
GUÍA PARA UN USO RESPONSABLE DE LAS TECNOLOGÍAS DIGITALES EN EL ÁMBITO EDUCATIVO

ÍNDICE:

1. Introducción y justificación.

Vivimos en una sociedad cada vez más conectada en la que Internet y las redes sociales adquieren mayor protagonismo, con una tecnología cada vez más asequible y que sigue evolucionando.

Las Tecnologías de la Información y la Comunicación (TIC) constituyen un elemento clave de nuestro modelo educativo No en vano, muchos han sido los esfuerzos por implantar un modelo educativo que tuviera presente el uso de estas herramientas, tanto en el aula como fuera de ella.

La sociedad actual no podría entenderse sin la presencia de las nuevas tecnologías. Por ello, en las últimas décadas, se está consolidando una educación 3.0 frente al modelo educativo tradicional con la incorporación en las aulas de proyectores, plataformas virtuales y un buen número de materiales didácticos (juegos interactivos o vídeos), lo que permite a los alumnos aprender los conocimientos de una manera muy diferente a la tradicional.

Las Tecnologías de la Información y la Comunicación (TIC) constituyen un elemento clave de nuestro modelo educativo. Nos hemos esforzado mucho por implantar un modelo educativo que tuviera presente el uso de estas herramientas, tanto en el aula como fuera de ella.

A pesar de lo extendidas que están, se echan en falta recursos que faciliten el conocimiento para un uso responsable y seguro, que debe primar cuando hablamos de personas menores de edad.

En este camino hacia la enseñanza digital no nos podemos olvidar de garantizar la salud física, mental y emocional de nuestro alumnado en su interacción con la red y los dispositivos electrónicos.

Esta guía es un instrumento de referencia práctico, dirigido a padres, madres, alumnos, profesionales de la enseñanza. También pretende prevenir conflictos a corto o largo plazo, así como indicar determinadas actuaciones que deben tenerse en cuenta cuando el problema ya se ha desarrollado.

Pero en este ascenso hacia la enseñanza digital no nos podemos olvidar de garantizar la salud física, mental y emocional de nuestro alumnado en su interacción con la red y los dispositivos electrónicos.

2. Objetivos.

- Asegurar que los alumnos del centro se benefician de las ventajas del uso de las TIC y las TAC (Tecnologías del Aprendizaje y Conocimiento) en la educación de forma efectiva y segura.

- Formar e informar sobre métodos de autoprotección y protección de otros en la red.

- Evitar el mal uso de las TIC y la TAC de forma intencionada o por desinformación.

- Ofrecer un marco ético y proponer buenas prácticas para favorecer un uso correcto de las tecnologías digitales.

- Aportar este recurso para conocer, sensibilizar, implicar y facilitar el uso responsable de las TIC

3. 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.

3.1 Profesionales de la enseñanza

Nuestra función como docentes consiste en enseñar con ordenadores desde una perspectiva constructivista. Esto significa plantear problemas para que los propios alumnos articulen planes de trabajo y desarrollen las acciones necesarias con las tecnologías para construir y obtener respuestas satisfactorias a los mismos de forma que aprendan a expresarse y comunicarse a través de las distintas modalidades y recursos tecnológicos.
El papel del docente en el aula debe ser más un organizador y supervisor de actividades de aprendizaje que los alumnos realizan con tecnologías, más que un transmisor de información elaborada.

Otra de nuestra labor como docente es:

√ Controlar el tiempo que se conectan a internet en clase.
√ Colaborar en el mantenimiento de todos los dispositivos tecnológicos del aula.
√ Fomentar la utilización de una posición correcta para el cuerpo frente al ordenador.
√ Fomentar el respeto a otros usuarios, evitando las burlas, difamaciones y agresiones.
√ Enseñar a navegar por internet de forma segura, accediendo solo a contenidos aptos para su edad.

- √ 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.
- √ 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.
- √ 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.
- √ 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.

3.2 Alumnado

Una de las metas relevantes del aprendizaje escolar consiste en ayudar al alumnado a reconstruir y dar significado a la multitud de información que obtiene extraescolarmente en los múltiples medios de comunicación de la sociedad del siglo XXI y desarrollar las competencias para utilizar de forma inteligente, crítica y ética la información.

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

- √ Controlar el tiempo de uso a los dispositivos, ya sea al ordenador, a la tablet, al móvil o a cualquier otro dispositivo similar.
- √ Cuidar su correcta posición corporal al usar cualquiera de estos dispositivos, sentándose correctamente.
- √ Ser prudentes y no concertar encuentros con personas que no conocen y que les proponen quedar a solas.
- √ Tener respeto a otros usuarios, evitando las burlas, difamaciones, humillaciones y agresiones.
- √ No suplantar la identidad de nadie en la red.
- √ Aprender a navegar por internet de forma segura, accediendo solo a contenidos aptos para su edad.
- √ 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.

- √ Entender que no se puede publicar información de otra persona sin su consentimiento. Siempre es aconsejable evitar publicar detalles o imágenes privadas.
- √ 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.
- √ Cuidar el mantenimiento de los dispositivos que utilizan, evitando derramar comida o líquidos sobre ellos.

3.3 Familia

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

√ 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.

√ 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.

√ 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.

√ 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.

√ 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.

√ 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.

√ Tener el ordenador en una zona de uso común, ya que facilitará tanto la supervisión del tiempo de utilización como las situaciones que puedan resultar incómodas para el menor, así como la revisión de las webs que visita. Buscar una ubicación en la que la luz sea la adecuada, evitando reflejos.

√ Enseñarles en qué consiste la privacidad, que los datos personales son información sensible y que pueden ser utilizados en su contra.

√ 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.

√ 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. Prácticas para un uso responsable de las TIC.

A continuación, te proponemos 7 buenas prácticas para el uso responsable y seguro de internet en los colegios con el fin de ayudar a que los alumnos utilicen internet sin asumir riesgos innecesarios.

1. Mantener actualizados los equipos del colegio.
2. Aprender a tener un horario de uso de internet.
3. No dar datos personales a desconocidos.
4. Asegurar las cuentas en los dispositivos y en las redes sociales (poner contraseñas seguras a nuestros dispositivos y cuentas).
5. Enseñar un uso responsable del correo electrónico.
6. Hablar con claridad sobre los peligros de la Red.
7. Informar sobre los derechos de propiedad intelectual.

5. Normas de uso de las tecnologías en el centro

- **Normas que quedan recogidas en la agenda escolar del Centro:**

  o No traer al colegio dispositivos móviles, smartwatch, cualquier dispositivo electrónico que no esté permitido. El colegio no se hace responsable de su pérdida.

  o Uso o sonido del móvil dentro del Colegio (y aún más grave la grabación de imágenes) y /o utilización de smartwatch o cualquier aparato electrónico que no este permitido dentro del colegio o en actividades complementarias o extraescolares organizadas por el centro. Se considera uso el participar activa o pasivamente en cualquier actividad no académica en la que esté involucrado el dispositivo, incluido posar en fotos o vídeos. Esta totalmente prohibido colgar en Internet imágenes realizadas en el colegio y/o su difusión a través de cualquier red social y es más grave aún si resultan degradantes u ofensivas para otros miembros de la comunidad educativa. EN CASO DE PERDIDA DEL MOVIL, EL COLEGIO NO SE HACE RESPONSABLE.

- Los recursos informáticos tienen como "finalidad servir de apoyo a la docencia "y por tanto deben emplearse para el trabajo y el estudio, no con otros fines

- El centro promoverá el uso de herramientas para aplicaciones, páginas... que necesiten registro por parte de los/as alumnos/as a través de ClassRoom.

- Debemos ser responsables y cuidadosos/as con los dispositivos que se tienen en el centro, tanto el profesorado como el alumnado y, por tanto, no se modificarán los programas existentes. Si hubiera que hacerlo o poner nuevas aplicaciones, programas... existe la figura del coordinador TIC.

- El profesorado del centro informará a los alumnos y alumnas sobre el uso adecuado de las herramientas o apps usadas.

- Sólo se podrán utilizar dispositivos autorizados por el centro.

- El profesorado del centro supervisará las actividades que precisan el uso de Internet.

- Respecto a la seguridad: no hay que compartir con nadie ningún dato: contraseñas, claves, acceso.

- El centro proporcionará formación sobre los peligros de la red, cómo evitarlos y promover un uso seguro de las TIC y las TAC.

- Cualquier persona de la comunidad educativa que encuentre material inapropiado en los dispositivos del centro, o durante una actividad, deberá comunicarlo inmediatamente para corregirlo.

- El centro pedirá autorización a las familias para la publicación, con fines educativos, de imágenes de los estudiantes.

- El centro no se responsabiliza de los materiales compartidos por terceros, ni del contenido accesible desde los vínculos que divulguen.

- Con objeto de respetar el buen uso de las redes, el centro educativo se reserva el derecho de eliminar cualquier aportación que contravenga los principios aquí expuestos.

COMUNICACIONES

- Comunicaciones del profesorado con el alumnado, en caso de disponer de un correo electrónico éste se utilizará exclusivamente para la actividad educativa. Las familias serán conocedoras del correo que usan los estudiantes para la actividad escolar y así poder supervisarlo.

- Las alumnas y alumnos harán comunicaciones mediante correo electrónico o redes sociales exclusivamente con fines educativos.

- Los estudiantes podrán en práctica las siguientes normas:

  - Mostrar respeto por uno mismo y todas las personas de la comunidad escolar.
  - Proteger la propia identidad y la de otras personas.
  - Respetar y proteger la propiedad intelectual.

- Se podrán emplear servicios en la nube para entregar las actividades, como Dropbox, Google Drive o similares.

- Cualquier persona de la comunidad educativa que se percate de un uso inadecuado de las comunicaciones deberá comunicarlo inmediatamente para tomar las medidas oportunas.

6. Medios, recursos humanos y materiales en caso de detección de conductas de acoso en red

Definición de acoso en red: Conducta hostil de uno o varios hacia otra persona, de forma sistemática, afectando a todos los niveles de la vida del acosado e incluso a su círculo más próximo. Se produce cuando hay un desequilibrio de poder entre acosador y acosado. En este apartado se aborda un listado de problemas que quizás sean los que más preocupación despiertan entre los docentes y entre los padres. Los peligros de la violación de la privacidad son, los siguientes entre otros:

- Ciberacoso o ciberbullying.
- Acceso a cuentas de correo, perfiles de redes sociales, etc.
- Estafa.
- Ciberdelitos.
- Spam.
- Malware o programas maliciosos que se instalan en el equipo y recogen datos de forma opaca.
- Suplantación de la identidad en redes sociales.

A continuación, vamos a definir el de mayor relevancia para el contexto escolar.

6.1 CIBERBULLYING

¿Qué es?

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

Tipos de ciberacoso:

- ciberbullying: acoso entre alumnos/as
- ciberbaiting: acoso de alumnos a un profesor/a
- grooming: acoso de un adulto a un menor

¿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.

6.2. 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 correos 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 online, 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.
- Advertirlessobrelatransmisióndevirusatravésdelcorreoelectrónico, especialmente mediante archivos adjuntos que deben analizar con un programa antivirus antes de su descarga.

¿Qué hacer?

- Informar o denunciar el caso.