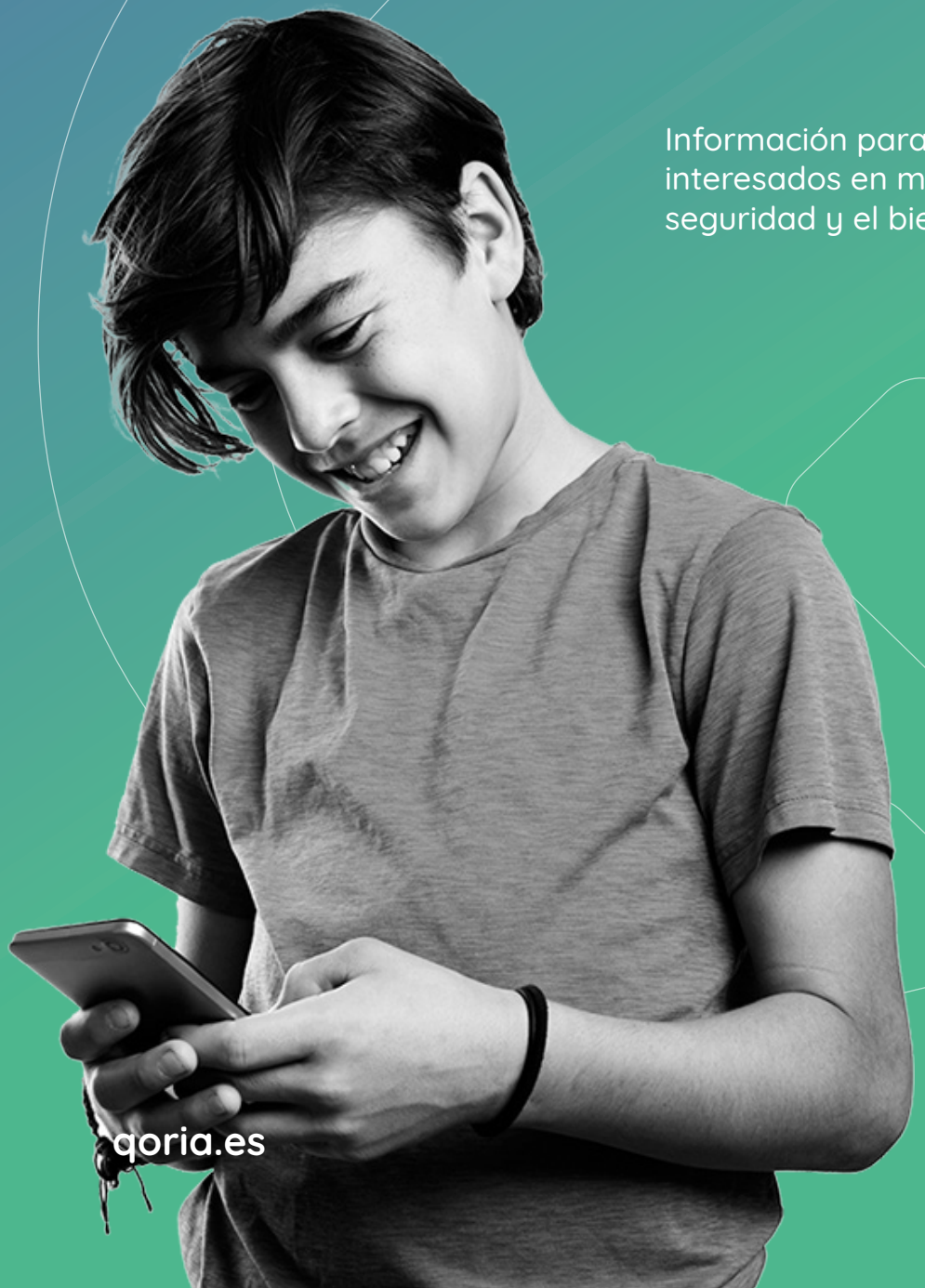
Qoria Insights

Los desafíos ocultos de la política BYOD en centros educativos

Información para los colegios interesados en mejorar la seguridad y el bienestar digital.



qoria.es

Qoria Spain

Contenidos

Introducción

A lo largo de los últimos 10 años, nuestra percepción de cuál debe ser el papel de los ordenadores portátiles y otros dispositivos electrónicos en el aula ha experimentado un cambio radical.

En la actualidad, ya no son meras plataformas para acceder a la información que los docentes utilizan periódicamente para reforzar los conocimientos de los alumnos en Internet, sino que se han convertido en un componente esencial de casi todas las asignaturas y se utilizan de forma constante a lo largo del día. Conscientes del papel fundamental que juegan estas plataformas digitales en el proceso de aprendizaje, y ante la imposibilidad de obtener una financiación estable por parte del gobierno que les permita costear sus proyectos tecnológicos, muchos centros han terminado adoptando un modelo ampliamente utilizado denominado BYOD —por las siglas en inglés de la expresión inglesa Bring your Own Device (Trae tu propio dispositivo)—.

Con frecuencia, los colegios han apostado por este tipo de programas principalmente por los supuestos beneficios que conllevan, como la posibilidad de aprovechar la familiaridad de los estudiantes con sus dispositivos personales y la reducción de costes que suponen de cara al centro.

Sin embargo, los costes ocultos del modelo BYOD pueden tener un impacto negativo en aspectos como la actividad docente, el aprendizaje, el soporte técnico y la seguridad. Estos desafíos acentúan claramente las diferencias socioeconómicas entre los alumnos, generan problemas de compatibilidad entre los dispositivos, incrementan la presión sobre los departamentos de TI y, lo que es más importante, derivan en una preocupante ausencia de visibilidad sobre la actividad de los estudiantes en Internet.

Aunque es posible que proteger a los alumnos no sea tu principal función como responsable de TI, este departamento desempeña un rol cada vez más relevante a la hora de apoyar y formar al personal encargado de su seguridad. Por ello, si te estás planteando la posibilidad de implementar un programa 1:1 en tu colegio o te preocupan las carencias de la política BYOD que utilizáis actualmente, esta guía te ayudará a entender por qué migrar a un modelo basado en dispositivos administrados os permitirá alcanzar un nuevo estándar de seguridad y bienestar digital.

Los programas BYOD: una introducción al modelo

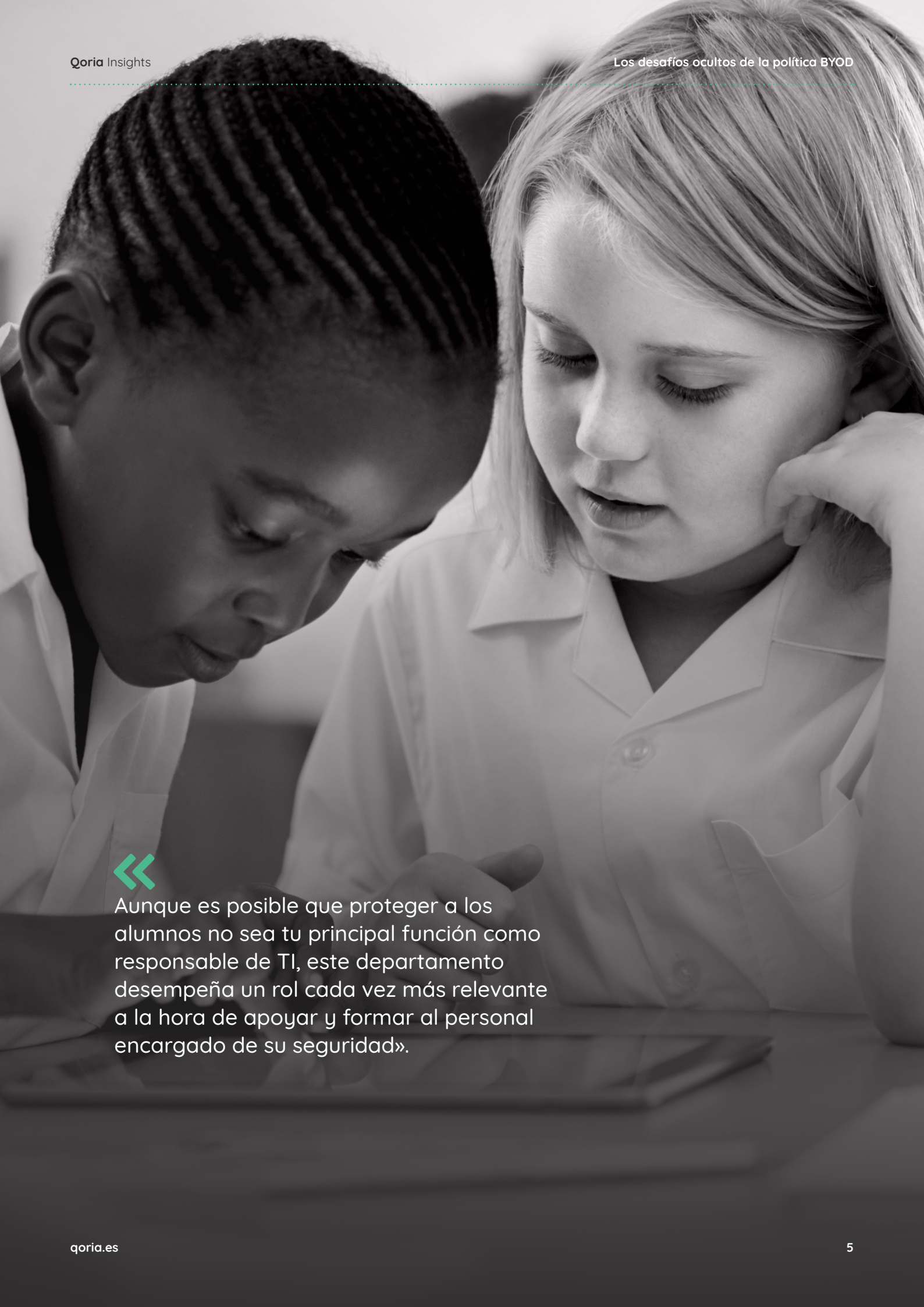
Antes de iniciar nuestro análisis, veamos cuál es la diferencia **entre las políticas BYOD y los programas 1:1.**

Los programas BYOD están diseñados para aprovechar la familiaridad de los estudiantes con la tecnología y minimizar los costes permitiéndoles que lleven sus propios dispositivos al colegio.

Por su parte, los programas 1:1 adoptan un enfoque diferente en el que se proporciona a cada alumno un dispositivo dedicado gestionado por el colegio, que es quien se responsabiliza de su administración y mantenimiento. En un programa 1:1, el centro suministra a todos los estudiantes los dispositivos que van a usar durante el proceso de aprendizaje —p. ej., ordenadores portátiles o tabletas—, lo que asegura la uniformidad y la correcta gestión de los recursos tecnológicos utilizados en el entorno docente. Estos dispositivos se seleccionan y configuran específicamente con el fin de satisfacer las necesidades educativas y los estándares del centro. El colegio, generalmente con el apoyo de un partner tecnológico, se encarga de todos los aspectos relacionados con el mantenimiento y el soporte técnico, lo que garantiza que sean seguros y se adecúen al uso que va a darles cada estudiante.

Descripción general de los programas BYOD y 1:1

	BYOD	Programas 1:1
Igualdad e inclusión	Acentúa las diferencias socioeconómicas	Ofrecen un acceso igualitario a todos los alumnos y un mayor número de ventajas
Uso de los dispositivos	Suele derivar en un uso inadecuado	Permiten supervisar los dispositivos para garantizar su uso adecuado
Compatibilidad	Los diferentes tipos de dispositivos y software pueden generar incompatibilidades durante las integraciones	El centro, generalmente con el apoyo de un partner tecnológico, se ocupa del suministro y la administración de los dispositivos, lo que facilita su integración
Soporte técnico	Puede ser lento e ineficiente	Todo el proceso se realiza de forma ágil y rápida gracias a los procedimientos establecidos
Seguridad	Aumenta los riesgos para la seguridad y la privacidad	Minimizan los riesgos para la privacidad y la seguridad
Supervisión	La actividad solo se puede supervisar de forma local	Permiten supervisar la actividad de formal local y remota



«Aunque es posible que proteger a los alumnos no sea tu principal función como responsable de TI, este departamento desempeña un rol cada vez más relevante a la hora de apoyar y formar al personal encargado de su seguridad».

Desventajas de las políticas BYOD: aspectos a considerar por parte del equipo directivo

1. Las desigualdades en el aprendizaje

Una de las principales desventajas de los programas BYOD es la forma en la que acentúan las diferencias socioeconómicas.

No todos los estudiantes disfrutan del mismo acceso a la tecnología. Es posible que algunos dispongan de dispositivos más nuevos y potentes, mientras que otros pueden utilizar modelos más antiguos o con menores prestaciones.

Estas diferencias podrían afectar a su capacidad para participar plenamente en las actividades de aprendizaje y sacar partido de los recursos educativos. Los alumnos que disponen de acceso limitado a los dispositivos o que usan tecnologías obsoletas pueden tener dificultades para realizar los trabajos escolares, acceder a los materiales en Internet o participar en proyectos colaborativos.

2. Las distracciones y el uso inadecuado de los dispositivos

La introducción de los dispositivos personales en el aula plantea problemas sobre cómo minimizar las distracciones y prevenir el uso inadecuado de estas herramientas.

La falta de supervisión puede provocar que los estudiantes se sientan tentados a utilizar los dispositivos con fines no educativos, como consultar las redes sociales o jugar a juegos, lo que puede desviar su atención de las actividades de aprendizaje.

Sin embargo, el uso inadecuado de los dispositivos personales puede ir más allá de las distracciones y afectar a su bienestar emocional.

El ciberacoso, que implica el uso de la tecnología con el fin de hostigar, intimidar o humillar a otras personas, se ha convertido en una preocupación muy real. Los dispositivos personales permiten a los alumnos acceder fácilmente a las redes sociales o las aplicaciones de mensajería, generando un entorno propicio para que se produzcan este tipo de incidentes.

> **«El 33,6% de los estudiantes en España asegura haber sufrido acoso escolar, y el 22,5% ciberacoso».**
>
> Impacto de la tecnología en la adolescencia», UNICEF España (2021).

3. Los problemas de compatibilidad entre dispositivos

Las políticas BYOD suelen crear un entorno tecnológico fragmentado dentro del aula, ya que los alumnos introducen una amplia gama de dispositivos con diferentes sistemas operativos y prestaciones técnicas.

Esta diversidad puede provocar problemas de compatibilidad que dificultan a los docentes la tarea de elaborar el currículo e integrar correctamente la tecnología en el proceso de aprendizaje.

Asimismo, proporcionar soporte técnico a toda esta variedad de dispositivos es un proceso complejo que requiere un gran número de recursos, lo que puede ejercer un impacto negativo en la calidad del servicio y obstaculizar la gestión efectiva de las aulas

4. Las complicaciones inherentes a la asistencia técnica

Gestionar el soporte en un programa BYOD puede convertirse en un auténtico desafío.

Cuando se ven obligados a administrar una amplia gama de dispositivos, sistemas operativos y versiones de software, muchos departamentos de TI tienen dificultades para proporcionar soporte técnico a los estudiantes de forma rápida y efectiva.

Además, es posible que cada dispositivo requiera un enfoque diferente a la hora de resolver las incidencias, lo que añade una presión adicional a los equipos de TI en un momento en el que estos profesionales ya se encuentran muy sobrecargados. Muchos de ellos carecen de la formación y los recursos necesarios para gestionar los múltiples problemas técnicos que esto conlleva, lo que hace que resulte aún más complicado proporcionar un servicio puntual sin interferir en el proceso de aprendizaje de los alumnos.

5. Los riesgos para la privacidad y la seguridad

En una era en la que es fundamental garantizar la máxima protección para los datos de los estudiantes, el uso de dispositivos personales no hace sino incrementar los riesgos de cara a la privacidad y la seguridad.

A diferencia de los dispositivos gestionados por el colegio, los dispositivos personales suelen carecer de las sólidas medidas de seguridad que se necesitan para proteger los datos de los alumnos frente a posibles filtraciones. Además, es posible que descarguen algún software peligroso o accedan a contenidos inadecuados para su edad de forma accidental, lo que puede generar una vulnerabilidad de seguridad en la red del centro.

Asimismo, existe la posibilidad de que los estudiantes intenten sortear las restricciones establecidas en la red o acceder a contenidos inapropiados a través de una VPN o un hotspot personal. Estas tecnologías podrían permitirles eludir los filtros y los cortafuegos del colegio, lo que a su vez podría comprometer la seguridad de la red y exponerles a contenidos perjudiciales o inadecuados en Internet.

> «En Europa, el sector educativo presenció un aumento del 11% en ciberataques, con un promedio de 2,256 ataques semanales en 2023, superando al sector militar».

Ventajas de los programas 1:1: sentando las bases para el futuro

La transición hacia una política para dispositivos educativos 1:1 ofrece **numerosas ventajas que pueden corregir las deficiencias del modelo BYOD** y contribuir a establecer unos objetivos educativos y de aprendizaje más efectivos.

1. Favorecen la igualdad y la inclusión

Uno de los principales objetivos en el ámbito de la educación es promover la igualdad y la inclusión, y migrar de una política BYOD a una 1:1 puede ser un paso importante para su consecución.

Garantizar la igualdad de acceso a la tecnología, ofrecer oportunidades de aprendizaje personalizadas y proporcionar un marco digital seguro permitirá a los colegios crear un entorno educativo inclusivo en el que todos los estudiantes tengan la oportunidad de desarrollar su potencial y alcanzar el éxito.

A. Reducen la desigualdad digital

La migración a una política 1:1 promueve la igualdad y la inclusión, puesto que garantiza el acceso igualitario a la tecnología y los recursos digitales por parte de todos los alumnos y los docentes. Al proporcionar un dispositivo a cada estudiante sin importar su situación socioeconómica, los centros contribuyen a cerrar la brecha digital y se aseguran de que todos tengan la posibilidad de participar en experiencias de aprendizaje digitales.

B. Garantizan la protección y la seguridad

Los colegios que utilizan políticas 1:1 disponen de un mayor grado de control sobre los dispositivos y pueden implementar unas medidas de seguridad robustas para proteger los datos y la privacidad de los estudiantes. De esta forma, además de garantizar la protección de la información personal de los alumnos, se genera un entorno de aprendizaje digital seguro que incentiva la confianza entre ellos, sus familias y los docentes.

C. Fomentan la igualdad de oportunidades de aprendizaje

Los estudiantes que utilizan dispositivos dedicados pueden acceder a una amplia variedad de recursos educativos y herramientas digitales que les permiten explorar, crear y disfrutar de experiencias de aprendizaje personalizadas. Esta mejora del acceso a la tecnología contribuye a construir un entorno educativo más inclusivo capaz de adaptarse a todo tipo de estilos y necesidades de aprendizaje.

D. Promueven la cultura de la colaboración

Los programas 1:1 fomentan la colaboración y la participación activa del alumnado proporcionándoles herramientas y plataformas para comunicarse, compartir archivos y trabajar en grupo. Los estudiantes pueden colaborar en proyectos, acceder a oportunidades de aprendizaje entre iguales y desarrollar habilidades esenciales para trabajar en equipo y comunicarse de forma efectiva. Esta cultura inclusiva y colaborativa genera un entorno de aprendizaje positivo en el que las opiniones de todos los alumnos se valoran por igual.

E. Contribuyen a mejorar la calidad del entorno docente

Los profesores también se benefician de este tipo de programas, ya que tienen acceso a un conjunto de dispositivos uniforme y fiable orientado al ámbito de la enseñanza. El hecho de disponer de una infraestructura tecnológica estandarizada les permite centrarse en desarrollar unidades didácticas innovadoras, sacar partido de los recursos digitales e incorporar la tecnología a los distintos aspectos de la práctica docente. De este modo, pueden crear un entorno educativo más inclusivo y dinámico que se adapta a diferentes necesidades de aprendizaje.

2. Garantizan la seguridad dentro y fuera del aula

Una de las ventajas de los programas 1:1 es la posibilidad de proteger la seguridad de los estudiantes fuera de clase de la misma forma que si se encontrasen dentro del recinto escolar.

Al proporcionarles un dispositivo dedicado y delegar en los colegios todas las tareas relacionadas con la compra, la administración y el mantenimiento, las políticas 1:1 refuerzan las medidas de seguridad y los mecanismos de soporte incluso cuando los alumnos no están conectados a la red local de su centro.

Los colegios pueden implementar protocolos de seguridad de calidad, como el filtrado de contenido y la administración de dispositivos, de forma que los estudiantes no puedan acceder a contenidos inapropiados o perjudiciales ni siquiera cuando se encuentran fuera de sus dependencias.

3. Ofrecen una experiencia coherente a los alumnos

Al implementar un programa 1:1, cada estudiante recibe un dispositivo dedicado adecuado a los estándares del centro.

Este planteamiento garantiza una experiencia de aprendizaje coherente para todos los alumnos, ya que tienen que utilizar las mismas configuraciones de hardware y software. Asimismo, permite que tanto ellos como los profesores puedan colaborar, compartir archivos y comunicarse de una forma más eficiente, eliminando las distracciones y las frustraciones que suelen producirse cuando se utilizan dispositivos con diferentes prestaciones en un entorno BYOD.

Por ejemplo, en un programa 1:1, los docentes pueden utilizar un software de gestión de aulas que les permita supervisar y controlar los dispositivos de los alumnos durante las clases para favorecer la concentración en el entorno de aprendizaje.

«

Los colegios que utilizan políticas 1:1 disponen de un mayor grado de control sobre los dispositivos y pueden implementar unas medidas de seguridad robustas para proteger los datos y la privacidad de los estudiantes».

4. Simplifican el soporte técnico

Las políticas 1:1 permiten al personal de soporte de TI concentrar su atención en los dispositivos y el software específicos que utilizan los estudiantes, lo que agiliza los procesos relacionados con el soporte técnico y mejora la eficiencia de la asistencia.

Esta especialización es fundamental para que el personal del departamento de TI pueda solventar las incidencias técnicas, resolver los problemas y llevar a cabo el mantenimiento de los dispositivos en el menor tiempo posible. Conocer en profundidad cómo funcionan los dispositivos y el software que utiliza el centro les permitirá proporcionar soluciones rápidas y efectivas cuando los estudiantes experimenten dificultades técnicas, minimizando las interferencias durante el proceso de aprendizaje.

5. Aumentan la visibilidad sobre el bienestar digital de los alumnos

La implementación de programas 1:1 proporciona a los colegios una información muy valiosa acerca del bienestar y los comportamientos digitales de los estudiantes.

El equipo docente tiene la posibilidad de visualizar la actividad de sus alumnos en Internet, lo que les permite supervisar lo que hacen e intervenir en caso necesario. Con una solución como Qoria, la plataforma para dispositivos escolares administrados líder en el mercado, los centros educativos pueden alcanzar un nuevo estándar de seguridad y bienestar digital independientemente del programa 1:1 que hayan elegido.

Conclusión

En resumen, realizar la transición de una política BYOD a una 1:1 en el entorno educativo genera **una serie de ventajas que contribuyen a corregir las limitaciones de este modelo** y hacen hincapié en la necesidad de garantizar una protección equitativa para todos los estudiantes.

La migración a un modelo 1:1 promueve una experiencia uniforme para los alumnos, favorece la integración y la compatibilidad entre dispositivos, facilita el soporte técnico, asegura la igualdad y la inclusión y fomenta la cultura de la colaboración. Las políticas 1:1 ejercen un impacto positivo sobre el entorno docente y garantizan la protección de los estudiantes tanto dentro como fuera del aula.

Este enfoque integral sienta las bases de un marco educativo más eficiente e inclusivo que prioriza el aprendizaje, el desarrollo y la seguridad de todos los alumnos.

Porque integrar la tecnología de una forma constructiva y consciente es un paso fundamental para ayudarles a alcanzar todo su potencial.

«Los programas 1:1 ejercen un impacto positivo sobre el entorno docente y garantizan la protección de los estudiantes **tanto dentro como fuera del aula».**

Qoria
Spain

Qoria es una empresa internacional de tecnología dedicada a proteger la seguridad y el bienestar de los estudiantes en el marco de su vida digital. Aprovechamos el potencial de la conexión para abordar los desafíos que enfrentan los jóvenes, ofreciéndoles apoyo en el colegio, en casa y en cualquier lugar.

Más información
www.qoria.es