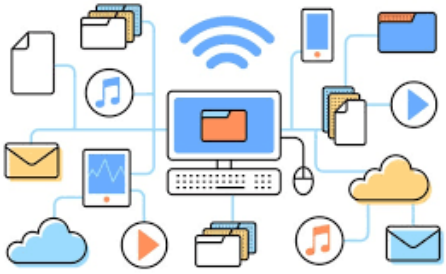
MANUAL DEL BUEN USO DE LOS MEDIOS INFORMÁTICOS



PROFESORADO

PROFESORADO

RIESGOS EN EL USO DE LAS TIC

1 PROBLEMAS PSICOLÓGICOS Y ACADÉMICOS

El uso abusivo o descontrolado de las nuevas tecnologías lleva aparejados cambios en los hábitos y rutinas de los usuarios, pudiendo convertirse en un serio problema cuando el tiempo y la atención dedicados a ellas sobrepasa ampliamente el tiempo dedicado al resto de las actividades.

Algunas de las disfunciones y desequilibrios que puede padecer el joven a nivel mental, emocional y de rendimiento escolar son estas:

1. Trastornos del sueño
2. Déficit /dispersión de la atención
3. Forma de escape de problemas y responsabilidades reales
4. Aislamiento, dejar de salir con amigos
5. Escaso control de pulsiones
6. Desinformación e intoxicación de ideas

   Falta de sentido crítico.

   Información falsa, credulidad.

   Desconfianza y/o relativización.

   Asumir valores y creencias perniciosas.
7. Autoestima vulnerable / reputación online
8. Adicciones a internet

   Cibersexo, pornografía.

   Ludopatía, juegos online.

   Chat.

   Blogging.

9. Otras adicciones relacionadas con las TIC

   Teléfono móvil.

   Videojuegos no online.

   Televisión.

10. Secuelas psíquicas de estas adicciones o del uso intensivo de las TIC:

    Síndrome de abstinencia.

    Sentimientos de culpabilidad.

2. PROBLEMAS SOCIALES

La disparidad de criterios entre los hijos y los padres sobre el tiempo y el uso que deben tener con las TIC deriva frecuentemente en situaciones complejas y conflictos que deben ser solucionados con charlas sinceras y razonadas, con acuerdos y horarios consensuados donde queden claras las responsabilidades y necesidades de cada uno, planteando actividades alternativas, pero siempre manteniendo el principio de autoridad. Los problemas parentales más frecuentes son:

1. Irritabilidad del joven al ser interrumpido
2. Mentiras.
3. Olvidar responsabilidades domésticas.
4. Presiones para comprar aparatos.
5. Privacidad.
6. Bajo rendimiento escolar en las tareas académicas.
7. Uso inadecuado de los equipos informáticos por los alumnos/as.
8. Uso encubierto del móvil.
9. Utilización inadecuada de las TIC por los alumnos en su aprendizaje..

3. PROBLEMAS DE SALUD FÍSICA

1. Sobrepeso.
2. Musculares y articulares.
3. Oculares. Anorexia/ bulimia.
4. Autolesiones.

CONSEJOS GENERALES PARA EVITAR ESTOS PROBLEMAS

Aunque cada edad y caso particular necesitan de unas soluciones concretas, nos permitimos enunciar unas pautas básicas generales que ayudarán a que los menores utilicen las TIC de manera más segura y gratificante:

A. Controlar el tiempo que se conectan a internet en clase.

B. Colaborar en el mantenimiento de todos los dispositivos tecnológicos del aula.

C. Fomentar la utilización de una posición correcta para el cuerpo frente al ordenador, siguiendo estas pautas:

   - Los ojos deben estar situados enfrente, y a una distancia mínima del doble de la diagonal de la pantalla.
   - La espalda recta, y reposada la zona lumbar contra el respaldo de la silla.
   - El ángulo de rodillas y codo ha de ser de 90º.
   - Es conveniente acostumbrar al menor a levantar la vista de la pantalla cada 15 o 20 minutos, fijándola en un punto alejado, y a no permanecer en la misma postura durante más de una hora.

D. Fomentar el respeto a otros usuarios, evitando las burlas, difamaciones y agresiones.

E. Enseñar a navegar por internet de forma segura, accediendo solo a contenidos aptos para su edad.

F. Crear un espíritu crítico sobre la información que aparece en la red y explicarles que no todas las webs tienen la misma credibilidad, que es importante filtrar y evaluar su calidad.

G. Enseñar a utilizar motores de búsqueda y contrastar varias fuentes sobre un mismo campo, evitando el “corta y pega”, para evitar plagios de trabajos ya realizados.

H. Advertir del derecho a la privacidad de la información personal del alumnado y a que no sea difundida sin su consentimiento por la red. Hay que tener cuidado con los datos que se comparten tanto en chat, redes sociales o por email (imágenes, datos, perfiles, números de teléfonos.), leyendo atentamente las condiciones de las páginas a las que nos suscribimos

I. De la misma manera, explicar que no se puede publicar información de otra persona sin su consentimiento. Siempre es aconsejable evitar publicar detalles o imágenes privadas.

4. OTROS PROBLEMAS: CIBERDELITOS

En este apartado se aborda un listado de problemas que quizás sean los que más preocupación despiertan entre los docentes y entre los padres.

4.1 VIOLACIÓN DEL DERECHO A LA IMAGEN Y A LA INTIMIDAD. PRIVACIDAD

Este problema es de vital importancia, ya que el desconocimiento del derecho a la privacidad es la base de otras situaciones mucho más graves. La mayoría de las personas, ya sean menores o adultos, desconocen qué es eso de la privacidad, cómo preservarla y, a la vez, respetar la privacidad de otros en la red.

Todo el mundo tiene derecho a la protección de sus datos personales. Como tales se consideran la información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a cualquier persona identificada o identificable. En contrapartida, todos tenemos el deber de respetar la privacidad de otros. No por ser menor se está eximido de estas responsabilidades y no por desconocer las leyes, se puede incumplirlas.

Nadie puede pedir a un menor sus datos personales sin el consentimiento de sus padres si el menor no tiene todavía los 14 años. Solo los mayores de 14 años pueden autorizar el tratamiento de sus datos de carácter personal.

Los peligros de la violación de la privacidad son, entre otros, los siguientes:

- Ciberacoso o ciberbullying
- Sexting
- Acoso sexual o grooming
- Estafa
- Acceso a cuentas de correo, perfiles de redes sociales, etc.
- Spam
- Malware o programas maliciosos que se instalan en el equipo y recogen datos de forma opaca
- Etiquetado de fotos en redes sociales para comprometer o perjudicar a la víctima

- Suplantación de la identidad en redes sociales
- Distribuir, sin querer y/o sin saberlo, imágenes o vídeos de pornografía infantil

Consejos para padres y educadores:

1. Hacerles ver a los menores que si revelan datos personales y ceden imágenes o vídeos personales a desconocidos tienen mayor probabilidad de ser víctimas de ciberacoso, acoso sexual, suplantación de identidad, etc.
2. Advertirles de no compartir contraseñas con nadie.
3. Ayudarles en la medida de lo posible en el uso de la seguridad en redes sociales, foros, etc.
4. Hacerles reflexionar a la hora de publicar sobre quién verá su información.
5. Hacerles ver la importancia de su reputación y comportamiento en la red y las consecuencias que de ello se pueden derivar de cara al futuro personal y profesional.
6. Asesorarles sobre los riesgos de la instalación en los dispositivos móviles de aplicaciones que demanden permisos no coherentes con la utilidad para la que han sido creadas.
7. Vigilar si se producen cambios de comportamiento en los menores, si experimentan síntomas físicos inusuales (molestias, dolores…), rechazo repentino a estar con amigos o asistir al centro escolar, o una bajada repentina del rendimiento escolar, por si estuviese relacionada con situaciones de acoso.

4.2 UN CASO ESPECIAL: LAS REDES SOCIALES

Una red social en internet no es más que una plataforma o portal web a través del cual sus usuarios se mantienen en contacto y comparten intereses, opiniones, multimedia, etc. Los usuarios, al darse de alta, pueden personalizar y administrar su perfil.

Las redes sociales pueden ofrecer una serie de **ventajas a los usuarios:**

1. Potencian la comunicación de los participantes con su entorno y, por tanto, las relaciones personales.
2. Son un lugar de intercambio de opiniones y de intereses.

3. Fomentan la colaboración entre los miembros de una comunidad, ya sea con el fin de ayudar o de elaborar trabajos de forma colaborativa.
4. Promueven el uso de herramientas tecnológicas.
5. Son una fuente de información continua y actualizada.

También su uso conlleva **riesgos:**

1. Si no se saben administrar las opciones de privacidad que ofrecen las redes sociales, los usuarios corren el riesgo de difundir datos personales y privados.
2. Los menores son vulnerables a sufrir ciberdelitos, al aceptar en su comunidad a usuarios que no conocen personalmente.
3. Muchas de las acciones personales que el usuario va seleccionando quedan registradas y almacenadas durante mucho tiempo.
4. Fomentan comunidades de conocidos y amigos virtuales que están totalmente desconectadas con el mundo real.

Muchas de las redes actualmente más usadas poseen una política para impedir el registro de usuarios demasiado jóvenes, como consecuencia de la normativa internacional COPPA, han añadido un lugar donde informar sobre abuso dentro de la red, botones o funcionalidades destinadas a denunciar abusos y falsedades, o han hecho más fácil la configuración de la privacidad dentro del perfil del usuario.

En cualquier caso, la responsabilidad final del uso de la red social recae en el mismo usuario, o, en el caso de un menor, en sus padres, quienes deben velar por la seguridad y privacidad de sus hijos cuando acceden a ellas, los datos que deben proporcionar y las cláusulas que aceptan al realizar el registro.

4.3 CIBERBULLYING

Se trata del acoso (insultos, chantaje, coacción, humillación, injurias, calumnias vejaciones) entre iguales, mediante el uso de las nuevas tecnologías (telefonía móvil, internet -foros, chats, correo electrónico…- o videojuegos online).

Hay que apuntar que el acoso escolar ha existido desde siempre, pero con las nuevas tecnologías se abre una nueva vía para que los acosadores actúen. Esta

situación ocurre por la desinformación de los propios menores sobre la repercusión de realizar este tipo de actos a través de la red o telefonía y sobre la importancia de la privacidad, pero también por la inacción de quienes contemplan estas acciones sin denunciarlas. No es lo mismo insultar en el patio del colegio que hacerlo a través de la red; la difusión es mayor y las repercusiones también, ya que se extienden en el espacio y en el tiempo, y pueden llegar a acorralar al acosado, dejándolo sin ámbito alguno de privacidad.

Para considerar el ciberbullying como tal se deben tener en cuenta estos aspectos:

1. Se desarrolla entre iguales, de un menor o de un grupo de menores a otro. Nunca de un adulto a un niño.
2. Tiene lugar en un entorno TIC.
3. No es un hecho aislado, sino que es reiterado y mantenido en el tiempo.
4. Se basa en la difamación de la víctima, sobre la que se vierten falsas acusaciones o informaciones vejatorias y difamatorias, que persiguen excluirla de sus grupos sociales por la vía del rechazo o de la vergüenza.
5. Con frecuencia, los acosadores implican a terceros, inicialmente pasivos, para que participen del hostigamiento.
6. No es de índole sexual ya que, en ese caso, se considera grooming.

El ciberbullying da pie al anonimato, sensación que, efectivamente, proporciona internet, pero hay que advertir que siempre se puede detectar desde qué equipo informático y lugar se lleva a cabo una determinada actividad.

¿Se puede prevenir?

En el caso de los profesionales de la enseñanza:

1. Incluir actividades relacionadas con la prevención y detección del ciberbullying en el Plan de Acción Tutorial y en el Plan de Convivencia del Centro acerca del buen uso y el mal uso de internet, ordenadores y dispositivos móviles.
2. Reflexión sobre los riesgos de internet, ordenadores y dispositivos móviles.

3. Establecer protocolos de actuación que favorezcan la detección del ciberacoso y estandaricen las acciones que, ante un caso, deban realizar los distintos estamentos del centro educativo.

¿Qué hacer?

Para profesionales de la enseñanza:

Si el ciberacoso procede del entorno escolar:

1. Informar al equipo directivo, al orientador y al tutor para aplicar el apoyo necesario al alumno, tanto si es víctima, acosador u observador.
2. Aplicar los protocolos de actuación que el centro pudiese tener para estos casos.
3. Recurrir a organizaciones especializadas en acoso escolar.
4. Informar a los padres de todos los menores implicados en el suceso, así como proporcionar información a la víctima y a su familia sobre las diferentes posibilidades de que disponen para denunciar.

4.4 GROOMING

Por tanto, es una forma de acoso, pero en este caso el fin perseguido es la satisfacción sexual del acosador, quien al principio contactará con la víctima haciéndose pasar por otra persona, entablando entonces una relación más estrecha con ella, hasta que llega a convencerla para realizar fotografías comprometidas. Entonces se inicia una fase cruel de chantaje donde el menor es amenazado con difundir las imágenes (sextorsión) si no cumple los caprichos del acosador, quien en casos extremos puede exigir una cita con el menor.

¿Se puede prevenir?

Existen algunas recomendaciones para evitar esta situación.

Para los padres o educadores:

1. Comprobar que lo que cuenta el menor es cierto, para lo que es necesario recabar toda la información posible, analizando qué actividad ha desarrollado el acosador y cuál es constitutiva de delito y demostrable.
2. Recopilar todas las pruebas de la actividad del acosador: mensajes,

multimedia...

3. Denunciar el caso.

4.5 SEXTING

Consiste en el envío de imágenes y vídeos pornográficos de menores, tomadas por ellos mismos, a través de teléfonos móviles.

Son muchas las razones que impulsan a los menores a actuar de esa manera. Entre ellas, la influencia de las amistades, el ganar notoriedad en el grupo de amigos, la diversión que eso puede generar, la confianza plena que tienen en el destinatario, la creencia de que una imagen en un móvil es segura, el no prever las consecuencias de la libre circulación de esas imágenes o vídeos y, por supuesto, la falta de madurez que acompaña la etapa de la infancia y adolescencia, que hace cometer actos con cierto riesgo sin pensar en las consecuencias.

¿Cómo prevenirlo?

Consejos para padres y educadores:

1. Insistir a los menores en la necesidad y la importancia de la privacidad.
2. Hablar abiertamente sobre el tema, incluso antes de que éste aparezca, y explicarles a los menores los riesgos del sexting y las consecuencias legales para el acosador y psicológicas para la víctima.
3. Generar en el menor la confianza suficiente para que, en caso de que sea víctima o testigo de un caso de sexting, sepa que debe dirigirse y recurrir a un adulto.
4. Consultar a especialistas como psicólogos, pedagogos, etc.
5. Observar conductas anormales en el menor, como tiempo excesivo en el empleo del móvil, hacerlo encerrado en su habitación, facturas del móvil de cuantía mayor de lo normal, alejamiento de sus actividades y amigos habituales, etc.

¿Qué hacer?

Si un alumno está sufriendo una situación de sexting, es obligatorio denunciarla, por ser un delito.

4.6 PHISHING

Consiste en el envío de correos electrónicos masivos que suplantan la identidad de bancos o empresas de internet, solicitando la actualización de los datos personales al usuario (contraseñas, número de la tarjeta de crédito, etc.) a través de una página de la empresa en cuestión que parece totalmente real y auténtica. Cuando el usuario introduce los datos en dicha página, éstos son captados o pescados por la red de ciberdelincuentes.

¿Cómo prevenirlo?

Consejos para padres y educadores:

1. Nunca se debe enviar información personal o financiera por correo electrónico.
2. Tener cuidado con los archivos adjuntos que se reciben a través del correo electrónico, así como con su descarga, ya que pueden ser maliciosos.
3. Nunca hacer clic en enlaces sospechosos que recibamos en el correo electrónico.
4. Desconfiar de correos que parecen provenir de compañías, empresas, etc., con las que el usuario mantiene relación y en los que se avisa o advierte de que se va a cancelar una cuenta bancaria, un servicio, etc., si el usuario no responde.
5. Hay que tener cuidado igualmente con aquellos correos que envían teléfonos a los que llamar para facilitar la información.
6. Eliminar los correos electrónicos de empresas que soliciten o pidan la actualización de la información personal (contraseñas, cuenta bancaria, números de tarjeta de crédito, etc.). Los bancos, compañías, etc., nunca van a operar de esa manera ni van a solicitar esos datos por correo electrónico.
7. Confiar en las páginas web que uno mismo escribe en la barra de navegación y que muestran indicadores de seguridad como “https” o el código de colores de los navegadores.
8. Revisar de vez en cuando las cuentas bancarias con el fin de detectar lo antes posible cualquier cargo no autorizado.

¿Qué hacer?

1. Se pueden enviar los mensajes recibidos a la empresa u organización suplantada para que esté en su conocimiento.
2. Denunciar el caso.

4.7 CORREOS FALSOS (HOAX, BULOS, CADENAS, SPAM)

Los bulos u hoax son cadenas de mensajes electrónicos que intentan hacer creer al que los recibe algo que es totalmente falso. El objetivo es recopilar direcciones de correo electrónico para después difundir información falsa, por ejemplo. Lo más común es alertar sobre virus que no existen.

El spam es el envío de mensajes y correos electrónicos no deseados, masivos y automatizados a correos personales, blogs, foros o grupos de noticias.

La ingeniería social consiste en hacer que los usuarios actúen de la forma deseada, valiéndose de correos electrónicos que invitan a descargar un archivo adjunto.

¿Se puede prevenir?

Consejos para profesionales de la enseñanza:

1. Advertir a los menores de que no toda la información que circula por la red es cierta.
2. Aconsejarles que, para el registro en redes sociales, juegos…, usen direcciones de correo que no contengan sus datos personales como edad, apellidos, etc.
3. Indicarles que usen distintas cuentas de correo para juegos, foros, amigos, etc.
4. Advertirles de que si reciben mensajes de personas desconocidas los eliminen de inmediato.
5. Advertirles sobre la transmisión de virus a través del correo electrónico, especialmente mediante archivos adjuntos que deben analizar con un programa antivirus antes de su descarga.

4.8 VIRUS, MALWARE, SPYWARE...

Los dispositivos que, potencialmente, pueden verse afectados son:

1. Ordenadores personales y servidores
2. Móviles
3. Tablets
4. Videoconsolas

Los virus se clasifican según el tipo de acción que realizan y según cómo se propagan. Dentro del primer grupo se encuentran, entre otros:

1. **Spyware**: programas que se incautan de información del equipo para enviarla posteriormente. La información puede ser desde la más simple (páginas visitadas y tiempo consumido en internet) hasta contraseñas y datos del usuario.
2. **Adware**: a su vez está relacionado con el anterior, ya que habiendo infectado el equipo, muestran publicidad, a la espera de que el usuario acceda a las páginas web publicitadas, y posteriormente envía información del equipo.
3. **Ladrón de contraseñas**: accede a ficheros del ordenador que contienen información sobre nombre de usuario y contraseñas.

Según cómo se propaguen se clasifican en:

1. **Virus**: suelen infectar a través de archivos ejecutables del tipo .exe o .bat y solo se propagan cuando se ejecutan dichos archivos.
2. **Troyanos**: no poseen una única vía de entrada, ya que pueden infectar el equipo a través de un programa o de una descarga de un programa inofensivo o al visitar una página web aparentemente sin riesgo.
3. **Gusanos**: no infectan ficheros, pero lo que hacen es realizar copias de sí mismos y se propagan a través de chats, mensajería instantánea, correo electrónico o redes de compartición de ficheros (P2P).

¿Se puede prevenir?

Se puede seguir una serie de consejos que son iguales tanto para los usuarios menores de edad como para los mayores de edad:

Tener especial cuidado con los archivos que se comparten y se instalan a través

de medios extraíbles como CD, DVD o memorias USB, así como con los archivos adjuntos de correos electrónicos.

En cuanto a la red WIFI:

1. Cambiar la contraseña, que por defecto, trae el router de fábrica.
2. Usar encriptación WAP, mejor que WEP.
3. Ocultar el nombre de la red WIFI (ESSID).
4. Apagar el router cuando no se use.

En cuanto a la navegación por internet:

1. Nunca navegar por internet con permisos de administrador del equipo.
2. Mantener actualizado el navegador.
3. No descargar archivos de páginas web sospechosas.
4. Analizar con un antivirus todo lo que se descarga de internet.
5. Configurar un cortafuegos para evitar accesos no deseados a y desde internet.

En cuanto al correo electrónico:

1. No abrir correo electrónico de personas u organismos desconocidos o sospechosos, así como tampoco descargar ficheros adjuntos de ellos.
2. Usar un filtro anti-spam para evitar la recepción de correo malintencionado.
3. Si se va a descargar un fichero, analizarlo con un antivirus inmediatamente después de la descarga.
4. No unirse a las cadenas de mensajes falsos que se reciban, así como no difundir públicamente la dirección de correo electrónico.

Juegos online:

1. Mantener actualizado el software.
2. No compartir usuario o contraseña con otros usuarios.
3. Mantener control sobre la cuenta y tarjeta de crédito asociados.

En cuanto a dispositivos móviles:

1. Instalar un programa antivirus y de seguridad para dispositivos móviles.

2. Cuando se acceda a redes de compartición de ficheros, nunca hacerlo desde la sesión de administrador del sistema, sino desde una cuenta limitada.

¿Qué hacer?

Aparte de seguir las recomendaciones anteriores, lo mejor es instalar un programa anti-malware para asegurar una protección en tiempo real contra la instalación no deseada de cualquier tipo de programa malicioso. Paralelamente, el programa anti-malware detecta y elimina todo programa que esté alterando el funcionamiento del equipo, escaneando todos los archivos del sistema operativo, los programas instalados y la memoria.

Para que el anti-malware sea efectivo y eficiente debe mantenerse actualizado continuamente.