Sé ciberinteligente:

Consejos para mantener a tus hijos a salvo en la red

kpmg.es

2021

Introducción

Niños y jóvenes de todas las edades, utilizan a diario sus dispositivos para aprender, jugar o interactuar con los amigos.

Este incremento del tiempo de consumo de Internet y uso de pantallas tras la pandemia, suma una preocupación más a los padres y tutores.

¿Cómo pueden comprobar los padres y tutores que sus hijos están seguros en Internet y que están tomando las decisiones adecuadas en este entorno?

Habla sobre seguridad en Internet e involúcrate

- Mantén conversaciones con tu hij@ sobre la seguridad en la red. Explícale por qué es importante tener cuidado en el entorno *online.*
- Enséñele a usar contraseñas seguras, a identificar cuándo las páginas web son seguras o está ante una estafa, a comportarse adecuadamente en Internet y cualquier habilidad básica que le permita desenvolverse con seguridad en la red.
- Revisa la actividad de Internet y las cuentas de redes sociales de tu hij@.
- Pregunta a tu hij@ qué hace en la red, qué sitios visita y con quién habla.
- Practica con el ejemplo respecto al uso que haces de las nuevas tecnologías.

Sé ciberinteligente

Ten en cuenta estos seis consejos para que tu hij@ esté seguro en Internet.

1. Establece algunas normas básicas

Establece límites sobre cuánto tiempo puede tu hij@ pasar en la red y qué puede hacer.

El tiempo de uso de pantallas no relacionado con las tareas escolares puede restringirse a después de terminar de estudiar, o a los fines de semana. Es recomendable que los ordenadores estén en una zona común y también supervisar la actividad en Internet de los hij@s.

2. Supervisa su acceso a Internet

Ajusta los controles parentales de acuerdo con la edad y madurez de tu hij@. Estar atento a lo que tu hij@ hace mientras está conectado te ayudará a protegerle. Confirma con tu hij@ qué sitios webs son apropiados para su edad.

3. Enséñale a no facilitar información personal

Recuerda a tu hij@ que nunca debe dar información personal, como su nombre completo, dirección, contraseñas, ubicación o número de teléfono a un desconocido en Internet, ya sea a través de redes sociales o en entornos de juegos *online.* Para mantener su información personal a salvo, pídele que cree contraseñas diferentes para cada cuenta que tenga en Internet, y que esté alerta para detectar cualquier actividad sospechosa.

Sé ciberinteligente

Ten en cuenta estos seis consejos para que tu hij@ esté seguro en Internet.

4. Cuidado con los desconocidos

Habla con tu hij@ de los riesgos de interactuar con extraños, ya sea a través de las redes sociales, foros de debate o juegos *online.* Enséñale a no aceptar nunca conocer a alguien fuera del chat.

5. Anímale a pensar dos veces antes de publicar

Enseña a tu hij@ a ser consciente de los comentarios y las fotos que publica en Internet. Explícale que, una vez que están publicados, permanecerán en Internet o en el ciberespacio de forma permanente. La huella digital es especialmente importante cuando los jóvenes crecen y buscan trabajo; muchas empresas hacen una búsqueda básica *online* de posibles candidatos. Habla con tu hij@ sobre su configuración de privacidad social y enséñale la diferencia entre salas de chat privadas y públicas.

6. Enséñale a identificar a un acosador

Habla con tu hij@ y edúcale para que te informe inmediatamente de posibles comentarios ofensivos que vea publicados en la red.

Si sospechas que está siendo acosad@ por Internet, mantén una comunicación fluida con él/ella, de modo que se sienta cómod@ diciéndote si está siendo objeto de esos comportamientos. Además, recuérdale que tenga cuidado con lo que dice, envíe, publique o incluye en blogs. Leer o reenviar mensajes da alas a los acosadores y aumenta el daño a las víctimas.

Juegos *online*

- Determina qué juegos son adecuados para la edad de tu hij@.
- Asegúrate de que tu hij@ conoce qué conversaciones son aceptables mientras juega con desconocidos.
- Fija normas sobre el tiempo que pueden jugar *online* y los juegos permitidos.
- Asegúrate de que tu hij@ entiende qué información es personal, y de que nunca debe compartirla durante el juego ni en la red.

Redes sociales

**La mayoría de las plataformas de redes sociales tienen restricciones de edad para crear cuentas. Asegúrate de seguir las pautas de restricción de edad y supervisar su uso.*

- Enseña a tu hij@ a pararse a pensar antes de publicar comentarios o imágenes, y a no compartir nunca información personal como su edad, colegio, dirección o su nombre completo.
- «Hazte amig@» de tu hij@ o «síguel@» para que puedas ver su actividad en las redes sociales. No es necesario que participes, simplemente echa un vistazo con la mayor frecuencia posible.
- Consulta páginas de orientación para padres en redes sociales y trabaja con tu hij@ para establecer la configuración de privacidad que mejor le proteja.
- Los datos proporcionados a una red social se almacenan y, la mayoría de las veces, se comparten por defecto. Asegúrate de que el perfil de tu hij@ esté configurado como "privado". Entra en la configuración y ayúdale a ajustar los controles predeterminados.

Ciberacoso

Comunicación

Habla con tu hij@ y enséñele a:

- Informarte inmediatamente sobre comentarios ofensivos o hirientes que vea publicados en la red, tanto si es contra él/ella, como si no.
- Tener cuidado con lo que dice, envía, publique o incluye en blogs sobre otras personas: el acoso no intencionado no deja de ser acoso.

Reconocimiento

Indicios de estar sufriendo ciberacoso:

- Enfado, depresión o frustración inesperadas después de usar cualquier dispositivo, o por el hecho de dejar de usar cualquier dispositivo.
- Inquietud ante el hecho de ir al colegio o participar en actividades de equipo.
- Aislamiento anormal con respecto a amigos habituales y miembros de la familia.

Acción

Es fundamental actuar de forma adecuada:

- Guarda comentarios/publicaciones/ correos electrónicos.
- No contestes y no los borres.
- Informa de la ID *online* (reporta como spam) y bloquea al usuario para evitar nuevas interacciones.
- Comunica el incidente al colegio o instituto de tu hij@ o a la policía si es necesario.

Clases en remoto

- Si tu hij@ necesita abordar sus clases en remoto, sigue las pautas de las clases a distancia de su colegio o instituto.
- Prepara a tu hij@ y ayúdale a llevar la agenda de tareas diaria.
- Familiarízate con el uso de la tecnología y asegúrate de que las aplicaciones de formación que utiliza tu hij@ estén actualizadas.
- Procura crear un entorno similar al del colegio o instituto, con un espacio dedicado al aprendizaje.
- Asegúrate de que tu hij@ tiene todos los materiales necesarios para realizar sus tareas.
- Recuerda a tu hij@ que mantenga la cámara web cubierta cuando no la esté usando.
- Ayúdale a estar motivado mientras estudia en remoto.
- No te olvides de programar tiempo de ocio para tu hij@.
- Procura que tu hij@ combine el tiempo de consumo de pantallas con medios de aprendizaje tradicionales, como la lectura de libros de texto, la toma de notas, etc.

¿Qué puedes hacer?

No tienes que ser un profesional de la ciberseguridad para proteger el ordenador de tu hij@ y su conexión a Internet.

Muchos dispositivos, ordenadores y routers Wi-Fi vienen con controles parentales integrados que a menudo se pasan por alto durante la configuración inicial, y que son muy fáciles de usar. Estos controles permiten establecer tiempos de acceso, controlar la actividad en Internet y bloquear categorías de sitios web. Estar atento a lo que tu hij@ hace mientras está conectado te ayudará a protegerlo.

Puedes utilizar los **controles parentales** para evitar que tu hij@ acceda a sitios web inapropiados y aplicarlos de forma general y a dispositivos concretos.

El **horario de Internet programado** se puede usar para restringir el acceso de tu hij@ a Internet en determinados horarios, como después de hacer los deberes, o los fines de semana.

Registrar y supervisar la red te permitirá revisar la actividad de tu hij@ en Internet para asegurarte de que está utilizando la red de forma segura. Revisa con tu hij@ qué webs son adecuadas para su edad.

El **antivirus** puede servir como la última línea de defensa para proteger tu ordenador y la información almacenada de virus peligrosos y otros tipos de *malware.*

Información adicional

Informándote podrás educar mejor a tus hijos, inculcándoles y reforzando buenos hábitos en Internet. Los siguientes recursos *online* pueden ser útiles para educarles sobre cómo estar seguros en Internet y cómo ser un buen ciberamigo, no un acosador.

- Contacta con la Policía Nacional si sufres o conoces algún caso de acoso escolar: 900 018 018; seguridadescolar@policia.es
- Policía Nacional: Plan director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos: https://www.policia.es/_es/colabora_participacion_plandirector.php
- Ministerio de Sanidad, Consumo y Bienestar Social - Instituto de la Juventud: Guía de actuación contra el ciberacoso: http://www.injuve.es/sites/default/files/Gu%C3%ADa%20de%20actuaci%C3%B3n%20contra%20el%20ciberacoso.pdf
- Agencia Española de Protección de Datos: Protección de datos personales menores: https://www.tudecideseninternet.es/aepd/
- Instituto Nacional de Ciberseguridad – Internet Segura For Kids: https://www.is4k.es/

home.kpmg/socialmedia

Diseñado por Evalueserve.

Nombre original de la publicación: Be cyber Smart: Tips to keep children safe online

Número de publicación: 137021b-G Fecha de publicación: Octubre de 2020