



# 5 Situaciones del mundo digital

EN LAS QUE DEBES AYUDAR A TU HIJO





## **Los niños de hoy son nativos digitales. ¿Qué significa esto?**

Básicamente nacieron cuando la tecnología ya era popular y ocupaba una gran porción de nuestra vida diaria. Obviamente, esta característica facilita que tengan un vínculo más fluido y cercano con Internet y la tecnología; en el mismo sentido, es muy posible que siempre sepan más de este mundo que tú (o por lo menos que te sorprendan con cosas que tú no conocías y ellos sí). No obstante, eso no implica que sepan cómo cuidarse y protegerse en Internet.

Por este simple motivo, los padres y adultos siempre seremos los guías, puesto que nuestro trabajo es el de aconsejar y enseñar cómo deben manejarse en la red para aprovecharla sin caer en engaños o resultar víctimas de ataques cibernéticos.

Desde Digipadres, queremos ser tus acompañantes en esta desafiante tarea de aprender sobre seguridad para extender ese conocimiento a los chicos. Y en esta ocasión, vamos a compartir un listado contigo sobre ciertas situaciones en las cuales debes ayudar a tu hijo y nunca dejarlo solo.

# 1

## USO DE CONTRASEÑAS

**La mejor analogía para entender lo que representan las contraseñas, es pensarlas como la llave de la casa.** En este sentido, cuanto más robustas y complejas sean, más difícil será que un atacante pueda robarlas o adivinarlas para ingresar a un servicio en línea, lo que representaría la casa.

En este sentido, debes estar junto a tu hijo al momento de crear su primer contraseña, dado que solo ahí le podrás explicar in situ cómo es la mejor forma de hacerlo y por qué es algo muy importante. Las recomendaciones son muchas: más de diez caracteres, números, letras, mayúsculas, minúsculas y caracteres especiales son algunas de ellas; pero quizá la más importante es que la clave en cuestión debe ser fácil de recordar y difícil de adivinar. Por ende, una buena idea es usar una frase que remita a algún personaje o programa de TV que sea fácil de recordar para tu hijo.

Si quieres saber más sobre contraseñas fuertes, visita este enlace de [WeLiveSecurity](#).



La clave en cuestión debe ser fácil de recordar y difícil de adivinar.

# 2

## REDES SOCIALES Y VIDEOJUEGOS SEGUROS

**Las redes sociales y los videojuegos son los espacios digitales que más reúnen a los niños en la actualidad.** Allí no solo pueden relacionarse con sus amigos y extender los momentos de divertimento, sino que también pueden aliarse en foros y redes LAN a otros usuarios para jugar y cumplir las misiones de algún juego de mundo abierto o de estrategia.

En este sentido, es importante que cuando tu hijo comience a usar este tipo de servicios le indiqués algunas cuestiones básicas de seguridad para que siempre esté protegido. Hablamos, por ejemplo, de que no debe aceptar contactos que no conozca, o que las personas de los foros no son realmente sus amigos como para que los agregue a sus perfiles y, así, evitar posibles casos de grooming. En el mismo sentido, hay que tener cuidado con actitudes de cyberbullying a otros amigos o compañeros, especialmente para no fomentarlas y magnificarlas.

Particularmente en el caso de los videojuegos, debes hablar con él para explicarle por qué no debe usar copias piratas, ni desactivar la solución de seguridad para reducir el impacto en el sistema. Si quieres saber más sobre este tema, puedes leer un [post dedicado](#) en **WeLiveSecurity**. Asimismo, si tu hijo todavía no juega en línea o utiliza las redes sociales más conocidas, es ideal que leas sobre [Bunis](#), un buscador seguro; [YouTube Kids](#), la versión para niños de YouTube; y otras [cinco redes sociales](#) para los más chicos.



Debes hablar con él para explicarle por qué no debe usar copias piratas, ni desactivar la solución de seguridad

# 3

## FOTOS Y GEOLOCALIZACIÓN

**Continuando con las redes sociales, un punto que hay que tratar por sí mismo es el de las fotos, particularmente para referirnos a la privacidad.** En este sentido, debes estar con él al momento de configurar la privacidad de sus cuentas, de modo que todos los contenidos que publique solo puedan ser vistos por sus amigos o aquellas personas que tú y tu hijo quieran.

En la misma línea, es ideal que desactives las funciones de geolocalización de tus tabletas o teléfonos inteligentes, de modo que al sacar una foto no quede registrada la posición de GPS donde se capturó.



Al sacar una foto no quede registrada la posición de GPS donde se capturó

# 4

## ACTUALIZACIONES DE APPS Y PROGRAMAS

**Las actualizaciones son muy importantes para todos los usuarios, niños y mayores por igual.** Siempre es importante estar atentos a ellas, dado que no solo ofrecen mejoras en los programas, sino que también se utilizan para corregir errores de programación, algo que se conoce como “parchear” posibles agujeros de seguridad.

Si tú lo tienes en cuenta, debes mostrárselo a tu hijo y explicar por qué nunca debe desear las notificaciones de actualización sin prestarles su debida atención. Una buena recomendación, es configurar los equipos para que se actualicen automáticamente, para así tener que evitar los momentos en los cuales no se pueden usar las apps e, incluso, tener que revisar qué actualizaciones están disponibles.



---

Una buena recomendación, es configurar los equipos para que se actualicen automáticamente

# 5

## PERMISOS DE APPS Y SOFTWARE

**Al momento de descargar una aplicación a la tablet o al smartphone siempre sentimos una cierta ansiedad, especialmente para poder ejecutarla y jugar a ese juego o usar tal servicio.** En los niños, esta sensación se magnifica, dado que su objetivo (en la gran mayoría de las veces) es el entretenimiento y la diversión, por lo que es casi imposible que lean lo que están haciendo o instalando.

Esto, lamentablemente, es peligroso dado que algunas apps requieren muchos permisos innecesarios que pueden poner en riesgo la privacidad de los chicos; y ahí es donde debes estar atento. Leer los permisos que piden los aplicativos es vital, ya que en algunas ocasiones verás que muchos no son importantes para dicho aplicativo y no debes de aceptarlos. Un ejemplo categórico que hemos visto, es el de algunas aplicaciones de calculadoras que piden permiso para utilizar la cámara de fotos.

Solo comprendiendo esto podrás transmitírselo a tus hijos para que también lo tomen como una costumbre cada vez que descargan e instalan un programa.



Algunas apps requieren muchos permisos innecesarios que pueden poner en riesgo la privacidad de los chicos



**Esperamos que esta lista haya sido de tu interés y puedas inculcarla en los hábitos de tu familia.** Tal como mencionamos, estas prácticas son cruciales para la seguridad de todos los usuarios, de modo que si tú las aplicas con rigor en tu vida digital, te será más fácil comunicárselas a tu hijo para que él pueda hacerlo también.

Como siempre te recordamos, ser un **Digipadre** no implica limitar o restringir el acceso a la tecnología, sino guiar y ayudar a los niños en ese camino de aprendizaje para que ellos puedan ser conscientes de lo que hacen allí y los riesgos que pueden encontrar.





SER PADRES ES MÁS FÁCIL CON ESET

[www.digipadres.com](http://www.digipadres.com)

