Qoria
Spain

La Violencia Digital en el Aula y la Atenuación de Riesgos

Estrategias prácticas para los equipos directivos y los coordinadores de bienestar en el marco de la LOPIVI

qoria.es

Contenido

Introducción

Ahora que el mundo digital constituye una parte integral de la vida de los niños, es fundamental que los adultos empecemos a tomar conciencia de cuáles son los peligros a los que pueden enfrentarse.

Si bien es cierto que Internet ofrece numerosas oportunidades para que nuestros hijos aprendan y exploren, el uso de las aplicaciones de redes sociales, chat, vídeo y videojuegos también lleva aparejada una serie de riesgos que pueden hacer que acaben expuestos accidentalmente a contenidos de carácter pornográfico y violento, comportamientos de acoso, intentos de captación por parte de pederastas y otras formas de violencia relacionadas con las nuevas tecnologías que demandan nuestra atención.

Desarrollar una actitud proactiva e informada es la mejor forma de que tanto los padres como los educadores y los legisladores puedan abordar de forma efectiva estos riesgos y crear un entorno digital más seguro que fomente el desarrollo de los más pequeños.

En este artículo examinaremos algunas de las complejidades relativas a la prevención de la violencia infantil en Internet y analizaremos brevemente algunas de las amenazas que se ocultan en el mundo virtual. Asimismo, y de conformidad con lo dispuesto en la ley para la protección integral de la infancia frente a la violencia (también denominada LOPIVI), aportaremos una lista de estrategias proactivas que los centros y los coordinadores de bienestar pueden implementar para ofrecer una experiencia segura a los niños en Internet y promover su bienestar digital.

Sección 1.

El panorama actual

Un punto de inflexión

A principios de 2024, los centros educativos de todo el mundo alcanzaron un punto de inflexión. En la actualidad nos encontramos en un momento decisivo en el que es esencial alcanzar una comprensión integral de los cambios que se están produciendo para poder abordar una cuestión central que ya no es solo inminente, sino que se ha convertido directamente en un tema ineludible.

El mundo digital ha pasado a ser un componente fundamental de la vida de los jóvenes que condiciona su forma de aprender e interactuar con el mundo que les rodea. En los últimos años, las tecnologías de IA han experimentado un desarrollo vertiginoso que a menudo ha desbordado la capacidad de adaptación de la escuela; de ahí que haya llegado el momento de que los responsables educativos comiencen a adoptar un enfoque más sólido y proactivo.

Los colegios se encuentran en una encrucijada trascendental marcada por dos retos clave:

i) Favorecer un entorno en el que la tecnología no sea meramente aceptada sino valorada por su potencial para mejorar la educación, y

ii) Garantizar de forma activa la seguridad y el bienestar de los menores en el marco de su vida digital.

Integrar las nuevas tecnologías en el ámbito de la enseñanza resulta complicado, sobre todo teniendo en cuenta la responsabilidad añadida que supone proteger a los alumnos en un espacio virtual en el que las medidas de seguridad suelen ser, en el mejor de los casos, insuficientes. Hace falta acometer una profunda transformación que, además de permitir que los centros utilicen estas nuevas tecnologías para potenciar su labor educativa, mejore también la comprensión que tienen de ellas y les ayude a implementarlas para proteger el bienestar de los menores. Los avances tecnológicos que se están produciendo en este sentido pueden convertirse en una herramienta imprescindible para poder combatir las diferentes ciberamenazas a las que están expuestos los más pequeños, incluida la violencia.

Respecto al futuro, es fundamental que los colegios adquieran conciencia de esta nueva realidad y la incorporen en sus estrategias; solo de esta forma podrán ayudar a las familias a afrontar estos cambios de forma efectiva.

En 2023, la escuela carecía de las herramientas necesarias para protegerse

La naturaleza dinámica y a menudo clandestina de las comunicaciones digitales constituye un auténtico desafío para los centros educativos cuando tienen que abordar las múltiples formas en las que los alumnos se relacionan en el mundo virtual. La variedad de espacios digitales en los que se desarrollan estas interacciones es enorme e incluye desde redes sociales a aplicaciones de chat, lo que complica la tarea de supervisar y comprender plenamente el amplio abanico de actividades y conductas de los jóvenes. Esta dificultad se ve asimismo agravada por la aparición de nuevas modas y plataformas digitales, lo que obliga a los centros a ir siempre un paso por detrás a la hora de gestionar el comportamiento digital imprevisible, y con frecuencia potencialmente peligroso, que muestra el alumnado.

El 2023 asistimos a nuevos fenómenos en el ámbito de la ciberseguridad:

La amplificación del ciberacoso mediante la IA

Los casos de ciberacoso, que comprenden conductas como el hostigamiento verbal, las amenazas o la exclusión social a través de los medios digitales, no son ninguna novedad. Sin embargo, el auge de las técnicas de deepfake ha provocado que las agresiones sean cada vez más personalizadas, focalizadas e hiperrealistas. Esta escalada ha generado una grave angustia, sentimientos de vergüenza y resentimiento y problemas de autoestima en cientos de niños. En algunos casos, el acoso ha llegado incluso a desencadenar comportamientos autolesivos y suicidios.

Según una encuesta realizada en 2023, el 9,2% de los estudiantes españoles asegura haber sufrido algún tipo de ciberacoso.[3]

Como responsables del bienestar físico, emocional y social de los más pequeños, es necesario que los colegios encuentren una forma de detectar este tipo de incidentes. A este respecto, es esencial saber si los alumnos estaban conectados a la red del colegio en el momento de la agresión, si esta ha tenido lugar dentro del recinto escolar o en el ámbito doméstico, y cómo puede intervenir el equipo docente mediante el sistema de seguridad del centro para evitar que el acoso se extienda de forma rápida y potencialmente incontrolable.

La desinformación y las noticias falsas

El año pasado, los niños y los jóvenes estuvieron expuestos a una gran cantidad de informaciones erróneas, rumores y noticias falsas en Internet. Este tsunami ha terminado afectando a su capacidad de evaluar de forma crítica la información que reciben y de formar opiniones informadas.

La desinformación sobre las tensiones geopolíticas, la polarización y las imágenes gráficas de conflictos bélicos han inundado las redes sociales. Muchos de estos contenidos están específicamente diseñados para alterar la percepción que tienen los más jóvenes sobre el estado del mundo y su posicionamiento político respecto a este.

El 40% de los alumnos españoles de secundaria no ha aprendido a detectar las noticias falsas.[4]

Aunque la regulación de las plataformas de redes sociales sigue siendo un desafío pendiente, los responsables educativos también tienen que abordar la cuestión fundamental de cuál debe ser su papel a la hora de prevenir que los alumnos accedan a este tipo de publicaciones en primer lugar, ya sea desde su casa o dentro del recinto docente.

En paralelo a este fenómeno, y de forma preocupante, en 2023 muchos adolescentes empezaron a recurrir a las redes sociales para informarse en detrimento de los medios tradicionales. Este cambio ha dado vía libre a los influencers a los que siguen, cuyas opiniones y motivaciones son, en el mejor de los casos, sesgadas y parciales, y en el peor carecen de credibilidad o de evidencias para respaldar sus afirmaciones. Sin embargo, para muchos jóvenes son la principal referencia moral a la hora de interpretar la compleja y poliédrica realidad que suele esconderse detrás de los acontecimientos mundiales.

[3] Ministry of Education and Vocational Training 2023
[4] Universidad Carlos III de Madrid (UC3M)

Los ciberdepredadores

En 2023, los casos de depredadores que utilizaban plataformas digitales, y concretamente las plataformas de videojuegos, como medio para engañar y explotar a menores batió todos los récords anteriores. Infinidad de niños y jóvenes estuvieron expuestos a situaciones de alto riesgo cuando interactuaban con desconocidos a través de chats y juegos multijugador, en muchos casos sin el conocimiento de sus padres.

La Alianza Mundial contra la Explotación Sexual Infantil en línea We Protect aseguraba en su informe de evaluación de amenazas globales del año pasado que la producción de pornografía infantil casera por parte de los menores de entre 7 y 10 años se había disparado un 360% en 2023. Este incremento nos lleva a plantearnos dónde tiene lugar este fenómeno y qué iniciativas pueden llevar a cabo los colegios para concienciar a las familias del riesgo que corren los más pequeños dentro de su propio hogar.

La IA generativa también es un factor fundamental en este incremento. Hay informes que indican que los ciberdepredadores han empezado a utilizar esta tecnología como una herramienta para prepararse, probar nuevas estrategias y ensayar las conversaciones con las que planean captar a los menores, lo que les permite adaptar su lenguaje y perfeccionar los mensajes que van a lanzar para aumentar aún más su influencia sobre las víctimas.

Cumplir su papel como garantes de la seguridad de los más jóvenes no es tarea fácil para los responsables docentes, ya que estos contactos se desarrollan habitualmente en espacios en los que los adultos no están presentes. Además, el problema tiende a agravarse si no tienen en cuenta los sentimientos de vergüenza que acompañan a estos incidentes y a los comportamientos subsiguientes.

Los estudios indican que las víctimas de estas agresiones rara vez denuncian o piden ayuda abiertamente en los momentos iniciales porque tienen miedo a que los adultos consideren que tienen la culpa de lo que ha pasado o las avergüencen. Por eso, es importante que los centros educativos adopten una actitud proactiva en lugar de reactiva ante este tipo de situaciones, y que empiecen a implementar soluciones de protección digital eficientes que permitan detectar en tiempo real las situaciones en las que existe un riesgo real para los menores. Estas soluciones deben proporcionarles la visibilidad que de otro modo no podrían obtener sobre las actividades virtuales para poder gestionar la seguridad y el bienestar de sus alumnos de la forma más efectiva posible.

29%

Instagram ha pasado a ser el principal medio de información de los jóvenes —actualmente lo utilizan el 29% de los adolescentes—, seguido de cerca por TikTok y YouTube.

Sección 2

Una mirada al futuro

La visibilidad y la protección digital del alumnado se han convertido en un imperativo estratégico.

A nivel global, en 2023 Qoria volvió a superar todos los estándares:

Cada
56 segundos
Detectamos a un niño expuesto a una amenaza potencialmente peligrosa.

Cada
4 minutos
localizamos a un menor implicado en un caso de alto riesgo relacionado con el ciberacoso, el acoso escolar u algún otro tipo de incidente violento.

Cada
5 minutos
Identificamos a un niño en situación de vulnerabilidad.

La continua aparición de nuevas amenazas es un reflejo de la compleja naturaleza del mundo virtual.

A medida que el mundo digital continuaba expandiéndose en 2023, empezamos a detectar una serie de patrones que creemos que serán determinantes para los colegios a la hora de enfocar el problema de la ciberseguridad. En esta sección enumeramos algunas de las principales tendencias que hemos identificado y que no solo son predominantes en la actualidad, sino que prevemos que se intensifiquen a lo largo de los próximos 12 meses como consecuencia del rápido avance que están experimentando algunas herramientas y tecnologías. Eso incluye tanto la IA generativa y la personalización de datos como la convergencia de las diferentes tecnologías de inmersión y realidad aumentada, entre las que se encuentran las denominadas RE (o realidades extendidas).

Estas tendencias subrayan la importancia de adoptar estrategias proactivas y adaptativas para mitigar el aumento de estos riesgos de manera efectiva.

El efecto silenciador

La elusión de los filtros escolares y los riesgos para la ciberseguridad

La desviación de los modelos de aprendizaje automático

El adelanto de la pubertad

El ciberacoso basado en los deepfakes

El efecto silenciador

El término «efecto silenciador» (TSE) hace referencia a la autocensura que se imponen los individuos a sí mismos cuando son víctimas de algún tipo de acoso, troleo o intimidación, sobre todo en el caso de las niñas y las personas pertenecientes a alguna minoría.

Por todo el planeta, hemos presenciado cómo numerosos miembros de estos colectivos se convertían sistemáticamente en el blanco de un aluvión de insultos y amenazas. Nuestra previsión es que el alcance de los ataques a estos grupos se incremente en el futuro, ya que los acosadores utilizan técnicas cada vez más sofisticadas para segmentar y personalizar este tipo de campañas.

El efecto silenciador es una experiencia a la que es probable que muchos niños y jóvenes tengan que enfrentarse en un momento u otro de sus vidas. En general, se encuentran en una edad en la que les cuesta expresar sus sentimientos, y muchas veces no disponen de las herramientas necesarias para identificar si una situación es lo bastante grave para denunciar. En este sentido, es fundamental que los responsables educativos aprendan a reconocer rápidamente los comportamientos asociados a este efecto y que establezcan un protocolo de intervención temprana para minimizar su impacto negativo.

Una de las tareas que tienen pendientes los colegios es la de evaluar diferentes fórmulas para que el personal docente pueda detectar el ciberacoso y ayudar a los alumnos a denunciarlo de forma anónima. Asimismo, deben elaborar estrategias efectivas para poder gestionar y prevenir las graves consecuencias que pueden tener estas situaciones a nivel social, emocional, psicológico o físico, de las cuales el efecto silenciador es tan solo un ejemplo.

La desviación de los modelos de aprendizaje automático

Cada vez son más las voces que alertan del riesgo que puede suponer la denominada desviación de los modelos de aprendizaje automático en el ámbito educativo. Este fenómeno provoca que los algoritmos y la información que se utilizan para entrenar estas tecnologías pierdan precisión con el paso del tiempo y expongan accidentalmente a contenidos problemáticos a los jóvenes que interactúan con ellos.

Los estudios de los que disponemos hoy en día indican que estamos ante un problema grave que ya ha dejado sentir sus efectos sobre el bienestar de los alumnos. Por ejemplo, recientemente los investigadores lograron demostrar que cualquier niño puede acceder a contenido para adultos con solo tres clics desde una aplicación como YouTube. Además, la producción de contenidos gráficos derivados de las tensiones geopolíticas se ha multiplicado a lo largo del último año, lo que ha convertido algunas plataformas como las redes sociales en auténticas armas al servicio de la propaganda.

A medida que los usuarios continuemos generando nuevos contenidos en la Red, la desviación de los modelos de aprendizaje será un factor cada vez más importante a la hora de promover agendas políticas cuestionables, modas perjudiciales y diversos tipos de desinformación.

Aunque la principal misión de los centros educativos es fomentar la alfabetización digital entre los alumnos y enseñarles a analizar y cuestionar de forma crítica la información a la que acceden en Internet, también es esencial que se detengan a considerar qué herramientas de filtrado y supervisión van a implementar para detectar y prevenir la exposición accidental, lo que en la práctica minimiza sus consecuencias de forma automática. Elegir una solución técnica flexible y personalizable es un requisito indispensable para mantenerse al tanto de las nuevas tendencias que irán emergiendo en 2024 y poder abordar los desafíos que plantean los fenómenos tecnológicos de este tipo.

La elusión de los filtros escolares y los riesgos para la ciberseguridad

Los alumnos llevan buscando la forma de evitar los filtros que configuran los colegios prácticamente desde que su uso comenzó a generalizarse. Sin embargo, la deriva que está tomando el mundo digital en la actualidad no solo conlleva riesgos cada vez mayores para su bienestar, sino también de cara a la posición de los centros en materia de ciberseguridad.

En 2023 volvimos a presenciar numerosos intentos de acceder a contenidos fuera de la red escolar por parte de los más jóvenes, lo que provocó que acabaran expuestos a técnicas fraudulentas como la falsificación de sitios web y las cuentas de suplantación de identidad. Es probable que a lo largo de 2024 los atacantes (tanto individuos como organizaciones) recurran con mayor frecuencia a este tipo de estrategias, y que estas evolucionen progresivamente hacia formas más complejas.

Además de la aparición de nuevas técnicas de automatización y del aumento del número de actividades fraudulentas, en Qoria creemos que a los ciberdelincuentes les resultará cada vez más fácil engañar a los jóvenes para que bajen la guardia y hagan clic en enlaces potencialmente peligrosos para la seguridad de su dispositivo y, como consecuencia, para la seguridad de la red del colegio.

En la actualidad, las consecuencias de la victimización que generan estos ataques supone un enorme perjuicio para la reputación de los centros que no han conseguido poner en valor las iniciativas adoptadas a la hora de paliar y gestionar estos comportamientos en el contexto digital actual.

Esta situación pone en evidencia las ventajas que ofrece la gestión de los dispositivos en el ámbito educativo. Los dispositivos gestionados proporcionan un entorno más seguro y controlado, lo que reduce en gran medida los riesgos a los que suelen estar expuestos los alumnos cuando acceden a Internet sin supervisión o hacen un uso inadecuado de los dispositivos. En este sentido, es fundamental que los centros elijan soluciones de filtrado y herramientas de gestión de red robustas y precisas que se adapten rápidamente a sus requisitos de ciberseguridad. Asimismo, los responsables docentes deben implementen las medidas necesarias para concienciar a los alumnos de las consecuencias que puede tener para ellos cualquier posible intento de sortear los filtros.

El ciberacoso basado en los deepfakes

Un deepfake es un medio sintético que ha sido editado digitalmente para sustituir la imagen de una persona por la de otra con el fin de inducir a error a los espectadores. La creciente popularidad de esta técnica entre los jóvenes genera nuevos desafíos en el ámbito educativo.

Los comportamientos de ciberacoso relacionados con este tipo de tecnologías empezaron a dispararse a finales de 2023, y a pesar de que muchos de sus autores han terminado respondiendo ante los tribunales, prevemos que el número de casos continúe aumentando.

Las consecuencias de los contenidos deepfake, que normalmente denigran a sus protagonistas utilizando imágenes de otras personas en un contexto pornográfico o sexual, pueden tener efectos muy graves sobre salud mental de las víctimas y ejercer un impacto negativo duradero sobre su huella digital.

Además, la proliferación de deepfakes a nivel global ha generado un gran debate en torno a la responsabilidad y la capacidad de los propios colegios a la hora de crear un entorno psicosocial seguro para los docentes después de que salieran a la luz numeroso incidentes protagonizados por alumnos que utilizaban este tipo de contenidos para acosar a sus profesores. Es importante que los centros educativos incorporen a su oferta formativa programas de ciudadanía digital diseñados para abordar estas nuevas tendencias, promover el uso ético de la tecnología entre los más jóvenes y sensibilizarlos sobre las consecuencias que puede tener la creación de contenidos perjudiciales.

El adelanto de la pubertad

Un estudio llevado a cabo por McCrindle define la denominada «pubertad precoz» como el proceso por el que «los niños han empezado a crecer más deprisa, y a edades cada vez más tempranas». Se trata de una tendencia a la que se enfrentan cada vez más padres y, en última instancia, los colegios, y que se asocia al aumento de la disponibilidad de las tecnologías digitales y el uso excesivo que hacen de ellas los alumnos. Las familias conviven con la tensión de saber que sus hijos necesitan desarrollar la alfabetización digital en el ámbito tecnológico, pero al mismo tiempo son conscientes de que los niños aún no han alcanzado el grado de madurez necesario para poder utilizar estos dispositivos de forma segura y responsable.

Numerosos padres y centros educativos ya han dado la voz de alarma respecto a las consecuencias que puede tener el hecho de que los niños crezcan demasiado rápido. Sin embargo, a medida que aumenta la presencia y la importancia de la tecnología en el proceso de aprendizaje, muchos menores terminan utilizando estos dispositivos y herramientas sin la supervisión necesaria, tanto en el ámbito educativo como en sus casas. Eso significa que pueden estar expuestos a contenidos inadecuados para su edad, y si esta exposición no va acompañada de la supervisión, la intervención o la participación necesarias por parte de los adultos, puede tener un grave impacto negativo sobre su bienestar.

El concepto de pubertad precoz ha puesto de manifiesto la urgente necesidad de establecer las herramientas y los protocolos necesarios para ayudar a los niños a disfrutar de experiencias e interacciones digitales adecuadas para su edad.

En este contexto, los centros educativos deben colaborar estrechamente con los padres para concienciarles sobre lo importante que es gestionar el uso que hacen sus hijos de la tecnología de forma acorde con su edad, así como proveer de recursos y oportunidades de aprendizaje a la comunidad educativa para proporcionarles orientación de forma regular y constante.

En concreto, los profesores necesitan disponer de las herramientas y los recursos necesarios para abordar los problemas conductuales que puede provocar una exposición temprana en el ámbito de la escuela y promover una buena comunicación con los alumnos para conocer los problemas de seguridad digital que les afectan.

Tener en cuenta todos estos aspectos y dedicarles la atención necesaria permitirá a los educadores intervenir y detectar proactivamente los riesgos que plantean fenómenos como el adelanto de la pubertad para ofrecer a los niños la atención que necesitan de forma específica y estratégica.

Sección 3

Estrategias de atenuación de riesgos que pueden implementar los centros actualmente

¿Cuál es el próximo paso?
La importancia de la visibilidad a la hora de promover el bienestar digital

Gestionar el uso que hacen los alumnos de la tecnología requiere considerar multitud de factores, y en ocasiones la complejidad del proceso puede resultar abrumadora para los responsables docentes. Por eso es importante recordar que la mejor forma de marcar la diferencia es ir dando pequeños pasos en la dirección correcta. La cuestión fundamental es en qué áreas deben enfocar los centros y los coordinadores de bienestar sus esfuerzos cuando hay que tener en cuenta tantos aspectos.

Para generar un impacto significativo, hay un ámbito prioritario que actúa como el principal factor clave a la hora de mejorar los resultados del alumnado. Se trata de la visibilidad digital.

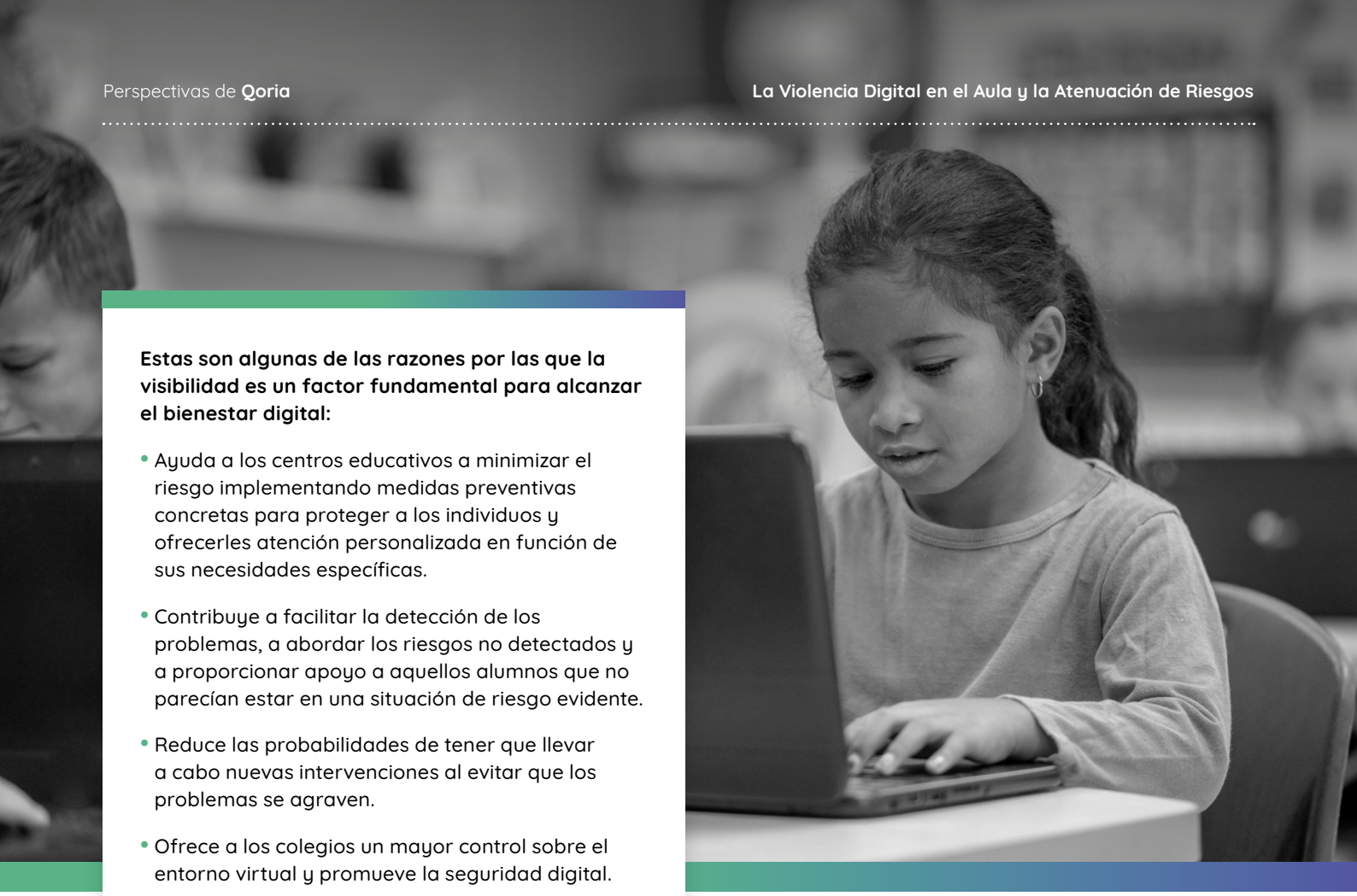
En Qoria creemos que la visibilidad digital es actualmente uno de los principales obstáculos para proteger el bienestar digital de los menores, y para muchos colegios de todo el mundo continúa siendo la gran asignatura pendiente.

Cuando hablamos de la «visibilidad», nos referimos a la capacidad de visualizar y comprender los hábitos, los comportamientos y los problemas que experimentan los niños y los jóvenes en el mundo virtual. Se trata de un elemento fundamental para el éxito de cualquier estrategia de seguridad y bienestar digital porque ayuda a los centros a reducir el riesgo mediante medidas preventivas que permiten proteger a los individuos y ofrecerles apoyo en función de sus necesidades específicas.

La buena noticia es que podemos detectar a la mayoría de los niños en situación de vulnerabilidad a partir de su comportamiento digital.

Obtener una mayor visibilidad permite a los responsables educativos detectar y abordar problemas de los que antes no eran conscientes, así como proporcionar atención a aquellos alumnos que no habían dado muestras de encontrarse en situación de riesgo o que no parecían tener ninguna dificultad en el ámbito digital. Supervisar el comportamiento del alumnado en la Red contribuye a identificar aquellos patrones y conductas que pueden tener efectos negativos sobre su bienestar. Además, disponer de una mejor visibilidad también proporciona un mayor control sobre el entorno digital de cada alumno, lo que a su vez contribuye a fomentar la ciberseguridad.

Adquirir una comprensión integral del funcionamiento de los diferentes dispositivos y servicios, así como de sus respectivos riesgos, es fundamental para poder adoptar decisiones claras e informadas sobre su uso y la protección de los datos personales. Cuando los centros disponen de visibilidad, pueden empezar a implementar prácticas de ciberseguridad proactivas en lugar de reactivas.



Estas son algunas de las razones por las que la visibilidad es un factor fundamental para alcanzar el bienestar digital:

- Ayuda a los centros educativos a minimizar el riesgo implementando medidas preventivas concretas para proteger a los individuos y ofrecerles atención personalizada en función de sus necesidades específicas.
- Contribuye a facilitar la detección de los problemas, a abordar los riesgos no detectados y a proporcionar apoyo a aquellos alumnos que no parecían estar en una situación de riesgo evidente.
- Reduce las probabilidades de tener que llevar a cabo nuevas intervenciones al evitar que los problemas se agraven.
- Ofrece a los colegios un mayor control sobre el entorno virtual y promueve la seguridad digital.
- Ayuda a los responsables educativos a tomar decisiones informadas y respaldadas por datosa la hora de abordar las estrategias e iniciativas de ciberseguridad.

Hacer visible lo invisible

Depender de nuestros ojos y nuestros oídos no es suficiente en el mundo digital...

Tradicionalmente, muchos colegios se basaban en las observaciones y la intuición de los profesores para detectar a los alumnos que necesitaban ayuda y llegar hasta la raíz del problema. Aunque las interacciones que mantienen los docentes siempre serán una herramienta indispensable para identificar las situaciones potencialmente conflictivas, no son un método infalible. La única forma de conocer lo que ocurre en la vida digital de los más jóvenes es con la ayuda de la tecnología.

Asimismo, confiar únicamente en la supervisión física reduce el margen de maniobra a la hora de descubrir patrones o analizar tendencias. Muchas veces, los incidentes aislados que parecen intrascendentes no tardan en olvidarse una vez resueltos; sin embargo, encontrar una conexión entre varias acciones digitales a menudo puede revelar riesgos que nunca se habían detectado.

Los colegios tienen la responsabilidad permanente de abordar los problemas en cualquier momento y lugar, lo que significa que cuando los alumnos cruzan las puertas del centro y están expuestos a las ciberamenazas, los responsables docentes deben estar preparados para intervenir del mismo modo que lo harían en el mundo real. Si bien la observación es una herramienta fundamental para comprender y fomentar el bienestar de los menores, no es suficiente por sí misma.

La mayoría de los niños tienden a ocultar sus problemas, y en algunos casos aún no han alcanzado la madurez necesaria para poder reconocer o verbalizar sus preocupaciones. Obtener una mayor visibilidad sobre su actividad es una buena forma de ayudarles a afrontar este tipo de situaciones.

¿Cómo pueden los colegios mejorar la visibilidad?

Según lo establecido en la LOPIVI, una de las principales funciones del coordinador de bienestar es asegurar el mayor grado de bienestar posible dentro del centro educativo. Para poder mejorar el bienestar de los alumnos, los responsables docentes deben considerar cuál es su grado de visibilidad en tres áreas clave: las emociones, las intenciones y las acciones.

Hay tres preguntas esenciales que también permitirán detectar las posibles carencias asistenciales y señalar aquellas áreas en las que puede ser necesario ampliar o reforzar la atención.

1. ¿Cómo podemos evaluar periódicamente el estado anímico de los alumnos?

Comprobar regularmente cuál es el estado emocional y el grado de bienestar de los alumnos es fundamental. La percepción que tienen los jóvenes sobre lo que está sucediendo en su vida suele ser un buen indicador, por lo que realizar un seguimiento de los cambios que se producen en su estado anímico o su comportamiento puede proporcionar información muy útil respecto a su bienestar. Implementar un método o un sistema eficaz para recabar su opinión y preguntarles periódicamente cómo se sienten es un buen punto de partida para poder abordar los posibles riesgos y actuar de forma temprana.

Los centros educativos de todo el mundo están virando progresivamente hacia un enfoque más especializado que aprovecha las posibilidades tecnológicas actuales a la hora de recopilar la opinión del alumnado. En particular, muchos colegios han empezado a utilizar plataformas de evaluación del bienestar y herramientas de supervisión semanal que permiten identificar a los alumnos y proporcionarles atención personalizada a nivel individual, así como obtener información accionable para tener una comprensión clara de las áreas en las que muestran un rendimiento sobresaliente y aquellas en las que necesitan un refuerzo adicional. Tras analizar más de 23 millones de informes de Qoria Pulse, hemos llegado a la conclusión de que una de las principales causas de malestar a nivel global entre los menores es (la ansiedad que sienten cuando cometen errores).

2. ¿Cómo podemos saber qué tipo de contenido buscan o consumen?

Entender cómo usan los alumnos los dispositivos escolares en Internet puede proporcionar información valiosa y descubrir patrones que pueden revelar cuáles son sus intenciones y sus aficiones, qué tipo de cuestiones les preocupan y qué probabilidades hay de que puedan estar expuestos a algún riesgo. Por ejemplo, es posible etiquetar determinados tipos de búsqueda para detectar qué pautas y conductas pueden tener efectos negativos sobre su bienestar. Además, esta información también resulta útil para detectar tendencias o problemas a nivel global, por lo general de forma agregada.

Las tecnologías de filtrado han avanzado considerablemente a lo largo de los años. Sin embargo, a la hora de considerar cuál es la solución más adecuada para mejorar la visibilidad digital, nuestra recomendación es que los centros otorguen prioridad a los filtros específicamente desarrollados para el entorno educativo. A diferencia de las soluciones diseñadas para la administración de sistemas empresariales, las tecnologías dirigidas al ámbito escolar se pueden configurar de forma que todo el personal clave, como los coordinadores de bienestar, pueda acceder a los informes.

¿Cómo pueden los colegios mejorar la visibilidad?

Otro aspecto importante a tener en cuenta es la posibilidad de poder adaptar los métodos de filtrado en función del comportamiento observado en el alumnado. Una solución de filtrado efectiva para colegios debería alejarse de un enfoque uniformador y centrarse en características como la adaptabilidad, la personalización, la visibilidad y la accesibilidad. Asimismo, debe ofrecer la flexibilidad necesaria para adaptarse a las diferentes necesidades de aprendizaje de cada alumno o curso, y al mismo tiempo brindar una protección completa en términos de ciberseguridad.

3. ¿Cómo es su experiencia en Internet?

Por último, es imprescindible tener en cuenta el complejo abanico de experiencias al que están expuestos los alumnos en la Red. Comprender las interacciones y los comportamientos que desarrollan en el mundo digital es una condición esencial para que los centros educativos puedan detectar cualquier tipo de actividad potencialmente peligrosa, como el ciberacoso o las interacciones inapropiadas para su edad. Esta información les permite implementar medidas de prevención individualizadas para proteger a los alumnos y proporcionarles apoyo en función de sus necesidades específicas.

El aumento del número y la escala de las amenazas virtuales ha alumbrado el inicio de una nueva era en el ámbito de la ciberseguridad marcada por la introducción de las tecnologías de detección de amenazas y supervisión digital.

Aunque el filtrado web continúa siendo una herramienta esencial para proteger a los alumnos del contenido perjudicial e inapropiado en Internet, en ocasiones no basta para revelar el contexto general en el que se desarrollan sus interacciones. La supervisión digital no significa únicamente bloquear contenidos. Este tipo de soluciones categorizan la actividad, alertan al personal cuando el comportamiento digital de un alumno sugiere que está a punto de sufrir una agresión y proporcionan información contextual vital, incluidos los factores que han desencadenado el incidente.

Con el fin de ayudar a los colegios a garantizar el cumplimiento de la legislación gubernamental, hemos desarrollado Qoria Monitor, una solución líder en supervisión y detección de riesgos.

El año pasado Qoria Monitor detectó a un menor en situación de vulnerabilidad grave cada 56 segundos.

10 preguntas fundamentales que deben empezar a plantearse los colegios:

En el entorno educativo actual, garantizar el bienestar digital de los alumnos requiere un enfoque proactivo y específico por parte de los centros educativos.

Con el fin de promover la reflexión y la acción, ponemos a vuestra disposición el siguiente cuestionario, dirigido a detectar los riesgos más inmediatos y mejorar la visibilidad en las tres áreas clave que hemos mencionado.

Identificar las carencias permite a los centros tomar las medidas activas necesarias para proteger a los alumnos y promover un entorno que favorezca su bienestar de forma tanto positiva como significativa.

Las preguntas que aparecen a continuación te ayudarán a detectar cualquier posible brecha en vuestra estrategia de ciberseguridad actual. El objetivo de este breve ejercicio es ayudarte a identificar y priorizar aquellas áreas de actuación que requieren una atención inmediata.

1. ¿Utilizáis un cortafuegos como solución de seguridad dedicada, o intentáis usarlo también para bloquear algún área específica de Internet? **SÍ/NO**
2. ¿Podéis crear reglas en vuestros filtros que os permitan responder de forma directa al comportamiento que habéis observado a nivel individual en el alumnado? **SÍ/NO**
3. ¿El personal no técnico recibe periódicamente informes y alertas en tiempo real sobre la actividad digital de los alumnos? ¿Estos informes incluyen información detallada sobre su comportamiento y las tendencias relativas a su bienestar y permiten identificar a los menores en situación vulnerable? **SÍ/NO**
4. ¿El/los sistema/s que utilizáis actualmente genera/n falsos positivos o informes erróneos que requieren algún tipo de investigación adicional por vuestra parte? **SÍ/NO**
5. ¿Los docentes están facultados para decidir a qué contenidos pueden acceder los alumnos en Internet durante sus clases? ? **SÍ/NO**
6. ¿Disponéis de algún sistema de supervisión o generación de informes que te permita identificar de forma proactiva a aquellos alumnos que hacen un uso potencialmente peligroso de los dispositivos? **SÍ/NO**
7. ¿Habéis establecido algún protocolo oficial a la hora de recopilar y evaluar periódicamente los datos relativos al estado emocional del alumnado? **SÍ/NO**
8. ¿Adaptáis vuestra oferta formativa sobre ciberseguridad al grado de madurez, las necesidades y las experiencias digitales previstos para los diferentes grupos de alumnos? **SÍ/NO**
9. ¿Cuando organizáis sesiones educativas sobre ciberseguridad para vuestros alumnos, ¿tenéis en cuenta las necesidades formativas de vuestro personal en esta área? **SÍ/NO**
10. ¿Las soluciones que habéis implementado se pueden configurar para permitir que los padres accedan a la actividad digital de sus hijos? **SÍ/NO**

Conclusión

Si analizamos el panorama digital actual, tu centro educativo desempeña un papel fundamental tanto a la hora de minimizar la violencia y otro tipo de ciberamenazas como para ofrecer una experiencia digital segura a los más pequeños, ya sea en casa, en el colegio o en el transcurso de cualquiera de sus desplazamientos.

Abordar proactivamente los problemas que se les plantean en el ámbito de la prevención, la detección temprana y la intervención, al igual que todas las dificultades asociadas a la educación y la participación, permitirá a los colegios crear un entorno más seguro para sus alumnos, y al mismo tiempo reforzará la confianza y proporcionará una mayor sensación de control a las personas encargadas de orientar la vida digital de nuestros hijos.

Si combinamos nuestros esfuerzos con la tecnología, las herramientas y los profesionales adecuados, estaremos más preparados para reaccionar de forma colectiva ante las diferentes facetas que intervienen en la protección digital de los alumnos.

Más información

Este artículo forma parte de nuestra serie La seguridad digital en el ámbito educativo. Haz clic aquí para visitar nuestra página de recursos dedicada.

Contacta con nosotros

Si quieres asesorarte sobre las líneas generales de tu estrategia o deseas obtener más información sobre nuestras soluciones individuales, no dudes en ponerte en contacto con nosotros.

Dirección de contacto: educacion@qoria.com
Sitio web: www.qoria.es

Estamos a tu disposición.

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