

Guía de uso responsable de la tecnología para las familias

1 Presentación

El acceso a todos los recursos educativos que ofrecen las **Tecnologías de la Información y la Comunicación** (TIC) permite a las familias y sus hogares convertirse en espacios de aprendizaje digital.

Junto con las **grandes oportunidades** que ofrecen los nuevos recursos, surgen nuevos retos, como el de usar **eficientemente la información**, contrastarla, **sabernos comunicar a través de los nuevos formatos digitales**, y saber hacer frente a los potenciales malos usos de las nuevas tecnologías.

Las familias deben desempeñar un nuevo papel en el uso correcto de las TIC que sus hijos/as hagan en el hogar y con los medios que les proporcionan (como los móviles): hay riesgos potenciales, pero también existen buenas prácticas preventivas y soluciones sencillas para la mayor parte de los casos.

Gracias a la interacción entre nuevos medios y métodos de aprendizaje, se logra que el alumnado desarrolle capacidades imprescindibles en el Siglo XXI:

- **Aprender por sí mismo** (autoaprendizaje) y aprender por descubrimiento de forma continuada en el tiempo.
- **Trabajar en equipo** y cooperativamente, de forma creciente, autónoma y planificada. Red XXI es la adaptación del trabajo escolar a los cambios en nuestra sociedad, para mejorar la calidad de la enseñanza y aumentar el éxito escolar.
- **Buscar, evaluar, procesar e interpretar información**, comunicarla y transformarla en conocimiento significativo.
- **Hacer un uso responsable de las tecnologías**, conociendo las buenas prácticas y los potenciales peligros, regulando satisfactoriamente su relación con ellas y sus hábitos de usuario.
- **Comunicarse y expresarse** con distintas intencionalidades y en diferentes situaciones, aprovechando todas las posibilidades que proporcionan las TIC, para desarrollar su creatividad y mejorar sus habilidades sociales.
- **Aprovecharse de la actualización permanente de los contenidos**, y personalizar su proceso de aprendizaje, adaptándolo a sus intereses, capacidades y necesidades.

2. Usos eficientes y contribución de las familias

2.1. ¿Cuándo y cuánto usar el ordenador?

Una de las primeras contribuciones de las familias es ayudar a sus hijos e hijas a planificar convenientemente los tiempos de uso del ordenador: **establecer y hacer cumplir un horario** (con cierta flexibilidad, pero con criterios claros)

Las posibilidades de consulta de información, ocio o relaciones sociales con las TIC son casi ilimitadas. Pero hay que **evaluar el tiempo de uso acumulado** o la proporción entre ese tiempo y el rendimiento obtenido.

Hay que evitar usos obsesivos. En casos extremos se puede llegar a generar un problema de aislamiento. **Las familias juegan un papel fundamental** en la regulación del tiempo de uso (marcando horarios para tareas escolares, y delimitando también un tiempo para el ocio o las relaciones sociales online), procurando también espacios y tiempos para interacción personal presencial.

La labor de las madres y padres ante el desarrollo de las tareas escolares cobra nuevos matices: los adultos no necesitan ser usuarios expertos de las TIC, pero deben mostrar sensibilidad ante las ventajas de su uso. Además, hay un amplio campo de apoyos que pueden y deben prestar.

En todo caso, las familias deben ser sensibles ante una nueva realidad: uno de los retos escolares actuales consiste precisamente en la habilidad de encontrar, evaluar, manipular y comunicar información procedente de un medio tan heterogéneo como Internet.

2.2. La información procedente de Internet

Algunas tareas escolares pasan por la **búsqueda de información en Internet**: hay que “filtrarla” y evaluar su calidad ¿Cómo?:

- Evaluando quién ofrece una información (particulares, organizaciones, entidades educativas, centros oficiales...), o **contrastando varias fuentes sobre un mismo campo**.
- Utilizando motores de búsqueda avanzados (que únicamente muestran las páginas web que cumplan determinadas características, como fecha de publicación, tipo de archivo, etc.)
- Las familias pueden ayudar a evitar uno de los defectos más frecuentes en los contenidos procedentes de Internet: el plagio de trabajos ya realizados (aunque sean de libre distribución).

2.3. Cuidados básicos del ordenador

Otra de las contribuciones que las familias pueden realizar para el buen uso de un ordenador son los siguientes cuidados básicos:

- Evitar riesgos físicos como: el derramar comida o bebida sobre el teclado (uno de los principales enemigos del portátil), poner equipos en focos de calor (radiadores, calefactores...), elevada exposición a rayos solares o radiaciones de otros tipos (microondas, televisores, frigoríficos...: debe evitarse dejarlo a menos de 20 cm. de electrodomésticos). Cuidado con los imanes.
- Manipular el ordenador evitando golpes bruscos o abatir con demasiada fuerza la pantalla, etc. No colocar nunca peso encima del portátil cuando esté cerrado.
- Limpiar la pantalla o los demás componentes externos sin emplear productos que lo dañen (alcohol o detergentes). La carcasa y teclado pueden limpiarse con un paño ligeramente humedecido. Evitar rayar la pantalla o el teclado. El producto usado debe echarse siempre en un papel/bayeta, no directamente en los equipos.
- Si es un portátil, respetar los periodos de carga de la batería (evitando el sobrecalentamiento) y descarga de la batería.
- Respetar el ciclo de apagado, evitando daños en la memoria al desconectar indebidamente la batería y cargador → No apagar con el botón de encendido.
- Si el equipo es del IES: no instalar o desinstalar ningún programa no indicado o autorizado por los centros escolares, ni modificar ningún elemento o configuración del mismo.
- Si el equipo es del IES: comunicar incidencias y fallos del aparato.

2.4. Una ubicación y una postura adecuadas

Las familias pueden contribuir a seleccionar la mejor ubicación del ordenador en el hogar, y favorecer las condiciones para la correcta salud postural por parte del menor. Por ejemplo, en www.espalda.org se tiene información detallada.

Se recomienda lo siguiente:

- Colocar el ordenador en un espacio común de la casa (salón...), o en un lugar accesible a los adultos. Muchos de los riesgos de uso se evitan cuando se impide que los ordenadores estén en funcionamiento en los dormitorios o cuartos de los menores.
- Situarlo en una superficie plana y estable, sin vibraciones, limpia de productos químicos y de polvo que puedan filtrarse a su interior, y a ser posible no brillante (evitando las de cristal) y de color claro.
- Buscar posiciones y ubicaciones en las que la luz sea adecuada, evitando reflejos, alto contraste entre la pantalla y la oscuridad del ambiente, etc.
- La postura respecto al ordenador debe respetar estas pautas: los ojos deben estar situados enfrente y a una distancia de 45-80 centímetros (al menos el doble de la diagonal de la pantalla), situando la parte superior de la pantalla ligeramente por encima de la altura de los ojos, la espalda recta y reposada la zona lumbar sobre

el respaldo de la silla (y los glúteos completamente apoyados en la superficie de la silla), el ángulo de rodillas y codos de 90°.

- Es conveniente acostumbrar al menor a levantar la vista de la pantalla cada 15-20 minutos, fijándola en un punto alejado, y no permanecer en la misma postura de trabajo durante más de una hora (es preciso hacer pausas, estirar las piernas y espalda, etc.).

2.5. La propiedad intelectual

Otra importante contribución de las familias al buen uso de las TIC es su contribución a preservar la **propiedad intelectual** en el uso de contenidos digitales.

Las familias deben concienciar a los menores de que los materiales circulantes en la red, pese a las facilidades de acceso y difusión, no siempre son de uso libre.

Algunas plataformas de intercambio de archivos (denominadas redes “P2P”) incurrir en prácticas ilegales, al difundir contenidos (películas, canciones, programas, libros, etc.) sobre los que existen derechos de autor sin una autorización. Participar en esta práctica puede ser constitutivo de delito. Lo mismo sucede con algunos contenidos como fotografías, etc.

Algunos buscadores permiten filtrar los contenidos en función del tipo de licencia que tengan (de libre distribución o uso, por ejemplo), mientras que algunos materiales se difunden con licencia Creative Commons (cc), que autoriza el uso y explotación de la obra publicada en Internet bajo diferentes condiciones.

2.6. El consumo de tecnología

Un nuevo reto es **educar a los menores como consumidores de productos tecnológicos**.

Una importante contribución de las familias a la correcta relación del menor con las tecnologías emergentes tiene que ver con sus actitudes como “consumidor”.

- Existen multitud de servicios y programas gratuitos, que pueden sustituir exitosamente a los de pago.
- Las prestaciones de gran parte de las tecnologías que un menor adquiere en el mercado son muy superiores a sus necesidades reales como usuario. Un buen uso y el correcto mantenimiento de su ordenador/móvil y otros aparatos pueden proporcionar mejores prestaciones que máquinas nuevas.
- Aunque desde los centros educativos se promueve esta dimensión de la educación en valores, es importante que las familias -quienes tienen la última palabra en las decisiones respecto al consumo de los menores- colaboren, haciendo reflexionar al menor sobre la necesidad de racionalizar su relación con estas tecnologías, que

usan un marketing sofisticado y recurren a productos muy atractivos e indudablemente con excesivo prestigio entre los jóvenes.

3. Riesgos y medidas que las familias pueden adoptar

3.1. Protección de la intimidad

Las redes sociales están diseñadas para interconectar personas, compartiendo información, contactando en tiempo real (chat, videoconferencia, audioconferencia...) o facilitando la posibilidad de ponerse en conexión con otros usuarios (si aceptan establecer esta relación).

Las familias deben adoptar algunas normas básicas respecto al uso de las redes sociales, consensuadas con sus hijas e hijos: como preguntar periódicamente por los contactos aceptados, e informarse si se producen comunicaciones o solicitudes extrañas. Por regla general, un diálogo natural e inteligente respecto al uso de las redes -sin excluir hablar de sus peligros- es más eficaz que una posición de rechazo frontal. Las redes sociales son uno de los cauces más frecuentes de socialización, y bien usadas son beneficiosas para el menor (desarrollan la empatía, habilidades comunicativas, solidaridad, etc).

El uso de redes sociales **puede generar algunos problemas que podemos evitar**: en ocasiones, los usuarios de la red no son conscientes de que los datos que indican en su perfil (edad y fecha de cumpleaños, gustos, aficiones, etc.) van a estar a la vista de cualquier persona, e incluso constituyen un bien codiciado por agencias de marketing o personas que pueden aprovecharlos para usos ilícitos.

Un criterio básico en el uso de la red social es no facilitar en el perfil público datos personales que no comunicaríamos a un desconocido, como domicilio, teléfono, lugar de estudio, profesión de los padres, datos sociológicos, económicos, ideas y creencias políticas, religiosas o de cualquier tipo, fotos, información sobre gustos y aficiones, etc.

Algunas recomendaciones a la hora de participar en una red social son:

- Asegurarse de que la plataforma tenga una política de protección de datos y que ésta sea siempre visible (no sólo en el momento de darse de alta) y que se pueda imprimir o descargar.
- En caso de que se desee saber qué datos personales han sido almacenados (y, en su caso, borrarlos, modificarlos o actualizarlos), se puede solicitar ejercitar los derechos de Acceso, Rectificación, Cancelación Oposición (ARCO). Si la plataforma no responde a esa petición puede recurrir a denunciar la situación a la Agencia Española de Protección de Datos www.agpd.es
- También es denunciante ante la AEPD la recepción de publicidad o información no deseada, que pudiera tener su origen en los datos proporcionados a redes sociales sin autorización del usuario.

Es preciso considerar que muchos de los materiales (fotos y vídeos, fundamentalmente) alojados en una plataforma social tienen una alta posibilidad de

resultar accesibles desde distintas páginas web por millones de usuarios. Un usuario autorizado a acceder a nuestras imágenes o vídeos puede (con distintas intenciones) acabar difundirlo. Por eso, las redes sociales que se usen deben tener formas de denunciar la difusión de contenidos inadecuados.

Podremos exigir a sus administradores la eliminación de un contenido personal, un comentario o un texto que se esté difundiendo sin nuestra autorización.

En caso de la difusión no consentida de datos de menores, es posible recurrir ante las distintas instituciones para la defensa del menor, así como de los Cuerpos y Fuerzas de Seguridad del Estado.

Es necesario concienciar a nuestras hijas e hijos de las ventajas de las redes sociales, pero también de los posibles riesgos que generan:

- No deben usarse redes sociales que no se conozca o no ofrezcan garantías. No debe aceptarse nunca una invitación de una red que no se conozca, aunque provenga (aparentemente) de un usuario conocido. Es fácil informarse en Internet sobre cada una de las redes sociales, antes de afiliarse a ella.
- No debe indicarse en el perfil una edad que no corresponda con la real, porque puede provocar que adultos desconocidos entren en contacto con el menor. Tampoco puede suplantarse una identidad.
- El perfil creado debe configurarse para que sólo puedan verlo las personas a quien autorice el menor, no dejándolo en modalidad pública.
- Nunca deben admitirse a personas que no se conozcan (aunque aparentemente sean amigos/as de amigos/as a los que ya se han admitido).
- Hay que asegurarse, en todos los casos, que el perfil de la persona con la que voluntariamente contactamos corresponda con quien aparenta ser. Es fácil recurrir a todo tipo de engaños: fotos falsas, perfiles falsos, empleo de nombres falsos - incluyendo suplantación-, etc.
- Al igual que en la vida real, en la red no deben nunca emplearse insultos, amenazas, comentarios hirientes, etc. Internet es un espacio público. Muchos casos de ciberacoso comienzan por incidentes surgidos en el uso de redes sociales.
- No deben aceptarse archivos adjuntos de ningún tipo si no se conoce y autoriza a quien los remite. También es importante ignorar recomendaciones como la de visitar páginas web desconocidas, y aceptar juegos u otros programas (que, entre otros peligros, pueden vulnerar los derechos de propiedad intelectual). Deben rechazarse las páginas en las que se solicite registrarse, dar el número de la cuenta corriente, etc., sin la presencia de un adulto responsable.
- Ante cualquier contacto no deseado, comentario inadecuado o extraño, incitación a una cita presencial sospechosa, petición de fotos u otro material, solicitud de información personal, o cualquier injuria u ofensa, el/la menor o los adultos responsables deben bloquear a la persona de la que provienen, denunciarlo a la red social, y evitar responder a provocaciones.

3.2. Ciberacoso y grooming o acoso sexual

Se puede hablar de ciberacoso para referirse a actuaciones como vejaciones, insultos o chantaje mediante TIC.

Una de las formas más frecuentes es el ciberbullying, que consiste en difundir información con objeto de causar daño mediante correo electrónico, redes sociales, teléfonos móviles, etc., incluyendo la publicación de fotografías o vídeos en las páginas web de difusión de contenidos. El acosador y el acosado (que en muchas ocasiones no sabe cómo actuar) suelen ser compañeros/as de centro educativo, grupo social o vecindario, coincidiendo físicamente en la vida real con frecuencia, y teniendo edades similares. Es frecuente que situaciones de acoso en la vida real, o incidentes de convivencia, sean los desencadenantes de ciberbullying.

Si la situación de ciberbullying se mantiene a lo largo del tiempo: es algo más que un episodio aislado que, por sí mismo, puede ser constitutivo de delito.

Si las familias sospechan o detectan que esta situación se está produciendo, se debe actuar:

- Evitar que el menor siga manteniendo cualquier contacto o relación con el acosador.
- Pedir que la información generada vejatoria sea retirada del servidor de contenidos de Internet en la que se encuentra, y posteriormente de los índices de los contenidos de buscadores en los que aparezca.
- Denunciar la situación a las Fuerzas y Cuerpos de Seguridad del Estado. Es conveniente aportar pruebas gráficas del material vejatorio o calumnioso (correos, comentarios en foros, fotos, etc.) que el acosador haya generado.

Se habla de grooming para referirse a un acoso realizado por un adulto con pretensión de mantener un control emocional o un chantaje respecto a un menor, para provocar posteriormente situaciones de abuso. El contenido de dicho acoso explícita o implícitamente tiene un contenido sexual.

En todo el proceso el menor se ve poco a poco violentado, actuando contra su voluntad, sintiéndose aislado e incapaz de confiar lo sucedido a la familia o adultos responsables.

Este tipo de situaciones deben ser denunciadas. La Policía tiene una [Brigada Central de Investigación Tecnológica](#), encargada de este tipo de labores, como la persecución de amenazas, injurias y calumnias por correo electrónico, SMS, foros, web, etc., protección al menor en el uso de las nuevas tecnologías, pornografía infantil, piratería digital, estafas en Internet, virus, sustracción de datos, suplantación de seguridad, etc.

Un consejo práctico es que las familias visiten también esas mismas redes sociales. Esta práctica permitirá conocer las posibilidades y amenazas que las mismas tienen, y proporcionará una cercanía y empatía con los menores bajo su protección.

3.3. Contenidos no deseables

Muchas páginas de Internet presentan contenidos no deseables para los menores (como pornografía, incitación a la violencia, etc.). Evitar que un menor acceda a ellas no siempre es fácil. Por eso es conveniente en la medida de lo posible estar alerta cuando los menores naveguen libremente por Internet, aunque sea en busca de información académica.

- Muchos de los buscadores de páginas web tienen opciones de filtrado, que evitan la mayoría del contenido inapropiado. Por ejemplo, Google puede configurar su búsqueda (parte superior derecha de la pantalla). Esto permite habilitar en su modo estricto el Filtro SafeSearch, que evita páginas con contenido sexual explícito. Yahoo puede editar y activar el Filtro Adulto (menú Opciones / Preferencias). En todo caso, estas opciones no son infalibles.
- Hay algunos programas que bloquean o filtran el acceso a contenidos no deseados.
- Hay determinados programas de monitorización y registro de uso del ordenador.
- También hay configuraciones que permiten que el ordenador sólo pueda usarse en una determinada franja horaria. Windows, por ejemplo (Inicio/Panel de control) permite establecer las restricciones al uso del ordenador mediante la opción "Control parental".
- Los programas de filtrado de salida ayudan a proteger los datos que el usuario de un ordenador sube a Internet (por ejemplo datos personales, etc.) En todo caso, es conveniente que los adultos revisen el historial de navegación del menor con cierta frecuencia, comprobando qué páginas ha visitado, y para qué.

3.4. Virus, spam y otras amenazas

Un virus informático es un programa creado para realizar acciones en un ordenador ajeno o móvil ajeno sin consentimiento del propietario: dañar archivos, sistemas y otros programas. Es importante saber que **los virus también afectan a los móviles**.

Entre otras consecuencias, ralentizan el funcionamiento del ordenador y/o móvil, muestran sin consentimiento publicidad en forma de ventanas emergentes o popup; instalan complementos (barras de navegación...), abren determinadas páginas web...

Muchos de los virus están pensados específicamente para el correo electrónico, mandando mensajes a todas las personas/contactos que figuren en la libreta de direcciones, etc. Es frecuente también la difusión masiva de correos supuestamente de entidades como bancos, instituciones oficiales, etc., pidiendo datos personales como cuentas corrientes, DNI, etc.

Entre las medidas que las madres y padres pueden adoptar para evitarlos se encuentran:

- No aceptar la instalación de programas de procedencia dudosa o no solicitada. Muchos virus también se difunden a partir de los contenidos de las redes P2P, redes sociales, etc.

- No proporcionar la dirección de correo electrónico salvo que exista completa confianza en la red o persona que lo solicita.
- **Instalar y actualizar periódicamente el antivirus, tanto en el móvil como en el ordenador**, y escanear el ordenador y el móvil completamente, incluyendo periféricos como las memorias USB, CD, DVD, etc.
- No abrir archivos adjuntos desde el correo electrónico si proceden de personas que no son de confianza. Y, en cualquier caso, analizar con el antivirus cualquier archivo difundido por Internet antes de abrirlo. No abrir correos que contengan caracteres extraños o que recibamos varias veces desde distintas cuentas de usuarios.
- Tener precaución sobre las páginas web visitadas. Algunas están programadas para ejecutar aplicaciones en nuestro ordenador (normalmente, el navegador avisará de esta circunstancia, ante la cual no debemos autorizar esa operación). Las páginas de instituciones, entidades educativas, etc., son más seguras que las páginas particulares y las de extensión .com.

Algunos virus, por ejemplo, pueden captar las teclas que el usuario pulsa en el teclado para obtener contraseñas o hacer un seguimiento de las páginas web visitadas por el usuario (por ejemplo, con fines comerciales, o para conocer los gustos del mismo, pero también para obtener las contraseñas del banco y/o aplicaciones bancarias).

4. Algunas herramientas y recursos digitales...

Internet pone a nuestro alcance un amplio abanico de **posibilidades de aprendizaje y comunicación**.

Muchos otros programas permiten al alumnado realizar otras actividades educativas: por ejemplo, crear radios escolares (mediante la tecnología del podcast), mapas de conceptos que se generan directamente en Internet, libros electrónicos en la red, vídeos (uno de los servicios de Internet más populares es Youtube, donde los usuarios pueden alojar sus producciones, algunas con orientación académica y gran calidad), ejes cronológicos, mapas creados por el usuario, mapas de etiquetas describiendo los lugares señalados, pósters multimedia en Internet, periódicos de elaboración propia online, y un larguísimo etcétera.

- **Correo electrónico** (con numerosos servidores gratuitos como Hotmail, Gmail, Eudora, etc.).
- **Chat** (comunicación en tiempo real, que luego puede ser archivada para volver a consultarla).
- **Foros** (sistemas de preguntas y respuestas, abierto a la colaboración de usuarios anónimos o registrados, según las configuraciones).
- **Herramientas colaborativas** para el intercambio o generación conjunta de documentos de todo tipo (como Google Docs), etc.

- Algunos servicios permiten conocer casi en tiempo real las novedades anunciadas por páginas web (servicios RSS).
- Las **redes sociales** integran estos servicios, y otros (perfil del usuario, servicio de búsqueda y agregación de amigos, etc.).

Cuando el usuario, además de obtener información de Internet, puede alojar sus aportaciones en forma de opiniones, fotos o archivos de otros tipos, y, en definitiva, interactuar con la red, se habla de herramientas de segunda generación, o web 2.0:

- **Blogs** (Blogger, WordPress...), páginas con estructura de artículos periodísticos abiertos en su caso a la colaboración u opinión de otros usuarios.
- Las **wikis** son colecciones de artículos realizadas cooperativamente por parte de usuarios, con una estructura de vínculos entre unas y otras (la más conocida es Wikipedia, aunque cualquier usuario puede crear su propio sitio wiki mediante servidores como Wikia, etc.).

5. Nuevas formas y métodos de aprendizaje

Los métodos de enseñanza de la Escuela Digital se basan en que el alumnado aprende de manera más autónoma (guiado por el/la docente), siendo capaz de buscar, filtrar, interpretar y comunicar la información, en entornos de cooperación con sus iguales y valiéndose de las oportunidades que proporcionan las nuevas tecnologías.

Todas estas herramientas y recursos didácticos educativos constituyen la oportunidad de un aprendizaje más motivador y eficaz (por la integración de distintas fuentes de información, incluidas las multimedia e interactivas), que pretende lograr una educación de calidad, más comprometida con las necesidades de la Sociedad del Conocimiento.

Uno de los ejes sobre los que gravita el sistema educativo en la actualidad es la adquisición de competencia digital, esto es, los conocimientos, habilidades y capacidades, en conjunción con valores y actitudes, para utilizar de manera eficaz y eficiente en todas las áreas de conocimiento los instrumentos y recursos tecnológicos.

6. Enlaces de interés

- [Recursos para padres y madres](#) Página web del Instituto de Tecnologías de la Educación, dependiente del Ministerio de Educación.
- [EDUCARED](#) Página web de la Fundación Telefónica con numerosos artículos, recursos, consejos, programas y recursos relacionados con el aprendizaje escolar a partir de nuevas tecnologías.
- [SAFEKIDS](#) Consejos y recursos sobre seguridad en la Red.

7. Agradecimientos

Esta guía es una modificación/adaptación a nuestro Centro de las guías de buenas prácticas del IES Paterna y de la [Junta de Castilla la Mancha](#), a quienes agradecemos sus contenidos e ideas.