Junta de Andalucía
Consejería de Educación y Deporte

# MANUAL DEL BUEN USO DE LOS MEDIOS INFORMÁTICOS

## ALUMNADO

**ALUMNADO**

# RIESGOS EN EL USO DE LAS TIC

## 1.1 PROBLEMAS PSICOLÓGICOS Y ACADÉMICOS

El uso abusivo o descontrolado de las nuevas tecnologías lleva aparejados cambios en tus hábitos y rutinas, 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 puedes padecer a nivel mental, emocional y de rendimiento escolar son estas:

### 1.1.1. Trastornos del sueño

Es frecuente que el uso de internet o la televisión sin un horario concreto o un control parental, se alargue por la noche sin una noción del paso del tiempo. Especialmente la navegación por la red es capaz de llenar muchas horas de estímulos y de informaciones nuevas, saltando continuamente de unas páginas a otras o enganchándote en chats o vídeos. Las horas restadas al sueño repercutirán en el rendimiento escolar y en el equilibrio psíquico.

### 1.1.2. Déficit /dispersión de la atención

Los estímulos, incitaciones y sobre-información que aporta la navegación por la red, así como las herramientas colaborativas de la Web 2.0, pueden, fácilmente, sobrepasar el interés que tienes por otras informaciones que te llegan por medio de tus profesores, padres o monitores de actividades.

En este contexto, es lógico que el desinterés y la falta de control de atención puedan aparecer, llevándote a una distracción continua entre pensamientos emergentes y estímulos exteriores.

### 1.1.3. Forma de escape de problemas y responsabilidades reales

Las nuevas tecnologías aportan un continuo flujo de diversión y alicientes que la vida "real", en contacto con nuestros semejantes y las responsabilidades asociadas, no tienen. Refugiarse y distanciarse de los problemas, obligaciones y desilusiones diarias es una tentación de todos nosotros lo que, en el caso de los adictos a las nuevas tecnologías, se convierte en un mecanismo automático, que solo podrá ser corregido con una atención personalizada.

### 1.1.4. Aislamiento, dejar de salir con amigos

Solemos elegir las compañías que mejor nos tratan o que más nos estimulan, divierten o enseñan. Pero si estos valores te los proporciona un videojuego, la comunicación virtual a través de redes sociales, los estímulos de ciertas páginas web o el juego online, entonces sentirás que no necesitas salir de su casa para reforzar tu autoestima, tus ganas de disfrutar y aprender. Un mal síntoma podríamos encontrarlo en la evitación continua y activa de los demás para encerrarte con tu ordenador o videojuego.

### 1.1.5. Escaso control de pulsiones

Este es otro síntoma del exceso de tiempo y/o atención dedicado a las nuevas tecnologías. Al mando del ratón, joystick o mando a distancia te convierte en un "rey" que controla a tu gusto qué, cuándo y cómo es lo que recibes, tu voluntad es la dueña. Pero, cuando apagas el aparato y vuelves a someterte a la disciplina y voluntad de otras personas, pierdes ese control que has tenido y puedes contrariarte, enfadarte, entristecerst o, de nuevo, aislarte. Cuanto más cree un mundo virtual a tu medida, peor aguantarás el mundo "real".

### 1.1.6. Desinformación e intoxicación de ideas

La niñez y la adolescencia están marcadas por una voracidad cognitiva, una tendencia innata a aprender y asumir valores, normas, intereses, límites, creencias y a desarrollar un mapa conceptual del mundo y de tí mismos. La sobreinformación que ahora te llega de televisión, películas e internet se une a las tradicionales fuentes (padres, profesores y lecturas) para trastocar y complicar estos aprendizajes. Los efectos perniciosos de esta sobreinformación son:

- **Falta de sentido crítico**. Dar por sentado que la primera información que se lee es correcta y adecuada. No contrastar la información con otras fuentes. No objetar nada ni criticar lo que se lee. Para remediar esto, la mediación del educador es imprescindible.
- **Información falsa, credulidad.** Una consecuencia del problema antes citado es que puedes creer informaciones erróneas e incluso malintencionadamente falsas. Pueden ser bulos, infamias o creencias argumentadas, pero falsas, llamadas hoax; estas últimas pueden atraer la atención del internauta porque suelen tratar temas de seguridad, salud..., y suelen ser trasmitidas viralmente por el correo electrónico. Al ser intercambiadas entre amigos o familiares se les da aún más crédito. También son populares y perniciosas las "cadenas" de mensajes, en las que "obligan" al lector a reenviar el mensaje recibido so pena de tener mala suerte en su vida o no alcanzar sus metas personales.

se convierte en un mecanismo de defensa que también se activará ante mensajes, avisos, consejos u órdenes de padres y profesores, influyendo negativamente en la educación en valores, porque, si para ellos todo es relativo, entonces todo vale.

- **Asumir valores y creencias perniciosas**. La supervisión por parte de padres y docentes de los contenidos que recibes de las TIC (incluidas la televisión, las canciones y las películas) es fundamental para que no te "intoxiquen" con ideas, valores, creencias o corrientes de pensamiento poco saludables o, directamente, enfermizas: homofobia, sectarismo, dogmatismo intolerante, justificación de la violencia para defender las ideas, machismo, odio a personas por su raza o procedencia, creencias conspiranóicas, ocultismo, sobrevaloración del dinero o el lujo, obsesión por la popularidad o la moda.

### 1.1.7. Autoestima vulnerable / reputación online

La autoestima e identidad personales están siempre vinculadas a la valoración que los demás hacen de nosotros. En los jóvenes, esa opinión de tus amigos, familiares y conocidos influye mucho más en tu autoestima. Los bulos, rumores o directas descalificaciones que sobre una persona concreta pueden aparecer en las redes sociales influirán en la reputación digital y la autoestima del descalificado. Somos complejos y cambiantes, pero una fotografía que se haya colgado en la red o una frase desafortunada en un tweet pueden marcarte para siempre, por mucho que después intente justificarse. Por lo tanto, debemos ser cuidadosos con qué escribimos, qué datos y fotografías colgamos en internet o mandamos por mensajería, porque enseguida estarán a disposición de todo el mundo.

### 1.1.8. Adicciones a internet

Como cualquier otro tipo de adicción, la de internet puede convertirse para tí en una obsesión, por la fruición que obtienes a nivel personal. Los distintos usos que hace de tu conexión captan tu curiosidad, interés y elevan tu autoestima de tal forma que no necesitas de otras actividades extras. Estas son algunas de las adicciones cibernéticas más frecuentes:

- **Cibersexo, pornografía**. Por cibersexo se entienden las conversaciones de tipo sexual tenidas a través de la red, con la finalidad de conseguir excitación y placer; muchas veces están relacionadas con el consumo de pornografía, disponible mediante internet. De estas actividades puede derivarse la instrumentalización de las personas del otro sexo como simples objetos de satisfacción sexual.

- **Ludopatía, juegos online**. Obsesión con los juegos online, sobre todo si existe remuneración. En todo caso, se exacerba la competitividad y la lucha por "ser más" que los demás a través del "tener más" que ellos. Son peligrosos los casinos virtuales en los que se engancha a los menores con victorias programadas al comienzo (utilizando dinero virtual), que les hacen pasar a una segunda etapa donde tienen que poner ellos el dinero real. En los juegos online un ingrediente importante de la adicción es el propio desarrollo del juego, que te puede llenar de tensión, expectación y una fuerte sensación de inmersión (realidad virtual). Existen juegos adecuados para cada edad que, además de enriquecerte mentalmente, no son tan competitivos ni adictivos.

- **Chat**. En este subtipo de adicción a internet se abusa de alguno o varios tipos de chat (servicios de mensajería, IRC, chat en web, etc.). En estos casos, la presencia y la interacción continua se vuelven apremiantes para no sentirse solo o desplazado. De este tema trataremos más adelante, al hablar de las redes sociales.

- **Blogging**. Es el abuso de blogs y foros en los que el menor tiene como objetivo narcisista el aparecer en más y más blogs y foros, luciendo sus conocimientos u opiniones.

### Otras adicciones relacionadas con las TIC

- **Teléfono móvil.** Abuso incontrolado del móvil, los SMS, WhatsApp, etc., en el que la relación continua y fluida con conocidos te da la sensación de estar integrado, aceptado y valorado ante otras personas o grupo de personas

- **Videojuegos no online**. Es una adicción fuerte causada por la emoción propia del desarrollo de cada juego, la sucesión de niveles y de dificultades, el grado de verosimilitud de las escenas o el reto de acabar el juego con más puntos o más rápido... todo ello provoca que el menor pueda estar enganchado horas y horas. Podemos ofrecer a nuestros hijos juegos enriquecedores y no adictivos u otras actividades lúdicas fuera de la mimada videoconsola.

- **Televisión**. Aunque la televisión no es de reciente aparición, no deja de ser una TIC y la adicción a series, programas de entretenimiento y concursos (ya sea en la televisión tradicional o a través de internet) se ha mantenido como

un problema desde hace años.

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

- **Síndrome de abstinencia**. Este es un síntoma o consecuencia de una adicción constatada. El menor se irrita, enfada y puede llegar a ser agresivo cuando se le impide continuar con su móvil, ordenador, televisión o videojuego o cuando se le castiga con no poder utilizarlo durante un tiempo determinado. La desproporción de su respuesta nos puede dar una idea del nivel de dependencia de una tecnología. La falta de apetito, cambio permanente de humor, silencio o aislamiento son síntomas a tratar.
- **Sentimientos de culpabilidad**. Como en cualquier otra adicción, la obsesión por el uso de una nueva tecnología de la información (móvil, internet, videojuegos, televisión) quita tiempo para otras muchas actividades, sean estas obligatorias (escolares o domésticas) o aficiones personales; ser consciente de esta pérdida puede sumir al joven en sentimientos de culpabilidad. Si el reproche no es propio, sino que viene de padres, amigos o educadores, puede sentirse igualmente culpable, pero también puede reaccionar con mecanismos de defensa: justificándose, mintiendo, aislándose, o con actitudes más agresivas. Hasta que no escape de su adicción no podrá realizar con tiempo suficiente, sosiego y calma sus actividades pendientes.

## 1.2. 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 pueden ser solucionados con charlas sinceras y razonadas, con acuerdos y necesidades de cada uno, planteando actividades alternativas, pero siempre manteniendo el principio de autoridad. Los problemas parentales más frecuentes son:

- **Irritabilidad del joven al ser interrumpido** en su conexión a internet, en su videojuego, al ver su programa favorito de la televisión, o al ser castigado con no poder utilizarlas. Los adolescentes se apropian y se identifican mucho con sus actividades rituales con la TIC (chat, amigos virtuales, blogs, logros en los juegos, personajes y series favoritas, canciones), por lo que entienden la prohibición de estos como un ataque a su privacidad y a su persona.
- **Mentiras**. Es fácil que, con unos padres poco preocupados y observadores, el hijo/a mienta con facilidad y eficacia sobre su actividad con las TIC: uso del ordenador, tiempo dedicado a la televisión, móvil o videojuegos… Muchos progenitores confían en que sus hijos, cuando están varias horas encerrados en su habitación, han estado trabajando, muchas veces fundados solo en la afirmación que ellos realizan, pero la realidad puede ser otra. De nuevo el control parental y la real confianza y sinceridad entre padres e hijos será la solución.
- **Olvidar responsabilidades domésticas**. La adicción y el exceso de tiempo que un joven

lógicas, pero que suelen ser falaces: *lo necesito para clase, sin él no puedo aprobar, todos mis amigos lo tienen y no quiero ser el raro del grupo, no volveré a pedir nada más, solo lo utilizaré tales días*… Incluso pueden llegar al chantaje emocional, esgrimiendo lo que se aburrirán sin ello o lo poco que les quieren sus padres si no se lo compran. No es buena idea ceder a las presiones por no enfrentarse a ellos, o negárselo sin razonar el porqué de la negativa. Tampoco es buena idea premiarlos con este tipo de tecnología cuando consiguen un éxito académico o cumplen cualquier otro cometido que es de su responsabilidad, pues se acostumbrarán a trabajar a cambio de una recompensa.

- **Privacidad**. o se les exige que digan con quién han estado hablando, se creará un evidente enfrentamiento y los hijos sentirán que se ha atacado su privacidad o intimidad. Todo esto puede solucionarse si hay una comunicación previa en la que los padres expresen sus miedos y recelos frente a la actividad TIC de sus hijos, explicando las consecuencias de un mal uso de internet, el móvil o las redes sociales.

- **Bajo rendimiento escolar en las tareas académicas**. El uso inadecuado de las nuevas tecnologías de la información puede tener como consecuencia un menor rendimiento en el aprendizaje de los alumnos dentro de sus labores académicas. Además de las causas ya citadas (excesivo tiempo de dedicación a estas actividades, poco tiempo de sueño…) puede haber otras, estas generadas dentro del propio ámbito escolar:

- **Uso inadecuado de los equipos informáticos por los alumnos/as**. En las ocasiones en que se permite el uso de los ordenadores sin un control suficiente, estos pueden ser utilizados para usos ajenos al aprovechamiento lectivo. Tener siempre actividades de sustitución y un control eficaz de que su uso les rinda académicamente son las soluciones ante las horas libres en el aula que puedan tener en una clase. Ni que decir tiene que este uso libre del ordenador es contraproducente en tutorías, apoyos o clases de repaso. Así mismo, es conveniente que el centro posea un filtro de contenidos y que el profesor use un gestor de equipos. Con todo, siempre es aconsejable mantener un control visual para saber qué están haciendo los chicos en sus puestos.

- **Uso encubierto del móvil**. El uso del móvil en el aula siempre distrae de la actividad educativa, aunque esté en modo silencioso. En el reglamento de régimen interno del centro debe estar especificado si los alumnos pueden llevar el móvil o no a clase, en qué condiciones pueden usarlo, así como qué hacer en caso de no cumplir las normas establecidas.

- **Utilización inadecuada de las TIC por los alumnos en su aprendizaje**. Internet es una herramienta muy útil para el trabajo escolar, pues facilita y amplía el acceso a la información. Pero esta facilidad puede volverse en contra el alumno/a si la utiliza sin entenderla ni estructurarla, utiliza la primera fuente encontrada o, por el contrario, se satura porque encuentra innumerables páginas.

  "Mal uso de internet es, por tanto, el copiar y pegar párrafos completos de páginas encontradas para usarlos en trabajos o presentaciones sin haberlos entendido; el obligarles a escribir el trabajo a mano no soluciona este problema, pues pueden seguir sin aprender lo que copian. Sí les ayuda el que hagan una explicación-presentación de viva voz en el aula, someterles a una serie de preguntas sobre ese

es decir, que el sobrepeso de ciertos jóvenes les haga apetecer las actividades cibernéticas o la televisión frente a otras que les exigen mayor esfuerzo físico, retroalimentando la falta de ejercicio y la temida obesidad. Causas que favorecen el sobrepeso también son la alimentación inadecuada (muchas calorías) y el comer descontroladamente (por ejemplo, mientras se juega ansiosamente o se ven películas o partidos). La solución es obvia: mayor ejercicio físico (mejor si está planeado y tiene su horario), control de las horas de comida, que esta sea equilibrada (menos grasas y azúcares y más fruta y verdura) y, sobre todo, reducir las horas que se exponen a las distintas pantallas (TV, ordenador, consola...).

- **Musculares y articulares**. Se deben a posiciones incorrectas delante del ordenador, porque la espalda no está en posición suficientemente erguida, inclina la cabeza de forma antinatural, coloca los brazos en tensión, por no apoyarlos lo suficiente, las manos y dedos realizan un sobreesfuerzo por el uso intensivo y alejado del ratón y del teclado, las piernas no se mueven lo necesario para un riego sanguíneo adecuado y porque no se hacen ejercicios de relajación o estiramientos cada cierto tiempo. El dolor cervical y de espalda son la primera señal para cambiar los hábitos ergonómicos del menor.
- **Oculares**: El ver reflejos en la pantalla y la luz ambiente no será muy distinta a la de la pantalla. Cada 10-15 minutos se deberá mirar de lejos para relajar la visión.
- **Anorexia/ bulimia**. La pérdida excesiva de peso buscada por jóvenes obsesionados por la imagen puede deberse a modelos estereotipados e insanos observados en los medios de comunicación, en comentarios de blogs y foros o en páginas que promueven estas disfunciones alimentarias. Las consecuencias en la salud pueden ser catastróficas. Es particularmente importante vigilar ciertas páginas de internet asociadas al movimiento que promueve estas alteraciones alimentarias (páginas **pro-ana** y **pro-mia**), ya que el daño que pueden provocar en los menores es inmenso. Muchas veces los nombres de estas páginas ofrecen, de modo más o menos oculto, el nombre de los movimientos (ana y mia), dato que puede servir para identificarlas bajo la apariencia de títulos juveniles.
- **Autolesiones**. El número de menores que se autolesionan no ha dejado de crecer en los últimos años. Existe todo un movimiento (**proSI**, de *self-injury*) que promueve este comportamiento como un medio de fomentar el autocontrol, de superar la frustración, liberar la rabia o controlar la angustia. Se basa en la idea de que cuanto mayor sea el aguante ante el dolor, también crecerá la capacidad de la persona que se autolesiona para controlar las situaciones negativas que vive. Con bastante frecuencia las autolesiones van asociadas a trastornos alimentarios, porque se establece una falsa relación entre el grado de tolerancia al dolor y la capacidad de adelgazar.

Los alumnos y alumnas deben saber y tener presentes los siguientes principios:

A. Controlar el tiempo que se conectan, ya sea al ordenador, a la tablet, al móvil o a cualquier otro dispositivo similar.

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

G. Saber que tienen derecho a la privacidad de su información personal 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 teléfono...), leyendo atentamente las condiciones de las páginas a las que nos suscribimos.

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

I. Saber que tienen el deber de pedir ayuda a una persona mayor cuando algo no les guste o lo consideren peligroso para chicos o chicas de su edad, incluso si no les afecta personalmente, para ver conjuntamente con el adulto si hay que denunciarlo a las autoridades competentes.

J. Cuidar el mantenimiento de los dispositivos que utilizan, evitando derramar comida o líquidos sobre ellos.

## 2. 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.

### 2.1 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, (algunos de ellos serán tratados en apartados posteriores), los siguientes:

- 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 infanti
- Internet no significa anonimato. Las acciones que se realizan en la red dejan un rastro digital fácilmente identificable por expertos.
- Las contraseñas deben ser seguras, con caracteres alfanuméricos y símbolos, para dificultar la labor de robots que intentan descifrarlas.
- Es mejor usar un nick o seudónimo que el nombre propio en entornos que no sean absolutamente seguros.
- Nunca se deben revelar datos personales, como dirección, DNI, teléfono, números de cuentas bancarias, etc., a desconocidos, o en situaciones de comunicación que no hagan imprescindible su conocimiento por la otra persona.
- En el uso de dispositivos móviles, revisar los permisos de las aplicaciones, muy particularmente los de aquellas que exigen acceder a nuestra libreta de contactos, escribir correos o publicar en redes sociales en nuestro nombre o identificar nuestra localización cuando las usamos.

## 3. 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.

Un criterio para agrupar las redes sociales podría ser el interés que el usuario persigue una vez es miembro:

- Interrelación en general: Facebook, Twitter, Google+, HiS.
- Interés profesional: Linkedin, por ejemplo.
- Interés por una actividad particular: Pinterest, Flickr, YouTube, etc.

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

- Potencian la comunicación de los participantes con su entorno y, por tanto, las relaciones personales.
- Son un lugar de intercambio de opiniones y de intereses.
- Fomentan la colaboración entre los miembros de una comunidad, ya sea con el fin de ayudar o de elaborar trabajos de forma colaborativa.
- Promueven el uso de herramientas tecnológicas.

y almacenadas durante mucho tiempo.

- 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.

## 3.1 CIBERBULLYING

**¿Qué es?**

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

**Se puede prevenir?**

- Usar un nick o seudónimo que sea conocido por sus amigos más cercanos y familiares, evitando difundir sus datos personales reales.
- Configurar adecuadamente el grado de privacidad de los perfiles sociales, de modo que la información personal no pueda ser conocida por personas ajenas al círculo más próximo.
- Ser prudentes en la aceptación de invitaciones o peticiones de amistad en las redes sociales.
- Tener especial cuidado con las imágenes, vídeos que se vayan a publicar en plataformas o redes sociales, ya sean propias o de otras personas, consultando y solicitando consentimiento, previa publicación de las mismas, a las personas afectadas. Evitar siempre enviar esos archivos multimedia a personas desconocidas.
- Evitar en la medida de lo posible la difusión de datos personales reales.
- No responder a las provocaciones.
- No establecer ningún tipo de relación virtual con personas a las que no se conoce personalmente.
- Comunicar de inmediato a padres o a educadores que se está siendo víctima de amenaza, chantaje, coacción, insultos, injurias o calumnias.

¿Qué hacer?

- Contar de inmediato a los padres el caso y, si se ha venido desarrollando en el ámbito del centro educativo, al tutor.
- No borrar ningún rastro del acoso recibido, ya que es una prueba del mismo.

## 3.2 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?

- Usar perfiles privados en redes sociales

- En el caso de ser víctima de grooming, no aceptar el chantaje ni eliminar las pruebas.

¿Qué hacer?

- Ante los primeros síntomas de acoso, pedir ayuda a los padres explicando todo lo sufrido.

## 3.3 SEXTING

**¿Qué es?**

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?

- No enviar multimedia de contenido pornográfico propio o de otra persona a través del móvil es la mejor manera de prevenir. Una vez enviado, ese material se vuelve incontrolable, ya que es imposible prever cómo pueden circular esas imágenes o vídeos y a quién pueden llegar.
- Si se recibe multimedia de pornografía infantil, debe borrarse inmediatamente ya que la pornorafía infantil es delito siempre que se cree, se posea o se distribuya.
- Si se toma una imagen o se graba un vídeo de alguien, no se tiene derecho a distribuir ese contenido. Aunque la persona haya dado permiso para tomar o grabar esas imágenes, no significa que se pueda pasar a otras personas.
- No ceder ante la presión o el chantaje de otros para distribuir cualquier contenido multimedia de índole pornográfico

## 3.4 PHISHING

**¿Qué es?**

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

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?

Se pueden reconocer los correos cuya intención es distribuir un bulo:

- Piden que se reenvíen.
- A pesar de su aspecto, que les da total credibilidad, no mencionan fuentes oficiales.
- Aprovechan la sensibilidad y credulidad del usuario para captar su atención y hacer que lo reenvíe a sus contactos.
- Normalmente no tienen fecha y circulan por interne indefinidamente.

Hay que tener en cuenta algunos consejos en torno al correo electrónico:

1. Eliminar los correos que provenga de personas que no se conozcan.
2. Mejor tener una cuenta de correo electrónico para comunicarse con la familia y amigos y otra cuenta para registros en redes sociales, juegos online, etc.
3. Nunca reenviar correos con mensajes falsos que piden reenvíos a los contactos.
4. Desconfiar de los archivos adjuntos; no descargarlos y, si se hace, analizarlos antes con un antivirus.

## 3.5 VIRUS, MALWARE, SPYWARE...

Los dispositivos que, potencialmente, pueden verse afectados son:

- Ordenadores personales y servidores
- Móviles
- Tablets
- Videoconsolas

Los virus se clasifican según el tipo de acción que realizan y según cómo se propagan. Dentro

sobre nombre de usuario y contraseñas.

Según cómo se propaguen se clasifican en:

- **Virus**: suelen infectar a través de archivos ejecutables del tipo .exe o .bat y solo se propagan cuando se ejecutan dichos archivos.
- **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.
- **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:**

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

**En cuanto a la navegación por internet:**

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

**En cuanto al correo electrónico:**

- No abrir correo electrónico de personas u organismos desconocidos o sospechosos, así como tampoco descargar ficheros adjuntos de ellos.

- No compartir usuario o contraseña con otros usuarios.
- Mantener control sobre la cuenta y tarjeta de crédito asociados.

**En cuanto a dispositivos móviles:**

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

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