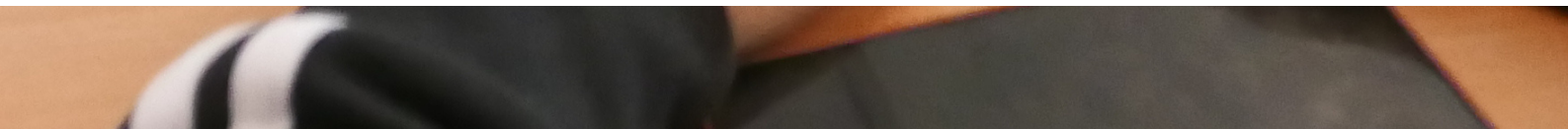
Guía para uso responsable de las TICS

Curso 2022-2023

Los Viveros
CENTRO PÚBLICO INTEGRADO DE FORMACIÓN PROFESIONAL



1. Introducción

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 y en constante evolución.

Las orientaciones de la UE relativa a la educación insisten en el desarrollo de un aprendizaje competencial que facilite la formación integral de la persona, acorde con la realidad rápidamente cambiante del mundo actual.

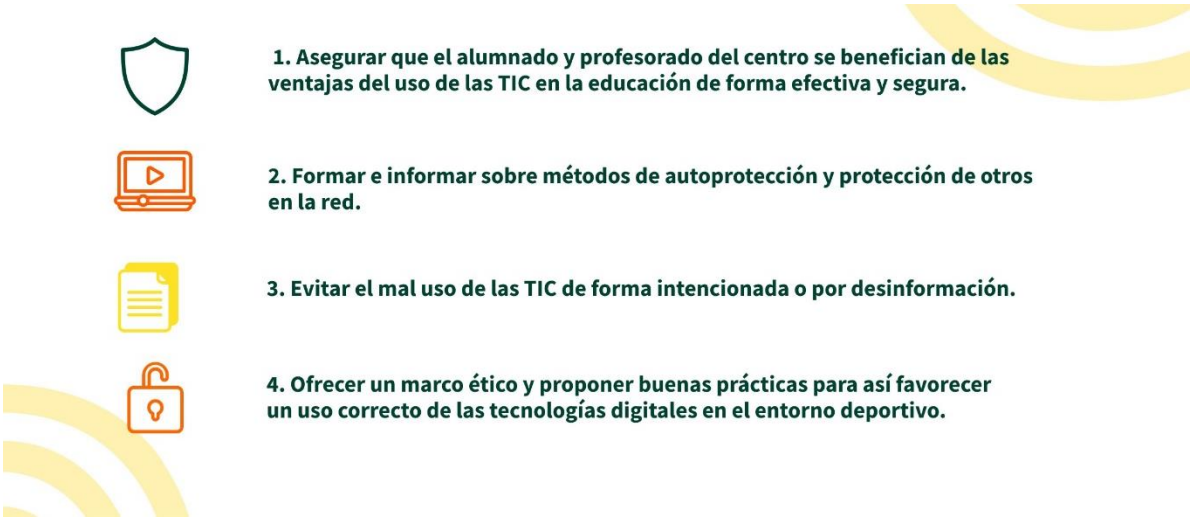
Las Tecnologías de la Información y la Comunicación (TIC) constituyen un elemento clave de nuestro modelo educativo. Por tanto, tenemos que garantizar la salud física, mental y emocional de nuestro alumnado y profesorado en su interacción con la red y los dispositivos electrónicos.

La competencia digital afecta no solo a las personas, sino que incluye a las organizaciones educativas y adquiere matices específicos cuando se refiere a determinados desempeños, como el docente.

Esta Guía es un instrumento de referencia práctico, dirigido a nuestra comunidad educativa y establece algunas recomendaciones para un uso responsable de las mismas

2. Objetivos

Los objetivos de la guía son los siguientes:



3. Normas y recomendaciones para el uso responsable del equipamiento informático del centro

3.1. Normas y recomendaciones para el alumnado

El objetivo de las siguientes normas generales, es promover el uso responsable y seguro del equipamiento informático y digital del Centro.

Además, tienen el objetivo de prolongar la vida útil de los equipos informáticos y que alumnado y profesorado lo pueda aprovechar y utilizar en las mejores condiciones:

- Los equipos informáticos son de **uso exclusivamente educativo** y solamente se pueden utilizar en horario lectivo y con la supervisión del profesorado.

- **No se pueden utilizar** los equipos informáticos del Centro para **juegos, música, vídeos** que no tengan relación con las clases, redes sociales o mensajería instantánea.
- Está prohibido **consultar, crear o compartir mensajes, imágenes, vídeos, páginas web o cualquier otro contenido de carácter ilegal o dañino.**
- Se debe proteger la información propia y de los demás.
- No se puede **suplantar la identidad** de nadie.
- No se puede publicar información de otra persona sin su consentimiento. Siempre es aconsejable evitar publicar detalles o imágenes privadas.
- No almacenar en los equipos información personal, imágenes, vídeos, ni permitir que éstos recuerden las contraseñas.
- No compartir las contraseñas con nadie.
- No personalizar configuraciones en equipos, ni instalar o desinstalar programas y aplicaciones.
- Acordarse siempre de cerrar sesión.
- Guardar los documentos de trabajo sólo en el lugar indicado por los docentes (carpeta online de Google Classroom o similar, por lo general).
- Hacer copias de seguridad en dispositivos extraíbles (memoria USB, tarjeta de memoria) o en la nube (Dropbox, Google Drive, OneDrive, etc.).
- Protegerse de virus y malwares.
- Al conectar un dispositivo extraíble (pincho USB, tarjeta de memoria) o descargar un archivo de Internet analizarlo siempre con el antivirus.
- **Desconfiar** de mensajes y enlaces sospechosos, extender enlaces cortos y analizar URLs antes de abrirlas.
- Cuidar de los recursos informáticos como si fueran tuyos.
- **Evitar golpes**, transportar los equipos portátiles con seguridad, usar fundas protectoras…
- **Evitar líquidos** cerca del equipamiento informático ya que puede perjudicar gravemente a los equipos, teclados, etc. si se derrama sobre ellos.
- **No desconectar los cables** bruscamente ya que podría dañar el propio cable, las clavijas, etc.
- **Evitar desconectar** cables de proyectores, ordenadores de aula, etc.
- Se podrán utilizar tanto dispositivos del centro como dispositivos electrónicos que traiga el alumnado.
- Si los equipos alertan sobre una posible amenaza, no hay que saltarse dichas restricciones de seguridad.
- Apagar siempre los equipos informáticos después de su utilización.
- Los equipos informáticos deben encenderse cuando vayan a usarse para prolongar su vida útil y ahorrar costes energéticos.
- Comprobar el estado del equipo al iniciar y terminar la clase. Ante cualquier problema informar al profesor para registrar la incidencia.
- Si hay algún problema con los dispositivos electrónicos, comunicárselo al profesorado.

3.2. Normas y recomendaciones para el profesorado

Además de todas las normas y recomendaciones anteriores, se añaden las siguientes normas específicas y recomendaciones:

- El profesorado **informará al alumnado sobre el uso adecuado de las herramientas** o apps usada, así como del uso de los equipos y dispositivos.
- Los equipos informáticos Smartv y proyectores, solamente deben encenderse cuando vayan a usarse para prolongar su vida útil y ahorrar costes energéticos.
- El profesorado que se encuentre a última hora en un aula será el encargado de comprobar que todos los equipos informáticos y proyectores estén apagados.
- Los equipos de los despachos y departamentos también deben ser apagados por el profesorado que los use en las últimas horas o cuando no vayan a ser utilizados.
- El profesorado del centro supervisará las actividades que precisan el uso de Internet.
- Cualquier persona de la comunidad educativa que encuentre material inapropiado en los dispositivos del centro, o durante una actividad, deberá comunicarlo de forma inmediata.
- Crear un espíritu crítico sobre la que aparece en la red, hablar del origen y credibilidad de las fuentes de información, sabiendo que es importante filtrar y evaluar la calidad de las mismas.
- **Hablar con claridad sobre los contenidos de la Red.** Aprender a no hacer clic en enlaces sospechosos previene el acceso a páginas web con amenazas capaces de infectar los ordenadores. Los enlaces sospechosos podemos encontrarlos un mensaje de un foro, en un correo electrónico o incluso en los primeros resultados de Google. Lo importante es analizar si son ofrecidos en alguna situación sospechosa, provienen de un remitente desconocido o remiten a una web poco confiable.
- **Informar sobre los derechos de propiedad intelectual.** Cada vez es más frecuente que el profesorado pida trabajos a nuestro alumnado que requieran buscar información en internet. Los estudiantes deben tener formación sobre los derechos de propiedad intelectual y saber que no se pueden utilizar libremente imágenes, textos u otros contenidos con derechos reservados sin citar la fuente.
- **Fomentar la utilización de una posición correcta** para el cuerpo frente al ordenador, siguiendo las siguientes pautas:
    - Los ojos deben estar situados enfrente, y a una distancia mínima del doble de la diagonal de la pantalla.
    - La espalda recta, u reposada la zona lumbar contra el respaldo de la silla.
    - El ángulo de rodillas y codo ha de ser de 90.

4. Prácticas para un uso responsable y adecuado de las TIC

El centro educativo tendrá que cuidar los siguientes aspectos:

- **Mantener actualizados los equipos del centro**. Una forma de evitar amenazas es mantener actualizados los sistemas operativos y las aplicaciones instaladas. Por ello, es recomendable descargar aplicaciones siempre de web oficiales y utilizar antivirus para proteger los dispositivos del centro de posibles amenazas.

- 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.
- **Proporcionará formación sobre los peligros de la red**, cómo evitarlos y promover un uso seguro de las TIC.
- Podrá comprobar los archivos guardados, descargados, histórico de la web y cualquier otro elemento como resultado del uso de Internet.
- El centro pedirá autorización 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.
- El centro proporcionará al alumnado un conjunto de normas de conducta, protección y autoprotección para tener comunicaciones efectivas y seguras en la red.

5. Normas de uso de las redes sociales en el centro educativo

• El alumnado no puede sacar fotos ni videos del alumnado del centro 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 (menores).

• Familias, alumnado y docentes del centro harán uso de las redes sociales teniendo en cuenta la normativa de convivencia del centro. Siempre publicando y comentado en ellas con máximo respeto y cuidado hacia todas las personas que integran la comunidad educativa.

• Tanto el alumnado como la comunidad educativa, 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.

• Además de utilizar los canales oficiales de comunicación, equipo directivo y profesorado intentarán hacer uso de las redes sociales como medio para difundir sus actividades habituales, con fines educativos.

• Tanto las imágenes como la música que se publiquen en las redes sociales del centro cumplirán la normativa respecto a los derechos de autor.

• Todas las familias y trabajadores del centro firmarán un documento en el que firmen su consentimiento o su negativa a aparecer en publicaciones del centro.

6. Normas de uso de los dispositivos móviles/ tablets /ordenadores personales

El uso de dispositivos móviles personales/tablets/ordenadores personales en el centro será permitido exclusivamente con fines educativos.

El uso de estos dispositivos en el centro se hará siempre bajo la supervisión del profesorado.

Cuando se requiera el uso de dispositivos personales por parte del alumnado el/la profesor/a responsable se asegurará de que todos los/las alumnos/as disponen de estos recursos.

Cuando el profesorado autorice o requiera el uso de dispositivos personales será el alumnado el responsable de su puesta a punto (batería, actualizaciones, aplicaciones requeridas…) así como de su custodia.

Se utilizarán sólo las aplicaciones móviles que exclusivamente pida el profesorado, y sólo se utilizarán en ese momento.

El profesorado también se encargará de realizar una lista con las aplicaciones que se pueden utilizar y otras que no. El profesorado dinamizará la creación y utilización de herramientas y aplicaciones digitales a las que el alumnado accederá mediante el uso de sus propios dispositivos

7. Sanciones

El mal uso de Internet o incumplimiento de la normativa puede conllevar sanciones e incluso la retirada del acceso a Internet de forma temporal o definitiva.

El centro podrá informar a las autoridades competentes de cualquier actividad ilegal detectada o situaciones que afecten a la integridad

Se consideran faltas graves:

- Utilizar el dispositivo para realizar fotografías/vídeos/audios sin el consentimiento del afectado.
- Acceder a páginas no apropiadas.
- Uso del dispositivo cuando no lo ha autorizado el docente.
- Acceso a redes sociales sin autorización del docente.
- Acceso a aplicaciones no autorizadas por el docente.
- Suplantar la identidad.
- Sustraer material informático del centro.
- Consultar, crear o compartir mensajes, imágenes, vídeos, páginas web o cualquier otro contenido de carácter ilegal o dañino.
- No se puede publicar información de otra persona sin su consentimiento. Siempre es aconsejable evitar publicar detalles o imágenes privadas.

8. Recomendaciones para crear y gestionar contraseñas seguras

Para evitar riesgos derivados de una mala gestión de las contraseñas, te facilitamos unos consejos muy fáciles de aplicar:

- **No compartir las contraseñas con nadie**. Si lo haces, dejará de ser secreta y estarás dando acceso a otras personas a tu privacidad.
- **Asegurar de que son robustas**. Están formadas por al menos 8 caracteres: mayúsculas, minúsculas, números, caracteres especiales. Utilizar alguna regla mnemotécnica para recordarlas. Evitar secuencias del tipo “123456” o “111111 como “contraseña1”. A mayor variedad, más impredecible y segura es la contraseña. Usar palabras poco comunes o inesperadas. Si la contraseña es una secuencia de palabras, desordenarlas para que sea poco predecible. No repetir contraseñas.
- **No utilizar la misma contraseña en diferentes servicios**. Siempre claves diferentes para servicios diferentes.

- **Cuidar con las preguntas de seguridad**. Si las utilizas, que sólo tú y nadie más sepa las respuestas.
- **Utiliza gestores de contraseñas.** Si te cuesta memorizar las contraseñas o utilizas muchos servicios, apóyate en estos programas, son muy útiles y sencillos de manejar.
- No almacenar contraseñas en aplicaciones como "Notas" en el teléfono móvil.
- No guardar las contraseñas en el autocompletado del navegador.

9. Amenazas más importantes en el uso de las TIC

- El **ciberbullying** es el acoso (bullying) llevado a las redes sociales, donde adquiere toda una nueva dimensión. Es uno de los peligros en las redes sociales que muchos adolescentes y también jóvenes sufren, continuando en muchas ocasiones el acoso sufrido en las clases al entorno virtual y con consecuencias que a veces pueden ser muy trágicas.

- El **grooming** consiste en un tipo de acoso sexual a través de Internet, en este caso de una red sexual, donde un adulto engaña y manipula al menor con una finalidad sexual. Se basa en conseguir la confianza del menor y con el tiempo, establecer vínculos emocionales con él para poder conseguir lo que desea de ellos; fotos o vídeos de contenido sexual protagonizados por el menor o, en el caso de tratarse de un pederasta, conseguir un encuentro físico con el menor.
  Cuando el depredador sexual consigue la primera foto o vídeo, lo habitual es que pasen al chantaje o la extorsión, amenazando con compartirlo con los conocidos del menor, para conseguir más imágenes o ese encuentro físico.

- **El sexting.** Consiste en enviar mensajes, fotos o videos de contenido erótico, sexual y pornográfico, mediante aplicaciones de mensajería en tiempo real. Los riesgos se encuentran en la exposición y divulgación de este contenido íntimo.

- **El phishing.** Es un tipo de estafa que intenta obtener datos, contraseñas, cuentas bancarias, números de tarjetas de crédito o del documento nacional de identidad de la víctima mediante engaño para utilizarlos en el robo o sustracción de fondos de sus cuentas.

- **Robo y suplantación de identidad.** Se produce cuando otra persona roba nuestra cuenta en una red social y se hace pasar por nosotros. Es el caso más extremo y problemático, porque además de perjudicar nuestra imagen o la imagen del menor, tiene acceso a toda la información y datos personales de su cuenta.
  También puede ocurrir cuando una persona roba una foto nuestra y la usa para crear un **perfil falso** con nuestro nombre, de nuevo, para hacerse pasar por nosotros o el menor y publicar en su nombre.

- **Ciberadicción.** Consiste en la «conexión compulsiva» y en la necesidad de tener que conectarse con frecuencia muchas veces al día. Esto tiene consecuencias como la dispersión de la atención, la búsqueda constante de contenidos relacionados con ciertos gustos o adicciones, la creación de distintas identidades, la sustitución de lo real por lo vivido en entornos virtuales, la pérdida de la noción del tiempo.
- **Fake News.** El riesgo para los jóvenes está en que estas noticias falsas, estos bulos, pueden distorsionar la realidad para ellos, haciéndoles creer cosas y hechos que no son verdad sobre determinados temas, colectivos o minorías. Además, se convierten

en «cómplices» de las mismas, cuando las comparten y contribuyen a su viralización. En este sentido, debe trabajarse la formación para acceder a la información en Internet con una actitud crítica y analítica.