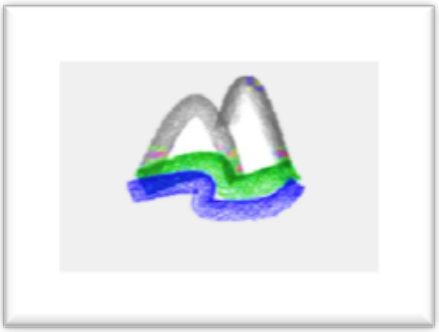
JUNTA DE ANDALUCIA
CONSEJERÍA DE EDUCACIÓN

I.E.S. "VALLE DEL GENAL"

# GUÍA PARA EL USO RESPONSABLE DE LAS TIC Y LAS TAC



## CURSO 2022 – 23

### 1. Contexto

La introducción de las TIC (Tecnologías de la Información y la Comunicación) y las TAC (Tecnologías del Aprendizaje y el Conocimiento) en el aula es una realidad tal, que hoy día no nos imaginamos una clase sin el uso de herramientas webs o apps.

Este rápido cambio en la educación es debido al interés del profesorado por innovar en su práctica docente, así como el entusiasmo del alumnado al poder utilizar en el aula estas herramientas.

Son muchos los beneficios que aportan las nuevas tecnologías a los procesos de enseñanza y aprendizaje; información actualizada y de fácil acceso, creación de contenidos, trabajo cooperativo... pero a la vez, la rápida evolución de todo este proceso y de las herramientas en sí mismas puede traer también problemas a la convivencia en el aula.

Como en casi todos los aspectos de la vida, la prevención es el mejor medio para evitar situaciones indeseables. Una formación específica, por parte de profesorado y alumnado, en Competencia Digital se hace necesaria. Tomando como base el Marco Común de Competencia Digital Docente, podemos concretar esta formación en:

- Área 1 (Información y alfabetización informacional)
- Área 2 (Comunicación y colaboración)
- Área 3 (Seguridad).

También se hace necesaria la regulación del uso de estas herramientas, apps e Internet en general en el centro mediante la presente guía para el uso responsable de las TIC y las TAC en el centro.

## 2. Objetivos

1. Asegurar que los alumnos del centro se beneficien de las ventajas del uso de las TIC y las TAC en la educación de forma efectiva y segura.
2. Formar e informar sobre métodos de autoprotección y protección de otros en la red.
3. Evitar el mal uso de las TIC y la TAC de forma intencionada o por desinformación.
4. Ayudar a las familias con pautas claras sobre su actuación ante el uso de TIC.

## 3. Normas de uso de la tecnología en el centro

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.

1. El centro promoverá el uso de herramientas que no necesiten el registro por parte del alumnado.
2. Debemos ser responsables y cuidadosos 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/a TDE que debe ser informado en todo caso.
3. El profesorado del centro informará al alumnado sobre el uso adecuado de las herramientas o apps usadas.
4. Sólo se podrán utilizar dispositivos cuando el profesorado lo autorice, ya sean los propios del alumnado como los que existen en el centro para su uso.
5. El profesorado del centro supervisará las actividades que precisan el uso de Internet y de dispositivos tecnológicos.
6. No compartir con nadie ningún dato: contraseñas, claves, acceso… Es conveniente que las claves no sean más cortas de 8 caracteres, que no sean DNI, fecha de nacimiento y se deberían cambiar con frecuencia.
7. Aunque no se puede garantizar que el alumnado no vaya a encontrar algún contenido inapropiado en la web, el centro analizará las páginas web, herramientas o apps utilizadas para la docencia, minimizando este riesgo en lo posible. En todo caso el alumnado no hará uso de este contenido y lo comunicará al profesorado que en ese momento se encuentre en el aula.

8. El centro proporcionará formación sobre los peligros de la red, cómo evitarlos y promover un uso seguro de las TIC y las TAC.
9. El centro podrá comprobar, en caso de que sea necesario, los archivos guardados, descargados, histórico de la web y cualquier otro elemento como resultado del uso de Internet.
10. Cualquier persona de la comunidad educativa que encuentre material inapropiado en los dispositivos del centro, o durante una actividad, deberá comunicarlo inmediatamente para corregirlo al coordinador/a TDE o a algún miembro del equipo directivo.
11. El centro pedirá autorización a las familias para la publicación, con fines educativos, de imágenes y videos de los estudiantes en la web y en las redes sociales del centro.
12. Tanto profesorado como alumnado trabajarán con la cuenta personal que el centro le asignará a cada uno dentro de la plataforma Google Suite para Centros Educativos. También solicitará el consentimiento de la familia para el uso de las herramientas alojadas en dicha plataforma.
13. El centro no se responsabiliza de los materiales compartidos por terceros, ni del contenido accesible desde los vínculos que divulguen.
14. El alumnado no accederá a cuentas de correo que no sean propias, y se abstendrán de interceptar, leer, borrar, copiar o modificar el correo electrónico dirigido a otras personas. Si encuentra alguna cuenta de correo abierta en algún dispositivo de uso compartido en el centro, la cerrará inmediatamente y se lo comunicará al profesorado con el que se encuentre en ese momento.
15. El alumnado y profesorado no accederán a mensajes de correo electrónico sospechosos de tener propósito dañino o malicioso durante el uso de los dispositivos compartidos del centro.
16. 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.

## 4. Comunicaciones

1. Las comunicaciones entre profesorado y alumnado, haciendo uso de las herramientas G-suite, serán únicamente con fines educativos.
2. Las familias serán conocedoras del correo que usan los estudiantes para la actividad escolar y así poder supervisarlo. Será el propio alumnado quien comparta las claves con su padre, madre o tutores legales.
3. Se podrán emplear servicios en la nube para entregar las actividades (Drive, Classroom,..)
4. Se hará uso de Google Meet para la realización de videoconferencias entre profesorado y alumnado en el caso que sea necesario.

5. El profesorado educará al alumnado en conductas de protección y autoprotección para tener unas comunicaciones efectivas y seguras en la red.
6. Los estudiantes pondrán en práctica las normas de netiqueta.
   - 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.

   Más información en http://www.netiquetate.com/
7. Cualquier persona de la comunidad educativa que se percate de un uso inadecuado de las comunicaciones deberá comunicarlo inmediatamente para tomar las medidas oportunas a la coordinadora TDE o a algún miembro del equipo docente.

## 5. Normas de uso de los dispositivos personales en el centro educativo.

1. Traer dispositivos personales al centro por parte del alumnado nunca será obligatorio. Para el caso de comunicaciones entre familias, alumnado siempre se puede hacer uso del teléfono del centro.
2. El uso de dispositivos personales en el centro será permitido exclusivamente con fines educativos siempre que el profesorado lo permita.
3. El uso de dispositivos personales en el centro se hará bajo la supervisión del profesorado.
4. Cuando se requiera el uso de dispositivos personales por parte del alumnado nunca será de forma obligatoria y el profesor/a responsable se asegurará de que todo el alumnado dispone de estos recursos y no se producen discriminaciones en este sentido.
5. Cuando el profesorado autorice o requiera el uso de dispositivos personales será el propio alumnado el responsable de su puesta a punto (batería, actualizaciones, aplicaciones requeridas…) así como de su custodia.
6. En ningún caso está permitido la grabación de vídeo, voz y la realización de fotos sin el conocimiento ni la autorización de la persona grabada. Queda totalmente prohibida por parte del alumnado, la difusión de dicho material, aun teniendo la autorización para su grabación.
7. El centro no se hace responsable, en ningún caso, de pérdida, robo o rotura de los dispositivos personales del alumnado, aunque hayan sido requeridos por el profesorado para la realización de alguna actividad educativa.
8. Se utilizarán sólo las aplicaciones móviles que exclusivamente pida el profesorado, y sólo se utilizarán en el momento de la actividad. El resto del tiempo el dispositivo permanecerá apagado y guardado.
9. La conexión a Internet a través de datos móviles está prohibida (ya que excede el control que desde el centro podemos ejercer sobre los lugares visitados y aplicaciones utilizadas), la conexión se realizará siempre a través de la Wifi del centro.

10. El profesorado dinamizará la utilización de herramientas y aplicaciones digitales a las que el alumnado accederá mediante el uso de sus propios dispositivos.
11. En el caso de que se vayan a usar programas que necesiten sonido, el alumnado traerá sus propios auriculares

## 6. Normas de uso de las redes sociales en el centro educativo.

1. Los alumnos no pueden sacar fotos ni videos de otros alumnos o alumnas ni del personal docente o no docente, ni hacerlos circular, publicarlos o difundirlos por ningún medio a no ser que cuente con el permiso de la persona (mayores de edad) o de padre/madre/tutor legal (menores).
2. Familias, alumnado y profesorado del centro harán uso de las redes sociales teniendo en cuenta la normativa de convivencia del centro. Siempre publicando y comentando en ellas con el máximo respeto y cuidado hacia todas las personas que integran la comunidad educativa.
3. Tanto el alumnado como profesorado y familias tienen la responsabilidad de poner en conocimiento del centro cualquier publicación que observen en las redes sociales que pueda perjudicar la imagen del centro o la de las personas que lo integran.
4. Además de utilizar los canales oficiales de comunicación, El Equipo Directivo y el profesorado intentarán hacer uso de las redes sociales y la web del centro como medio para difundir sus actividades habituales y para publicar información relevante.
5. Mediante el uso de la cuenta del centro se facilitará al profesorado enlaces a documentos (textos, videos, infografías…) que faciliten su formación.
6. Todas las familias firmarán un documento vía Pasen en el que den su consentimiento o su negativa a que sus hijos/as aparezcan en las publicaciones del centro tanto en la web como en las redes sociales y siempre con fines educativos.
7. No se permite la participación del alumnado en chats o espacios de características similares, excepto cuando se trate de una actividad de contenido educativo que cuente con la aprobación de un docente.

## 7. Sanciones

1. El mal uso de Internet o incumplimiento de la normativa puede conllevar sanciones disciplinarias recogidas en el ROF del Centro e incluso la retirada del acceso a Internet de forma temporal o definitiva.
2. El maltrato de los dispositivos tecnológicos disponibles en el centro así como de accesorios, cables, cargadores, teclados, ratón, etc. pueden conllevar sanciones disciplinarias y el pago de los desperfectos ocasionados.
3. El centro podrá informar a las autoridades competentes de cualquier actividad ilegal detectada o situaciones que afecten a la integridad de una persona.

4. El centro informará a las familias ante cualquier acto de los reseñados anteriormente.

## 8. Puesto educativo en el hogar

La Consejería de Educación y Deporte ha suscrito con el Ministerio de Educación y Formación Profesional y con Red.es, entidad pública adscrita al Ministerio de Asuntos Económicos y Transformación Digital, el convenio “Educa en Digital” cuyo objetivo es emprender actuaciones para apoyar la transformación digital del sistema educativo mediante la dotación de dispositivos y de otros recursos educativos digitales, la adecuación de las competencias digitales del personal docente y la aplicación de la inteligencia artificial a la educación personalizada.
Entre las actuaciones de dotación establecidas en Educa en Digital, el “Puesto educativo en el hogar” (PEH) consiste en la entrega a los centros docentes andaluces de equipos informáticos, susceptibles de ser prestados al alumnado en situación de vulnerabilidad. El PEH está destinado de forma prioritaria a alumnado en situación de vulnerabilidad digital, es decir, aquel que tiene dificultades en el acceso a Internet y/o no dispone de un equipamiento tecnológico que le permita acceder a los recursos educativos digitales.

Tanto el alumnado como su familia al que se le hace el préstamo de un PEH se comprometen a:

1. La devolución del equipamiento en la fecha establecida, en el centro de origen según protocolo que el centro elabore para ello, procediendo a registrar la devolución y el estado del equipo, teniendo como plazo máximo el 30 de junio o hasta que se produzca un traslado de centro durante este curso escolar.
2. Comunicar cualquier incidencia a la persona encargada de la coordinación #TDE para su gestión.
3. Si la incidencia es por pérdida o sustracción del dispositivo deberá notificarse de inmediato a la persona que ejerza las funciones de dirección en su centro educativo.
4. En general, hacer un uso correcto del equipamiento; en caso contrario, cualquier deterioro deberá ser reparado a su cargo, debiendo reintegrar un equipo nuevo en caso de un desperfecto que lo haga inutilizable.
5. No realizar ninguna modificación de hardware o software en el dispositivo (incluido Sistema Operativo).
6. Reintegrar el equipo limpio de contenidos propios.
7. Utilizar el dispositivo únicamente para fines profesionales.
8. No conectar el dispositivo a redes abiertas o que no sean de confianza.
9. No almacenar datos de carácter personal. En caso de ser necesario, la información deberá estar encriptada.
10. No usar la opción "guardar contraseñas" de los navegadores para las credenciales de acceso a aplicaciones educativas de uso por el centro, como por ejemplo Moodle Centros.

11. Adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso por parte de personas no autorizadas.

## 9. Pautas intervención familias

En los últimos tiempos y tras la pandemia mundial que estamos sufriendo, se ha visto claramente que las tecnologías de la información han venido a quedarse. Por las necesidades impuestas, tanto en lo laboral como en lo educativo y para el tiempo de ocio, se está haciendo uso de estas herramientas de una manera más generalizada que antes del confinamiento, en toda la sociedad. Tanto los padres como sus hijos e hijas están aprendiendo a utilizar nuevas herramientas, como son videoconferencias (Meet, Zoom, Skype,...), videollamadas (WhatsApp), tanto por las responsabilidades laborales, escolares o por ocio. El recurso de las TIC normalmente tiene los siguientes objetivos: trabajo, aprendizaje y formación, relaciones sociales y tiempo de ocio. Dependiendo del uso que se haga de ellas habrá beneficios o perjuicios, por lo que se debe hacer un uso responsable y conocer algunos de los efectos perjudiciales que pueden tener. El estilo educativo familiar, junto al uso que los adultos hacen de las TIC (modelo de conducta), condicionará el manejo adecuado o inadecuado de las mismas por parte de sus hijos/as.

A. Recomendaciones para un uso responsable en familia

1. Las pantallas no son “niñeras/os”. Evitar que, en caso de niños de menor edad, se les dé un uso prolongado con la única finalidad de tenerlos entretenidos.

2. Intercalar las TIC con otros tipos de actividades (juegos de mesa, juegos tradicionales,....)

3. Los niños/as menores deben estar acompañados e interactuando con los adultos mientras las usan. 4. Fomentar unos buenos hábitos de consumo, acordando en la familia unas normas sobre su uso: límite de tiempo y espacios; aprender a utilizar adecuadamente los dispositivos, respetar la intimidad de los otros -en caso de compartir pantallas-.

5. No deben reemplazar -en lo posible- otras interacciones personales y presenciales, como salidas y encuentros con amigos, familia, etc.

6. Preservar algún lugar y momentos libre de tecnología (para niños y adultos) que facilite la “desconexión” y permita la convivencia y comunicación entre los miembros de la unidad familiar. Acordar y respetar momentos en familia sin uso de las TIC, como por ejemplo durante las comidas. 7. Permitirse tiempos de “aburrimiento”, que faciliten la relajación y disfrutar de los propios pensamientos o sensaciones, apreciar el valor del silencio, sonidos de la naturaleza, música, etc.

8. Compórtate como en la vida real: “Orientaciones prácticas para la convivencia digital” (elaborado por el EOEP de Convivencia Escolar de Murcia).

B. Indicadores de riesgo de un mal uso de las TIC.

1. Horario excesivo en la utilización de estas tecnologías o problemas a la hora de cumplir los horarios establecidos.

2. Dependencia de algún dispositivo concreto (móvil, videoconsola, tablet,...).

3. Dependencia de las redes sociales.

4. Las TIC se convierten en la única manera que tiene la familia para regular la conducta del niño/a (cuando están cansados, en las salidas, control de rabietas...).

5. Es el único elemento de ocio de los menores.

6. Cuando se utilizan como una forma de evitar el contacto social y personal, por tener dificultades o escasas habilidades sociales y/o comunicativas.

7. Sirve para todo: castigar, chantajear, recompensar, consolar, comprar conducta, "respiro familiar"….

8. Riesgo de acoso entre compañeros (ciberbullying).

9. Envío inadecuado de mensajes, fotografías o vídeos de carácter sexual a través de Internet (sexting).

10. Posible malestar generado en los menores por situaciones de chantaje de tipo sexual (sextorsión), donde el extorsionador chantajea a la víctima con contenido privado del usuario, normalmente fotos o vídeos sexualmente explícitos.

11. Riesgo de acoso sexual a menores en la red (grooming) por acciones y estrategias que lleva a cabo un adulto para ganarse la confianza de un menor, a través de Internet, con el objetivo de conseguir favores de índole sexual.

C. Consejos para padres sobre el sexting, la sextorsión y el grooming.

1. Habla con tu hijo/a sobre la gran difusión que pueden tener los archivos en Internet.

2. Hazle entender que tener permiso para sacar o recibir una foto de alguien para uso privado no quiere decir que tenga permiso para difundirla.

3. Explica que aunque mande los archivos a un amigo o pareja de forma privada, terceras personas se pueden hacer con ellas con fines nocivos.

4. Haz conocer a tu hijo/a los métodos que usan los delincuentes para acceder a los archivos privados.

5. Rastrea el ordenador en búsqueda de software malicioso y elimínalo.

6. Si crees que tu hijo/a puede estar sufriendo chantaje, usa el diálogo y la comprensión. Es un tema serio que debe ser tratado.

7. Si tu hijo/a sufre sextorsión o grooming guarda todas las pruebas del chantaje y denuncia.

8. Coloca el ordenador en un lugar común o al que puedas acceder fácilmente a dar un vistazo. Dale privacidad pero ten la capacidad de saber qué está haciendo.

9. Restringe el uso de la webcam y tápela cuando no esté en uso. Los malwares pueden acceder a ella.

10. Asegúrate de que usa un sobrenombre en la red.

11. Conoce a sus amigos, y si es posible a sus contactos del teléfono.

12. Busca ayuda, y si es necesario denunciar ante las Fuerzas y Cuerpos de Seguridad del Estado. https://www.volvamosmascercanos.com/wp-content/uploads/2020/09/5.5.3.8-TIC_uso-responsable-enFamilia.pdf

D. Recursos para el “buen uso” o “abuso de las TIC”.

En caso de tener problemas con tus hijos en el uso de nuevas tecnologías, existen los siguientes recursos de ayuda:

1. Internet Segura for Kids www.is4k.es

2. INCIBE: Instituto Nacional de Ciberseguridad de España https://www.incibe.es Página web dirigida a menores, jóvenes, familias, educadores y profesionales del ámbito del menor con el objetivo de sensibilizar y formar a éstos, ofrecer un servicio de línea de ayuda para hacer frente a los riesgos de Internet: contenidos perjudiciales, contactos dañinos y conductas inapropiadas. Además de reducir la disponibilidad de contenido criminal, dando soporte a las Fuerzas de Seguridad del Estado.

3. Oficina de Seguridad del Internauta (OSI) https://www.osi.es/es En la Oficina de Seguridad del Internauta (OSI) de INCIBE proporcionamos la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.

4. Teléfono 017 centraliza los servicios de atención telefónica que ofrece INCIBE (Instituto Nacional de Seguridad). Atiende varios tipos de consultas: − Ciudadanos: la protección de dispositivos, conexiones, privacidad, tipos de fraudes e infecciones por virus y programas maliciosos. − Entorno del menor: los padres y educadores recibirán asesoramiento psicosocial, técnico y legal sobre situaciones de riesgo y conflictos de los menores en Internet, en temas como uso excesivo de pantallas, redes sociales y videojuegos;

ciberacoso; comunidades peligrosas; mediación y control parental y privacidad y reputación online, entre otros.

E. Control parental

Definición de control parental:

− Es un software que permite crear filtros y restricciones para controlar el acceso a determinados contenidos no acordes a su edad.

− Los dos sistemas operativos móviles más universales son Android y iOS (Apple) y ambos incluyen funcionalidades restrictivas en su sistema, sin necesidad de instalar aplicaciones adicionales.

− Las restricciones funcionan estableciendo contraseñas que limitan el acceso a las aplicaciones o contenido que los padres decidan, una vez que se activan, solo la contraseña puede eliminarlas.

− Con el control parental también podemos administrar las horas de uso y disfrute de los móviles y otros dispositivos, estableciendo horarios de manera automática y bloqueando el dispositivo cuando las horas determinadas se hayan agotado.

1. Para aplicar el control parental en un dispositivo iOS (iPhone, iPad, iPod touch) puede hacerlo siguiendo las instrucciones de esta página web: a. https://support.apple.com/es-es/HT201304

2. Para aplicar el control parental de un dispositivo Android puede hacerlo instalando alguna de las siguientes aplicaciones, disponibles en la Play Store (tienda de aplicaciones móviles de Android)

a. QUSTODIO: https://www.qustodio.com/es

b. SECUREKIDS: https://securekids.es