BIENVENIDOS AL CEIP STA CAPILLA DE SAN ANDRÉS



MANUAL DEL BUEN USO

MEDIOS INFORMÁTICOS

Elaborado por José Manuel Martín Fernández · Jefe de Estudios del CEIP "Las Huertas" (Pedrera)

Índice

1.-Principios sobre el buen uso de las Tic

- **1.1-El Alumnado**
- **1.2.-La Familia**
- **1.3.-El profesorado**

2.-Riesgos en el uso de las Tic

- **2.1.-Problemas psicológico y académicos.**
  - **2.1.1.-Transtornos del Sueño**
  - **2.1.2.-Deficit/Dispersión de la Atención**
  - **2.1.3 Forma de escape de problemas y responsabilidades reales**
  - **2.1.4 Aislamiento, dejar de salir con amigos**
  - **2.1.5.-Escaso control de pulsiones**
  - **2.1.6.-Desinformación e intoxicación de ideas.**
  - **2.1.7.Autoestima vulnerable. Reputación Online**
  - **2.1.8.-Adicciones a Internet**
  - **2.1.9.-Otras adicciones relacionadas con Internet**

3.-Otros problemas. Ciberdelitos

- **3.1 Violación del Derecho a la Imagen y a la Intimidad. Privacidad.**
- **3.2.-Ciberbulliyng**
- **3.3.-Grooming**
- **3.4.-Sexting**
- **3.5-Phishing**
- **3.6.-Virus, Malware, Spyware…**

1. PRINCIPIOS SOBRE EL BUEN USO DE LAS TIC

Hoy en día, y de la misma forma que educamos en hábitos más arraigados en nuestra sociedad, estamos obligados a indicar a nuestros hijos y alumnos, desde bien pequeños, cuáles son las virtudes y los peligros de las TIC.

1.1 ALUMNADO

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.
B. Cuidar su correcta posición corporal al usar cualquiera de estos dispositivos, sentándose correctamente.
C. Ser prudentes y no concertar encuentros con personas que no conocen y que les proponen quedar a solas.
D. Tener respeto a otros usuarios, evitando las burlas, difamaciones, humillaciones y agresiones.
E. No suplantar la identidad de nadie en la red.
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.

1.2 FAMILIA

Es muy importante la contribución de las familias en los siguientes principios:

A. Estar al día en todo lo relativo a internet y nuevas tecnologías, ya que cuanta más información se tenga sobre estas realidades mejor podrán ayudar y acompañar a sus hijos o hijas en el buen uso de ellas.
B. Acordar unas normas de uso claras, estableciendo y haciendo cumplir un horario. Es importante que los menores tengan claro lo que pueden y no pueden hacer y sepan sus consecuencias. Se debe marcar un tiempo para tareas escolares y un tiempo para el ocio.
C. Crear un espíritu crítico sobre la información que aparece en la red y explicarles que no todas las web tienen la misma credibilidad, que es importante filtrar y evaluar su calidad.
D. Enseñar a utilizar motores de búsqueda y contrastar varias fuentes sobre un mismo campo, evitando el “corta y pega”, de modo que sus tareas no se conviertan en plagios de trabajos ya realizados.

E. Fomentar el diálogo sobre hábitos de utilización de las TIC y sus riesgos. Es importante que el menor sienta que cuando le suceda algo extraño o le incomode, puede decírselo a sus padres sin sentirse culpable.
F. Utilizar filtros de control de acceso a la red y programas de control parental, con los que se evitará que los menores accedan a páginas de contenido inapropiado y proporcionarán herramientas de regulación del tiempo de uso de los dispositivos digitales.
G. Tener el ordenador en una zona de uso común, ya que facilitará tanto l supervisión del tiempo de utilización como las situaciones que puedan resultar incómodas para el menor, así como la revisión de las web que visita. Buscar una ubicación en la que la luz sea la adecuada, evitando reflejos.
H. Cuidar la postura respecto al ordenador, que debe seguir 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.
I. Enseñarles en qué consiste la privacidad, que los datos personales son información sensible y que pueden ser utilizados en su contra.
J. Explicarles que en las redes hay que respetar a los demás, que detrás de cada apodo hay una persona y que siempre hay que ser educado.
K. Cuidar el ordenador, tablet, móvil…, evitando riesgos físicos, como derramar comida o bebida sobre ellos, ponerlos en focos de calor, que sufran golpes, y mantener limpios todos los componentes.

1.3 El Profesorado

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 alejad, 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 web 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

l. 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.

2. RIESGOS EN EL USO DE LAS TIC

2.1 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:

2.1.1 Trastornos del sueño

Es frecuente que el uso de internet o la televisión por los jóvenes, sin un horario concreto o un control parental, se alargue por la noche sin una noción del paso del tiempo por parte del usuario. 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 enganchándoles en chats o vídeos. Las horas restadas al sueño repercutirán en el rendimiento escolar y en el equilibrio psíquico del menor.

2.1.2 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 los jóvenes tienen por otras informaciones que les llegan por medio de sus profesores, padres o monitores de actividades. Si no asumen el valor y la necesidad que tienen de los contenidos y valores de sus educadores, pueden desatenderlos o despreciarlos. A esto se une el tipo de recepción de información a la que se están acostumbrando al navegar por la red: desorganizada, deshilvanada, acelerada y caótica; y que contrasta con la que les ofrecen sus educadores: más lenta y estructurada y que requiere de un esfuerzo de comprensión y aprendizaje. En este contexto, es lógico que el desinterés y la falta de control de atención puedan aparecer, llevándoles a una distracción continua entre pensamientos emergentes y estímulos exteriores.

2.1.3 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.

2.1.4 Aislamiento, dejar de salir con amigos

Solemos elegir las compañías que mejor nos tratan o que más nos estimulan, divierten o enseñan. Pero si a un joven estos valores se los proporciona un videojuego, la comunicación virtual a través de redes sociales, los estímulos de ciertas páginas web o el juego online, entonces sentirá que no necesita salir de su casa para reforzar su autoestima, sus ganas de disfrutar y aprender. No hay que alarmarse, porque el joven está probando y cambiando temporalmente de "compañeros de viaje", como lo hacen otras personas con sus aficiones, y lo más probable es que, con el tiempo, vuelva a necesitar del contacto directo con otras personas. Un mal síntoma podríamos encontrarlo en la evitación continua y activa de los demás para encerrarse con su ordenador o videojuego.

2.1.5 Escaso control de pulsiones

Este es otro síntoma del exceso de tiempo y/o atención dedicado a las nuevas tecnologías, dentro de las cuales el adolescente se expresa y siente de manera libre y sin cortapisas. Al mando del ratón, joystick o mando a distancia se convierte en un "rey" que controla a su gusto qué, cuándo y cómo es lo que recibe, su voluntad es la dueña. Pero, cuando apaga el aparato y vuelve a someterse a la disciplina y voluntad de otras personas, pierde ese control que ha tenido y puede contrariarse, enfadarse, entristecerse o, de nuevo, aislarse. Cuanto más cree un mundo virtual a su medida, peor aguantará el mundo "real".

2.1.6 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 sí mismos. La sobreinformación que ahora les 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 el joven puede 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.
- **Desconfianza y/o relativización**. En el lado opuesto a la ingenuidad anterior está el exceso de sentido crítico que lleva a relativizar y minusvalorar cualquier información que llegue al chico/a. Suele estar asociado a una larga exposición a la sobreinformación. Es pernicioso, porque desdeñar y criticar 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 cada joven recibe de las TIC (incluidas la televisión, las canciones y las películas) es fundamental para que no se "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 conspiranoicas, ocultismo, sobrevaloración del dinero o el lujo, obsesión por la popularidad o la moda... Los recursos para minimizar estos envenenamientos son el hablar abierta y razonadamente con ellos sobre estos temas y proponer ejemplos claros y cercanos en los que se desmontan esas teorías.

2.1.7 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 sus amigos, familiares y conocidos influye mucho más en su 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 marcar a esa persona 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.

2.1.8 Adicciones a internet

Como cualquier otro tipo de adicción, la de internet puede convertirse para el menor en una obsesión, por la fruición que obtiene a nivel personal. Los distintos usos que hace de su conexión captan su curiosidad, interés y elevan su autoestima de tal forma que no necesita 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 les puede llenar de tensión, expectación y una fuerte sensación de inmersión (realidad virtual). Existen juegos adecuados para cada edad que, además de enriquecerles 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. Suele afectar a personas más adultas.

2.1.9 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 les da la sensación de estar integrados, aceptados y valorados 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 para nuestros jóvenes desde hace años. Incluso la comodidad de llenar sus mentes durante horas, cambiando
  de programa o de vídeo, también puede enganchar, haciéndoles perder un tiempo valioso.

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.

2.2 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 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:

- **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 puede dedicar a su dispositivo preferido puede causar que pierda la noción del tiempo mientras lo usa, pasándole los minutos y horas sin darse cuenta. Consecuencia: sus padres le llamarán para merendar, cenar, ir a ciertas actividades extraescolares, sacar al perro y, en general, hacer labores domésticas rutinarias, porque al hijo/a se le habrá "pasado". Se pueden evitar estas pequeñas tensiones con organización, que incluye control parental, horario (hasta con alarma o despertador) y sanciones consensuadas en caso de no cumplir con las obligaciones.
- **Presiones para comprar aparatos**. Es cada vez más frecuente la presión que ejercen los hijos sobre sus padres para adquirir nuevos aparatos, conexiones o software. El llamado tecnonarcisismo no solo se da en niños de clases pudientes. Todos esgrimen razones 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**. Si los menores se consideran espiados, saben que sus correos electrónicos o chats son leídos por sus padres, 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 tema, pedirles que resuman en otra hoja el trabajo realizado o crear un duelo dialéctico entre alumnos sobre ese contenido. Por otro lado, orientarles sobre dónde encontrar los mejores contenidos en la red o utilizar técnicas tipo WebQuest les ahorrará tiempo y complicaciones en su búsqueda en internet.

2.3 PROBLEMAS DE SALUD FÍSICA

- **Sobrepeso**. Es una consecuencia del sedentarismo que propicia el pasar muchas horas sentado (o tumbado) frente a la pantalla. También puede pasar a la inversa; 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**. Los síntomas son el estrés visual, el ver borroso o doble al mirar a distancias largas, lagrimeo y enrojecimiento de los ojos. Las causas posibles ya nos indican cómo debe organizarse el menor para prevenir los síntomas descritos: la pantalla debe estar de frente (perpendicular) al usuario, por debajo de su horizontal visual y a una distancia de sus ojos de 40-50 cm. No se recomiendan monitores muy pequeños o con mucha densidad de píxeles, porque los textos serán minúsculos para ser leídos a esa distancia. No debe haber 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.

Las autolesiones pueden ser menores (golpearse en las muñecas con elásticos cuando algo no sale bien en clase) o mayores (quemaduras de cigarrillo, cortes con cúter o tijeras), y se realizan mayoritariamente en zonas no visibles del cuerpo (antebrazos y muslos). Los menores que llevan a cabo esta práctica se resisten a mostrar estas partes del cuerpo, incluso cuando, por temperatura, sería razonable que lo hicieran.

2.4 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:

- **Informarse** de los riesgos que entrañan los usos de las nuevas tecnologías en los jóvenes. Hay decenas de páginas con avisos y datos sobre estos peligros.
- **Observar** a nuestros hijos/alumnos por si ya están padeciendo alguno de los problemas citados o están en vías de hacerlo.
- **Que los padres sepan manejar el ordenador, tablet o teléfono**, y entiendan cómo utilizan sus hijos los mismos. Así será también más fácil compartir contenidos y experiencias, charlar sobre estas tecnologías e incluso poder jugar con ellos, siempre buscando su beneficio.
- **Acordar normas de uso claras de los dispositivos digitales**. Para ello hay que empezar mostrándoles, con sinceridad y sin alarmismos, los problemas a los que se pueden ver sometidos. Las normas incluirán contenidos, aplicaciones y programas que no pueden usar (por su edad o por su peligro) y el horario de utilización para el trabajo académico y para el uso personal.
- **Dialogar frecuentemente** y sin presiones sobre el uso de las TIC, así como de las dificultades y logros que ambos (padres e hijos) puedan tener con estas tecnologías. En este ambiente de confianza el hijo/a podrá pedir ayuda o comentar sus problemas sin esconderlos ni sentirse culpable.
- **Es recomendable colocar el ordenador y la videoconsola en un lugar común**, siempre que se pueda, para controlar su uso y el tiempo que dedican a ello.
- **Utilizar tecnologías de software para proteger el equipo y a los menores**. Entre ellos son imprescindibles los antivirus, anti-spyware y firewalls, siendo también recomendables los filtros de contenidos, los controles parentales o el repaso del historial de páginas visitadas de su navegador. Existen muchas soluciones eficaces en el mercado, tanto gratuitas como de pago.
- **Extremar el cuidado con las descargas de software**, especialmente las gratuitas, ya que en muchos casos son el origen de problemas en los equipos (instalación de malware, robo de datos…). Especialmente se debe extremar el cuidado en Windows con archivos .exe que no se sepa exactamente para qué sirven y que no provengan de una fuente segura, y con los permisos de instalación de aplicaciones en tablets y teléfonos móviles.
- **Desconfiar de correos de remitentes desconocidos o anónimos** que piden que se realicen acciones en el equipo, o que se haga clic en un enlace.
- **Concienciar del fraude que supone utilizar programas o juegos piratas**. No solo es una estafa que no nos gustaría que nos hicieran a nosotros, también es un peligro potencial por virus que puedan contener y por la posible desconfiguración del sistema operativo.
- **Acordar actividades alternativas saludables** al uso abusivo de las nuevas tecnologías. Existen muchas actividades, deportes, cursos, talleres, aficiones, asociaciones, ONG, etc., en las que el menor puede divertirse, aprender y sentirse realizado. Lo que se busca sobre todo será movilizar físicamente al joven y socializarle para evitar la posible vida sedentaria que tendrá si dedica mucho tiempo a las TIC.

- **Tener claro el papel de padre como educador** y no como "colega", para no ceder ante las presiones de los hijos que reclaman más tiempo de ocio frente al ordenador, menor control y la compra de más aparatos. La realización de nuestros hijos/alumnos a medio y largo plazo es más importante que su satisfacción inmediata.

3. 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.

3.1 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:

- 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

¿Cómo prevenirlo?

Consejos para menores:

- Cualquier información personal vertida en la red se mantiene durante mucho tiempo, por lo que hay que extremar el cuidado al compartir datos personales propios o ajenos, muy especialmente las imágenes.
- 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.

Consejos para padres y educadores:

- 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.
- Advertirles de no compartir contraseñas con nadie.
- Ayudarles en la medida de lo posible en el uso de la seguridad en redes sociales, foros, etc.
- Hacerles reflexionar a la hora de publicar sobre quién verá su información.
- 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.
- 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.
- 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.

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.

Existen muchas redes sociales, entre las más populares se encuentran:

- Facebook
- Twitter
- Instagram
- Snapchat
- Tuenti
- Google+
- Linkedin
- HiS
- MySpace
- Flickr
- Ning
- Edmodo
- Fotolog
- Netlog
- Pinterest

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.
- Son una fuente de información continua y actualizada.

También su uso conlleva riesgos:

- 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.
- Los menores son vulnerables a sufrir ciberdelitos, al aceptar en su comunidad a usuarios que no conocen personalmente.
- Muchas de las acciones personales que el usuario va seleccionando quedan registradas 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.

3.2 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 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.

¿Cómo reconocer el ciberacoso?

- Descubrir un perfil falso, que la víctima no ha creado (a veces aparece incluso con su foto) a su nombre, en el que se vierten datos personales y aspectos falsos sobre la misma.
- Recibir amenazas, insultos a través de SMS, correos electrónicos, mensajería multiplataforma (WhatsApp, Line, etc.) de forma reiterada.
- Usurpar fotografías comprometidas de la víctima (reales o realizadas mediante montaje), datos personales y distribuirlos por la red avergonzándola.
- Apropiarse de datos de acceso a chats, foros, correo electrónico, mensajería multiplataforma, etc. y usarlos de manera indiscriminada, vertiendo mensajes ofensivos, etc., para hacer creer que la víctima es la responsable de toda esa actividad.

¿Se puede prevenir?

En el caso de los menores:

- 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.

En el caso de los padres:

- Establecer normas sobre el uso de ordenadores y dispositivos móviles y acceso a internet.
- Colocar el ordenador en zonas comunes del hogar, con el fin de conocer el tiempo de uso de los mismos, su actividad en la web, de modo que estas acciones sean controladas sin necesidad de intromisión en la intimidad del menor.

- Establecer una comunicación con el menor e instruirle acerca de los peligros que supone la difusión de imágenes y datos personales en la red, así como de las consecuencias que conllevan conductas poco adecuadas y agresivas hacia otras personas.
- Mantener una supervisión periódica de los dispositivos y cuentas de servicios que usa el menor para conocer su actividad: sitios web que visita, historial de búsqueda, etc.

En el caso de los profesionales de la enseñanza:

- 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.
- Reflexión sobre los riesgos de internet, ordenadores y dispositivos móviles.
- Tomar conciencia de qué es el ciberbullying y sus consecuencias.
- Análisis del rol del observador pasivo que ve lo que ocurre y no actúa.
- Fomentar la reflexión entre el alumnado de las diferencias entre chivar y denunciar.
- Realizar dinámicas que permitan reconocer los distintos roles que participan en un caso de ciberbullying (víctima, acosador, observador…).
- 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 menores:

- 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.

Para profesionales de la enseñanza:

Si el ciberacoso procede del entorno escolar:

- Informar al equipo directivo, al orientador y al tutor para aplicar el apoyo necesario al alumno, tanto si es víctima, acosador u observador.
- Aplicar los protocolos de actuación que el centro pudiese tener para estos casos.
- Recurrir a organizaciones especializadas en acoso escolar.
- 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.

Para padres:

En este caso, los padres pueden encontrarse con que su hijo ha sido víctima, agresor u observador. En cualquier caso:

- Se debe escuchar al menor y dejar que exponga cuanto desee sobre el asunto.
- Comprobar que se trata de una situación real y no es producto de su imaginación. En ningún caso arrojar dudas injustificadas sobre la situación relatada por el menor.
- Intentar aplicar alguna estrategia para detener el daño que pueda estar recibiendo u originando el menor.

- Si el hecho se ha producido en el ámbito escolar, ponerse en contacto con el tutor del menor y solicitar información y una intervención por parte del centro.
- Denunciar ante las autoridades.

3.3 GROOMING

¿Qué es?

Bajo el nombre de grooming se incluye toda actividad llevada a cabo por cualquier usuario adulto que intenta contactar con menores con fines sexuales. Normalmente los objetivos son conseguir imágenes del menor desnudo o realizando actos sexuales mediante la cámara web del propio ordenador de la víctima, aunque también puede perseguir establecer un contacto directo con finalidad sexual con el menor.

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 el menor:

- Usar perfiles privados en redes sociales.
- No aceptar invitaciones, contactos o comunicaciones de personas que no conozca personalmente.
- No revelar datos personales íntimos ni mostrar imágenes o vídeos propios o de amigos en webs o plataformas públicas.
- No aceptar mensajes de contenido pornográfico o sexual.
- En ningún caso posar para fotos o grabaciones de vídeo de contenido sexual, o de tono comprometido, incluso si tienen como destino amigos o amigas cercanos.
- En el caso de ser víctima de grooming, no aceptar el chantaje ni eliminar las pruebas.

Para los padres:

- Hablar abiertamente del tema con el menor, explicándole en qué consiste el acoso sexual.
- Advertirles de los peligros de hacer públicos sus perfiles en redes sociales, datos personales o imágenes y vídeos comprometidos.
- Hacerles ver que la webcam no es imprescindible para usar la red y que, en caso de usarla, lo hagan con prudencia.
- Insistir en la idea de que en la red no se debe hacer nada que no se haría en la vida real.
- Aconsejarles sobre el riesgo de aceptar amistades que no conocen en persona.
- Estar atentos sobre la actividad del menor en la red:
  → Si pasa muchas horas y si lo hace por la noche.
  → Si se encuentran archivos multimedia pornográficos en su ordenador.
  → Si el menor se comporta de forma extraña, se aísla, no sale ya con sus amigos, presenta síntomas físicos de difícil explicación o sufre una brusca alteración de su rendimiento escolar.

- Comprobar si el menor accede a internet en lugares diferentes al hogar e intentar que explique el motivo.
- Generar en el menor la suficiente confianza para que solicite ayuda en caso de ser víctima de acoso sexual.
- No borrar nunca las pruebas del delito.

¿Qué hacer?

Para los menores:

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

Para los padres o educadores:

- 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.
- Recopilar todas las pruebas de la actividad del acosador: mensajes, multimedia... • Denunciar el caso.

3.4 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?

Consejos para menores:

- 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 pornografía infantil es delito siempre que se cree, se posea o se distribuya. En estos casos, hay que comunicárselo a un adulto.
- No distribuir nunca multimedia de nadie sin su consentimiento, ya que la imagen de una persona es un dato personal cuyo uso está protegido por la Ley.
- Nunca confiar en la seguridad de las redes sociales, en herramientas de mensajería instantánea ni en redes wifi públicas, ya que pueden ser atacadas por hackers y acceder a los datos, imágenes y vídeos personales.

- No solicitar a nadie imágenes o vídeos de ese tipo, ni aceptar peticiones para realizarlas, incluso si provienen de personas muy cercanas.
- 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.

Consejos para padres y educadores:

- Insistir a los menores en la necesidad y la importancia de la privacidad.
- 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.
- 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.
- Consultar a especialistas como psicólogos, pedagogos, etc.
- 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 se es menor de edad, o si un hijo o alumno está sufriendo una situación de sexting, es obligatorio denunciarla, por ser un delito.

3.5 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 (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 menores:

- No se debe responder a ningún correo que pida datos personales.
- Nunca hacer clic en enlaces sospechosos que recibamos en el correo electrónico.
- Antes de introducir contraseñas en páginas web, comprobar que son las reales y las auténticas a través de elementos como el “https” o el código de colores de los navegadores: verde, la página es real, o blanco, hay que ser precavido, ya que la página no proporciona información sobre su propietario.

Consejos para padres y educadores:

- Nunca se debe enviar información personal o financiera por correo electrónico.
- Tener cuidado con los archivos adjuntos que se reciben a través del correo electrónico, así como con su descarga, ya que pueden ser maliciosos.
- Nunca hacer clic en enlaces sospechosos que recibamos en el correo electrónico.

- 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.
- Hay que tener cuidado igualmente con aquellos correos que envían teléfonos a los que llamar para facilitar la información.
- 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.
- 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.
- Revisar de vez en cuando las cuentas bancarias con el fin de detectar lo antes posible cualquier cargo no autorizado.

¿Qué hacer?

- Se pueden enviar los mensajes recibidos a la empresa u organización suplantada para que esté en su conocimiento.
- Denunciar el caso. 3.6 CORREOS FALSOS (HOAX, BULOS, CADENAS, SPAM)

¿Qué es?

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.
- Indican que hay que reenviarlo a todos nuestros contactos.
- Piden información personal (dirección, DNI, número de cuenta, etc.).

Para ello se valen de información que puede atraer la curiosidad, solidaridad, etc. del usuario (correos sobre injusticias, delitos, catástrofes, etc.).

¿Se puede prevenir?

Para menores y padres:

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 internet indefinidamente.

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

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

Consejos para profesionales de la enseñanza:

- Advertir a los menores de que no toda la información que circula por la red es cierta.
- Aconsejarles que, para el registro en redes sociales, juegos…, usen direcciones de correo que no contengan sus datos personales como edad, apellidos, etc.
- Indicarles que usen distintas cuentas de correo para juegos, foros, amigos, etc.
- Advertirles de que si reciben mensajes de personas desconocidas los eliminen de inmediato.
- 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.

¿Qué hacer?

3.6 VIRUS, MALWARE, SPYWARE...

¿Qué es?

Son virus, gusanos o troyanos; es decir, programas cuyo objetivo es alterar el funcionamiento del equipo que infectan, sin que el usuario lo note y lo consienta. En general se conocen con alguno de los términos: malware (del inglés malicious software, software malintencionado), o código o software malicioso. Actúan bien robando información personal y sensible del usuario, usando el equipo para, desde él, cometer otros actos delictivos, o bien eliminando datos del equipo, o encriptándolos y solicitándole al usuario dinero a cambio de recuperarlos.

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 del primer grupo se encuentran, entre otros:

- **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.
- **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.

- **Ladrón de contraseñas**: accede a ficheros del ordenador que contienen información 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:

En cuanto al equipo:

- Mantenerlo actualizado con la última versión de sistema operativo y del software instalado.
- Instalar un antivirus y mantenerlo actualizado.
- Hacer, de vez en cuando, copias de seguridad de los datos.
- Nunca usar software pirateado.
- Crear usuarios con permisos limitados en la configuración del equipo.
- 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.
- Usar un filtro anti-spam para evitar la recepción de correo malintencionado.
- Si se va a descargar un fichero, analizarlo con un antivirus inmediatamente después de la descarga.

- No unirse a las cadenas de mensajes falsos que se reciban, así como no difundir públicamente la dirección de correo electrónico.

Juegos online:

- Mantener actualizado el software.
- 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.
- No activar el bluetooth si no se va a usar.
- Borrar SMS sospechosos y nunca aceptar las descargas de sitios aparentemente peligrosos.
- No descargar e instalar software no confiable.

Redes P2P:

- No se debe compartir software de forma ilegal.
- Analizar todos los ficheros que se descarguen con un antivirus.
- 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.