

aprende **ntef**

Conductas en la red: tú decides en Internet

Es importante como padres, tutores o educadores transmitir a los menores la importancia de reflexionar antes de publicar cualquier contenido en la red, de no realizar acciones o comentarios que no les gustaría que les hicieran a ellos y recordarles que deben desconectar y dedicar tiempo a otras actividades.

Estos son algunos **consejos** que ofrece la Agencia Española de Protección de Datos (AEPD) para que los menores ejerzan una ciudadanía digital responsable, saludable y segura:

1. No utilices Internet para hacer daño, nunca participes en un acoso. Y no te calles. Tanto si te pasa a ti como si le pasa a un compañero, debes contárselo a tus padres o tus profesores. No es ser un chivato, es ser un buen compañero.

En este partido nos la jugamos

2. Protege tu identidad, tus datos personales no son solo tu dirección, tu teléfono o tu fecha de nacimiento. Pequeños detalles sin importancia, el sitio donde estás o el aspecto que tienes en un cierto momento también dan información sobre ti y pueden llegar a ser usados maliciosamente. No compartas datos personales con gente que no conoces en persona.

Planazo de fin de semana

3. Las cosas que envías por Internet dejan huella y tu rastro digital te va a acompañar durante mucho tiempo y puede tener consecuencias, buenas o malas, depende de ti.

Un vídeo muy especial

4. Internet y las redes sociales son geniales. Pero hay más cosas geniales en la vida y algunas de ella solo se pueden disfrutar cuando estás desconectado de Internet.

Un crack del BMX

PARA SABER MÁS:

- ["Tú decides en Internet "](#) Agencia Española de Protección de Datos (AEPD).
- ["Convivencia y respeto en Internet"](#) INCIBE a través de IS4K.
- ["Familia cibersegura VI: Edúcale para ser un buen ciudadano digital"](#) INCIBE a través de IS4K.
- ["Educando en ciberseguridad V: Relaciones positivas y convivencia"](#) INCIBE a través de IS4K.
- [Ciudadanía e identidad digital](#), publicación del MEFP a través de INTEF.
- [Practica la netiqueta en Internet](#), vídeo de INCIBE a través de IS4K.

La mediación parental

De manera genérica, al conjunto de pautas y estrategias que utilizan padres, madres, tutores o educadores para proteger a los menores en Internet se le denomina **mediación parental**. Estas medidas o estrategias tienen como finalidad:

- Conocer y aprovechar los beneficios que ofrece la red.
- Entender y prevenir posibles riesgos del uso de Internet.
- Detectar y gestionar problemas en el entorno digital.

Según la **guía de mediación parental del INCIBE** estas estrategias se clasifican en:

- Estrategias activas:
 - Supervisión
 - Acompañamiento
 - Orientación
- Estrategias restrictivas:
 - Normas y límites de uso

- Aplicación de herramientas de control parental
- Configuración de opciones de privacidad

Combinar ambos tipos de estrategias es la opción más efectiva y segura. Es importante que padres, madres, tutores o educadores, además de utilizar apoyos técnicos para hacer un seguimiento del tiempo de uso y los contenidos a los que acceden los menores a partir de unas normas claras y consensuadas, conozcan con quién se relacionan en Internet y qué tipo de contenidos consumen.

Es esencial establecer una relación de confianza que permita a los menores comentar y pedir ayuda o consejo ante cualquier incidencia o problema con el que se encuentren. Para ello, es conveniente compartir algunas actividades en la red en familia, crecer juntos y aprender de los errores propios o ajenos, y aprovechar para potenciar las habilidades sociales y el pensamiento crítico en los más pequeños, siendo capaces de gestionar como adultos las propias conexiones tecnológicas y enseñar de manera paralela a los menores a hacer lo mismo.

A continuación, vamos a profundizar en este tema y conocer cómo aplicar estas estrategias con:

1. Un [vídeo sobre la mediación parental](#) como respuesta a nuestras preocupaciones ante los riesgos del uso cotidiano e intensivo de las tecnologías por parte de los y las menores.
2. Un [vídeo sobre la importancia de hablar en familia](#) para estar al tanto del día a día de los menores en Internet, conocer sus inquietudes, detectar posibles problemas y mantener su confianza para resolverlos juntos.
3. La [Guía de mediación parental del INCIBE](#), formada por fichas con los aspectos principales que tener en cuenta, recomendaciones y pautas de fácil aplicación para reflexionar y ajustar el acompañamiento y la supervisión de niñas, niños y adolescentes en Internet.

4. El artículo [Competencias digitales en familia](#) nos aporta las claves para utilizar la tecnología de forma crítica y segura como adultos, para contribuir efectivamente a la educación digital de los hijos/as.

PARA SABER MÁS:

- [Infografía : Protección del menor en Internet - AEPD](#)
- [Campaña sobre mediación parental](#) de INCIBE a través de IS4K.
- [Artículo "Familia cibersegura I: Preparados para la mediación parental"](#), de INCIBE a través de IS4K.

Herramientas de control parental

Como hemos visto en el apartado anterior, dentro de las estrategias restrictivas se incluyen el uso de herramientas que ayuden a los adultos a proteger a los menores en su navegación y su acceso a la red. Su utilización **permite limitar el acceso de los menores a contenidos inadecuados**, a través del filtrado y bloqueo de los mismos. Además de esta funcionalidad, estas herramientas dan la opción de aplicar controles de tiempo, bloqueo de aplicaciones, seguimiento de actividad, alertas de notificaciones y geolocalización, entre otras. Veamos brevemente en qué consisten estas funcionalidades mediante esta infografía: [Mediación y herramientas de control parental](#):

En la página de menores de la AEPD [Tú decides en internet](#) y en [Internet Segura for Kids](#) de INCIBE, se puede acceder a contenido sobre control parental que puede ser de gran utilidad para la elección, instalación y uso de estas herramientas. Podemos encontrar:

- Buscadores seguros y *apps* de contenido exclusivo para niños.
- Control parental ofrecido por los sistemas operativos de los fabricantes.
- Opciones de control parental ofrecido por los operadores de telefonía.
- Otras aplicaciones de control parental.
- Alternativas al uso de aplicaciones de control parental.

PARA SABER MÁS:

[Evitar el acceso a contenidos inadecuados - AEPD](#)

[Guía de Herramientas de control parental](#)

[Límites técnicos para el día a día](#)

[Catálogo de herramientas de control parental de IS4K](#)

Uso del teléfono móvil

El uso del *smartphone* está tan extendido que, para muchas personas, se ha llegado a convertir en un complemento imprescindible en el día a día. No es extraño que niños y niñas de entre 10 y 11 años soliciten insistentemente tener su propio teléfono móvil, por lo que la pregunta: *¿cuál es la edad ideal para comprar el primer smartphone?*, suele ser una cuestión recurrente entre padres o tutores de menores.

Pero la respuesta a esta pregunta no es tanto una edad concreta, sino más bien saber valorar cuál es el momento adecuado. Para ello, [en este artículo](#) del Instituto Nacional de Ciberseguridad de España (INCIBE), se propone tomar la decisión valorando:

- Las **necesidades** que motivan esa petición: ¿son reales?, ¿cuánta relevancia tienen?, ¿qué impacto tiene en el menor, o en su círculo social, la no disponibilidad de un móvil?
- La **madurez y responsabilidad** del menor más allá de su edad.

Para ayudar a los padres, madres o tutores en esta cuestión, INCIBE, a través de IS4K, pone a su disposición una serie de [pactos o contratos familiares](#), como el [Contrato familiar para el buen uso del móvil](#), un recurso muy eficaz que permitirá realizar en familia una mejor gestión de este asunto.

Otro aspecto importante es [saber cómo configurar el primer móvil](#).

En el caso de que el primer *smartphone* sea un teléfono móvil heredado, la configuración y personalización del mismo es otro aspecto importante que vamos a aprender a realizar paso a paso a través de este artículo de IS4K: "[Mi primer teléfono heredado](#)".

Antes de finalizar este apartado, no podemos olvidar recordar las normas de [uso del móvil en el centro educativo](#) .

PARA SABER MÁS:

- "[¿Está protegida la información privada que guarda tu hijo/a en su móvil?](#)", artículo del blog de IS4K de INCIBE.
- "[Familia cibersegura IV: Prepárale para proteger sus datos, dispositivos y evitar fraudes](#)", artículo del blog de IS4K de INCIBE.
- "[Educando en ciberseguridad IV: Configuraciones seguras, protección ante virus y fraudes](#)", artículo del blog de IS4K de INCIBE.

Uso de redes sociales

Las redes sociales permiten abrir un perfil con datos personales para comunicarse y compartir información con otras personas, de forma pública o restringida. Estos servicios en línea abren muchas posibilidades, pero también implican [ciertos riesgos](#), especialmente en un colectivo tan vulnerable como el de los menores.

Algunos de estos riesgos son:

- Los relacionados con la **publicación de datos personales**:

- Suplantación de identidad: un usuario utiliza datos o imágenes de otra persona para crear un perfil falso y publicar en su nombre.
- Engaño pederasta o *grooming*: un adulto puede hacerse pasar por un menor con el objetivo de ganarse, poco a poco, la confianza de otro menor y obtener datos o imágenes comprometidas para después chantajearle.

- Los relacionados con un **uso incorrecto de las redes sociales**:

- Ciberacoso: la realización de comentarios y publicaciones negativas o humillantes en redes sociales supone una forma de acoso en el entorno digital. Dar *me gusta*, compartir las burlas o no denunciarlas también implica ser cómplice.
- Uso excesivo: el no establecer límites de tiempo, descuidando otras actividades tan importantes como la comida, la actividad física o el descanso, puede generar en muchos casos síntomas de dependencia o adicción.

- El acceso a **contenidos inadecuados** puede exponer a los menores a bulos y fraudes, discursos de odio y publicaciones de comunidades peligrosas en las que se fomentan malos hábitos relacionados con desórdenes de alimentación, autolesión, consumo de drogas, etc.

Para evitar estos riesgos, es recomendable que los adultos configuren la privacidad de sus cuentas personales en redes y ayuden a los menores a hacer lo mismo con las suyas. Para ello, es conveniente establecer el perfil personal como privado, limitar la visibilidad de sus publicaciones y la recepción de mensajes y comentarios solo a sus contactos, aceptar como amigos solo a quienes conocen en persona, así como evitar la entrada de publicidad personalizada y no deseada.

[¿Cómo configurar las opciones de privacidad de los navegadores, redes sociales, aplicaciones de mensajería instantánea y sistemas operativos más comunes?](#)

Además, es necesario ayudar a los menores en la construcción de una identidad digital correcta siendo un modelo para ellos y haciéndoles conscientes de la importancia de pensar muy bien antes de publicar algún comentario o imagen en la red que pudiera perjudicarlos social, personal o profesionalmente en un futuro. En la siguiente infografía "[Promueve una identidad digital positiva en familia](#)", podemos ver algunos consejos:

Sin duda, es posible utilizar las redes sociales de forma positiva y segura, todo depende del uso que el menor haga de ellas y su actitud a la hora de relacionarse con otros usuarios/as. Por ello, la función de acompañamiento de los padres, madres, tutores o educadores es de gran importancia. Para orientar y profundizar en esta cuestión el Instituto Nacional de Ciberseguridad (INCIBE) ha publicado esta [Guía de seguridad en redes sociales para familias](#) de fácil y rápida consulta.

En [Redes sociales para la adolescencia](#), de IS4K de INCIBE, también podrás conocer cuáles son sus espacios sociales favoritos y encontrar respuesta a muchas preguntas habituales respecto a este tema.

PARA SABER MÁS:

[Aplicaciones, juegos y redes sociales más populares entre los menores de IS4K.](#)

[Campaña sobre alfabetización mediática, noticias falsas, sesgos en Internet y bulos.](#)

[Campaña sobre ciberacoso.](#)

[Campaña sobre menores y sexting.](#)

Recursos para familias y educadores

Tanto en la web de IS4K como en la de la AEPD, se pueden encontrar multitud de recursos de utilidad para acercar la ciberseguridad a los menores, tanto en familia como desde los centros escolares. Algunos de ellos son:

- [Ciberseguridad para el ámbito educativo](#)
- [Ciberseguridad para familias](#)
- [Guía para centros educativos](#)
- [Quién es quién en el tratamiento de los datos personales en tu centro educativo](#)
- [Contacto de los delegados de protección de datos en educación por CC. AA.](#)
- [Juegos en el catálogo de recursos de IS4K](#)
- [Guías e informes en el catálogo de recursos de IS4K](#)
- [Materiales didácticos](#)
- [Organizador digital familiar](#)

Línea de ayuda en Ciberseguridad de INCIBE (017 (servicio gratuito y confidencial), para orientar ante cualquier duda o problema relacionado con la seguridad en Internet de los menores, sus familias y educadores, además de ciudadanía en general, profesionales y empresas. El servicio está disponible en el teléfono gratuito y confidencial 017, mediante WhatsApp ([900 116 117](#)), Telegram ([@INCIBE017](#)) o el [formulario web](#).

La AEPD cuenta con un servicio de ayuda dirigido tanto a menores como a familias y docentes donde se podrán plantear cuestiones relacionadas con protección de datos personales en el ámbito de los menores. Estas consultas podrán realizarse tanto por correo electrónico canaljuven@aepd.es como por teléfono llamando al 901 23 31 44.