Digipadres

UNA INICIATIVA DE saferkidsonline by eset

Aulas Modernas:
¿cómo proteger la tecnología de tus hijos?

¿Cómo está cambiando la tecnología en el aula moderna?

Y lo que es más importante, ¿qué podemos hacer para protegerla?

¿Cómo es un aula tecnológica?

Antes de entrar de lleno en las tecnologías que todo padre debería conocer, es necesario **entender cómo encajan en el aula moderna**. Muchos padres recuerdan épocas en las que la tecnología en las aulas no iba más allá de un proyector, una radio y quizás una computadora personal.

Hoy en día, la mayoría de los profesores utilizan computadoras portátiles suministradas por la escuela para dar clase. No sería de extrañar que los alumnos lo sigan desde otros equipos portátiles que se guardan en el aula. El conjunto de computadoras portátiles podría complementarse con otros elementos, como pizarras inteligentes, reproductores multimedia de streaming e impresoras.

Y por supuesto, también están *los smartphones personales de los alumnos*. **Todo tipo de conectividad.**

La mayoría de estos dispositivos, si no todos, están conectados a alguna red. Según *EducationSuperhighway*, el 99% de las escuelas estadounidenses cuentan con conexión a Internet de fibra escalable y más de 43 millones de estudiantes tienen conexión a Internet. Esto significa que los alumnos pueden utilizar los dispositivos para acceder a páginas web, programas de software de colaboración y otras aplicaciones, más allá de que asistan a la escuela en forma presencial o desde casa.

¿Cuáles son las tecnologías que se suelen usar en las aulas y cómo mantenerlas seguras?

Lamentablemente, no existe una solución universal y 100% infalible para proteger a los niños que usan tecnología. Por ejemplo, el hecho de que el smartphone de tu hijo bloquee el acceso a contenido de sitios web inapropiados **no significa que el smartphone de su compañero también lo haga**.

Entonces, **¿cómo podemos mantener a nuestros hijos seguros mientras usan la tecnología del aula?** La mayoría de los padres ya deberían estar familiarizados en gran medida con las leyes pertinentes, en particular con la Ley de Derechos Educativos y Privacidad de la Familia, y la *Ley de Protección de la Privacidad de los Niños online de 1998.* Aunque se da por sentado que las tecnologías utilizadas en las aulas cumplen con estas leyes, vale la pena confirmarlo con cada institución. Además, te recomendamos que te familiarices con algunas de las *mejores prácticas para mantener a tus hijos seguros online.*

Por último, haz una lista de los dispositivos, el software y la tecnología que tus hijos utilizan a diario. La mayoría de ellos pertenecerán a las siguientes **cinco categorías**:

1 Equipos portátiles, tabletas y smartphones

Según el mismo informe de EducationSuperhighway citado anteriormente, *el 87% de los profesores dicen* que utilizan los medios de aprendizaje digital en sus aulas varias veces a la semana. Aunque hay muchas modalidades, los dispositivos predominantes son tres: los equipos portátiles, las tabletas y los smartphones.

En el caso de los dispositivos suministrados por la escuela, **comprueba que la institución cuente con una política de seguridad para supervisar el acceso y controlar el contenido**. Además, deberías hacerles algunas preguntas como:

? *¿Cuánto tiempo pasan los alumnos frente a la pantalla en el aula?* ¿Es demasiado?

? Cuando los alumnos están en la escuela, ¿se les permite utilizar los dispositivos para acceder a Internet, comunicarse con otros o incluso participar en las actividades del aula?

? ¿Pueden llevarse los dispositivos a casa?

Las respuestas a estas preguntas determinarán qué acciones deberás tomar para proteger esos dispositivos. En el caso de los dispositivos personales, como los smartphones, considera la posibilidad de instalar una *solución de seguridad para dispositivos móviles* con el fin de **controlar el uso que tu hijo hace de los dispositivos** tanto dentro como fuera de la escuela.

Otros dispositivos comunes en el aula:

- **Pizarrones inteligentes**
- **Smart TVs y reproductores multimedia de streaming (Apple TV, por ejemplo)**
- **Dispositivos de fitness para controlar la actividad física**
- **Parlantes y cámaras**
- **Microscopios digitales**
- **Impresoras y escáneres**
- **Proyectores y cámaras de documentos**

2 Sistemas de gestión del aprendizaje

Una vez que tienen los dispositivos en la mano, ¿a qué se conectan los estudiantes? Descubrirás que el sistema de gestión del aprendizaje conforma, al menos, **una parte de la experiencia diaria de tu hijo en el aula**. Un sistema de gestión del aprendizaje es un programa de software al que se puede acceder desde cualquier dispositivo o navegador web. Los alumnos y profesores utilizan estos sistemas para cargar documentos y acceder a ellos, programar los deberes, calificar las pruebas y mucho más.

La mayoría de estas herramientas se consideran bastante fiables por la ausencia de anuncios y de spam, así como por su acceso seguro. No obstante, ciertas plataformas como Google Classroom tienen tableros de mensajes que **son difíciles de moderar**, y que a menudo dan espacio para que los estudiantes **envíen mensajes inapropiados**. Más que proteger el sistema de gestión del aprendizaje de sus hijos, los padres deberían guiarlos en su uso correcto y conversar con ellos sobre el comportamiento aceptable a la hora de enviar mensajes, compartir archivos e interactuar de otra manera a través de la plataforma.

Sistemas de gestión del aprendizaje más comunes:

- Canvas
- Clever
- Classcraft
- Google Classroom
- Schoology

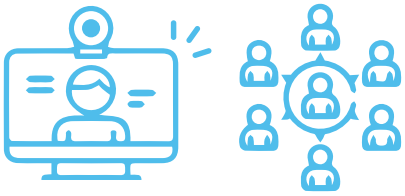
3 Correo electrónico

Queremos pensar que la mayoría de las comunicaciones por mensajería instantánea o correo electrónico se realizan en un entorno más controlado, como a través del sistema de gestión del aprendizaje. Sin embargo, no es raro que **los alumnos tengan sus propias direcciones** de correo electrónico y las utilicen para comunicarse con los profesores y otros alumnos.

En primer lugar, enséñale a tu hijo las mejores prácticas de seguridad y a identificar las amenazas provenientes del correo electrónico. El *Phishing*, por ejemplo, sigue siendo una de las principales amenazas de seguridad en el correo electrónico. Compartir contraseñas, información personal e incluso archivos multimedia confidenciales como fotografías es otra vulnerabilidad común del correo electrónico. Por último, muchos niños no saben que no deben abrir archivos sospechosos o desconocidos. **Charla con ellos sobre todos estos temas y enséñales a que piensen dos veces o te consulten antes de hacer clic en algo o compartir información por correo electrónico**.

Una opción es que los mismos padres creen la cuenta de correo electrónico de sus hijos. Ve más allá de los proveedores comunes, como Gmail, *y busca proveedores de correo electrónico para niños* que incluyan capas adicionales de protección.

4 Plataformas de video, colaboración y aprendizaje social



Independientemente de que el aula de tu hijo sea 100% presencial, 100% aprendizaje a distancia o una combinación de ambos, es muy probable que incluya algún tipo de tecnología de video, colaboración y aprendizaje social. Las soluciones de videoconferencia como Zoom, por ejemplo, se utilizaron en gran medida durante la pandemia para llevar a cabo la educación a distancia; **en algunos casos, Zoom pasó a ser el aula**.

En muchos sistemas de gestión del aprendizaje, plataformas de colaboración y de aprendizaje social, el video es una de las formas que tienen los estudiantes para compartir sus trabajos, hacer comentarios o incluso enviar mensajes. Las soluciones como *Flipgrid* y *Padlet* son ejemplos de las llamadas plataformas de aprendizaje social, **en las que los estudiantes pueden compartir sus trabajos e interactuar con el trabajo de otros**, todo moderado por el instructor (admiten videos pesados).

Las dos principales preocupaciones de seguridad para las plataformas de video, colaboración y aprendizaje social son **el acceso y la moderación**. Controlar el acceso a estas plataformas debería ser una prioridad. Por ejemplo, aunque las aulas de Zoom se pueden proteger con una contraseña, no son inmunes a las intrusiones no deseadas (*Zoombombing*). Moderar lo que se comparte, se dice o se envía en estas plataformas también puede ser todo un desafío. Recomendamos buscar soluciones que **ofrezcan mecanismos de protección para acceder y compartir, así como funcionalidades sólidas para moderar las interacciones de los estudiantes.**

5 Juegos

Una de las tendencias más recientes es la gamificación en el aula. En lugar de depender de los libros de texto, las escuelas están recurriendo a programas de software interactivos y divertidos que fomentan una mayor participación de los alumnos. Soluciones como *Gimkit* o Kahoot! ofrecen una variedad de juegos y actividades en las que los estudiantes ganan puntos, insignias y suben de nivel al participar. Si bien las preocupaciones de seguridad relacionadas con estas plataformas son menos importantes que las demás, no deja de ser una tecnología moderna para el aula que los padres deben conocer.

Para terminar, mantente al tanto y actúa proactivamente

Cuando se trata de la seguridad de los niños en el aula moderna, **la concientización gana la mitad de la batalla**. Si bien esta lista de recursos tecnológicos modernos para el aula es bastante detallada, la tecnología seguirá evolucionando a un ritmo vertiginoso. Los padres pueden contribuir en gran medida a proteger a sus hijos simplemente **manteniéndose al día con lo que ocurre y lo que sus hijos usan en el aula**.

Más allá de estar informados y ser conscientes, los padres pueden educarse a sí mismos y a sus hijos *sobre las mejores prácticas de seguridad para estar online*. Estas mejores prácticas se aplican sin importar la tecnología, el dispositivo o la interfaz empleada, y sin importar qué tan rápido evolucione la tecnología.

Finalmente, los padres pueden valerse de *soluciones de seguridad creadas especialmente para mantener a los niños seguros* mientras usan sus dispositivos personales. Muchas escuelas ya protegen sus propios dispositivos, incluyendo los que entregan a los estudiantes. De todas formas, los padres pueden añadir otra capa de protección a los dispositivos personales que los niños usan para conectarse desde casa.

Una vez más, lo principal es que los niños **se conecten al aula, aprendan eficazmente y se mantengan seguros**. La presente guía te ayudará a lograr estos tres objetivos mientras el mundo va volviendo a clase.

Queremos que más **Digipadres** potencien a los niños
y les enseñen a navegar seguros.

¿Estás listo para acompañarnos en este desafío?

www.digipadres.com