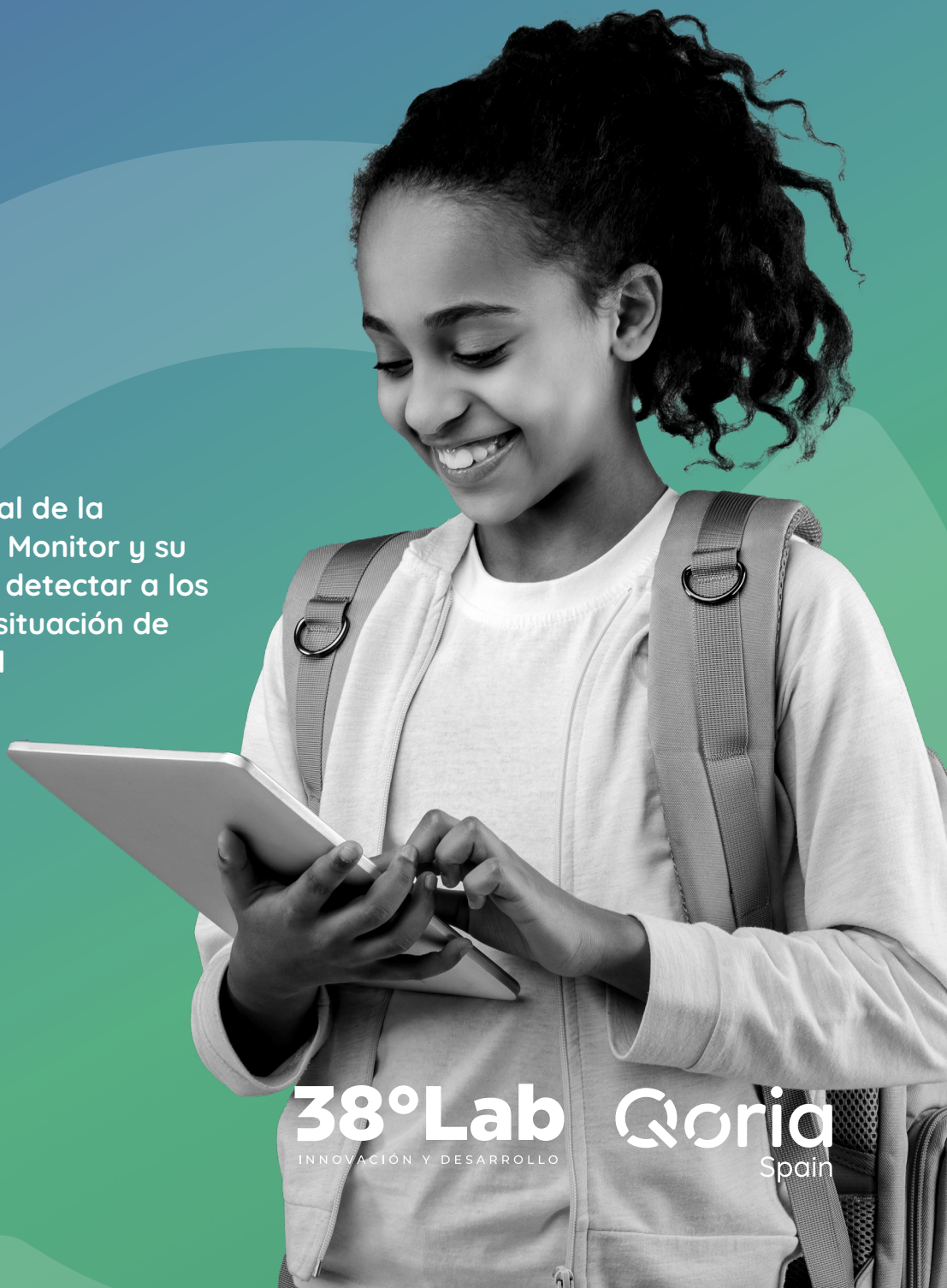
Qoria Insights

Guía completa para una supervisión digital responsable en colegios

Una guía integral de la herramienta de Monitor y su aplicación para detectar a los estudiantes en situación de riesgo potencial



38°Lab INNOVACIÓN Y DESARROLLO

Qoria Spain

qoria.es

Contenidos

Acerca de esta guía

El presente documento ha sido elaborado por los especialistas en seguridad digital de Qoria para ayudar a los colegios a establecer unos mecanismos de supervisión digital adecuados que contribuyan a proteger a los estudiantes, los docentes y las redes TIC de las posibles ciberamenazas.

A lo largo de sus páginas, encontrarás una aproximación general al concepto de supervisión digital y una serie de pautas para ayudar a los centros a integrarlo en su estrategia de seguridad actual.

Asimismo, también abordaremos las principales cuestiones que nos plantean los docentes en este ámbito y expondremos algunos ejemplos reales de cómo funcionan este tipo de sistemas.

Esta guía va orientada a los siguientes perfiles: integrantes de equipos directivos, coordinadores de bienestar y protección del alumnado, directores y cualquier otro profesional que desee obtener más información sobre el cumplimiento de la normativa de protección de menores en contextos escolares o cuyas responsabilidades abarquen este ámbito.

Si tienes alguna duda sobre el concepto de supervisión digital, su aplicación en el entorno educativo o el campo de la ciberseguridad en general, no dudes en contactar con el equipo de Qoria.

Estaremos encantados de ayudarte.

Correo electrónico: enquiries@qoria.es

Web: www.qoria.es/contact

1.0 Introducción

Internet, los ordenadores y los dispositivos móviles **forman parte de la vida cotidiana** de muchos niños.

La mayoría de las familias disponen como mínimo de un dispositivo conectado en sus hogares y, si fijamos la vista en los centros, descubriremos que Internet y los ordenadores se han convertido en un componente habitual del proceso de enseñanza y aprendizaje.

Y si bien la tecnología ofrece enormes oportunidades, también lleva aparejada una serie de riesgos.

El acoso (o maltrato entre compañeros) dentro de las aulas no es precisamente un fenómeno nuevo. Sin embargo, a diferencia de los niños de generaciones anteriores, que podían escapar de sus agresores en la seguridad de sus casas, la naturaleza viral de la vida digital ha provocado que en la actualidad los más pequeños ya no tengan ningún sitio en el que refugiarse. El acoso ha pasado a ser una forma de maltrato constante.

Niños y adolescentes pueden convertirse en el blanco de mensajes de carácter humillante o degradante e imágenes o vídeos sexuales de manera permanente. Asimismo, corren el riesgo de ser víctimas de la explotación, la ciberpederastia, la captación por parte de bandas, la radicalización, la violencia de género y toda clase de tráficos ilegales.

La principal consecuencia de esta realidad es que el número de casos de menores y jóvenes que desarrollan problemas de salud mental debido al uso de los medios digitales ha empezado a multiplicarse de forma exponencial.

El Instituto Nacional de Estadística de Reino Unido ha detectado que existe una «clara asociación» entre el uso intensivo de las redes sociales y la prevalencia de estas patologías en los menores. Según un estudio llevado a cabo por el Servicio Nacional de Salud británico en 2023, 1 de cada 5 jóvenes mostraba síntomas compatibles con algún trastorno psicológico.

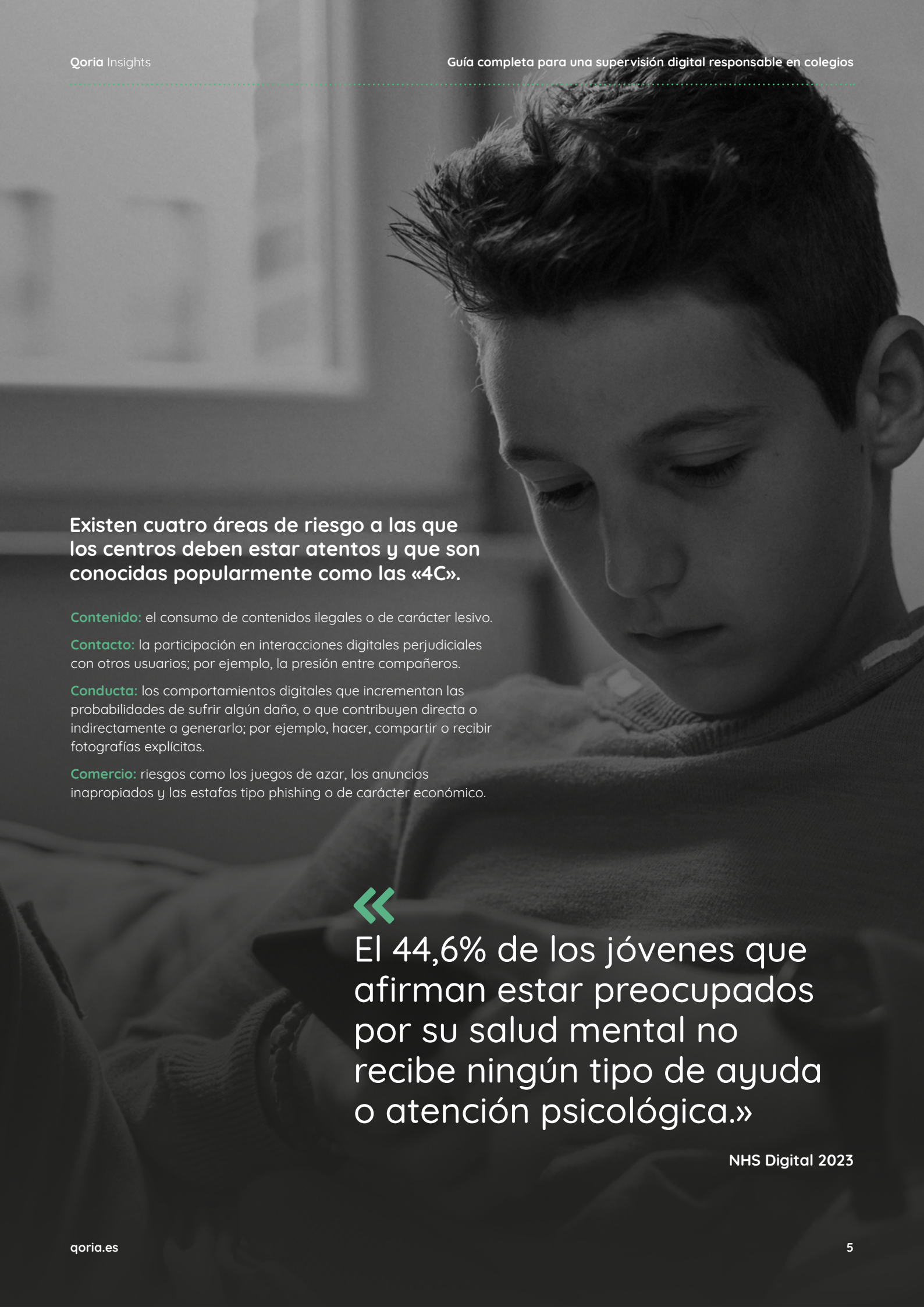
Nuestros propios estudios indican que el 95% de los docentes está convencido de que sus alumnos acudirían a ellos si sufrieran algún tipo de ciberacoso. Sin embargo, únicamente un 5% de los niños afirma que pediría ayuda a un profesor si se encontrase en esa situación. Se trata de una brecha alarmante.

La ciberseguridad de los menores constituye un problema cada vez mayor, y las autoridades de todo el planeta están empezando a reconocer ya la necesidad de que los colegios establezcan medidas de protección en este ámbito.

Esta tarea requiere necesariamente el uso de sistemas de supervisión digital, y la responsabilidad debería recaer conjuntamente sobre los equipos directivos y los coordinadores de bienestar y protección.

Muchos centros, sin embargo, aún no tienen muy claro en qué consiste el concepto de supervisión digital y qué rol debe desempeñar en su estrategia de seguridad digital.

Este documento ha sido concebido como una guía práctica para ayudar a los colegios a tomar conciencia del desafío al que se enfrentan y a responder de una manera adecuada.



Existen cuatro áreas de riesgo a las que los centros deben estar atentos y que son conocidas popularmente como las «4C».

Contenido: el consumo de contenidos ilegales o de carácter lesivo.

Contacto: la participación en interacciones digitales perjudiciales con otros usuarios; por ejemplo, la presión entre compañeros.

Conducta: los comportamientos digitales que incrementan las probabilidades de sufrir algún daño, o que contribuyen directa o indirectamente a generarlo; por ejemplo, hacer, compartir o recibir fotografías explícitas.

Comercio: riesgos como los juegos de azar, los anuncios inapropiados y las estafas tipo phishing o de carácter económico.

«El 44,6% de los jóvenes que afirman estar preocupados por su salud mental no recibe ningún tipo de ayuda o atención psicológica.»

NHS Digital 2023

2.0 Los retos que afrontan los centros educativos en este ámbito

Los colegios están sometidos a una presión cada vez mayor para supervisar lo que los estudiantes hacen, dicen y comparten a través de los dispositivos digitales.

Identificar todos los riesgos a los que los menores están expuestos puede parecer misión imposible, sobre todo en el caso de aquellos centros cuya plantilla es escasa o que se encuentran ya saturados. Por si fuera poco, la aparición de estas ciberamenazas se produce en un momento en el que la carga de trabajo de los docentes es cada vez más insostenible.

Acoso escolar

1 de cada 5 alumnos ha sufrido algún tipo de **acoso escolar a través de la Red.**

Fuente: Encuesta sobre delincuencia de Inglaterra y Gales (CSEW), 2023

Social Media

4 de cada 5 jóvenes confiesa que las redes sociales **agudizan su sensación de ansiedad.**

Fuente: Informe de la Real Sociedad para la Salud Pública

Ciberpederastia

Los delitos relacionados con los ciberengaños pederastas se han incrementado un **82%** a lo largo de los últimos cinco años.

Source: NSPCC 2023

Abusos sexuales

Más de **300 millones** de niños son **víctimas cada año de explotación y abusos sexuales a través de Internet.**

Fuente: Childlight Global Child Safety Institute, Universidad de Edimburgo, 2024

A la vista de estos desafíos, es fundamental que los centros identifiquen de forma proactiva los posibles problemas y ciberamenazas y que elaboren una estrategia integral de prevención y atención temprana.

La tecnología puede ser una herramienta educativa extraordinaria. Sin embargo, también constituye un importante factor de riesgo que puede exponer a los jóvenes a infinidad de peligros, como el ciberacoso, la explotación sexual, la radicalización y el daño que pueden conllevar para su salud mental y su integridad física. Nuestra recomendación es que compruebes periódicamente si el entorno de tu colegio utiliza las soluciones más efectivas para detectar a los estudiantes en situación de vulnerabilidad.

Con frecuencia, los centros carecen de información

Los jóvenes de hoy en día viven en un universo completamente distinto al nuestro. Para ellos, el mundo digital es inseparable de la realidad. Las redes sociales tienen una presencia constante en su día a día. Esta obsesión permanente por obtener el mayor número de rachas o me gusta lleva a muchos de ellos a contactar con desconocidos, lo que puede exponerles a un gran riesgo.

Por desgracia, en el mundo digital no hay botón «Deshacer». Los incidentes que se producen fuera del colegio pueden terminar afectando al ámbito escolar, y viceversa. Independientemente de si hablamos de la publicación de mensajes ofensivos o del envío de determinadas imágenes, no todos los centros pueden mantenerse al día, y a menudo carecen de información sobre lo que ocurre. Los alumnos en situación de vulnerabilidad y aquellos con discapacidades y necesidades educativas especiales suelen ser los más indefensos.

Los episodios más graves suelen compartirse a través de Internet. Tanto si un estudiante introduce un cuchillo en el recinto escolar, tiene intención de suicidarse o se dispone a consumir alguna sustancia ilegal, en ocasiones la única forma de detectar las señales de alarma es a través de su actividad digital.

La enorme gravedad que va asociada a estos riesgos exige una detección y una respuesta tempranas, y a menos que dispongan de una solución de supervisión digital, hay pocas probabilidades de que los colegios puedan atender sus obligaciones legales ni actuar con la diligencia debida.

El impacto a largo plazo de subestimar los riesgos

Según la NHS Foundation Trust de la Universidad de Manchester, 1 de cada 3 de las patologías mentales diagnosticadas en adultos está directamente relacionada con la vivencia de experiencias traumáticas durante la infancia. Asimismo, el 50% de estos trastornos empiezan a manifestarse alrededor de los 14 años, y el 75%, en torno a los 24 (Gov.uk). Intervenir de forma temprana mediante la supervisión digital puede contribuir a reducir considerablemente estas cifras.

La responsabilidad de los centros

Es esencial que los colegios comprueben periódicamente si utilizan las soluciones más efectivas para detectar a los estudiantes en situación de vulnerabilidad. Las soluciones de supervisión digital basadas en la tecnología les permiten identificar posibles incidentes que de otro modo podrían pasar inadvertidos. Estas herramientas proporcionan una radiografía más detallada de los problemas y las ciberamenazas, detectan las situaciones de riesgo en una fase temprana y proporcionan evidencias claras que son fundamentales a la hora de asegurarse de que los jóvenes reciben la asistencia adecuada.

> «En 2023, Qoria Monitor detectó un niño en una posible situación de especial vulnerabilidad cada 2 minutos, lo que supone **un incremento del 33% frente al año anterior.»**
>
> Datos de Qoria Monitor

3.0 El rol fundamental de la supervisión digital

A medida que el número de ciberamenazas se multiplica, también emergen nuevas tecnologías capaces de neutralizarlas.

¿En qué consiste la supervisión digital?

El concepto de «supervisión digital» hace referencia a un sistema tecnológico que monitoriza constantemente los dispositivos digitales del centro en busca de posibles señales que indiquen que hay un alumno en peligro.

Una forma de detectar riesgos

Los sistemas de supervisión digital os permiten identificar rápidamente a aquellos estudiantes que se encuentran en una situación de vulnerabilidad. Las amenazas graves como el suicidio, la ciberpederastia o la pertenencia algún tipo de grupo violento se pueden detectar en tiempo real si los niños utilizan el teclado de alguna manera para acceder a contenidos, enviar mensajes, buscar información o expresar sus emociones por escrito, aunque borren el texto inmediatamente o nunca lleguen a pulsar el botón «Enviar» o «Intro».

El objetivo de estas herramientas es ayudaros a identificar y reaccionar ante los problemas de los que antes no teníais constancia y a ofrecer apoyo a los menores que hasta ese momento no habían dado señales de alarma. Asimismo, en el caso de aquellos alumnos que ya se encontraban en una situación vulnerable, podéis comprobar si el problema se ha agravado y poner las pruebas a disposición de los organismos y autoridades competentes.

La supervisión digital funciona como una red de seguridad para aquellos docentes que, debido a la carga de trabajo inherente a sus responsabilidades, no siempre pueden detectar lo que sucede en Internet.

Cómo funciona

En líneas generales, hay dos tipos de soluciones de supervisión digital disponibles:

1. Soluciones no moderadas por personal externo.
2. Soluciones moderadas por personal externo.

Soluciones no moderadas por personal externo

Cuando un estudiante o un miembro del personal escribe o ve algo alarmante en un dispositivo digital, el sistema de supervisión realiza una captura de pantalla. Esta captura puede ser de un navegador, un correo electrónico, un documento de Microsoft, una red social o una sala de chat. La supervisión digital no funciona como la cámara de un circuito cerrado; en lugar de grabar todo, únicamente captura aquellos instantes en los que la persona muestra algún indicio de peligro.

El sistema procede a evaluar la gravedad del riesgo a partir del análisis de la imagen. Los colegios pueden revisar las alertas de riesgo, lo que les permite actuar inmediatamente ante los casos más graves.

Todas las alertas quedan registradas en una consola. Eso significa que podéis consultar los detalles sobre ellas al iniciar sesión y decidir cuáles son falsos positivos y cuáles podrían requerir atención inmediata. Las alertas de bajo nivel no se descartan. Las soluciones más completas las analizan en busca de patrones y tendencias que puedan resultar preocupantes.

Por ejemplo, el hecho de que un niño busque en Internet las palabras «bola de algodón» y más tarde chatee en Facebook Messenger sobre una dieta podría indicar la existencia de un trastorno de alimentación que, sin la ayuda del análisis de tendencias del sistema, habría pasado inadvertido.

Soluciones moderadas por personal externo

El otro tipo de herramientas de supervisión digital son las moderadas por personal externo. En estas soluciones más avanzadas, se realiza una captura del mismo modo que en el caso anterior. A continuación, una inteligencia artificial (IA) analiza la imagen y genera un perfil a partir del contexto en el que se ha producido la alerta. La IA también se encarga de filtrar los falsos positivos.

El siguiente paso es enviar la captura a un moderador humano para que la revise. El analista evalúa la imagen y establece la gravedad de la alerta. En este punto, también se descarta cualquier falso positivo que haya podido superar la fase anterior.

Las alertas graves se ponen inmediatamente en conocimiento del centro de forma telefónica, y las alertas menores se pueden enviar como un informe en el momento que os resulte más conveniente. Muchas empresas ofrecen un portal de seguridad en el que podéis iniciar sesión, consultar el contexto completo en el que se ha producido la alerta y recopilar cualquier evidencia adicional que necesitéis.

Principales diferencias

Soluciones no moderadas por personal externo

- Tienen un coste más asequible.
- Permiten a los colegios personalizar el entorno de forma individual.
- Evalúan el nivel de gravedad de cada alerta.
- No requieren de conexión a Internet.
- Disponen de una consola que facilita a los centros la tarea de acceder a los datos y analizarlos.

Recomendadas para: colegios cuyo coordinador de bienestar dispone del tiempo necesario para analizar y evaluar los riesgos.

Soluciones moderadas por personal externo

- La elaboración de perfiles mediante IA permite obtener una perspectiva clara del contexto en el que se ha producido cada alerta, lo que contribuye a minimizar el número de falsos positivos y, por lo tanto, a reducir la carga de trabajo del coordinador de bienestar.
- Un moderador humano —miembro de un equipo profesional— revisará todas las capturas de pantalla del centro para analizar su grado de prioridad y eliminar cualquier falso positivo que haya podido eludir los filtros.
- No requieren de conexión a Internet.
- Permiten ahorrar tiempo, ya que descartan la mayoría de los falsos positivos.

Recomendadas para: colegios cuyo coordinador de bienestar compagina esta tarea con otro tipo de responsabilidades y necesita una ayuda adicional.

4.0 Las herramientas de supervisión en la detección de riesgos: casos reales

Los siguientes ejemplos ilustran el rol que puede desempeñar la supervisión a la hora de detectar situaciones de riesgo. Estos supuestos están basados en historias reales, aunque los nombres y los detalles de cada caso se han modificado para proteger la privacidad de los menores implicados.

Sistema de supervisión utilizado: **ninguno**

Roberto, 13 años

Tipo de riesgo:
Conducta violenta hacia otros alumnos

1. Roberto se llevó un cuchillo al colegio.
2. En un determinado momento, le envió a uno de sus compañeros un mensaje diciendo que iba a «darle su merecido» a otro estudiante.
3. Esa misma tarde, apuñaló al niño al que había amenazado.
4. El registro de ese mensaje fue descubierto al día siguiente por el técnico del centro después de llevar a cabo un minucioso análisis forense del ordenador que había estado usando Roberto.

Si la escuela hubiera utilizado un sistema de supervisión digital, habrían podido detectar el riesgo y evitado el apuñalamiento.

Daniel, 14 años

Tipo de riesgo:
Consumo de drogas

1. Daniel estaba trabajando en un documento compartido con un amigo.
2. En un momento dado, escribió un mensaje que decía: «¿Te apetece echar un canuto?». Su amigo aceptó y a continuación eliminó el mensaje.
3. Cuando llegó la hora del recreo, Daniel fue a buscar a su amigo y compartieron un porro.
4. Nadie se enteró de que consumían marihuana hasta que un profesor encargado de la vigilancia del patio les descubrió fumando semanas más tarde.

Si el centro hubiera utilizado un sistema de supervisión digital, habrían podido detectar este incidente y prevenir el consumo de drogas.

Lucía, 15 años

Tipo de riesgo:
Salud mental

1. Lucía estaba usando uno de los ordenadores de la biblioteca del colegio.
2. En un momento dado, escribió las palabras «cómo tratar la depresión y la ansiedad» en Google.
3. Cuando su depresión se agravó, acudió a un foro online sobre el tema y empezó a cortarse.
4. Lucía se pasó semanas cubriéndose los brazos y las piernas para ocultar las lesiones que se producía. Su profesora de Educación Física no notó las cicatrices hasta que no comenzaron el bloque de Gimnasia.

Si el colegio hubiera utilizado un sistema de supervisión digital, habrían podido detectar que Lucía se encontraba en una situación de riesgo y habría podido recibir tratamiento.

Sistema de supervisión utilizado: una solución no moderada por personal externo

Mateo, 12 años

Tipo de riesgo:
Violencia

1. Mateo se encontraba en clase de Matemáticas. El profesor había propuesto un ejercicio de repaso que debían resolver en el ordenador en un periodo de 20 minutos.

2. Mientras el profesor ayudaba a un compañero al otro lado del aula, Mateo escribió esta nota en la pantalla: «Creo que Adrián tiene un cuchillo».

3. En ese instante, el sistema activó una alerta y se la envió al coordinador de bienestar. Mateo le dio un codazo a su mejor amigo para que leyese la nota. Este vio el mensaje, pero entonces el profesor de Matemáticas empezó a regañar a la clase por no prestar atención. Mateo borró inmediatamente lo que había escrito.

El coordinador de bienestar que estaba de guardia vio la alerta y el nivel de gravedad que el sistema le había asignado. Como disponía de una panorámica completa de todos los datos referentes a la seguridad del colegio, consiguió averiguar a qué Adrián se refería la nota. La escuela evitó que la situación fuera a más aplicando el protocolo de actuación previsto en su estrategia de seguridad para la confiscación de armas.

Sara, 13 años

Tipo de riesgo:
Acoso entre compañeros

1. Una riña entre dos amigas provocó que un grupo de niñas crease un sitio web titulado «Club de haters de Sara Marcos».

2. Las niñas se dedicaban a publicar mensajes maliciosos anónimos en el sitio para burlarse de ella.

3. Sara le contó a un profesor lo que estaba pasando, pero no sabía quiénes eran los responsables.

El colegio personalizó la configuración de detección del sistema para recibir una alerta cada vez que alguien escribiera el nombre «Sara Marcos» en ese sitio web. El coordinador de bienestar recibió cinco alertas de niñas que habían publicado comentarios en el sitio en un periodo de 24 horas y pudo llevar a cabo un seguimiento del caso.

Sistema de supervisión utilizado: **una solución moderada por personal externo**

Laura, 15 años

Tipo de riesgo:
Discriminación

1. Laura grabó un vídeo sobre una compañera llamada Sofía y pegó una foto de su cabeza encima del cuerpo de un perro. Sofía padecía el síndrome de Marcus-Gunn.
2. Laura creó una página titulada «Sofía, la perra».
3. Natalia, una amiga de Laura, visitó el sitio web desde su Chromebook y escribió un comentario que rezaba «Menuda perra está hecha».
4. El sistema activó una alerta y se la envió a un moderador humano.
5. El moderador evaluó la situación y avisó al centro.
6. El coordinador de bienestar inició sesión en la consola de supervisión para revisar toda la información del contexto en el que se había producido la alerta.

El coordinador pudo activar inmediatamente el protocolo de actuación del colegio para este tipo de situaciones.

Mohamed, 15 años

Tipo de riesgo:
Tendencias suicidas

1. Mohamed buscó en Google las palabras «cómo suicidarse sin dolor».
2. Aunque nunca llegó a pulsar el botón «Intro», el sistema registró sus pulsaciones y envió una alerta al moderador humano.
3. El moderador comprobó que Mohamed había buscado previamente las palabras «paracetamol» y «codeína» y se puso inmediatamente en contacto con el coordinador de bienestar del centro.

El coordinador de bienestar inició sesión en la consola, localizó la ubicación de Mohamed, trazó rápidamente un plan para activar el protocolo de actuación para menores en situación de riesgo e intervino antes de que fuera demasiado tarde.

Harry, 10

Tipo de riesgo:
Conducta autolesiva

1. Lucas buscó en Google las palabras «¿Es posible cortarte el pelo tú mismo?».
2. El sistema activó una alerta por conducta autolesiva porque el mensaje incluía el término «cortarte».

La IA y el moderador humano descartaron esta alerta como un falso positivo. Los sistemas de supervisión digital basados en moderadores humanos os permiten responder rápidamente ante las alertas y ahorrar tiempo filtrando los falsos positivos como en el caso anterior. Las empresas proveedoras que adoptan un enfoque más proactivo suelen desarrollar perfiles individuales y aprender de las experiencias pasadas para ofreceros una radiografía clara de la situación en la que se encuentran los alumnos.

5.0 Pautas para elegir la herramienta de supervisión adecuada

Hay algunas medidas que todos los colegios pueden poner en práctica para asegurarse de que disponen de la herramienta de supervisión adecuada.

1. Pide a tu centro que revise las políticas de supervisión que aplica actualmente con ayuda de la tabla que aparece a continuación.

2. Evaluad las áreas en las que el sistema implementado no se ajusta a vuestras necesidades o resulta insuficiente para determinar qué tipo de solución necesitáis.

1. Pide a tu centro que revise las políticas de supervisión actuales

Recomienda a tu colegio que compruebe si está usando las soluciones más efectivas para detectar a los estudiantes en situación de vulnerabilidad. La siguiente tabla contiene una serie de pautas recomendadas* acompañadas de un código de colores tipo semáforo para ayudaros a identificar las posibles brechas de vuestro sistema de supervisión actual.

*Estas pautas han sido elaboradas a partir de las directrices proporcionadas por el gobierno de Reino Unido, pero los principios en los que se basan son aplicables a cualquier contexto global.

Política/ configuración	Verde	Ámbar	Rojo
Políticas de supervisión	Aplicamos una política de buenas prácticas que entronca con la cultura de nuestro centro y que nos sirve de principio rector para educar en ciberseguridad.	Aplicamos la misma política de buenas prácticas a todos los estudiantes.	Les proporcionamos una serie de pautas sobre lo que pueden hacer y lo que no cuando se conectan a Internet.
Dispositivos	Nuestro sistema supervisa todos los dispositivos del colegio.	Nuestro sistema es compatible con todos los dispositivos administrados del centro.	Nuestro sistema solo es compatible con dispositivos de escritorio o únicamente supervisamos los dispositivos de forma física.
Configuración multicentro	El sistema es totalmente personalizable y nos permite ajustar la configuración de forma granular para obtener una panorámica completa de toda la red de centros y una vista individual de cada colegio. Alternativamente, disponemos de un sistema de moderación humana con un portal de acceso independiente para cada centro.	Nuestra institución utiliza un sistema de supervisión a nivel global, pero los colegios no disponen de un portal para consultar la actividad que se ha detectado en su centro a nivel individual.	Nuestra solución no dispone de ninguna vista granular. Tenemos que utilizar un sistema independiente para cada centro.
Procesos			
Gestión de las alertas en función del grado de prioridad	Visualizamos las alertas en tiempo real, lo que permite que el coordinador de bienestar pueda reaccionar inmediatamente ante las situaciones de riesgo en caso necesario. El sistema detecta una amplia variedad de acciones tanto en línea como sin conexión.	Las alertas se catalogan en función del grado de riesgo, pero no se muestran en tiempo real. No siempre podemos detectar los incidentes que se producen fuera de los navegadores. El sistema presenta ciertas limitaciones a la hora de realizar capturas de pantalla.	El coordinador de bienestar debe revisar manualmente el historial de registros para detectar los posibles problemas. El sistema ofrece pocas opciones para gestionar las alertas en función de su prioridad o es imposible hacerlo. Disponemos de poco margen para catalogar las diferentes amenazas. Los profesores dejan una nota cada vez que detectan un incidente.
Flexibilidad	Utilizamos un sistema de análisis y elaboración de perfiles inteligente para obtener una radiografía completa de la actividad de los alumnos. Asimismo, hemos implementado un mecanismo de moderación humana para asegurarnos de que únicamente se filtran las situaciones de riesgo que se ajustan a los criterios y el nivel de gravedad establecidos.	Cada colegio puede personalizar los niveles de gravedad y los términos utilizados para adaptarlos a las características del alumnado. Además, podemos adaptar la supervisión a los distintos grupos de clases para evitar que el software realice capturas de pantalla relacionadas con el currículo.	Nuestra solución apenas ofrece opciones de personalización y no incluye ningún módulo de elaboración de perfiles ni de IA. Dependemos íntegramente de la supervisión presencial.

	Verde	Ámbar	Rojo
Procedimientos			
Elaboración de informes y recopilación de evidencias	Podemos consultar un informe con toda la información referente al contexto de cada alerta. Analizamos las tendencias que surgen entre los diferentes grupos y perfiles de estudiantes.	Obtenemos información contextual a través de capturas de pantalla que utilizamos como evidencia.	Tardamos mucho tiempo en comprobar el historial de registros para asegurarnos de que no hemos pasado nada por alto. Nuestra capacidad para recopilar pruebas es limitada. No disponemos de información contextual. Cada tutor notifica los incidentes al coordinador para que los anote.
Almacenamiento de datos	Almacenamos los datos en una ubicación externa protegida por un avanzado sistema de ciberseguridad con múltiples capas de protección.	Almacenamos los datos en una ubicación segura protegida por un buen sistema de ciberseguridad.	Almacenamos físicamente los datos a nivel local y no disponemos de ningún sistema de seguridad adicional.
Impacto			
¿Cuál es el objetivo y el grado de impacto de vuestra estrategia de supervisión?	Las alertas de riesgo se evalúan en tiempo real mediante IA y un sistema de moderación humana. Los falsos positivos se descartan y los coordinadores de bienestar únicamente tienen que responder ante las alertas reales.	El orden en el que se enumeran las alertas depende del grado de riesgo. Eso significa que el coordinador de bienestar tiene que revisarlas manualmente una a una. El sistema proporciona evidencias textuales.	No respondemos ante las alertas con la rapidez necesaria. Las pruebas que podemos recopilar son muy limitadas. Existe el riesgo de que los profesores no detecten el uso indebido de los dispositivos o los posibles incidentes porque los niños pueden ocultar fácilmente lo que aparece en pantalla.
Escalabilidad			
Por tamaño de la institución, la plantilla o el ratio de alumnos	Nuestro sistema de supervisión es apto para cualquier red de centros que desee integrar los controles granulares en sus soluciones actuales de forma efectiva.	Nuestro sistema de supervisión es apto para entornos en los que los colegios no necesitan acceder de forma individual a las tendencias que indican las evidencias y están satisfechos con el tipo de informes que genera.	Nuestro sistema no es apto para redes de centros.
Restricciones			
Posibles limitaciones	No podemos controlar íntegramente el sistema de supervisión desde los centros que conforman nuestra red.	Tardamos más en descartar los falsos positivos y corremos el riesgo de no disponer de la evidencia necesaria para imponer medidas disciplinarias.	Velamos por la seguridad de cientos de estudiantes. Tenemos que comprobar manualmente los archivos de registro o vigilar por encima del hombro lo que hacen los niños. A veces no interpretamos correctamente los registros.

2. Evaluad las áreas en las que el sistema implementado no se ajusta a vuestras necesidades o resulta insuficiente para determinar qué tipo de solución necesitáis

El resultado de esta revisión os permitirá establecer cuál debe ser el siguiente paso. Si vuestro centro tiende a mantenerse en la zona verde de la tabla, el número de medidas a adoptar será relativamente bajo. Si la evaluación revela que algunas áreas presentan más deficiencias que otras, deberíais considerar la posibilidad de utilizar una solución de supervisión basada en la tecnología.

Si a lo largo de la evaluación la mayor parte de las áreas muestran un nivel de deficiencia entre ámbar y rojo, es posible que debáis implementar un sistema de supervisión digital a todos los niveles para adecuar lo antes posible vuestra protección a los estándares exigibles.

«Una buena solución de supervisión digital no debería invadir la privacidad de los alumnos, sino contribuir a identificar aquellas situaciones de riesgo que entran en nuestro ámbito de responsabilidad según lo establecido por las administraciones competentes».

6.0 Cómo integrar la supervisión digital en vuestra estrategia de seguridad

A la hora de implementar una solución de supervisión digital, es importante que se integre de forma efectiva y eficiente en el plan de protección actual del centro.

En caso contrario, puede entrar en conflicto y generar tensiones con vuestros protocolos de actuación, lo que a su vez puede derivar en incumplimientos y negligencias a la hora de detectar los riesgos y, en última instancia, acabar comprometiendo la seguridad de los menores.

A continuación, enumeramos algunos aspectos clave que debéis tener en cuenta para poder elegir la solución adecuada y evitar problemas durante el proceso de integración.

Integración con los planes de prevención

- ¿Vuestra solución de supervisión digital es coherente con los protocolos que habéis establecido para identificar a los estudiantes en situación de riesgo?
- ¿El coordinador de bienestar puede acceder fácilmente al sistema para poder evaluar el grado de riesgo de forma rápida y eficaz sin pasar por alto ningún aspecto importante?
- Aseguraos de que las funciones que incluye la solución evalúen la gravedad y cataloguen el tipo de riesgo de acuerdo con lo previsto en vuestros protocolos de actuación.
- ¿La solución permite a vuestro centro reaccionar rápidamente ante los problemas? Comprobad cuántos minutos tardan en activarse las alertas y si el proceso se lleva a cabo en tiempo real.
- ¿El sistema permite realizar capturas en línea y sin conexión de los navegadores, aplicaciones de correo electrónico, documentos de Microsoft y salas de chat? Las alertas pueden producirse tanto en un documento de Word como en un espacio más previsible, como una sala de chat o una aplicación de correo electrónico. Carecer de este grado de penetración afecta a la capacidad del colegio de detectar las situaciones de riesgo.
- Si es necesario, aseguraos de que el sistema permite supervisar varios idiomas al mismo tiempo.

Integración con las políticas de seguridad

- ¿Vuestra solución de supervisión os permite detectar cualquier señal de alarma en diferentes contextos, tanto en el supuesto de que un desconocido utilice el correo electrónico o un chat web como en el marco de una conversación digital entre dos estudiantes?
- ¿El sistema os proporciona una imagen más clara de aquellas situaciones de riesgo que se desarrollan fuera del recinto escolar o del ámbito doméstico?
- Una buena solución de supervisión digital no debería invadir la privacidad de los alumnos, sino contribuir a identificar aquellas situaciones de riesgo que entran en el ámbito de responsabilidad del centro según lo establecido por las administraciones competentes.
- Aseguraos de comprobar cuál es el período de retención de los datos y si el lugar de almacenamiento dispone de las medidas de seguridad necesarias.
- Averiguad desde qué país opera y proporciona asistencia técnica el desarrollador. Comprobad que disponen de una normativa de protección de datos apropiada.

Integración con los protocolos de actuación

- Aseguraos de que, en el caso de que detectéis una situación de riesgo, vuestra solución de supervisión digital sea compatible con los protocolos que habéis establecido para estos supuestos.
- ¿La solución os permite recopilar evidencias e información para compartirla con los padres o con los organismos correspondientes?
- ¿Recopila información contextual sobre las capturas de pantalla para proporcionar una panorámica completa de la situación?
- ¿Es apta para todas las edades? Aseguraos de que es posible adaptar el grado de supervisión y los contenidos que se monitorizan en función de los diferentes grupos de edad y los proyectos curriculares. De esta forma, os resultará más fácil priorizar las alertas y evitar las capturas falsas.

7.0 Preguntas frecuentes

¿Cuál suele ser el precio de las soluciones de supervisión digital?

El precio de este tipo de soluciones varía dependiendo del número de estudiantes, la calidad y el grado de alcance de la supervisión, si evalúan en tiempo real la gravedad de las alertas, si cuentan con un sistema de moderación humana o basado en la IA y otros factores. La mayoría de las empresas proveedoras de referencia, como Qoria, ofrecen una amplia gama de soluciones dependiendo de las necesidades y el presupuesto de los colegios.

¿En qué partida presupuestaria se suelen englobar?

El origen de los fondos puede diferir de un centro a otro. Dado que el principal responsable de proteger la seguridad digital de los alumnos dentro del ámbito de responsabilidad del colegio es el coordinador de bienestar, algunos centros deciden sufragar este gasto con cargo a las partidas reservadas para la seguridad o la prevención de riesgos, mientras que otros optan por utilizar alguna asignación de carácter general o la dotación prevista para el departamento de TIC.

¿Cómo podemos asegurarnos de que el sistema de supervisión almacena los datos de forma segura?

Uno de los aspectos que debéis tener en cuenta es la protección de la información confidencial. Las empresas proveedoras suelen disponer de mecanismos para demostrar dónde almacenan los datos. En el caso de Qoria, garantizar vuestra privacidad en este ámbito es una de nuestras principales prioridades. Toda la información se aloja en un centro de datos de Microsoft Azure protegido según lo dispuesto en el RGPD y en las normativas de protección de datos locales.

¿Cómo podemos estimar el impacto que tendría una solución de supervisión digital en nuestros sistemas de TI?

Es recomendable que discutáis con la empresa proveedora hasta qué punto resulta invasivo el software y si disponéis de la capacidad necesaria para ejecutarlo en la red de vuestro centro. La solución de supervisión digital de Qoria no ejerce ningún impacto sobre el rendimiento de vuestro sistema y se ejecuta en segundo plano de forma silenciosa. Los usuarios no son conscientes de que se está supervisando su actividad digital ni de que se ha realizado una captura de pantalla.

¿Cuáles son los pasos a seguir a la hora de implementar este tipo de soluciones?

El proceso de instalación puede variar dependiendo de la empresa proveedora. Preguntadles si es necesario que vuestro personal disponga de conocimientos técnicos específicos y si el sistema está basado en la nube. En el caso de Qoria, la instalación es relativamente sencilla, y no hace falta ningún tipo de conocimiento técnico.

Si ya disponemos de un sistema de filtrado web, ¿por qué necesitamos otro de supervisión digital?

Los sistemas de filtrado web bloquean el contenido para evitar que los estudiantes puedan acceder a él. En este sentido, juegan un papel fundamental. Sin embargo, estos sistemas no permiten supervisar lo que los niños escriben en sus dispositivos. La mayoría no dispone de ninguna función para recibir alertas en tiempo real, algo que resulta fundamental para poder tomar medidas rápidamente. Los sistemas de supervisión digital y filtrado web trabajan conjuntamente para proporcionar una sólida capa de protección digital que contribuye a garantizar la seguridad de los más pequeños.

El sistema de nuestro colegio ya está al límite de sus capacidades. ¿Incorporar la supervisión digital no incrementará el número de incidentes de seguridad que tenemos que gestionar?

La mayoría de las empresas proveedoras están familiarizadas con esta problemática y ofrecen una amplia gama de soluciones que se adaptan al nivel de capacidad de cada centro. En Qoria disponemos desde opciones para evaluar la gravedad de los riesgos de forma manual hasta sistemas de moderación humana y basados en la IA que permiten ahorrar varias horas a la semana.

¿Los sistemas de supervisión pueden realizar capturas innecesarias de los temas que componen el currículo?

Algunas soluciones permiten personalizar la configuración de detección de riesgos para eliminar los temas centrales del currículo de determinadas asignaturas. Sin embargo, deberíais tener cuidado a la hora de hacerlo para no eliminar ningún contenido que pueda resultar necesario en un momento dado. Cada colegio tiene necesidades diferentes; de ahí que los mejores sistemas de supervisión digital sean modulares y ofrezcan la flexibilidad necesaria en términos de configuración para adaptarse a vuestro entorno.

¿Estas soluciones se pueden escalar para instituciones más grandes?

Si formáis parte de una institución educativa más grande, es esencial que comprobéis qué opciones de escalabilidad ofrece la empresa proveedora. Solicitad información sobre los plazos de entrega y el proceso de instalación. Todas las soluciones de supervisión digital de Qoria son fácilmente escalables gracias al impacto mínimo que ejercen sobre las redes, su portal basado en la nube, la simplicidad del proceso de instalación y la posibilidad de recibir actualizaciones automáticas.

¿Tienes alguna duda?

Ponte en contacto con nuestros especialistas en seguridad digital. Estaremos encantados de ayudarte.

Correo electrónico: enquiries@qoria.es

Sobre Qoria

Qoria es una empresa de tecnología internacional dedicada a proteger la seguridad y el bienestar de los más pequeños en el mundo digital. Conocida anteriormente como Family Zone, comenzó su andadura en 2015, cuando cuatro padres tomaron la determinación de hacer de Internet un lugar más seguro para sus hijos con la única ayuda de un puñado de diapositivas.

Nuestro crecimiento ha sido tan rápido como espectacular. En la actualidad, nuestro equipo está integrado por más de 500 profesionales repartidos a lo largo y ancho de 3 continentes; supervisamos más de 29 0000 escuelas, ofrecemos apoyo a más de 6 millones de padres y jugamos un papel fundamental a la hora de garantizar la seguridad de 24 millones de niños.

Nuestra familia de profesionales está compuesta por los siguientes equipos:

Nuestra familia de profesionales está compuesta por los siguientes equipos:

Qoria Europe (EMEA)

Linewize (América del Norte, Australia, Nueva Zelanda)

Smoothwall (Reino Unido)

Qustodio (España, América del Norte)

ySafe (Australia)

Disponemos de un alcance global y experiencia local, lo que nos permite ampliar al máximo la disponibilidad de nuestras soluciones y al mismo tiempo satisfacer las necesidades únicas de los colegios y las comunidades con los que colaboramos.

Nuestra misión es posicionarnos como un socio de confianza para estos centros; acercarles a sus objetivos en el plano normativo y ayudarles a abordar los retos que afrontan en el ámbito de la seguridad sin perder de vista el contexto cultural en el que se mueven.

Hemos realizado grandes progresos desde el nacimiento de Qoria, pero los desafíos a los que siguen enfrentándose los niños constituyen una demostración de que todavía nos encontramos muy lejos de nuestra meta.

El viaje continúa.

Contacto

Plantéate la siguiente pregunta

¿Estás seguro de que tu centro dispone de unos mecanismos de supervisión efectivos y está capacitado para proteger la seguridad de los más pequeños en tiempo real?

Si la respuesta es negativa, ha llegado el momento de comprobarlo. Si no estás seguro de cómo hacerlo o tienes alguna duda, contacta con los especialistas en seguridad digital de Qoria, los cuales estarán encantados de ayudarte.

Solicita una demostración gratuita

Si deseas solicitar una demostración gratuita sin compromiso de Qoria Monitor o hacernos alguna pregunta, ponte en contacto con 38 grados.

Web: www.38grados.com
Correo: contacto@38grados.com

Qoria

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 a los que se enfrentan los jóvenes, ofreciéndoles apoyo en el colegio, en casa y en cualquier lugar.

Más información:
www.qoria.es

38°Lab
INNOVACIÓN Y DESARROLLO

Somos un Laboratorio que integra y desarrolla soluciones innovadoras para organizaciones educativas y empresariales en América Latina.

web: **www.38grados.com**
Correo: **contacto@38grados.com**