Junta de Andalucía
Consejería de Educación y Deporte

MANUAL DEL BUEN USO DE LOS MEDIOS INFORMÁTICOS

FAMILIAS

FAMILIAS

RIESGOS EN EL USO DE LAS TIC

1. PROBLEMAS PSICOLÓGICOS Y ACADÉMICOS

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

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

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. Las horas restadas al sueño repercutirán en el rendimiento escolar y en el equilibrio psíquico del menor.

Déficit /dispersión de la atención. Los estímulos, incitaciones y sobre-información que aporta la navegación por la red 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. 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.

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 en el caso de los adictos a las nuevas tecnologías.

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. Un mal síntoma podríamos encontrarlo en la evitación continua y activa de los demás para encerrarse con su ordenador o videojuego.

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".

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.
- Información falsa, credulidad.
- Desconfianza y/o relativización.
- Asumir valores y creencias perniciosas.

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.

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.
- Ludopatía, juegos online.
- Chat.

Otras adicciones relacionadas con las TIC

- **Teléfono móvil.** Abuso incontrolado del móvil, los SMS, WhatsApp, etc.,
- **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.
- **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.
- **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.

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.
- **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.

- **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".
- **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..
- **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.
- **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.
- **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.
- **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.

3. PROBLEMAS DE SALUD FÍSICA

- **Sobrepeso**. Es una consecuencia del sedentarismo que propicia el pasar muchas horas sentado (o tumbado) frente a la pantalla.

- **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.

- **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.

CONSEJOS GENERALES PARA EVITAR ESTOS PROBLEMAS

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 webs 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.

4. OTROS PROBLEMAS: CIBERDELITOS

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

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.

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
- 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:

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

UN CASO ESPECIAL: LAS REDES SOCIALES

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

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

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

4. Promueven el uso de herramientas tecnológicas.
5. Son una fuente de información continua y actualizada.

También su uso conlleva riesgos:

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

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

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

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

1. Se debe escuchar al menor y dejar que exponga cuanto desee sobre el asunto.
2. 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.
3. Intentar aplicar alguna estrategia para detener el daño que pueda estar recibiendo u originando el menor.
4. 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.
5. Denunciar ante las autoridades.
6. Hablar abiertamente del tema con el menor, explicándole en qué consiste el acoso sexual.
7. Advertirles de los peligros de hacer públicos sus perfiles en redes sociales, datos personales o imágenes y vídeos comprometidos.
8. Hacerles ver que la webcam no es imprescindible para usar la red y que, en caso de usarla, lo hagan con prudencia.
9. Insistir en la idea de que en la red no se debe hacer nada que no se haría en la vida real.
10. Aconsejarles sobre el riesgo de aceptar amistades que no conocen en persona.
11. Estar atentos sobre la actividad del menor en la red:
12. Generar en el menor la suficiente confianza para que solicite ayuda en caso de ser víctima de acoso sexual.
13. No borrar nunca las pruebas del delito.

14. 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.
15. Recopilar todas las pruebas de la actividad del acosador: mensajes, multimedia.
16. Insistir a los menores en la necesidad y la importancia de la privacidad.
17. 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.
18. 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.
19. Consultar a especialistas como psicólogos, pedagogos, etc.
20. 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.
21. 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.
22. Nunca se debe enviar información personal o financiera por correo electrónico.
23. Tener cuidado con los archivos adjuntos que se reciben a través del correo electrónico, así como con su descarga, ya que pueden ser maliciosos.
24. Nunca hacer clic en enlaces sospechosos que recibamos en el correo electrónico.
25. 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.
26. Hay que tener cuidado igualmente con aquellos correos que envían teléfonos a los que llamar para facilitar la información.
27. 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.
28. 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.
29. Revisar de vez en cuando las cuentas bancarias con el fin de detectar lo antes posible cualquier cargo no autorizado.
30. Se pueden enviar los mensajes recibidos a la empresa u organización suplantada para que esté en su conocimiento.
31. Denunciar el caso.

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

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

5. VIRUS:

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:Tener especial cuidado con los archivos que se comparten y se instalan a través de medios extraíbles como CD, DVD o memorias USB, así como con los archivos adjuntos de correos electrónicos.

En cuanto a la red WIFI:

1. Cambiar la contraseña, que por defecto, trae el router de fábrica.

2. Usar encriptación WAP, mejor que WEP.
3. Ocultar el nombre de la red WIFI (ESSID).
4. Apagar el router cuando no se use.

En cuanto a la navegación por internet:

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

En cuanto al correo electrónico:

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

Juegos online:

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

En cuanto a dispositivos móviles:

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

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