



EXPERIENCIA DE AULA



## SEGURIDAD EN REDES SOCIALES EN EL MARCO EDUCATIVO



MATERIALES DIDÁCTICOS CRFP



GUÍA PARA PADRES



Centro Regional de  
Formación del Profesorado  
Castilla-La Mancha



## MATERIALES DIDÁCTICOS CRFP

Cristina Alba Peinado (ed.)

Antonio Quintanilla Rodríguez (coord.)

Vicente Núñez Armero  
Pedro Antonio Ortega Palazón  
Miguel Ángel Rodríguez Cubas  
Isabel Valverde López

ISBN 978-84-16077-22-9

### LICENCIA CC



***Seguridad en Redes sociales en el ámbito educativo. Guía para padres*** de Centro Regional de Formación del Profesorado de Castilla-La Mancha es un material que se publica al amparo de la licencia *Creative Commons Reconocimiento-NoComercial 4.0 Internacional License*.

Se puede copiar, distribuir y comunicar públicamente el contenido de esta publicación, así como hacer usos derivados de la misma siempre que no conlleve un uso comercial. Si el contenido se publica en un blog o sitio web, se debe enlazar el artículo original. Si se reproduce en un medio impreso, se debe hacer referencia expresa de la autoría y web original.





# Descripción

**ESTA GUÍA** pretende ser un recurso práctico para ayudar a los padres en su labor educativa en el ámbito de las nuevas tecnologías.

Desde la plataforma virtual del [Centro Regional de Formación del Profesorado](#), se ha trabajado en el Grupo Colaborativo “**Seguridad en Redes Sociales en el marco educativo**” creando materiales útiles para abordar en las aulas con los alumnos la temática en cuestión. No obstante, consideramos fundamental la formación de los padres en esta materia, ya que es en el ámbito doméstico donde el alumno suele hacer uso de estas tecnologías.

Para ello, presentamos unas propuestas que parten de una evaluación inicial definiendo el ESTILO EDUCATIVO que los padres adoptan en el uso de las nuevas tecnologías, para continuar aplicando un ESTILO EDUCATIVO DEMOCRÁTICO, a través de una serie de tareas que fomentarán el **aprendizaje colaborativo** entre padres e hijos en el uso del móvil, ordenador, tablets, etc...

## ¡CONÉCTATE!



### Descripción

### Objetivos

### Contenidos

### Propuestas

*¿Qué estilo educativo aplicamos en casa?*

*Recomendaciones de los expertos*

*Contrato padres / hijos*

*Configuración del control parental de un ordenador*

### Evaluación

### Webgrafía

### Recursos

Visita la web





# Objetivos

**A TRAVÉS DE** las propuestas y recursos proporcionados, se persigue alcanzar los siguientes objetivos:

1. Entender la importancia de la implicación educativa de los padres en el mundo de las nuevas tecnologías.
2. Reflexionar sobre los hábitos familiares del uso de las TIC.
3. Conocer las principales aplicaciones que los menores hacen de Internet, y los riesgos que cada una de ellas conllevan.
4. Fomentar la implicación y el compromiso de los padres en el control, ayuda y supervisión del uso de las nuevas tecnologías por parte de sus hijos.
5. Conocer el decálogo de normas de seguridad informática proporcionado por expertos y autoridades.
6. Saber actuar y reaccionar cuando se sufre algún tipo de ataque a través de medios informáticos.
7. Establecer unas pautas de acción a la hora de establecer normas de uso de las TIC de los menores.
8. Conocer herramientas informáticas que ayudan en el control del uso del ordenador de los menores.



# Contenidos

**LOS CONTENIDOS** que se trabajan en la guía son los siguientes:

Estilos educativos aplicados al control y supervisión en el uso de las nuevas tecnologías.

Aplicaciones informáticas más comunes usadas por los menores.

Peligros a los que están expuestos los menores en el uso de las aplicaciones más comunes: ciberacoso, *sexting*, *grooming*, *phishing*, *malware*, etc.

Recomendaciones preventivas a menores para evitar los peligros en Internet.

Respuesta a los ataques sufridos en Internet.

Decálogo de la navegación segura (para adultos y menores).

Contratos de compromiso entre padres e hijos.

Responsabilidad paterna en los delitos cometidos por sus hijos.

Programas de control parental.





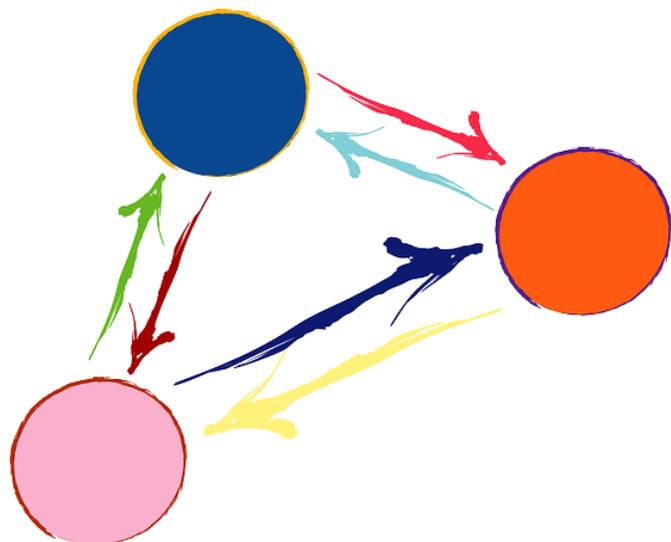
# Propuestas

**LAS PROPUESTAS** que aquí presentamos son parte de la experiencia que llevamos a cabo los miembros del Grupo Colaborativo en nuestras aulas, a través fundamentalmente de charlas con los padres de nuestros alumnos, quienes muestran continuamente su preocupación por asuntos relacionados con la seguridad en Redes Sociales.

Nuestras propuestas se basan en dos pilares fundamentales:

La formación de los padres en la utilización de las Redes Sociales, centrándonos en cuestiones básicas de seguridad y aportando herramientas útiles para su control.

Fomentar la confianza y comunicación entre padres e hijos, adquiriendo obligaciones y compromisos entre ambos, que facilitarán un uso responsable de las nuevas tecnologías y una base firme para la identificación de problemas que puedan surgir.





## PROPUESTA I.

### ¿QUÉ ESTILOS EDUCATIVO APLICAMOS EN CASA?

#### Descripción:

Proponemos comenzar completando una encuesta y después leer la opinión de expertos para entender la importancia del control, supervisión y compromiso con nuestros hijos en el uso de las nuevas tecnologías de la información y comunicación.

#### Destinatarios de la actividad:

Padres de alumnos de todas las edades.

#### Metodología:

Se propone realizar la siguiente encuesta con 5 preguntas sencillas, para saber qué estilo educativo estamos aplicando en el uso de las nuevas tecnologías, tanto con nuestro hijo como con nosotros mismos.

El objetivo es concienciar a los padres de la importancia de **establecer normas en el uso de las TIC y de Internet:**

#### Recursos:

→ Recomendamos una primera lectura de los diferentes estilos educativos existentes, para saber las ventajas e inconvenientes de cada uno y reflexionar si se está dispuesto a aplicar este estilo. Se puede consultar la web de psicología: <http://www.psicoglobalia.com/los-estilos-educativos-de-los-padres-ventajas-e-inconvenientes/> o picha en la imagen para acceder:





## USO DE LAS NUEVAS TECNOLOGÍAS EN MI HOGAR

### Pregunta 1: ¿Cuánto tiempo dejo a mi hijo/a utilizar el ordenador para conectarse a Internet?

- No dejo usar Internet a mi hijo porque es muy peligroso, y si lo necesita para realizar trabajos es conmigo al sentado a su lado.
- Le dejo conectarse siempre que lo necesite, y a cualquier hora.
- No hemos establecido normas respecto al horario y la cantidad de tiempo que puede estar conectado.
- Hemos negociado el tiempo que puede usar Internet al día y el margen horario.

### Pregunta 2: ¿Dónde está el dispositivo a través del cual se conectan los hijos a internet?

- Solo pueden usar la tablet sentados a mi lado y el portátil para hacer trabajos cuando yo estoy en la misma habitación.
- Tienen libertad para usarlo en el salón, en su cuarto o donde quieran.
- No sé cómo se conectan a Internet.
- Trato de que se conecten en las zonas donde normalmente estamos toda la familias (cocina, salón, cuarto de estar).

### Pregunta 3: ¿Conoces el usuario y claves de los diferentes servicios que utiliza tu hijo?

- Sí, yo les doy de alta en aquellos servicios que quieren usar, previo consentimiento mío.
- No, porque quiero respetar su intimidad. Y les dejo que pongan el usuario y contraseña que más les guste.
- No, porque no sé qué servicios de Internet utilizan.
- Sí, los tengo anotados en un cuaderno por seguridad, aunque no los utilizaré salvo una urgencia. Además, les aconsejé no poner información personal en el usuario y cómo poner contraseñas seguras

### Pregunta 4: En casa, ¿está actualizado el sistema operativo, el navegador y el antivirus?

- Sí, confío plenamente en las aplicaciones de seguridad de mi ordenador, que está libre de cualquier virus o programa malicioso.
- No lo sé, de eso se encarga mi hijo o un familiar que entiende de informática.
- No lo sé.
- Sí, aunque sé que nunca estoy seguro al 100%.

### Pregunta 5: ¿Utilizas el ordenador para realizar compras o para consultar las operaciones bancarias?

- No, porque hay mucho fraude y no me fío.
- Sí, nunca me ha pasado nada. Hasta mi hijo compra sin problemas.
- Alguna vez, pero no recuerdo qué página web era.
- Sí, pero solo desde mi ordenador y comprando en páginas que tienen Identidad verificada y segura



En función de lo contestado:

**Si la mayoría de las respuestas son del “tipo a”:** la persona que ha contestado tiene un **ESTILO EDUCATIVO AUTORITARIO Y/O DESCONFIADO**.

Como ventaja, se puede decir que es una persona que controla todos los ámbitos educativos con normas rígidas, inflexibles, en ocasiones no adaptadas a los niños.

Por el contrario, muchas veces el exceso de control provoca una inmadurez y falta de responsabilidad de sus hijos, ya que entienden que hay que seguir las normas para evitar los castigos. Estos niños tratarán de esquivar a sus padres en el uso de las TIC, y tendrán poca confianza en acudir a ellos cuando tengan dudas o se sientan incómodos.

**Si la mayoría de las respuestas son del “tipo b”:** la persona que ha contestado tiene un **ESTILO EDUCATIVO PERMISIVO**, delegando la educación en los gustos y preferencias de los niños o en otros especialistas (profesores, educadores, abuelos, etc.).

Como consecuencia, los hijos están muy expuestos a los peligros de Internet, y es fácil sufrir estafas económicas.





**Si la mayoría de las respuestas son del “tipo c”:** la persona que ha contestado tiene un **ESTILO EDUCATIVO INDIFERENTE**, no se implica en este ámbito de la educación de su hijo.

Como consecuencia, el hijo tendrá poca confianza en su padre o madres para la resolución de los conflictos que surjan en Internet, además de estar muy expuesto a todos los peligros.

**Si la mayoría de las respuestas son del “tipo d”:** la persona que ha contestado tiene un **ESTILO EDUCATIVO DEMOCRÁTICO Y/O ASERTIVO**.

Este sería el modelo educativo adecuado: implicación, compromiso y razonamiento desde el sentido común en el uso de las TIC con nuestros hijos.

Es la base para que nuestro hijo confíe en nosotros, nos consulte dudas y seamos el punto de auxilio en caso de tener problemas.

**¿Cómo mejorar los hábitos del uso de las TIC de mi familia para llegar a ser un educador del estilo democrático y asertivo?**

Una buena opción es seguir las recomendaciones de los expertos, relacionadas con las preguntas de la encuesta anterior, que encontraremos en nuestra siguiente propuesta.



## PROPUESTA 2.

### RECOMENDACIONES DE LOS EXPERTOS

---

#### Descripción:

Es fundamental para los padres estar informados y conocer los peligros que pueden conllevar las Redes Sociales. Por ello, proponemos visitar algunas webs donde los expertos hacen recomendaciones que creemos que serán muy útiles para los padres para entender la importancia del control, supervisión y compromiso con nuestros hijos en el uso de las nuevas tecnologías de la información y comunicación.

#### Destinatarios de la actividad:

Padres de alumnos de todas las edades.

#### Metodología:

Tras realizar la encuesta anterior y, en función de los resultados, proponemos intentar mejorar los hábitos del uso de las TIC en la familia para llegar a ser un educador del estilo democrático y asertivo.

Todas las recomendaciones son de expertos y para conocerlas visitaremos sus páginas web, los enlaces que sugerimos e iremos orientándonos hacia los asuntos que más nos preocupen en relación con nuestros hijos.





Algunas de estas recomendaciones (pincha en las imágenes para acceder):

### ***Decálogo de navegación segura de la Guardia Civil***

con explicación a cada recomendación (extraemos algunos puntos de la web oficial; puedes verlo completo, accediendo desde el enlace de la derecha):

- *Actualice de forma regular el sistema operativo*
- *Utilice un navegador actualizado*
- *Elija contraseñas seguras y diferentes para cada servicio de Internet*
- *Utilice un antivirus con licencia y actualizado e instale un firewall*
- *Desconfíe de los mensajes cortos y extraños que pueda recibir por redes sociales, sobre todo si incluyen un enlace para acceder a otro contenido*
- *No piense que es inmune al software malicioso porque utilice un determinado sistema operativo o un dispositivo portátil*
- *No confíe ciegamente en las aplicaciones de seguridad instaladas, éstas no reemplazan a la navegación responsable ni a la prudencia del usuario*
- *Si dispone de un router inalámbrico para conectarse a internet, cambie las contraseñas por defecto y establezca una más segura.*
- ...

**EN DEFINITIVA, UTILICE EL SENTIDO COMÚN COMO MEJOR ANTIVIRUS Y NO CONFÍE CIEGAMENTE EN LOS SISTEMAS Y SUS APLICACIONES.**

→**Decálogo de navegación segura de la Guardia Civil** (pincha en la imagen para acceder):





## Consejos de seguridad de la Policía Nacional

(extraemos algunos consejos de la web oficial; para acceder al documento completo, pincha en el enlace de la derecha):

- En las redes sociales: mantén tu perfil privado, evite las contraseñas fáciles de adivinar
- Utilice contraseñas “de calidad” (con letras, números y otros caracteres). Cámbielas periódicamente.
- Nunca ofrezca datos personales por Internet, a menos que sea en sitios de total confianza. **COMPRUEBE LOS CERTIFICADOS.**
- ...

→ [Consejos de seguridad de la Policía Nacional](#) :



Además de estos expertos, hay algunas webs especializadas, que ofrecen recomendaciones muy interesantes específicas para padres. Destacamos:

## Recomendaciones para padres en Segu-Kids

(extraemos algunos de la web, pero recomendamos 100% su lectura completa a todos los padres; pincha en el enlace de la derecha para acceder):

→ [Recomendaciones para padres en Segu-Kids](#):

*Coloca el ordenador en lugares de tránsito o visibles y evitar que los niños chateen, naveguen o establezcan relaciones en internet con la puerta cerrada o en su habitación.*

*Pregunta a tus hijos quiénes son sus contactos y nuevos amigos y relaciones en Internet y quién está detrás de cada correo electrónico, pero no invadas su privacidad.*

*Explica a tus hijos que la diferencia entre lo que está bien y lo que está mal es la misma en Internet que la vida real.*

...





**Recomendaciones en el Centro Internet Segura** (visita la web desde el enlace de la derecha):

En esta web los padres encontrarán respuesta a estas preguntas:

**¿QUÉ NORMAS BÁSICAS DE SEGURIDAD DEBEN CONOCER MIS HIJOS?**

En este apartado distingue recomendaciones específicas para cada medio. **MUY RECOMENDABLE** para todos los padres.



**Correo electrónico**



**Salas de chat**



**Redes sociales**

**¿QUÉ RESPONSABILIDADES TIENEN MIS HIJOS EN INTERNET?**

**¿CÓMO PUEDEN USTEDES AYUDARNOS SI TENEMOS UN PROBLEMA EN INTERNET?**

También en **Ciberfamilias**, se pueden encontrar recomendaciones muy prácticas sobre **¿Cómo prevenir desde casa?** Por ejemplo:

*Navegar en familia*

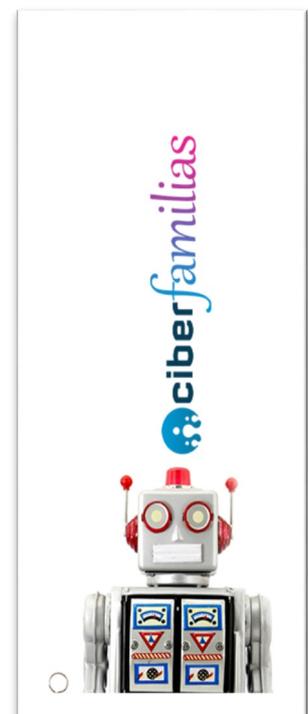
*Ordenador en un lugar común*

*Hacerles conscientes de la importancia de cuidar su privacidad*

*Informar sobre las citas a ciegas*

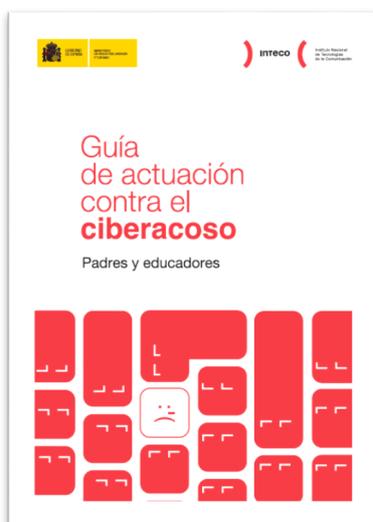
*Limitar el tiempo que usan internet, el móvil, la videoconsola, etc...*

→ **Centro Internet Segura: Padres asegurando a los menores en internet** (pincha en la imagen para entrar):





Finalmente, creemos que puede ser también muy útil esta **Guía de actuación contra el ciberacoso**, dirigida a padres y educadores. Pincha en la imagen para descargarla (PDF):



### Experiencia previa en el desarrollo:

Es una forma más de explicar contenidos, pero de forma inductiva: a partir de preguntas concretas, se trata de obtener consejos razonados globales.

Esta propuesta se ha llevado en cabo en las diferentes presentaciones de la seguridad en Internet a los padres, con muy buenos resultados. Antes de comenzar las diferentes charlas, se les hacía preguntas genéricas, y tras comentar las recomendaciones, todos tenían muy claro **qué hábitos cambiar en sus respectivos hogares**.



### PROPUESTA 3.

## CONTRATO PADRES-HIJOS PARA EL USO DEL ORDENADOR/TABLET/MÓVIL

---

#### Descripción:

Mediante esta propuesta, padres e hijos firman un contrato donde se especifican las normas de uso del ordenador/tablet/móvil. Desde la confianza mutua, permite consensuar el uso de los terminales en casa, estableciendo compromisos por ambas partes.

#### Metodología:

La actividad propuesta está dentro del denominado “ESTILO EDUCATIVO DEMOCRÁTICO”. Por tanto, se recomienda a los padres una primera lectura de los diferentes estilos educativos existentes, para saber las ventajas e inconvenientes de cada uno y reflexionar si se está dispuesto a aplicar este estilo. Para ello, consulta los enlaces de la derecha.

En segundo lugar, es importante conocer el uso que cada niño realiza con los terminales de conexión a Internet. En el enlace de la derecha se puede consultar las principales aplicaciones usadas según el rango de edad, aunque lo más apropiado es hablar directamente con el menor y preguntar qué aplicaciones utiliza o quiere utilizar.

#### Recursos:

→Se puede consultar la web de psicología: <http://www.psicoglobalia.com/los-estilos-educativos-de-los-padres-ventajas-e-inconvenientes/>

→Principales aplicaciones según rangos de edad en <http://www.segukids.org/docentes/edad-menores.html>

<http://www.>



Finalmente, se trata de hacer un documento donde tanto el padre/madre como el hijo/a se comprometan y acuerden diferentes aspectos del uso de los terminales. Algunos aspectos importantes a tratar son el tiempo de uso de estos terminales, las aplicaciones que se usarán, mantener la privacidad, ser respetuoso, etc.

A modo de ejemplo, en Internet existen varios modelos. En el apartado de la derecha ofrecemos un enlace directo a un [ejemplo de contrato para padres y para hijos](#).

El contrato debe revisarse periódicamente para su cumplimiento íntegro, adaptándolo al uso y necesidad del niño con las nuevas tecnologías.

### Destinatarios de la actividad:

Padres de alumnos en el inicio del uso de los dispositivos tecnológicos que permiten el acceso a internet o a las redes sociales. De forma general:

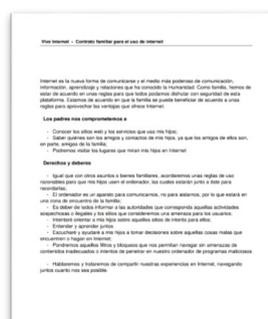
Para padres del segundo o tercer ciclo de primaria que empiezan a usar el ordenador o la tablet con cierta frecuencia.

Padres de niños del primer ciclo de la ESO de secundaria que se inician en el uso del móvil o la tablet como terminal de comunicación.

**Tiempo destinado al desarrollo:** 1 hora (negociación y firma del contrato)

→ Desde aquí puedes descargar un ejemplo de contrato que ofrece la web **Vive internet**. Pincha en las imágenes para acceder:

### Compromiso de los padres:



### Contrato para los hijos:





### Tiempo de preparación: 2 horas.

El tiempo de preparación consiste en leer las **recomendaciones de expertos para el uso de los terminales TIC** (ordenadores, tablets y teléfonos), preparar el contrato adaptando los compromisos a los objetivos que nos hemos marcado previamente y finalmente negociarlo con el hijo/a y llegado el caso firmarlo.

### Experiencia previa en el desarrollo:

Es un ejemplo de los llamados *CONTRATOS DE CONDUCTA*, donde se pretende desarrollar conductas positivas y disminuir conductas negativas o peligrosas.

Al ser el mundo de las TIC muy variado, dinámico y diverso, estableciendo pequeñas condiciones en el uso de las nuevas tecnologías a los niños a cambio de un compromiso por parte de los padres, se consiguen consolidar buenos hábitos al inicio del uso de los dispositivos TIC, desde la confianza mutua y la responsabilidad.

Los contratos de conductas es una técnica muy usada en pedagogía que ahora se está aplicando al mundo de las nuevas tecnologías con gran éxito, especialmente entre los alumnos de primaria.

Algunas recomendaciones de expertos:

→ [Decálogo de navegación segura de la Guardia Civil](#) (con explicación a cada recomendación):

→ [Consejos de seguridad de la Policía Nacional](#)

→ [Recomendaciones para padres de SegurKids](#):

→ [Recomendaciones para familias de Ciberfamilias](#)



## PROPUESTA 4. CONFIGURAR EL CONTROL PARENTAL DE UN ORDENADOR

### Descripción:

Proponemos una guía para poder configurar el Control Parental de Microsoft en los ordenadores con sistema operativo Windows 7.

El Control parental permite limitar el tiempo que los hijos pasan frente al equipo y controlar los programas y los juegos que pueden usar y cuándo hacerlo.

Además, se dejan indicaciones para aumentar el control en aquellos alumnos que hayan tenido conductas negativas en el uso de Internet.

### Destinatarios de la actividad:

Padres de alumnos en el inicio del uso del ordenador (segundo y tercer ciclo de Educación Primaria) o de alumnos que han tenido malas conductas en el uso del ordenador y se quiere limitar su uso (normalmente, primer ciclo de ESO coincidiendo con el inicio de la adolescencia). En este segundo caso, se recomienda hacerlo de forma paralela a una reeducación en el uso de las nuevas tecnologías.

### Recursos:

→ [Descarga este PPT](#) para ver todas las imágenes y gráficas que aparecen en este apartado a tamaño grande (pincha en la imagen):



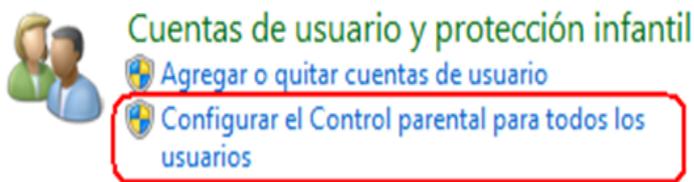


### Metodología:

Para activar el “Control Parental” que viene instalado en Windows 7, previamente debemos de tener una ID de Windows-Hotmail.

Los pasos a seguir son:

1°. Hacemos clic en el botón “Inicio”, después en “Panel de control” y, a continuación, en “Cuentas de usuario y protección infantil”. Hacemos clic en “Configurar el Control parental para todos los usuarios.” (Si se le solicita una contraseña de administrador o una confirmación, escribimos la contraseña o damos la confirmación):



2°. Haz clic en “Crear cuenta nueva de usuario”, que será la cuenta que creemos a nuestro hijo/a y la que podremos supervisar. Nos aparece un menú con las cuentas que tenemos en el ordenador y, entre otras, la que acabamos de crear. Marcamos la casilla “Supervisar cuenta” para esta última y damos a “Guardar”.

3°. Configuramos la cuenta pulsando en “familysafety.live.com”. Así, nos llevará a una ventana como la siguiente, desde donde podemos configurar todas las opciones que permite este control parental:

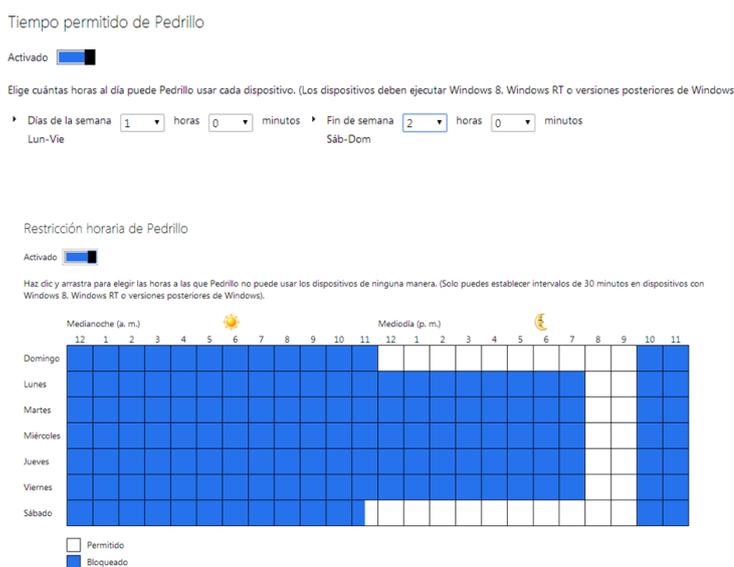


Algunos de los valores que se pueden ajustar son los siguientes:

**Límites de tiempo.** Podemos establecer cuánto tiempo al día y en qué horas queremos que nuestro hijo pueda conectarse. Es interesante negociar con ellos estos dos parámetros, explicando que tienen que realizar otras tareas a lo largo del día y que, además, no pueden conectarse a ciertas horas al ordenador, especialmente a las redes sociales (se ha demostrado que el *Grooming* comienza a altas horas de la noche).

La cantidad de tiempo y el horario debe adaptarse a la edad y madurez de nuestro hijo.

Por ejemplo, en las siguientes pantallas muestran cómo configurar 1 hora semanal y 2 los fines de semana, junto con el horario permitido (pincha [AQUÍ](#) para ver las imágenes en grande):





**Juegos.** Se puede controlar el acceso a los juegos, elegir los tipos de contenido que desea bloquear y decidir si desea permitir o bloquear juegos específicos o sin clasificar.

Permitir o bloquear programas específicos. Se puede impedir que los niños ejecuten determinados programas. Como en el caso de los juegos, si tratan de abrir un programa nuevo que necesitan al que no tienen acceso, con nuestra ID de Windows-Hotmail podemos permitirselo en pocos segundos.

Por último, Microsoft nos da tres sugerencias al inicio del uso del Control Parental, que son las siguientes (pincha [AQUÍ](#) para ver la imagen en grande):

Protección infantil de Microsoft

## Protección infantil

Tres sugerencias para empezar a usar Protección infantil

- 1** **Configurar Protección infantil en todos los equipos**  
Si tus hijos tienen acceso a varios equipos, deberías instalar y configurar Protección infantil en todos ellos. Si asocias todos los equipos que tu hijo usa con una cuenta, un solo informe reunirá toda la actividad de tu hijo.  
[Completar la configuración](#)
- 2** **Personalizar la configuración de tu hijo en línea**  
Con Protección infantil, puedes decidir los sitios web, las aplicaciones y los juegos que pueden usar tus hijos, además de cuándo y por cuánto tiempo pueden usar el equipo. También puedes cambiar o actualizar esa configuración en Internet en cualquier momento.  
[¿Cómo se personaliza la configuración?](#)
- 3** **Crear cuentas de Windows separadas**  
Cada uno de tus hijos debería tener su propia cuenta de Windows estándar. Así, con cuentas separadas, puedes controlar las actividades de cada uno en el equipo.  
[¿Por qué usar una cuenta estándar?](#)



4°. Para una mayor protección, Microsoft recomienda la instalación de dos programas:

**Windows Media Center:** este programa es un reproductor multimedia con todas las aplicaciones de cualquier reproductor, pero además permite bloquear el acceso a determinados tipos de vídeos y películas previa configuración.

**Windows Live Protección infantil:** este programa permite controlar qué páginas Web puede nuestro hijo consultar, con quién puede conversar mediante las redes Messenger, tener reportes de la actividad de nuestro hijo en Internet, etc.

5°. Además de las explicaciones anteriores, se pueden consultar los siguientes apartados, algunos con vídeos tutoriales (encontrarás los enlaces en la derecha):

Utilizar el control parental

Introducción a Windows Media Center

**Tiempo destinado al desarrollo:** 1 hora.

**Tiempo de preparación:** 2 horas.

El tiempo de preparación consiste en leer la información de los [enlaces](#) comentados en el desarrollo de la actividad.

→ [Windows Media Center](#) disponible en

→ [Windows Live Protección infantil](#) disponible en

- [Instalar "Windows live Protección Infantil"](#):
- [Configurar "Windows live Protección Infantil"](#):



### Experiencia previa en el desarrollo:

En las diferentes charlas dadas a los padres, una de las mayores inquietudes que tienen es la adicción que el uso de las nuevas tecnologías está generando a sus hijos. Mediante estos programas, de fácil instalación y configuración y con gran cantidad de información en la red de cómo utilizarlos, podemos limitar el uso del ordenador de forma automática, previa negociación razonada con nuestros hijos.

Si bien es mejor educar que prohibir, esta herramienta es adecuada para limitar el acceso a la red de aquellos chicos que hayan tenido malas conductas, en una fase de reeducación, gracias a la cantidad de filtros y de control de la actividad del chico.





# Evaluación

**PARA VALORAR** si se ha alcanzado los objetivos a través de las tareas propuestas, se realiza un proceso de autoevaluación, valorando de 1 (poco) a 5 (mucho) los siguientes indicadores:

Indicadores de autoevaluación	Valoración
Entiendo y comparto la idea de la responsabilidad de la educación en el uso de las nuevas tecnologías como un campo más de la educación que tengo que ofrecer a mis hijos.	
He analizado el tiempo que mis hijos dedican al uso de las nuevas tecnologías.	
Me he informado de las aplicaciones que suelen utilizar mis hijos en Internet y a través del móvil.	
Conozco los principales peligros potenciales de las aplicaciones que usan mis hijos	
He explicado a mi hijo los peligros a los que está expuesto en las redes sociales y en las aplicaciones de mensajería multimedia.	
He transmitido a mi hijo mi ayuda ante cualquier situación incómoda a la que se exponga.	
He comprendido las principales recomendaciones preventivas de seguridad que los expertos ofrecen en el uso de Internet.	
Me he informado cómo reaccionar si algún miembro de mi familia sufriera algún incidente a través de las nuevas tecnologías.	
He consensuado con mi hijo las normas de uso del teléfono, ordenador y tablet.	
He aprendido a manejar los programas de control parental de mi ordenador.	



# Webgrafía

**ADEMÁS DE** los recursos que hemos ofrecido a lo largo de esta guía, queremos destacar en este apartado una serie de enlaces que pueden ser muy útiles a los padres para obtener información y herramientas de educación en materia de seguridad en Redes Sociales:

BRIGADA DE INVESTIGACIÓN TECNOLÓGICA DE LA POLICÍA NACIONAL (28/04/2014), “BIT-Consejos de Seguridad”, [http://www.policia.es/org\\_central/judicial/udef/bit\\_conse\\_segurid.html](http://www.policia.es/org_central/judicial/udef/bit_conse_segurid.html)

GRUPO DE DELITOS TELEMÁTICOS, UNIDAD CENTRAL OPERATIVA, GUARDIA CIVIL (28/04/2014), “Decálogo de navegación segura”, <https://www.gdt.guardiacivil.es/webgdt/cusuarios.php>

OPTENET S.A. (01/04/2014), “Ciberfamilias”, <http://www.ciberfamilias.com/seguridad/>

AGENCIA CANARIA DE INVESTIGACIÓN, INNOVACIÓN Y SOCIEDAD DE LA INFORMACIÓN (28/04/2014), “Vive Internet”, <http://www.viveinternet.es/buen-uso/contrato-familiar-para-el-uso-de-internet>

MICROSOFT (28/04/14), “Protección infantil de Windows Live”, <http://www.microsoft.com/spain/windowslive/familysafety.aspx>



# Recursos

## PROTEGELES.COM

Destacamos esta página por su labor de prevención y formación en el uso seguro de Internet y las TIC. Tiene una sección muy interesante donde se proponen webs y otros materiales como vídeos, guías o folletos que tratan sobre temas como el acoso escolar en Internet, adicciones a las TIC, uso seguro de las redes y telefonía móvil, entre otros. Los vídeos son en su mayoría spots publicitarios para la sensibilización en el uso seguro de la red. Además podemos encontrar estudios sobre temas como el uso que los menores hacen de la red o los videojuegos.



## KIDDIA.ORG

Intenta responder a necesidades en cuanto a juegos relacionados con las TIC para niños y ofrece contenidos para que los padres y madres enseñen a sus hijos cómo manejar de forma segura las TIC. Su principal objetivo es educar y proteger a los menores en el uso de las TIC.

Tiene distintos apartados diferenciados para adultos y niños/as, además de ofrecer noticias interesantes sobre el uso de las TIC y un apartado dónde profundizar más sobre aspectos concretos.

También dispone de un foro con temas diferenciados dependiendo del tipo de usuario (niños/as, padres, madres y profesores). Resulta muy interesante, ya que sirve de orientación a los padres, en cuanto a la educación y protección de niños/as, ya en ocasiones se desconocen el uso apropiado de las TIC.





## MATERIALES DIDÁCTICOS CRFP



### LICENCIA CC



**Seguridad en Redes sociales en el ámbito educativo. Guía para padres** de Centro Regional de Formación del Profesorado is licensed under a [Creative Commons Reconocimiento-NoComercial 4.0 Internacional License](https://creativecommons.org/licenses/by-nc/4.0/).

Se puede copiar, distribuir y comunicar públicamente el contenido de esta publicación, así como hacer usos derivados de la misma siempre que no conlleve un uso comercial. Si el contenido se publica en un blog o sitio web, se debe enlazar el artículo original. Si se reproduce en un medio impreso, se debe hacer referencia expresa de la autoría y web original.

