jóvenes, es lo lógico; porque es necesario. Básicamente hay dos opciones respecto al control y la supervisión del uso: se puede realizar de forma directa, revisando el dispositivo (preferentemente con naturalidad, delante del propietario) o indirecta, a través de una herramienta específica. No hay razones para argumentar a favor o en contra de cada alternativa. Dependerá de muchas circunstancias, entre ellas:

- De la edad, obviamente el conocimiento de los actos y el control no es el mismo con un joven de 12 años que con uno de 16.

- De los antecedentes; si existe desconfianza por algún episodio concreto, o una situación de mayor seguimiento por cualquier circunstancia que lo justifique, tendrá mayor sentido que la intensidad del conocimiento y control sean mayores.

- Del conocimiento que tengamos como padres o familiares sobre las RRSS. Primero deberá existir un mínimo conocimiento para saber qué debemos seguir o controlar. Porque si desconocemos todo, o casi todo sobre el tema: ¿cómo podremos regularlo?.

- Del tiempo que lleve usando el dispositivo y de su propia trayectoria con las RRSS. Lo ideal es, al entregar el dispositivo, marcar unas pautas de uso. Incluso, con jóvenes de 12 ó 13 años incluir el control y revisión como una rutina habitual. Establecer horarios de uso, lugares de uso, comunicación a un adulto de las RRSS en las que quiere participar (posibilitando que un progenitor la use también), restricciones relacionadas con edades recomendadas, contenidos no adecuados, indicaciones de contacto: informarles directamente del riesgo de establecer contacto o comunicación con extraños. Es decir, aclarar que tener un dispositivo, no supone poder hacer cualquier uso del mismo.

- De las circunstancias personales del menor en cada momento.

En relación con las aplicaciones de control parental, existen muchas con una variedad importante de funciones y posibilidades. Realmente, puede ser interesante pararnos un rato a reflexionar sobre los aspectos que queremos regular, o directamente, si queremos ejercer algún mecanismo de control directo. Como orientación, referimos algunas de las posibilidades que ofrecen estas Apps; así, en función de nuestro caso concreto, podremos elegir si utilizarlas o no, y qué utilidades se ajustan más a nuestras demandas. En general, la información o acciones más demandadas son:

- La información relativa al uso, tanto el tiempo que está conectad@ como a qué Apps o RRSS dedica el tiempo de conexión.

- La información, con más o menos detalle, sobre los contenidos, mensajes o imágenes que comparte en las RRSS.

- La información o historial de todo lo que ha consultado el menor en su dispositivo.

Incluido el registro de llamadas y conexiones a aplicaciones.

- La información, en algunos caso en tiempo real, sobre qué uso concreto está haciendo en un momento determinado.

- El acceso a la lista de contactos y mensajes enviados (de texto o imágenes).

- La posibilidad de bloqueo horario: en este caso, el dispositivo se apaga en la hora establecida. Por ejemplo, a partir de las 10 de la noche, durante una reunión familiar o el horario lectivo del colegio.

- La ubicación geográfica en cada momento.

- La posibilidad de establecer un perímetro geográfico. Así, en el momento en que el menor salga de ese área, se le comunicará al adulto inmediatamente.

- La posibilidad de bloquear juegos o aplicaciones en un dispositivo, de esa forma no se podrán ejecutar.

Estas posibilidades, como hemos comentado con anterioridad, deben ser valoradas en función de cada circunstancia y menor. No hay fórmulas universales. Pero es relevante que la decisión que se tome respecto al seguimiento o control, sea conocido por el menor, y se justifique su necesidad o utilidad. El dispositivo les da autonomía, pero deben de gestionarla. El control por el control sobre un adolescente sólo generará, en la mayor parte de los casos, la búsqueda de una vía de escape, que es el resultado opuesto a nuestra intención.

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 apren¬dizaje 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 So¬ciales: La Construcción de la Identidad Juvenil en Inter¬net". Edit. Fondo de Cultura Económica de España. Argen-tina.

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

RECURSOS WEB

Ciber Corresponsal: www.cibercorresponsal.org Una red que funciona como un periódico digital hecho por las/los 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: minoviomecontrola.com y también en 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. Cuanta con material educativo audiovisual, programa para centros escolares, apoyo a padres y madres etc.

Protege tu información: 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.

Suicide Machine: suicidemachine.org Para borrar nuestro rastro al darnos de baja en una red social.

Tú decides: www.tudecideseninternet.es Aspira a concienciar a los jóvenes (10-15 años) 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