

Tecnología

TU TECNOLOGÍA · CIBERSEGURIDAD · PRIVACIDAD · INTELIGENCIA ARTIFICIAL · INTERNET · GRANDES TECNOLÓGICAS · ÚLTIM

CIBERSEGURIDAD >

Del toque de queda digital al bloqueo de ‘apps’: cómo protegen los expertos en tecnología a sus hijos en internet

Seis expertos en ciberseguridad, protección de datos y ciberacoso explican a EL PAÍS cómo garantizar la seguridad de los menores en línea



Una niña mira el móvil bajo la supervisión de una persona adulta.
GIANLUCA BATTISTA



ISABEL RUBIO

23 ABR 2025 - 05:20 CEST

      5 

Desde hace dos décadas, las búsquedas en Google sobre “control parental” [no han parado de crecer](#). internet permite a los menores estar en contacto con amigos, acceder a información y desarrollar habilidades. Sin embargo, el mundo digital también conlleva riesgos, como la pérdida de privacidad, el ciberacoso, la suplantación de identidad, los fraudes y la exposición a contenido inapropiado. Mientras cada vez más padres buscan orientación sobre seguridad digital, los expertos en tecnología tienen una perspectiva privilegiada sobre los peligros y las soluciones en línea. EL PAÍS ha consultado a seis profesionales en ciberseguridad, protección de datos y ciberacoso para conocer qué medidas aplican y sus recomendaciones para las familias.

Elena Carrera Murciego, técnico de conocimiento y concienciación de menores del Instituto Nacional de Ciberseguridad (INCIBE)

Los hijos de [Elena Carrera Murciego](#), de nueve y 12 años, aún no disponen de sus propios móviles. “Usan el mío si necesitan comunicarse con algún compañero”, explica. Para las tareas escolares que lo requieran o el ocio, utilizan una tablet o el ordenador. En su casa, los dispositivos son “compartidos”: “No son suyos exclusivamente, sino que son un préstamo y siempre se usan en lugares comunes, como la cocina o el salón”. Si tienen que usarlos para alguna tarea escolar y lo hacen en sus zonas de estudio, la puerta permanece abierta.

En los dispositivos, tienen configurados controles parentales que bloquean el acceso a determinadas páginas web o a la descarga de aplicaciones. Los menores aún no tienen redes sociales y tienen un pacto con sus padres sobre el tiempo que dedican a las pantallas. [En la web de INCIBE sobre menores](#), las familias disponen de una sección con herramientas prácticas como [un modelo de pactos familiares](#), [vales de tiempo](#) para regular el tiempo de juego, [un organizador digital](#) para acordar normas y límites de uso, [un catálogo de](#)

[herramientas de control parental](#) y [talleres gratuitos](#) para promover el uso seguro de internet en la familia. Ante cualquier duda o problema, Carrera anima a recurrir al servicio gratuito [Tu Ayuda en Ciberseguridad](#) llamando al 017.

La experta recomienda conocer el entorno digital de los niños: “No se trata de que seamos informáticos, sino de conocer mínimamente las aplicaciones de moda, las que más les gustan, para qué las utilizan, con quién hablan en línea...”. Carrera enseña a sus hijos a aplicar las mismas precauciones en línea que en la calle. Les advierte sobre los riesgos en redes sociales y la importancia de proteger su privacidad. Les recuerda que las fotos son parte de su vida privada y “no hay que exponerlas”. “Si lo hacen, deben recordar que no debe aparecer nadie más que ellos sin su consentimiento y que van a perdurar en el tiempo, pase lo que pase, por lo que no pueden saber si en un futuro les perjudicarán”, explica.

La supervisión parental, según la experta, debe comenzar desde el primer contacto con la tecnología: “Cuando son pequeños, de tres a cinco años, hablamos de ‘acompañamiento’, compartiendo contenido de calidad y dando ejemplo con nuestras reacciones y comportamientos en línea”. A medida que crecen, es clave un uso con propósito, con tiempos cortos y conversaciones sobre su actividad digital. “Lo más importante es que tengan confianza para decirnos si tienen dudas, si les sale un aviso o reciben un mensaje extraño... que sepan que estamos ahí para escucharles y ayudarles”.

Francisco Pérez Bes, adjunto a la presidencia de la Agencia Española de Protección de Datos (AEPD)

[Francisco Pérez Bes](#) recuerda dos situaciones que le contaron sus hijos. Por un lado, la de un menor de 11 años que fue a jugar a casa de otro, que le sugirió hacerse fotos desnudo para subirlas a una plataforma. Por otro, la de unos niños que fueron a dormir a casa de un amigo, cuyos padres les dejaron una tablet sin supervisión, lo que permitió que accedieran a webs pornográficas. “Estas historias demuestran que los niños usan la tecnología para hacer cosas ‘de mayores’, sin ser conscientes de los riesgos en los que incurren”, señala el experto, que destaca que algunas familias provocan situaciones de riesgo por desconocimiento.

No está a favor de prohibir, ni de demonizar, pero sí defiende un uso

moderado y consciente. A sus hijos, de 11 y 12 años, les explica por qué existen contenidos inapropiados en internet y por qué no son adecuados para su edad. Además, les anima a compartir con él cualquier contenido inapropiado que encuentren, para poder analizarlo juntos y explicarles los recursos disponibles para denunciarlo y bloquearlo. “El objetivo último no debe ser controlar lo que hacen, sino asegurarnos de que comprenden el impacto y las consecuencias de sus acciones y son capaces de identificar y mitigar las situaciones de riesgo”, señala.

Pérez tiene un acuerdo con sus hijos para que jueguen en línea solo después de haber hecho sus tareas escolares. Establece un límite de tiempo —que puede ser de unos 15 minutos diarios— para que disfruten del juego y aprendan a gestionarlo. Además, no les permite usar pantallas antes de dormir ni navegar solos en casa. A las familias les aconseja consultar [*La guía que no viene con el móvil*](#), de la AEPD, que recoge consejos antes y después de entregar un móvil a un menor. Por ejemplo, fijar normas para que su uso no le quite tiempo de actividades clave como dormir o estudiar, configurar juntos los perfiles de redes sociales para que no todo el mundo pueda ver lo que publica, estar atentos a sus emociones tras un uso intensivo y establecer momentos sin tecnología.

Álvaro Orts Ferrer, abogado experto en privacidad e inteligencia artificial y director de Orts Consultores

Hasta hace poco, [Álvaro Orts](#) pensaba que el principal peligro para los menores en internet era el acceso a contenido inadecuado. Ahora, con la combinación de internet e inteligencia artificial, destaca que el problema se amplía a una gran proliferación de contenidos falsos. “Sin ir más lejos, hay contenidos de TikTok que me enseñan mis hijos que están descaradamente manipulados”, indica. Además, incita a pensar en otro hábito: “Estamos acostumbrando a nuestros hijos a preguntar a internet o a la inteligencia artificial cualquier cuestión que nosotros no le sabemos contestar, por lo que somos nosotros mismos los que estamos otorgando una sensación de que internet y la IA no se equivocan”.

Los hijos de Orts, de 9 y 13 años, usan el móvil y la tablet. Él utiliza la [app Google Family Link](#) para “organizar” el tiempo de uso de los dispositivos, restringir el acceso a determinadas aplicaciones y configurar el tipo de contenidos a los que se puede acceder. Además de controlar el “tiempo de exposición”, está atento al uso que los menores hacen de internet y las redes

sociales, así como a los juegos que descargan y a aquellos a los que dedican más tiempo.

A pesar de estas precauciones, Orts asegura que no monitoriza todo lo que sus hijos hacen en línea y no entra en sus cuentas para ver qué actividad han tenido. “No creo que sea lo ideal, ya que no sería un ejemplo muy sano para nuestros hijos, que podrían pensar que el control que ejercen sus padres es algo normal que pueden, con el tiempo, reproducir con su pareja y en sus relaciones personales”, afirma. Para él, la mejor forma de proteger a los menores es “ayudarles a saber discernir e identificar qué les puede hacer daño”. Para ello, evita imponer reglas o prohibiciones sin una argumentación y aprovecha el día a día para explicarles los posibles riesgos: “Si sale una noticia o vemos un contenido que acaban de ver, todo eso nos da pie a hablar de los riesgos de internet”.

Sara Antúñez, abogada penalista y presidenta de Stop Haters

[Sara Antúñez](#) es hermana de un adolescente de 12 años y [presidenta de la asociación contra el acoso en la red Stop Haters](#). Recuerda que, cuando su hermano tuvo acceso por primera vez a los dispositivos, le restringieron el acceso a internet para evitar que ingresara accidentalmente a contenidos inapropiados. Con el tiempo, fueron relajando las restricciones. “Cuando les damos su primer móvil, que normalmente es a los 11 años, tiene que haber un control exhaustivo, al menos durante el primer año, que debe ir relajándose paulatinamente”, afirma la experta.

Recuerda un día en el que su hermano estaba buscando información sobre el cuerpo humano para un trabajo de conocimiento del medio y apareció una página porno. Su táctica consiste en hablar con los menores sobre lo que pueden encontrar en la red: “Esto incluye hablar de pederastia, pornografía y otros temas que, aunque sean incómodos, deben tratarse”. “Es importante que conozcan que detrás de muchos chats online puede haber hombres adultos y que tienen que tener cuidado con su intimidad”, añade.

La madre del hermano de Antúñez supervisa tanto los sitios que visita su hijo como las personas con las que interactúa. Para restringir el acceso a contenido inapropiado y controlar el tiempo de uso, utiliza el control parental. Además, limita el uso de consolas y el tiempo que ve la televisión. Y

le da tres consejos fundamentales para su seguridad en la red: “No dar nunca datos personales ni contraseñas, no mandar fotos y no hablar con adultos o jóvenes que le saquen más de tres años”.

Marc Rivero, experto en ciberseguridad de Kaspersky

[Marc Rivero](#) es padre de un niño de 10 años. Considera que no es necesario ser un experto para tomar medidas efectivas de protección digital. Para él, la clave está en educar a los menores sobre los riesgos y cómo protegerse. “Uno de los consejos más importantes que doy es nunca compartir información personal, especialmente en redes sociales o aplicaciones de mensajería”, señala el experto, que recomienda a los padres consultar [los recursos de la iniciativa Familia Segura](#). A su hijo le explica, además, que “datos como la dirección de casa, el nombre del colegio o incluso fotos personales pueden ser utilizados de manera malintencionada por desconocidos”.

Del mismo modo, le enseña a no aceptar solicitudes de amistad o mensajes de personas que no conoce y a identificar situaciones sospechosas, como mensajes que le piden descargar archivos, hacer clic en enlaces o compartir contraseñas. “También le animo a contarme cualquier situación que le haga sentir incómodo o inseguro, sin miedo a ser juzgado o castigado”, añade.

Según el informe [Estar en línea: niños y padres en internet](#), el 38% de los menores en España pasa entre una y dos horas diarias en internet, mientras que un 30% permanece conectado más de dos horas. Por este motivo, Rivero aconseja establecer acuerdos familiares claros sobre el uso de dispositivos, involucrando a los niños en el proceso para que comprendan el porqué de las reglas. Por ejemplo, sugiere fijar un “toque de queda digital” o designar momentos libres de pantallas, como las comidas o las horas previas a dormir. Las herramientas de control parental también “son una gran ayuda”: “El objetivo no es espiar o invadir la privacidad de los niños, sino garantizar su seguridad y bienestar digital”.

Josep Albors, responsable de Investigación y Concienciación de ESET España

[Josep Albors](#) no es padre, pero ha enseñado a muchos progenitores sobre los riesgos de internet. Desde hace más de una década, realiza ponencias y talleres dirigidos a menores y padres en centros educativos, congresos de

ciberseguridad y otros eventos. En ellos, explica que los menores pueden acceder a contenido inapropiado de manera voluntaria o involuntaria, por lo que es crucial que sepan cómo reaccionar adecuadamente si se topan con él.

Por este motivo, resulta vital “realizar un acompañamiento activo para que aprendan que está bien y que está mal en internet”. A los padres les recomienda [los recursos online que ofrece el INCIBE en su apartado para familias](#) o aquellos de [empresas especializadas en ciberseguridad](#). El experto advierte que abusar de un control estricto puede ser contraproducente, ya que genera desconfianza hacia los padres, lo que podría llevar al menor a buscar maneras de eludir ese control o a utilizar los dispositivos sin supervisión.

El tiempo que los menores dedican a las pantallas se puede controlar de forma activa o pasiva. “Si usamos una herramienta de control parental o configuramos, por ejemplo, nuestro *router* doméstico para que desconecte los dispositivos que queramos durante ciertas horas, estaremos haciendo un control pasivo”, comenta. Un control activo es aquel en el que “nosotros controlamos personalmente el tiempo y, si es posible, garantizamos que el uso de los dispositivos se realice en una sala común, fomentando que los niños acudan a nosotros cuando tengan alguna consulta”.

SOBRE LA FIRMA



Isabel Rubio

VER BIOGRAFÍA

Recibe cada semana el boletín de Tecnología



COMENTARIOS - 5

[Normas ›](#)

MÁS INFORMACIÓN



Un estudio señala los peligros que supone la IA para la salud mental de niños y adolescentes

RAÚL LIMÓN
