Programa de Jornadas Escolares

Promoción del uso seguro y responsable de Internet entre los menores

---

Uso seguro y responsable de las TIC

Unidad Didáctica y contenidos de apoyo al docente

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

Licencia de contenidos

CONTENIDO

1. Presentación de la Unidad Didáctica

Esta Unidad Didáctica aborda una panorámica generalista sobre los principales riesgos relacionados con el uso de las TIC por parte de los menores, con objeto de reconocerlos y saber actuar ante ellos, promoviendo buenas prácticas para realizar un uso seguro y responsable de la tecnología.

De esta manera, a lo largo de Unidad Didáctica trataremos aspectos relacionados con la importancia del **uso crítico de la información**, puesto que tan necesario como que los más jóvenes puedan acceder a la gran cantidad de información compartida a través de Internet es el hecho de fomentar en el alumnado una **actitud crítica** hacia el contenido que encuentran, dotándoles de criterio y herramientas que les permitan filtrar y analizar la veracidad de la información. Concretamente trataremos aspectos relacionados con **contenido no adecuado, bulos, mensajes en cadena, virus y fraudes.**

Por otra parte, se hace imprescindible abordar la necesidad de preservar la **privacidad en la red**. Apuntaremos conceptos como **identidad digital y reputación online**, teniendo en cuenta que, por lo general, es difícil para muchos preadolescentes pensar en términos de futuro cuando se trata de acciones que quieren tomar hoy.

Desgraciadamente el **ciberbullying** se está convirtiendo en uno de los principales riesgos del uso de Internet entre los más jóvenes. A pesar de la aparente familiaridad y destreza de éstos a la hora de utilizar la tecnología, su uso real no siempre va por el derrotero esperado y son muchos los menores y adolescentes que, enfrentados a situaciones de riesgo como el **ciberacoso**, carecen de estrategias y pautas para abordar éstas con éxito. Por ello es necesario abordar este riesgo y fomentar valores como el respeto y el diálogo para mantener relaciones sanas y una actitud de rechazo ante este tipo de conductas.

También en la red es necesario seguir una serie de normas sociales que faciliten la convivencia, al igual que en cualquier otro tipo de comunidad o relación social. Así, el último aspecto a tratar en esta Unidad Didáctica será la **Netiqueta**, entendida como conjunto de pautas de buen comportamiento o de buenas prácticas para comunicarse en la red que, construida de forma natural y de manera colaborativa entre las personas que utilizamos la red, fomenta que este espacio sea agradable y seguro para todos.

Al finalizar la Unidad Didáctica el alumnado será capaz de entender los principales riesgos relacionados con el uso de las TIC, detectar situaciones de riesgo, utilizar estrategias para actuar ante ellas y desarrollar prácticas de prevención para disfrutar de la tecnología de forma segura.

2. Ficha descriptiva

Destinatarios		Alumnado de 6º de Primaria y ESO.
Duración		2 sesiones de 50 minutos
Objetivos didácticos	**General**	Identificar los principales riesgos asociados al uso de las TIC, abordando estrategias y pautas de conducta que ayuden a prevenirlos y/o saber actuar ante ellos.
	Específicos	• Identificar y reconocer la presencia de contenidos inapropiados e ilícitos en la Red, contenidos falsos, bulos, leyendas urbanas… y saber cómo actuar ante ellos, aplicando las precauciones y pautas adecuadas. • Reconocer la importancia de proteger todos los dispositivos electrónicos frente a los posibles riesgos derivados de virus y fraudes, sabiendo tomar las medidas de prevención oportunas. • Entender el concepto de ciberacoso, identificando los riesgos que conlleva, el daño que produce y los factores que ayudan a prevenirlo. • Comprender los conceptos de privacidad, identidad digital y reputación online y tomar conciencia de su importancia, tanto en la actualidad, como de cara al futuro, sabiendo adoptar pautas para una correcta gestión de la privacidad. • Entender la conveniencia de promover el comportamiento cívico en la Red, identificando pautas básicas de actuación.
Contenidos de aprendizaje		• Contenidos apropiados e inapropiados. Riesgos asociados. • Virus y fraude electrónico. Medidas de prevención. • Conceptos de ciberacoso: ciberbullying o ciberacoso escolar. • Conductas y pautas para la prevención del acoso escolar. • Conceptos de privacidad, identidad digital y reputación online. • Importancia y consecuencias positivas y negativas de la información que se comparte en la Red. • Concepto de Netiqueta. Principales buenas prácticas en las interacciones digitales.

Áreas competenciales	**Digitales***	**Área Información (nº 1)**: Identificar, localizar, obtener, almacenar, organizar y analizar información digital, evaluando su finalidad y relevancia para las tareas docentes Y en concreto con las competencias: • **Evaluación de la información (1.2)** Reunir, procesar, comprender y evaluar información de forma crítica. **Área Comunicación (nº 2):** Comunicarse en entornos digitales, compartir recursos por medio de herramientas en red, conectar con otros y colaborar mediante herramientas digitales, interaccionar y participar en comunidades y redes educativas. Y en concreto con las competencias: • **Interacción mediante nuevas tecnologías (nº 2.1)** Interaccionar por medio de diversos dispositivos y aplicaciones digitales, entender cómo se distribuye, presenta y gestiona la comunicación digital, comprender el uso adecuado de las distintas formas de comunicación a través de medios digitales, contemplar diferentes formatos de comunicación, adaptar estrategias y modos de comunicación a destinatarios específicos. • **Netiqueta (nº 2.5)** Conocer y respetar las normas de conducta en interacciones en línea o virtuales, reconocer la diversidad cultural, ser capaz de protegerse a sí mismo y a otros de posibles peligros en línea (por ejemplo, el ciberacoso), desarrollar estrategias activas para la identificación de las conductas inadecuadas. • **Gestión de la identidad digital (nº 2.6):** Crear, adaptar y gestionar la identidad digital, ser capaz de proteger la propia reputación digital y de gestionar los datos generados a través de las diversas cuentas y aplicaciones utilizadas. **Área Seguridad (nº 4):** Protección de información y datos personales, protección de la identidad digital, medidas de seguridad, uso responsable y seguro. Y en concreto con la competencia: • **Protección de datos personales e identidad digital (nº 4.2):** Entender los términos habituales de uso de los programas y servicios digitales, proteger activamente los datos personales, respetar la privacidad de los demás, protegerse a sí mismo de amenazas, fraudes y ciberacoso. • **Protección de la salud (nº 4.3)**: Evitar riesgos para la salud relacionados con el uso de la tecnología en cuanto a amenazas para la integridad física y el bienestar psicológico. *Referencia «Marco Común de la Competencia Digital Docente» INTEF (Instituto de Tecnologías Educativas y de Formación del Profesorado) (2013)

	Clave	• **Sociales y cívicas (CSC):** adquirir habilidades para relacionarse digitalmente de manera cívica y respetuosa, desarrollando un pensamiento crítico que le ayude a comprender los códigos de conducta en el entorno digital y que prevengan de actitudes y conductas de ciberacoso, favoreciendo el respeto y la mejora de la convivencia. • **Aprender a aprender (CPAA)**: desarrollar habilidades para que, de manera autónoma, comprenda la necesidad de conocer las peculiaridades de los servicios y aplicaciones que utilice en la red, para saber cómo establecer relaciones correctas y seguras mientras haga uso de ellos. Debe ser capaz de identificar los riesgos de seguridad vinculados con la privacidad en nuevos servicios y comenzar a construir de forma positiva su identidad digital como elemento motivador para preservar y seguir desarrollando una buena gestión de la privacidad y de su reputación online. • **Conciencia y expresiones culturales (CEC):** comprender las singularidades de la red como medio de comunicación e información y valorar la libertad de expresión respetando la diversidad cultural. • **Comunicación lingüística (CCL)**: el alumnado conocerá y aprenderá a utilizar el lenguaje específico relacionado con contenidos digitales, contenidos inapropiados e ilícitos, privacidad, identidad digital, reputación online, ciberbullying, etc. autorregulando mediante éste su pensamiento, emociones y conducta. • **Sentido de la iniciativa y espíritu emprendedor (SIE)**: el alumnado desarrollará su iniciativa personal, por ejemplo, para rechazar las dinámicas de ciberacoso, denunciarlas y oponerse públicamente a ellas y para fomentar la buena convivencia en la red mediante la Netiqueta.

3. Temporalización y secuenciación

Sesión	Contenido / actividad	Duración	Metodología
Sesión 01	Actividad 01 *¡Ojo! Tampoco en Internet es oro todo lo que reluce.*	15 min.	Expositiva + Demostrativa + Debate
	Actividad 02 *¡Prevenir mejor que curar!*	15 min.	Expositiva + Trabajo en grupo
	Actividad 03 *Gran Hermano*	20 min.	Expositiva + Debate
Sesión 02	Actividad 04 *Se abre el telón… ¡el ciberacoso a escena!*	30 min.	Role-playing
	Actividad 05 *Introducción a la Netiqueta*	10 minutos	Expositiva + interrogativa
	Actividad 06 *Autoevaluación*	10 minutos	Autoevaluación

4. Orientaciones didácticas

4.1. Metodología.

A lo largo de esta Unidad Didáctica el formador impulsará la reflexión y la actitud crítica acerca de tener un comportamiento adecuado y educado en Internet respetando a los demás y fomentando, además, cuidar nuestra privacidad y la de otras personas.

Las actividades propuestas para el desarrollo de la Unidad Didáctica combinan el método **expositivo**[1] e **interrogativo**[2]. El método expositivo centrado en la transmisión de información, facilita ésta de forma rápida y generalizada. El método interrogativo se centrará más en la aplicación práctica del contenido a trabajar y se basará en el proceso de comunicación que se establece entre el docente y

[1] **METODOLOGÍA EXPOSITIVA:** centrada en la transmisión de información, posibilita la transmisión de conocimientos ya estructurados, facilitando demostraciones de tipo verbal y la transmisión de información y conocimiento, de manera rápida y generalizada.

[2] **METODOLOGÍA INTERROGATIVA**: centrada en el proceso de aplicación del contenido a trabajar, basada en el proceso de comunicación que se establece entre docente y grupo, a través de ***la pregunta***. Esta se convierte en elemento dinamizador, que desencadena el proceso de enseñanza aprendizaje.

el alumnado, a través de preguntas que motiven a la participación y la reflexión y/o a orientar al profesor en el conocimiento de partida del alumnado sobre la materia a tratar.

El docente actuará también como facilitador de una sesión participativa, utilizando el **debate**[3] y la visualización de vídeos con objeto de animar a compartir información, ideas, inquietudes y dudas. Se buscará en todo momento promover un entorno que favorezca la motivación del alumnado.

Además, esta Unidad Didáctica incluye una actividad en la que se desarrollará un **Role Playing,** técnica a través de la cual se simula una situación que se presenta en la vida real. Al practicar esta técnica, una o varias personas deben adoptar el papel de un personaje concreto y crear una situación como si se tratara de la vida real. El objetivo es ponerse en la piel del otro e imaginar la forma de actuar y las decisiones que tomaría cada uno de los personajes en situaciones diferentes.

En definitiva, la metodología propuesta promoverá la construcción del conocimiento a partir de la permanente reflexión, facilitando recursos, información y ejemplos vinculados a la realidad objetiva del perfil del alumnado destinatario. El profesor deberá utilizar un lenguaje acorde con objeto de un entendimiento claro de las actividades propuestas, contribuyendo a su buen desarrollo.

4.2. Recursos

Recursos requeridos para el desarrollo de la Unidad Didáctica:

- Recursos logísticos:
  - Ordenador con conexión a Internet para el docente, conectado a un proyector o pizarra electrónica.
  - Pizarra o papelógrafo.
- Recursos didácticos:
  - Presentación de contenidos dirigida a los menores, que acompaña a la presente Unidad Didáctica.
  - Sitios web, imágenes y vídeos previamente seleccionados por el docente. Con este objeto se reúne en esta Unidad Didáctica, en la descripción de cada actividad propuesta y en el apartado 6. Bibliografía /Documentación complementaria, una muestra a modo orientativo de posibles ejemplos a utilizar.

[3] ***El DEBATE EN EL AULA***, nos permite estimular el análisis y el cambio de actitudes por medio de la presentación de distintos puntos de vista

4.3. Descripción de las actividades a abordar

Actividad 01: ¡Ojo! Tampoco en Internet es oro todo lo que reluce

Descripción	Introducción y análisis del concepto de 'contenidos inapropiados e ilícitos' en la Red
Metodología	Expositiva + Demostrativa + Debate (opcional)
Duración	15 minutos
Recomendaciones	A lo largo de esta actividad proponemos abordar diferentes conceptos y ejemplos relacionados con el **contenido no adecuado** que podemos encontrar en Internet, referenciados en los materiales específicos sobre la temática que adjuntamos en el apartado '**Bibliografía / Documentación complementaria'** de la presente Unidad Didáctica, facilitando al alumnado pautas y recomendaciones de actuación para afrontar con éxito esta situación. Entendemos por **contenido no apropiado (adecuado)** todo aquel que percibido por el menor de edad pueda ser dañino o molesto para él/ella, representado a través de imágenes, vídeos o textos que manifiestan valores negativos y moralmente reprobables. Los ejemplos de contenidos no apropiados pueden ir desde el acceso a contenidos violentos o pornográficos, a contenidos falsos o carentes de rigor (bulos, mensajes en cadena o vídeos virales), juegos de apuestas o fraudes que se distribuyen a través de Internet. Proponemos reflexionar sobre ello en base a algunos ejemplos destacados como: • **La existencia de sitios web que fomentan conductas de odio, racismo y violencia:** El informe RAXEN, editado por la Asociación *Movimiento contra la Intolerancia* y la *Red Europea contra los Crímenes de Odio*, denuncia la presencia de más de 1.500 webs de contenido xenófobo, convirtiendo Internet en un espacio 'privilegiado' para propagar el odio, la discriminación y la violencia, tal como recoge **esta noticia**. • **Páginas que fomentan hábitos y conductas que dañan la salud física y psicológica**: como las páginas *ProAna* (a favor de la anorexia y sus hábitos y conductas) y *ProMía* (que promueven la bulimia, como estilo de vida). Podemos presentar el ejemplo a través de este **vídeo**, realizado para apoyar la petición de retirar las páginas pro-anorexia y pro-bulimia de Internet, a través de la plataforma **Change.org**. • **Malas prácticas,** como las recogidas en la noticia **"Tampodka, eyeballing y oxy-shots: las prácticas con alcohol más arriesgadas"**, difundidas a través de Internet.

- **Bulos, mensajes en cadena y fraudes**, divulgados a través de Internet, especialmente en redes sociales y mensajería instantánea. A continuación mostramos un ejemplo de bulo muy viralizado entre los usuarios por WhastsApp: "**WhatsApp te cobrará 37 céntimos por cada mensaje que envíes a menos que reenvíes esto a todos tus contactos**".

> *Hola, soy Germán Menafre, director de WhatsApp. Este mensaje es para informarles a todos nuestros usuarios de que sólo nos quedan 530 cuentas disponibles para nuevos teléfonos, y que nuestros servidores han estado recientemente muy congestionados, por lo que estamos pidiendo su ayuda para solucionar este problema. Necesitamos que nuestros usuarios activos reenvíen este mensaje (...) Mañana empiezan a cobrar los mensajes por WhatsApp a 0,37 centavos. Reenvía este mensaje a más de 9 personas de tus contactos y te será gratuito de por vida.*

Es necesario estar atentos a este tipo de bulos y fraudes y acudir siempre a fuentes oficiales de referencia sobre la temática para verificar/contrastar la información antes de creérsela.

- **Virus/Malware**. Un ejemplo reciente lo podemos encontrar en el enorme éxito del juego de realidad aumentada **Pokémon Go.** Muchas personas no esperaron a que la app estuviese publicada en los mercados de aplicaciones oficiales y se descargaron algunas de las numerosas versiones que circulaban por Internet, sin ser conscientes de que algunas de éstas estaban manipuladas para llevar a cabo acciones maliciosas en el dispositivo en el que se instalase. En este artículo de OSI podemos encontrar más información **"Mi hijo ahora quiere ir de paseo para cazar Pokémons con el móvil... ¿riesgos?"**.

El docente podrá conocer y utilizar más ejemplos de bulos, contenidos no adecuados y fraudes extendidos a través de Internet en páginas como: la **recopilación de bulos de la OCU (Organización de Consumidores y Usuarios)**, **el sitio web cazahoax** o los canales **en Twitter de Policía Nacional** y **Guardia Civil**, con información permanentemente actualizada sobre ello.

Es importante comentar con el propio alumnado que el acceso a contenidos como los expuestos, así como otros relacionados con el extremismo ideológico (*ultraderecha, extrema izquierda*), religioso (*Daesh*) o deportivo (*hooligans*), o con la incitación a conductas autolesivas (pérdida de peso; consumo de alcohol y otras drogas; suicidio), pueden ser una fácil entrada a **comunidades peligrosas en línea**[4], favorecidas por la falsa sensación de anonimato de la Red y por la facilidad de difusión a través de otros medios tecnológicos como redes sociales, *WhatsApp, Telegram, Snapchat,*

[4] Podemos definir las **comunidades en línea** como un grupo de personas cuyas interacciones están marcadas por intereses comunes y que tienen una identidad dentro de un espacio en Internet.

	valorando con ellos la importancia de rechazar este tipo de conductas y contenidos extendidos en la Red. **Observaciones:** a continuación se incluyen pautas para la realización de un pequeño debate en grupo como **actividad opcional** en el caso de disponer de tiempo (dentro de los 15 minutos programados para la actividad 01). Tras el análisis de algunas de las situaciones representadas en estos y otros ejemplos, el docente puede introducir en el aula un pequeño DEBATE EN GRUPO que, en torno a uno de los contenidos inapropiados trabajados, permita la reflexión y análisis crítico por parte del alumnado. Proponemos, a modo de ejemplo, abordar en pequeños grupos (de 3-4 alumnos/as) el artículo **"Tras los pasos de Ana y Mía: las webs que fomentan la anorexia son legales en España"**, relacionado con las páginas **pro-anorexia y pro-bulimia** que se pueden encontrar en Internet. Tras la lectura, cada grupo deberá reflexionar **sobre si deberían prohibirse las páginas pro-Ana y pro-Mía en España,** compartiendo las conclusiones finales de cada grupo en voz alta de manera que se establezca el debate y se dé pie a hablar de la importancia de dotarnos de estrategias y recursos que nos prevengan del efecto de contenidos como éstos. Sugerimos cerrar el debate remarcando la importancia de acudir SIEMPRE a un adulto de referencia para el menor o joven en caso de acceder a contenidos que le provocan malestar o incomodidad. Educadores y familia tenemos un destacado papel en el fomento del uso responsable de las TIC, necesario de cara a la prevención, entre otros, de hábitos peligrosos para la salud y el bienestar por el acceso a contenidos inapropiados, debiendo ofrecer seguridad y cercanía al menor ante este tipo de situaciones además de conocer y practicar algunas recomendaciones y buenas prácticas destacadas (explicadas en el **epígrafe 'Marco teórico de apoyo al docente'** de esta Unidad Didáctica).

Actividad 02: ¡Prevenir mejor que curar!

Descripción	Conocer medidas de prevención a aplicar para actuar frente a virus y fraudes informáticos
Metodología	Expositiva + trabajo en grupo
Duración	15 minutos
Recomendaciones	Se trabajarán las medidas **de seguridad y prevención** con apoyo de vídeos como: **'Usa un escudo e impide el avance de los virus'**. Se complementará la información con una visita guiada a la **página de OSI,** donde encontraremos, entre otras cosas, información sobre **herramientas gratuitas para proteger nuestros dispositivos**. Tras esta introducción se propondrá proponer en el aula el siguiente **trabajo en grupo.** El alumnado elaborará, en grupos de 4-5 personas, una lista con todas las medidas que conoce y/o recuerda, para la prevención de virus y

fraudes en sus dispositivos. Con las respuestas recogidas, que se apuntarán en una pizarra o dispositivo, se elaborará una **lista conjunta de pautas y recomendaciones.**

Los consejos y recomendaciones para prevenir y protegernos ante virus y fraudes son sencillos y aplican el sentido común, fomentando el uso responsable de la tecnología a través de sencillas pautas, entre las que destacamos:

- Instalación y correcta actualización de programas antivirus, tanto en ordenadores como en tabletas y smartphones, descargándolos desde la web oficial del fabricante.
- Configuración de cortafuegos (integrado en el sistema operativo) que bloquea el acceso no autorizado a nuestros dispositivos, permitiendo las comunicaciones autorizadas.
- Tener el equipo constantemente actualizado (sistema operativo, navegadores y programas).
- Limitación de permisos de usuarios a través del perfil de "usuario administrador", el único con permiso para la instalación de aplicaciones y actualizaciones del sistema operativo.
- Descargar programas y aplicaciones sólo desde páginas oficiales. Llevar a cabo instalaciones seguras a través de sitios oficiales de descarga, es decir, aplicaciones de confianza procedentes de desarrolladores destacados, con un importante número de descargas y valoraciones positivas. Así los dispositivos no se verán comprometidos.
- No ejecutar un programa o seguir un enlace que llega por correo y parece extraño.
- Tener precaución con los enlaces cortos (tipo bit.ly y goo.gl) que pueden dirigir a páginas web fraudulentas que contengan malware. Es necesario utilizar analizadores que confirmen la legitimidad del sitio web al que dirigen. En este artículo de OSI se puede encontrar más información **"El peligro de las URLs acortadas, vigila donde haces clic"**.
- No conectar al equipo un USB o cualquier otro dispositivo como tarjetas de memoria, CD, DVD, programas, vídeos y archivos descargados, cuya procedencia se ignore o sea dudosa. Siempre es necesario analizarlos previamente.
- Realizar copias de seguridad en soportes alternativos al dispositivo para no perder la información.
- Llevar a cabo una buena gestión de contraseñas (secretas, robustas y no repetidas).
- Cifrar la información para evitar que personas que no tengan permiso (la clave de descifrado) accedan a ella.

	• Cambiar periódicamente la contraseña de la conexión wifi del router para que nadie se conecte sin permiso y pueda llevar a cabo acciones maliciosas a través de ella. • Tomar precauciones al utilizar dispositivos públicos y conectarse a redes wifi públicas ya que no sabemos quién está conectada a dichas redes ni con que fines. • Evitar la navegación por páginas web sospechosas. • Intentar estar al día de las amenazas que circulan por la red, porque estar informado es clave para identificar los riesgos y poder combatirlos. • Utilizar el sentido común. Ser precavido ante cualquier cosa que veas en Internet y te parezca dudosa. Cada alumno deberá anotar en su cuaderno de trabajo aquellas que ha utilizado hasta la fecha.

Actividad 03: Gran Hermano

Descripción	Debate sobre privacidad: Visualización de vídeos que muestren diferentes situaciones de pérdida de privacidad con el objetivo de fomentar el debate, la reflexión y llegar a un consenso en la elección de al menos 4 recomendaciones para evitar la pérdida de privacidad.
Metodología	Expositiva + Debate
Duración	20 minutos

Recomendaciones	Los vídeos propuestos permiten trabajar la privacidad desde diferentes puntos de vista y son perfectamente adecuados para los niveles educativos propuestos. • **Tu vida entera está en Internet… y pueden usarla contra ti** Este vídeo forma parte de una campaña de sensibilización con el objetivo de llamar la atención del peligro que conlleva compartir la vida privada en Internet. Se invitó a participar a personas anónimas que paseaban por la calle para que Dave, un supuesto adivino con dotes paranormales, les hablase sobre sus vidas. En realidad se trataba de un actor que a través de un minúsculo auricular en su oído recibía información de un grupo de hackers que buscaban información sobre la vida de los visitantes a través de lo que ellos mismos habían publicado en sus redes sociales. ○ ¿Cuál fue el precio de su casa? ○ ¿Cuánto dinero hay en su cuenta bancaria? ○ ¿Cuánto gastó en ropa y en bebida el mes pasado? ○ ¿Cuál es el número de su tarjeta bancaria? Son algunas de las preguntas que el adivino Dave sabe responder de las personas que tiene delante. Pregunta de reflexión: ¿Qué información se podría descubrir sobre nosotros en función de la información que publicamos en nuestras redes sociales? • **Privacidad de la Información (permisos aplicaciones móviles)** Para utilizar algunas de las aplicaciones más populares en nuestro móvil cedemos permisos sobre nuestra información personal y dispositivos. Por ejemplo: ○ Acceso a tu localización exacta. ○ Enviar mensajes y/o realizar llamadas sin la mediación del usuario. ○ Cambiar nuestras contraseñas. ○ Leer nuestro registro de llamadas ○ Historial de navegación ○ Acceder a nuestras fotos y archivos multimedia. **Preguntas de reflexión:** ¿Sabemos qué permisos hemos cedido por utilizar las aplicaciones que tenemos descargadas en nuestro Smartphone? ¿Cuál es nuestra opinión sobre el acceso por parte de terceros a nuestros datos? En sistemas Android accediendo a Ajustes > Aplicaciones se puede comprobar los permisos a los que puede acceder cada aplicación que descargada.

Los usuarios de iPhone pueden bloquear el acceso de las aplicaciones a sus fotos, contactos o funciones del GPS accediendo a Ajustes > Privacidad.

- **Si todo estaba perfecto… ¿Qué falló?**

  Vídeo desarrollado por chicos y chicas de 12 a 18 años en el marco de un concurso "*Tecnología Sí. Conéctate con responsabilidad*" de Latinoamérica que tiene por objetivo premiar cortos que aborden aspectos relacionados con el uso seguro de la tecnología.

  Este vídeo en concreto aborda la importancia de la entrevista de trabajo y cómo la imprudencia, la ignorancia sobre privacidad, identidad digital y reputación online y la falta de conocimiento a la hora de utilizar la tecnología pueden perjudicar seriamente ante la posibilidad de obtener un empleo.

  Según lo que se publica y lo que publican los demás, la gente con la que se tiene relación, lo que nos "gusta", etc. se crea (consciente o inconscientemente) una imagen en Internet (identidad digital) que provoca en los demás una valoración (reputación digital). No se trata de que sea mejor o peor, sino de que ser conscientes de que todo lo que se hace en Internet contribuye a la imagen y reputación.

***Observaciones:** el sonido de este vídeo no es óptimo pero el hecho de que tanto su guionaje como realización esté elaborado por menores y dirigido precisamente a menores, hace que se considere relevante incluirlo. Es un ejemplo de cómo los propios menores pueden participar de manera activa en el desarrollo de materiales dirigidos a sí mismos, observando cómo son capaces de dar consejos certeros cuando se les pide reflexión y análisis, utilizando su propio lenguaje de forma que los resultados pueden llegar a ser mejor acogidos por sus iguales.

La proyección de cualquiera de los vídeos incluidos ha de servir para motivar al alumnado para iniciar un debate en torno a la importancia la identidad digital y el cuidado de la privacidad.

Se proponen algunos ítems para favorecer la reflexión y debate:

- ¿Qué les sucede a los protagonistas de los vídeos?
- ¿Cuáles creéis que son los motivos?
- ¿Creéis que esta situación podría afectar a alguien que conocéis? ¿por qué?
- ¿Qué aconsejaríais cambiar al personaje del vídeo sobre cómo construye su Identidad Digital?

El concepto de privacidad es subjetivo, cada persona debe encontrar un equilibrio entre los beneficios de exponerse públicamente y los riesgos de tal exposición. Lo importante es que los usuarios tomen la decisión de manera informada, siendo conscientes de los riesgos que asumen al publicarla. Por el mismo motivo, hay que ser respetuoso con las fotos de terceros (una foto en una fiesta puede que a alguien le parezca estupenda

	para que la vea cualquiera, pero otra persona puede considerarla privada y no querer que se muestre). El alumnado, en grupos de trabajo de 4 ó 5 personas, deberá llegar a un consenso en torno a la importancia de cuidar la privacidad, la identidad digital y, por tanto, sobre la utilización adecuada de la tecnología. Se deberá llegar a un consenso en la elección de al menos 4 recomendaciones para evitar la pérdida de privacidad y una mala construcción de nuestra identidad digital. El profesorado deberá reconducir las conclusiones en caso de que no se ajusten al objetivo buscado. Las recomendaciones buscadas deben estar en relación con aspectos como: • Leer las condiciones y políticas de privacidad antes de aceptar crear un perfil o al abrir una cuenta en una red social. • Configurar adecuadamente las opciones de privacidad al crear el perfil. • Revisar periódicamente las opciones de privacidad de nuestro perfil. • No publicar excesiva información personal y tener presente siempre: "pensar antes de publicar".

Actividad 04: Se abre el telón… ¡el ciberacoso a escena!

Descripción	Análisis de las características del ciberacoso, desde la perspectiva de acosadores, víctimas y sus círculos de amistad (amigos, compañeros, familiares)
Metodología	Role-playing
Duración	30 minutos
Recomendaciones	El docente propondrá un trabajo en grupos que, utilizando la técnica del **Role playing,** invite al alumnado a ponerse en el lugar de la otra persona: unos como víctima, otros como acosadores y otros como compañeros/amigos de la víctima, mientras representan qué haría esa persona ante una situación de ciberacoso escolar. Para plantear el trabajo de role playing, el docente podrá basarse en algunas de las principales manifestaciones del ciberbullying: • **Las humillaciones públicas**, por ejemplo la publicación de fotos humillantes o de comentarios que intentan ridiculizar a la víctima. • **Amenazas**. • **Chantajes** (por ejemplo *si no me envías otra foto tuya, publicaré en todas las redes la que ya tengo*).

- El **acoso virtual**. Por ejemplo mandar mensajes constantes a través de las redes sociales a pesar de que la víctima no contesta, o seguir insistiendo en todas sus redes.

La clase se dividirá en 3 grupos, cada uno de los cuales asumirá un papel concreto de los principales perfiles intervinientes en casos de ciberacoso: "víctimas, "acosadores" y "observadores". Deberán trabajar el papel a desempeñar en cada perfil, mensajes a trabajar, cómo actuar… De esta manera todos trabajaran en el guionaje del Role playing, si bien sólo se realizará una "función" con un representante de cada grupo.

Se elegirá una de estas conductas (o alguna similar relacionada con el ciberacoso escolar), identificando claramente qué sienten y experimentan cada uno de los personajes de la escena (víctima, acosador/a, amigos).

Por ejemplo, se puede escoger las humillaciones públicas, una de las acciones más habituales en este tipo de acoso. El guionaje, en este caso, se podría concretar a partir de una situación como la siguiente:

Contexto:

Un alumno de clase es acosado por otro a través de unas fotos humillantes que hace circular por WhatsApp con constantes comentarios de burla. Toda la clase es conocedora de la situación y una gran parte participa con la subida de comentarios que continúan con la humillación. Otra pequeña parte de la clase no ha intervenido nunca en las humillaciones, simplemente se ha mantenido al margen.

Acosador (al inicio de la representación):

El acosador enseña su móvil a otros compañeros para que vean la última burla realizada contra la víctima y la comparte a través de WhatsApp.

Observadores (que se suman al acoso)

Suben comentarios sumándose a la burla y promueven su propagación reenviando a otros compañeros.

Otros no publican nuevos comentarios ni reenvían, pero asumen la "gracia".

Víctima

El alumno acosado cada vez se siente peor, baja su rendimiento escolar, deja de hablar con sus amigos…

Observadores

Dos compañeros de clase de los que no han intervenido en la humillación deciden hacer algo: se dan cuenta de que no pueden consentir más esta situación y se posicionan claramente al lado del alumno acosado mostrándole su apoyo en privado y pidiendo ayuda a uno de sus profesores para que éste pueda ayudar a la víctima.

Acosador (al final de la representación)

Poco a poco van consiguiendo que el acosador se quede sólo en sus acciones humillantes. Ahora es él quien se siente desplazado por sus compañeros y finaliza el acoso.

Tras la escenificación, el docente propondrá un breve debate que sirva como reflexión sobre las conductas representadas y cómo cree el resto del grupo que se siente el otro

	ante una situación de esas características, destacando la importancia de valores como el respeto y el diálogo para afrontar una relación sana, así como la necesaria actitud de rechazo a este tipo de conductas. El docente podría proponer otro final, por ejemplo uno en el que nadie se posiciona del lado de la víctima. Hará especial relevancia en el papel que puede desarrollar el perfil que hemos llamado "observadores" no siendo meros espectadores pasivos de esta situación, pasando a desarrollar una actitud de repulsa y de oposición frente a este tipo de acoso.

Actividad 05: Introducción a la Netiqueta

Descripción	Introducción del concepto de Netiqueta, objetivo y avance de las normas básicas de conducta que se deben aplicar en las comunicaciones digitales
Metodología	Expositiva + interrogativa
Duración	10 minutos
Recomendaciones	Se puede iniciar la actividad preguntando al alumnado sobre su conocimiento en relación a la temática con preguntas del tipo: • ¿Crees conveniente seguir una serie de normas al hablar con alguien? ¿Por qué? • ¿Qué normas sigues tú cuando te comunicas con otras personas a través de Internet? • ¿Has tenido algún problema con algún amigo/compañero por un malentendido en una conversación de Internet? • ¿Has oído hablar de la Netiqueta? ¿Sabes lo qué es? A continuación, la visualización del vídeo "**Reglas de Netiqueta**" ayudará a introducir el concepto de Netiqueta, observar por qué es necesaria y avanzar unas primeras normas de comportamiento a seguir en la Red. El docente completará la información del vídeo destacando el **concepto de Netiqueta**, haciendo observar al alumnado que se trata de una serie de sugerencias dirigidas a fomentar la buena convivencia en la red. Que implica también conocer las peculiaridades de la comunicación digital y las características de los servicios y/o aplicaciones que usamos para utilizarlos de forma correcta y respetuosa. De esto se puede deducir que algunas de estas normas de buen comportamiento pueden cambiar con la propia evolución de Internet. La Netiqueta favorece la comunicación online, evita causar molestias a los demás usuarios y no comprometer su privacidad y seguridad, ni la nuestra. Como material de apoyo al contenido de esta actividad, el docente podrá utilizar varios enlaces y documentos referenciados en el apartado **Bibliografía / Documentación complementaria** de esta Unidad Didáctica.

Actividad 06: "Autoevaluación"

Descripción	Test de autoevaluación individual
Metodología	Autoevaluación individual
Duración	10 minutos
Recomendaciones	Se elaborará un test de autoevaluación sencillo (de uso individual) que evalúe los criterios marcados en el siguiente epígrafe ('**Criterios de evaluación'**), facilitando la verificación de que el alumnado ha entendido y asimilado conceptos y buenas prácticas relacionados con cada uno de los contenidos trabajados.

4.4. Criterios de evaluación

Se ha elaborado un **Test de Autoevaluación** relacionado con las competencias alineadas con la Unidad Didáctica tomando como referencia *el* **Marco Común de Competencia Digital Docente**[5].

- El alumno valora la validez de los contenidos que encuentra o recibe, interpreta la información y sabe cómo proceder ante contenidos inapropiados y/o engañosos.
- Reconoce la necesidad de aplicar medidas y pautas para la protección en ordenadores, tabletas y dispositivos móviles.
- Conoce los riesgos de compartir determinada información a través de la Red, tanto para él como para terceros.
- Es capaz de identificar los riesgos que conlleva el ciberacoso escolar y de cómo actuar ante un caso.
- Conoce las normas básicas de conducta que rigen la comunicación con otros mediante herramientas digitales.

El objetivo del test es que el alumnado compruebe por sí mismo los conocimientos adquiridos sobre el "Uso seguro y responsable de las TIC". En el **Anexo 2** se dispone de las respuestas correctas.

Se sugiere al docente la opción de realizar el test de autoevaluación antes de comenzar las actividades planteadas para la Unidad Didáctica y/o al final, con objeto de que el alumnado sea consciente de los conocimientos que tiene sobre la temática y al final estableciendo una comparativa y observando los avances obtenidos tras la realización de todas las actividades.

También se puede pedir a los alumnos que aporten alguna pregunta que pudiese ser incluida en el test. Desafiar a sus compañeros siempre es un reto atractivo para el alumnado, de esta manera fomentaremos su curiosidad y espíritu competitivo en beneficio del aprendizaje.

Se sugiere resolver el test de forma grupal, preguntando a los alumnos los motivos de escoger cada respuesta. Como una forma más atractiva de ejecutar la actividad.

[5] Marco Común de Competencia Digital Docente V 2.0
http://educalab.es/documents/10180/12809/MarcoComunCompeDigiDoceV2.pdf/e8766a69-d9ba-43f2-afe9-f526f0b34859

5. Marco teórico de apoyo al docente

Se incluyen a continuación orientaciones y recomendaciones para abordar los distintos conceptos que integran esta Unidad Didáctica.

5.1. Contenido inapropiado, bulos, mitos y fraudes

Entre los muchos contenidos que encontramos en Internet no es difícil 'toparse' con páginas y anuncios que nos enlazan con **contenido no adecuado** (y en ocasiones ilícito), que muestran y/o fomentan racismo, violencia, terrorismo, el uso de armas, la pertenencia a sectas, pornografía y abusos infantiles, tráfico y/o consumo de drogas, apuestas ilegales o trastornos físicos y mentales (autolesiones, inducción al suicidio, anorexia y la bulimia). Este tipo de contenido puede provocar, sobre todo en el caso de menores, sentimiento de confusión, tristeza o miedo, emociones que es importante detectar y canalizar enseñando a los menores a solicitar la ayuda y opinión de las personas adultas de referencia en cada caso (familia y profesorado esencialmente).

Es importante analizar los riesgos vinculados al acceso reiterado a contenidos no apropiados, incorporando ejemplos cercanos al perfil del alumnado que aporten claridad sobre éstos. De este modo, el debate planteado como opcional y complementario a la actividad 01 puede permitir la reflexión y análisis crítico sobre conductas y contenidos compartidos a través de Internet que pueden poner en riesgo nuestra salud (física y/o mental), valorando la importancia de dotarnos de estrategias y recursos que nos prevengan del efecto de contenidos como éstos.

Es importante tener en cuenta que el acceso a contenidos no apropiados relacionados con el extremismo (ideológico, religioso, deportivo, etc.) o con la incitación a conductas autolesivas (pérdida de peso, consumo de alcohol y otras drogas o suicidio) puede ser una forma de contacto con comunidades peligrosas, favorecidas por la creencia errónea de anonimato que proporciona la Red y por la facilidad de difusión a través de medios como redes sociales, WhatsApp, Telegram, Snapchat. Como se recoge en el monográfico editado por RED.ES sobre "**Comunidades peligrosas en línea**" (enumerado en la **Bibliografía** de esta Unidad Didáctica), las comunidades en línea no suponen un peligro en sí mismas pero se convierten en un riesgo en el momento en el que el contenido es inapropiado para los menores o se trata de comunidades peligrosas.

Otro tipo de contenido no apropiado al que los jóvenes tienen fácil acceso, son los **bulos** (también denominados "hoax"), **mitos y fraudes** divulgados a través de la Red. Todos los días llegan a nuestro buzón de correo o a través de redes sociales noticias falsas e incluso fraudes que, no basándose en hechos reales, son difundidos con gran rapidez y viralidad a través de Internet.

Se propone abordar este tipo de contenidos extrayendo ejemplos de mitos, leyendas, habladurías o fraudes de su propia realidad y que se utilizarán para analizar tanto las posibles consecuencias de este tipo de contenido y su propagación masiva a través de la red como la capacidad de muchos de ellos para infectar dispositivos y robar de éstos información personal, contactos y direcciones IP con el objeto de emprender campañas de spam e incluso cometer fraude económico.

Tendremos en cuenta algunas recomendaciones básicas para discernir este tipo de información:

- No están personalizados ni se identifica a la persona emisora.
- Suele ser enviado por un contacto de confianza que ha sido víctima del engaño.
- Solicitan el reenvío a otros contactos.

- Se caracterizan por contener frases amenazantes si el destinatario no cumple con lo que se le solicita.
- Pueden ofrecer regalos falsos, donaciones a instituciones o cualquier otro beneficio para incitar al destinatario a reenviar el mensaje.
- Su contenido muestra errores ortográficos y gramaticales.

5.2. Virus

Cuando hablamos de virus nos referimos a *"programas informáticos que buscan alterar el funcionamiento de los dispositivos (ordenadores, tabletas, teléfonos móviles, etc.) y, en muchos casos, robar información del usuario"*[6].

A día de hoy, estos virus informáticos son creados con el principal objetivo de **obtener información de los usuarios infectados** (datos bancarios, número de tarjetas de crédito, información personal, contraseñas de acceso al correo electrónico y redes sociales, etc.) que les pueda comprometer y obtener un **beneficio económico con ellos**. Los **principales mecanismos y vías de infección** son**:**

- **Correo electrónico.** Es una de las principales vías de entrada de virus a través de ficheros adjuntos peligrosos o enlaces a páginas web maliciosas.
- **Dispositivos de almacenamiento externo** (USB, discos duros, tarjeta de memoria, etc.). Al copiar archivos infectados de un USB a nuestro equipo, en ocasiones, simplemente por el hecho de conectar un USB a un equipo podemos resultar infectados, ya que algunos virus tienen la capacidad de autoejecutarse.
- **Descarga de ficheros desde Internet.** Al abrir o ejecutar ficheros (programas, contenido multimedia, documentos, etc.) pueden traer camuflado algún tipo de malware. Hay que tener especial precaución con lo que se descarga mediante programas de compartición de ficheros (P2P) u obtiene en las páginas web de descarga de contenidos, ya que pueden ser más propensos a contener virus.
- **Páginas web maliciosas** preparadas para infectar al usuario que la visita aprovechando **problemas de seguridad de un navegador no actualizado** o de los complementos instalados: *Java, Flash*, etc. En ocasiones las páginas web legítimas pueden haber sido manipuladas por ciberdelincuentes, **redirigiendo a una web maliciosa o fraudulenta**. La forma de llegar a éstas puede ser a través de **enlaces acortados** en Twitter u otras redes sociales, a través de webs poco fiables o enlaces en correos electrónicos fraudulentos.
- **Redes sociales,** utilizadas para infectar los dispositivos debido a la gran cantidad de usuarios que las frecuentan y el alto grado de propagación que facilitan. Se debe ser precavido frente a enlaces a páginas web que resulten "raras" o poco fiables, solicitudes para instalar programas para acceder a un contenido o aplicaciones que solicitan autorización no justificada para el acceso a **información personal**.
- **Vulnerabilidades y fallos de seguridad** en los sistemas operativos, aplicaciones, plugins o programas instalados en el dispositivo. Son aprovechadas para infectar los equipos, a veces sin que el usuario tenga que realizar una acción que le haga consciente de ello.

[6] Definición extraída del Monográfico sobre Protección ante virus y fraudes**,** elaborado por RED.ES (recogido en el apartado Bibliografía / Documentación complementaria de esta Unidad Didáctica).

Los virus actuales más comunes no requieren siquiera de la acción humana para ser activados en un determinado dispositivo electrónico. Se propagan más fácilmente consiguiendo, a través de técnicas denominadas **de ingeniería social**, engañar y manipular al usuario para infectar sus dispositivos y sustraer su información personal y privada.

Las consecuencias de una infección de dispositivos pueden ser el robo de información personal, la suplantación de identidad, el cifrado y/o borrado de la información almacenada, el uso del ordenador de la víctima para realizar ataques a otros ordenadores, la ralentización… Ante el posible ataque de un virus informático todos los dispositivos deben estar protegidos aplicando de forma habitual las siguientes **pautas y recomendaciones:**

- Llevar a cabo instalaciones seguras a través de sitios oficiales de descarga. Descargar programas y aplicaciones sólo desde páginas oficiales.
- Instalación y correcta actualización de programas antivirus, tanto en ordenadores como en tabletas y smartphones, descargándolos desde la web oficial del fabricante.
- Instalación de cortafuegos (integrado en el sistema operativo) que bloquea el acceso no autorizado a nuestros dispositivos permitiendo las comunicaciones autorizadas.
- Actualizaciones: especialmente del sistema operativo y los navegadores, pero también de los demás programas.
- Realización de copias de seguridad.
- Cifrado de la información.
- Gestionar el acceso a dispositivos con cuentas de usuario limitadas. De este modo sólo se permiten la instalación de aplicaciones y las modificaciones en la configuración a través del perfil '*administrador*'.
- Llevar a cabo una buena gestión de contraseñas (secretas, robustas y no repetidas).
- Cambiar periódicamente la contraseña de la conexión wifi del router.
- Tomar precauciones al utilizar dispositivos públicos y conectarse a redes wifi públicas.
- Tener precaución con los enlaces cortos (tipo bit.ly y goo.gl) antes de acceder a ellos ya que pueden dirigir a páginas web fraudulentas que contienen malware. Es necesario utilizar analizadores que confirmen la legitimidad del sitio web al que dirigen.
- Evitar la navegación por páginas web sospechosas.
- Evitar conectar a los dispositivos medios de almacenamiento extraíbles (USB) de dudosa procedencia, que pueden ser una puerta de entrada para los virus.
- No rootear ni hacer jailbreak porque podría poner en peligro la seguridad del dispositivo (se trata de significa dotar de máximos privilegios a un smartphone o tableta, evitando las limitaciones que impone el fabricante del dispositivo o la operadora). Por tanto, respetar las restricciones del fabricante.

5.3. Privacidad

La **Privacidad** se define como el ámbito de la vida personal que se tiene derecho a proteger de cualquier intromisión. La privacidad proporciona seguridad y resguarda de la mirada de los otros. La privacidad es necesaria, las personas tienen diferentes facetas y en cada una de ellas su privacidad es diferente, es decir no se comportan de la misma manera con amigos que con profesores, padres

o pareja. Cada uno elige el grado de privacidad de cada una de las relaciones y gracias a esto se pueden tener relaciones sociales enriquecedoras y variadas que permiten desarrollarse. La privacidad también tiene que ver con aquello que se comparte solo con uno mismo.

La privacidad permite tener parcelas de intimidad para hacer cosas que no se harían en público, estar relajados, no tener que cuidar la apariencia, etc.

En definitiva, la información privada dice mucho sobre alguien o sobre su familia, entorno, etc. En función de la cantidad de datos que se faciliten se expondrá en mayor o menor medida la vida privada, que puede ser utilizada para fines malintencionados.

Un exceso de información genera vulnerabilidad

La información que hace referencia a gustos, aficiones, creencias, etc. también forma parte de la privacidad. Al igual que los datos personales como la dirección, el número de móvil, dirección de correo electrónico, imagen (vídeos, fotos) e incluso voz son datos personales. También son datos personales los relacionados con la salud -enfermedades, pruebas médicas o tratamientos-, los datos bancarios como el número de cuenta o de tarjeta, los datos asociados a la vida laboral como por ejemplo el salario, los datos biométricos como las huellas dactilares, etc.

Los datos personales están protegidos por la (LOPD) Ley Orgánica de Protección de Datos y eso quiere decir que nadie puede hacer un uso fraudulento de ellos. Por ello es necesario protegerlos.

Las personas utilizan diferentes identidades parciales en función de las diferentes actividades que desarrollan online. Cada identidad parcial está sustentada por un servicio o aplicación de Internet. Por ejemplo, se puede tener un perfil en Facebook, Twitter, subir fotos a Instagram, crear vídeos en Youtube, participar en diferentes foros o blog del colegio… En cada uno de estos servicios se crea una identidad digital y parcial, que pueden estar o no relacionadas con el resto.

Cuando se navega por Internet, se realizan búsquedas, etc. también se va dejando rastro aunque no se dejen aparentemente datos en ningún formulario, es lo que se llama huella digital.

La suma de todas estas identidades parciales permite construir una **identidad digital** y una imagen de la persona en Internet.

En base a esta información, se proyecta una imagen que es como los demás ven a cada persona. Y esta imagen puede resultar positiva o negativa, es lo que se llama **reputación online**.

Por estos motivos se hace necesario realizar esfuerzos encaminados a entender la importancia de preservar la privacidad y construir una identidad digital positiva. Se exponen a continuación una serie de recomendaciones:

- **Utilizar contraseñas seguras y no compartirlas**. La contraseña es personal e intransferible, es decir no se debe compartirse con nadie. Una contraseña segura no debe contener ninguna información relacionada con el usuario, no debe contener su nombre, ni su edad, año de nacimiento, nombre de su macota… Debe tener un mínimo de 8 caracteres incluyendo mayúsculas, minúsculas, dígitos y caracteres especiales. Es muy importante igualmente que se utilicen diferentes contraseñas para los diversos servicios y/o aplicaciones.
- **Utilizar patrones de seguridad.** Es increíble la cantidad de datos que se alojan en los smartphones (datos/imágenes personales, datos que afectan a la privacidad, incluso datos que pueden afectar a la privacidad de terceros).
- **Revisar los permisos que solicitan las aplicaciones que se instalan en el smartphone**: poner en una balanza el servicio que da esa aplicación y los permisos que se ceden.

- **Informarse sobre las condiciones y políticas de privacidad antes de aceptar crear un perfil en una red social.** Tomarse el tiempo necesario para comprender los términos, la información que comparten y como protegen la privacidad frente a terceros.
- **Configurar adecuadamente las opciones de privacidad al crear el perfil**. Ante cualquier duda, las principales redes sociales tienen **centros de seguridad** donde se puede encontrar información para resolver dudas.
- **Revisar periódicamente las opciones de privacidad.** Las redes sociales cambian sus parámetros de privacidad o su política de privacidad y no siempre avisan por lo que se puede pensar que están bien configurada las opciones de privacidad y no ser así, es una buena práctica revisar cada cierto tiempo las opciones de privacidad en redes sociales.
- **Conectarse a páginas seguras para transacciones importantes o informaciones sensibles**. Son aquellas que empiezan por https. Todos los bancos tienen este protocolo y ahora también las redes sociales lo tienen. Al activar el cifrado toda la información que se envíe será encriptada y en caso de ser interceptada no será legible.
- **Valorar cuándo tener activado servicios como la geolocalización**, ya que se estaría transmitiendo la ubicación e incluso hábitos de desplazamiento. Además, los smartphones y la mayoría de las cámaras digitales actuales registran la posición GPS del lugar donde se toma una determinada foto y esa información se añade a los metadatos de la misma, quedando accesible a cualquiera a quien llegue la foto. La mejor solución pasa por deshabilitar en general la conexión GPS cuando no se esté utilizando.
- **No publicar excesiva información personal y tener presente: "pensar antes de publicar".** No por ser esta recomendación la última es la menos importante, todo lo contrario, subir una fotografía comprometida o realizar un comentario polémico tal vez pueda pasar desapercibido en el presente, pero puede pasar factura en el futuro. Es necesario pensar siempre en las consecuencias que puede suponer tanto para la propia reputación online como para la de los demás.

5.4. Ciberacoso escolar

Un buen punto de partida para introducir el problema del ciberacoso escolar es abordar su **definición,** así como la definición de otros términos relacionados como **Ciberbullying**, y **Sexting**, identificando claramente en cada caso sus características. Siguiendo la definición facilitada en el **Monográfico sobre Ciberacoso escolar** publicado por *Red.es (*referenciado en la Bibliografía de esta Unidad Didáctica), entendemos por **ciberacoso**: "*la acción de acosar a otra persona mediante el uso de medios digitales".*

En el caso del **Ciberacoso escolar o ciberbullying**, se define éste como un tipo de ciberacoso que se lleva a cabo entre iguales, ambas partes menores de edad. De este modo, podemos definir el ciberbullying como **"el daño intencional y repetido infligido por parte de un menor o grupo de menores hacía otro menor, mediante el uso de medios digitales"**.

El ciberbullying tiene las siguientes características:

- **Causa daño**: la víctima sufre un deterioro de su autoestima y dignidad personal dañando su estatus social, provocándole victimización psicológica, estrés emocional y rechazo social.

- **Es intencional:** el comportamiento es deliberado, no accidental. Sin embargo, hay que tener en cuenta que la intención de causar daño de modo explícito no siempre está presente en los inicios de la acción agresora.
- **Es repetido:** no es un incidente aislado, refleja un patrón de comportamiento.
- **Medios digitales**: el acoso se realiza a través de ordenadores, teléfonos y otros dispositivos digitales, lo que lo diferencia del acoso tradicional.

Dentro de la definición de ciberbullying, es importante conocer las diferencias y semejanzas entre el acoso 'cara a cara' o presencial y el virtual (ciberbullying), resumidas en este cuadro:

SEMEJANZAS	DIFERENCIAS DEL CIBERBULLYING
• Premeditación • Intencionalidad del acosador/a • Carácter repetitivo • Relación asimétrica de control y poder-sumisión entre acosadores y acosados	• **Violencia invasiva** facilitada por la **conexión permanente** (SMS, llamadas, correos electrónicos, mensajes privados, comentarios en redes sociales). El acosador puede acceder a la víctima 24h/día, 7 días semana. • **Viralidad.** Extensión rápida del mensaje, con gran capacidad de aumentar audiencia en muy poco tiempo. • **Rapidez y comodidad para el acosador** (un simple gesto, un click, sirve para acosar y hacer daño). • **Inconsciencia o falta de culpabilidad** del acosador, escondido tras una pantalla y la sensación de que en Internet nadie la va a descubrir. Se provoca **sentimiento de invencibilidad**. • **Disminuye la percepción del daño causado.** Gracias a la distancia física que facilita la tecnología se debilitan las restricciones sociales y se desinhiben las conductas.

El **ciberbullying** puede darse en todo tipo de víctimas. Cualquiera puede ser 'el elegido', sin un motivo o causa aparente. En algunos casos, la observación de determinadas conductas en el alumnado, entendidas como indicios que nos hacen sospechar – pero necesitaremos contrastar – pueden ayudar a identificar a una posible víctima de acoso escolar:

- **Cambios** en su comportamiento: deja de querer ir al colegio, está nervioso por el hecho de tener que hacerlo, deja de hablar con sus amigos de siempre, abandona sus aficiones, está triste, muestra cambios de humor y baja el rendimiento escolar, etc.

- **Signos físicos o psicosomáticos**: mareos, dolores de cabeza, sensación de asfixia y opresión, alteraciones del estado de ánimo.

Es importante destacar que en todos los casos de ciberacoso escolar intervienen distintas personas, no sólo víctimas y agresores, también personas que son conscientes de su existencia y lo presencian (testigos).

De esta forma, el docente establecerá unas pautas claras de actuación a tener en cuenta por el alumnado (con independencia de su edad y/o nivel educativo), dirigidas a enfatizar conductas que nos permiten tanto la **prevención** como una **actuación positiva y decidida a acabar con una posible situación de acoso** en el entorno.

Dirigidas tanto a los jóvenes y menores de forma genérica y preventiva como a posibles víctimas de ciberacoso y a los instigadores de este tipo de conductas, estas pautas permitirán actuar tanto antes de una situación de ciberacoso (en su prevención) como durante ella, destacando las siguientes recomendaciones:

MEDIDAS PREVENTIVAS	CÓMO ACTUAR EN CASO DE CIBERACOSO	PAUTAS GENERALES
• Pensar, antes de publicar, sobre las consecuencias de compartir esa información. • Configurar de forma adecuada y personalizada la privacidad en redes sociales. • Respetar siempre a los demás y a uno mismo. • Comportarse con educación y respeto en la Red. Netiqueta.[7] • Protegerse. No facilitar datos personales. • Valorar la visibilidad que tiene todo aquello que se publica a través de Internet (WhatsApp, redes sociales) y su capacidad para hacerse extensivo y quedar fuera de control.	• No contestar a las provocaciones. • Si alguien molesta pedir ayuda. • Ante un acoso guardar las pruebas. • Informar o denunciar la situación de acoso a través del administrador del servicio web (Twitter, Facebook, Instagram, etc.). • No sentirse culpable. Es quien acosa, quien está cometiendo un delito. La víctima no tiene la culpa. • Pedir ayuda siempre a un adulto de referencia y confianza. Si la amenaza es grave, pedir ayuda con urgencia. • Reflexionar sobre la responsabilidad de cada uno en lo que hace, dice y difunde, siendo crítico antes	• Comunicar lo que se piensa de forma asertiva: hablando clara y honestamente, tomando decisiones propias, pidiendo lo que se quiere y diciendo 'no' a lo que no gusta o se quiere. • Tratar a los demás con amabilidad y respeto. • Comportarse con educación y respeto también en la Red. *Netiqueta*. • No hacer en la Red lo que no se haría en persona. • Fomentar la empatía, en las relaciones, siendo capaz de ponerse en la piel del otro. • Cuidar y mantener las relaciones sociales. Los amigos son los mejores aliados a la hora de protegerse.

[7] Aspecto sobre el que profundizaremos con más detalle en otra de las Unidades Didácticas elaboradas, dentro del Programa "Escuela Cibersegura: promoción del uso seguro y responsable de Internet entre los menores".

	de seguir el patrón de conducta de los demás. Rechazar 'seguir la corriente' ante un caso de ciberacoso.	• No callarse ni ocultarlo (confiar en familia, profesores, mediadores). Si se detecta o sospecha de una situación de posible acoso no se debe dudar en ofrecer ayuda, observar qué sucede y reportar el caso a un adulto que pueda ayudar a analizar y buscar una posible solución al problema.

En todo caso, el equipo educativo tendrá presente la importante y necesaria colaboración entre **familia y escuela** a la hora de abordar las consecuencias del ciberacoso escolar e incluso antes, en su prevención y denuncia. En esta línea funcionan ya **protocolos de actuación** (se ejemplifica uno de ellos en la Bibliografía anexa a esta Unidad Didáctica), establecidos y coordinados en la comunidad educativa entre el centro y la familia, que suponen una buena práctica a la hora de abordar el ciberacoso y ser más efectivos en su respuesta.

5.5. Netiqueta

Las normas sociales son necesarias en cualquier comunidad. Se trata de convenciones que facilitan la convivencia. Como la red se ha convertido en un espacio de interacción, de aprendizaje, de comunicación… representa una forma más de socialización. Por tanto, también en la red es necesario seguir una serie de normas sociales que faciliten la convivencia.

Se trata de la **Netiqueta,** un conjunto de pautas de buen comportamiento o de buenas prácticas para comunicarse en la red. Estas buenas prácticas no están escritas en ningún reglamento, se construyen de forma natural y de manera colaborativa entre las personas que utilizan la red y que quieren que este espacio sea cada vez más agradable y seguro para todos.

Es algo tan sencillo como tener y mostrar consideración por las personas con las que de alguna manera se establece relación a través de la red.

La Netiqueta es necesaria porque a veces en el contexto digital se dan unas pautas de comportamiento que no se ocurriría de ningún modo hacer de forma presencial.

Algunas peculiaridades de la comunicación digital pueden influir en este aspecto, como la falta de empatía, la falsa sensación de anonimato que proporciona la Red, la ausencia de lenguaje corporal, entonación y matices, la alta probabilidad de malentendidos, la selección del entorno y polarización de opiniones, la búsqueda de posicionamiento social o el componente depresivo o de frustración en las redes sociales.

A continuación se incluyen algunas pautas que forman la Netiqueta y que se deben entender como buenas prácticas con objeto de seguir y promover las buenas conductas en Internet:

- **Cuidar los mensajes para evitar malas interpretaciones.**

  Aunque muchos sistemas de comunicación digitales incorporan la voz o la imagen, son muchas las ocasiones en las que la comunicación se realiza solamente con texto, es decir, se

carece del resto de complementos que ayudan a interpretar el mensaje, como el tono de voz u otros elementos que conforman la comunicación no verbal. Por ello se debe ser muy cuidadoso con los mensajes para evitar malas interpretaciones y evitar agresiones como el uso de mayúsculas y signos o símbolos hirientes.

- **Cuidar la imagen de los demás, resaltar los aspectos positivos de las personas y no los negativos.**

  Valorar lo adecuado o no de enviar determinados mensajes por la red que puedan dañar a los demás. Pedir permiso para cualquier publicación que implique información sobre otras personas. Valorar la importancia de tratar a los demás como se quisiera gustaría que te tratasen.

- **Respetar la privacidad propia y de los demás.**

  En la red se debe ser muy cuidadoso con la gestión de la privacidad. Se debe respetar y ser consciente de que un exceso de información sobre uno mismo genera vulnerabilidad. Del mismo modo, se debe respetar la privacidad de los demás. Es necesario, antes de subir una foto de otra persona, preguntarle si tiene algún inconveniente o no en que se publique. Siempre son necesarios unos segundos de reflexión antes de publicar un comentario. Permitirá darse cuenta de si puede perjudicar, tanto a uno mismo como a otras personas.

- **Seguir en la red los mismos estándares de comportamiento que cara a cara.**

  Recordar que la red no es un espacio sin ley. Al igual que en cualquier otro lugar, determinados comportamientos o actos pueden conllevar consecuencias sociales e incluso penales. A veces es tan sencillo como pensar si lo que se va a hacer a través de la red se haría en el cara a cara.

- **Compartir el conocimiento respetando los derechos de autor.**

  Internet ofrece innumerables posibilidades para buscar la información y ampliar conocimientos, pero es imprescindible respetar siempre la propiedad intelectual de los contenidos digitales, cuidando, respetando y valorando el trabajo publicado por otras personas y compartido a través de Internet.

- **No alimentar discusiones sin sentido en Internet.**

  Los troles son personas cuya forma de estar en Internet es siempre sembrar discordia, saturar por el gran número de mensajes que envían o quejarse constantemente. En muchas ocasiones se hacen pasar por otra persona para ello. Su único propósito es molestar y provocar.

  Ante este tipo de acciones la pauta a seguir es ignorar totalmente estos ataques y, si se considera necesario, denunciarlos a través del administrador del servicio o web donde realizan sus publicaciones ofensivas.

- **No abusar de poder o conocimiento.**

  No todas las personas tienen el mismo nivel de conocimientos para desenvolverse en el ámbito digital. Por ejemplo, muchas no conocerán las reglas básicas de la Netiqueta. Se debe ser flexible con los errores de los demás y ayudarles a que no los vuelvan a cometer informándoles de lo que es más correcto, pero siempre de manera educada.

- **Ejercitar la empatía.**

  Una buena práctica de Netiqueta es precisamente **empatizar**, la habilidad de entender y compartir las emociones y las experiencias de otros.

La empatía permite ponerse en el lugar de la otra persona, ser capaz de sentir lo mismo aunque no se esté pasando por la misma situación o no se tenga delante.

- **Cuando se utilice un servicio nuevo: observar y aprender.**

  Las normas de comportamiento pueden variar en función del tipo de servicio o aplicación que se utilice y también en función del entorno. Así, por ejemplo, un mensaje de correo electrónico siempre será más formal que una conversación por chat, del mismo modo que el uso de una red social para uso personal será diferente que para uso profesional, haciendo un uso privado en el primer caso y público en el segundo.

6. Bibliografía / Documentación complementaria

Contenidos inapropiados

- Monográfico Acceso a contenidos inapropiados. Red.es
- Monográfico Comunidades peligrosas en línea. Red.es
- Recopilación de bulos de la Organización de Consumidores y Usuarios (OCU)
- Cazahoax
- BIT Policía Nacional
- GDT Guardia civil
- Web de Internet Segura for Kids (IS4K): **información básica sobre contenido inapropiado**
- Web de Internet Segura for Kids (IS4K): **información básica sobre uso y configuración segura**

Privacidad, identidad digital y reputación online

- Monográfico Gestión de la privacidad e identidad digital. Chaval.es
- Vídeo “Adivino Dave. Privacidad en redes sociales”
- Vídeo “Si todo estaba perfecto… ¿Qué falló?”
- Vídeo “Privacidad de la información (permisos aplicaciones móviles)”
- Vídeo “Identidad digital, privacidad y reputación”
- Artículo “En Internet cuida tu privacidad”
- Artículo “Tu identidad digital”
- Artículo “Tu reputación es muy importante ¡Cuídala!”
- Web de Internet Segura for Kids (IS4K): **información básica sobre privacidad**

Ciberacoso

- Informe “Acoso escolar y ciberacoso: propuestas para la acción”. Protocolo de actuación ante el acoso escolar y el ciberacoso. Save the Children. 2014

- Guía de recursos didácticos para centros educativos "Ciberbullying, prevenir y actuar". Protocolo de intervención en casos de Ciberbullying en los centros educativos. Colegio Oficial de Psicólogos de Madrid y Fundación A3Media
- Monográfico "Ciberacoso escolar. Ciberbullying". Red. es
- Noticia publicada en el Diario El País "Ni chivatos ni policías: cibermediadores". Octubre 2015).
- Web de Internet Segura for Kids (IS4K): **información básica sobre ciberacoso**

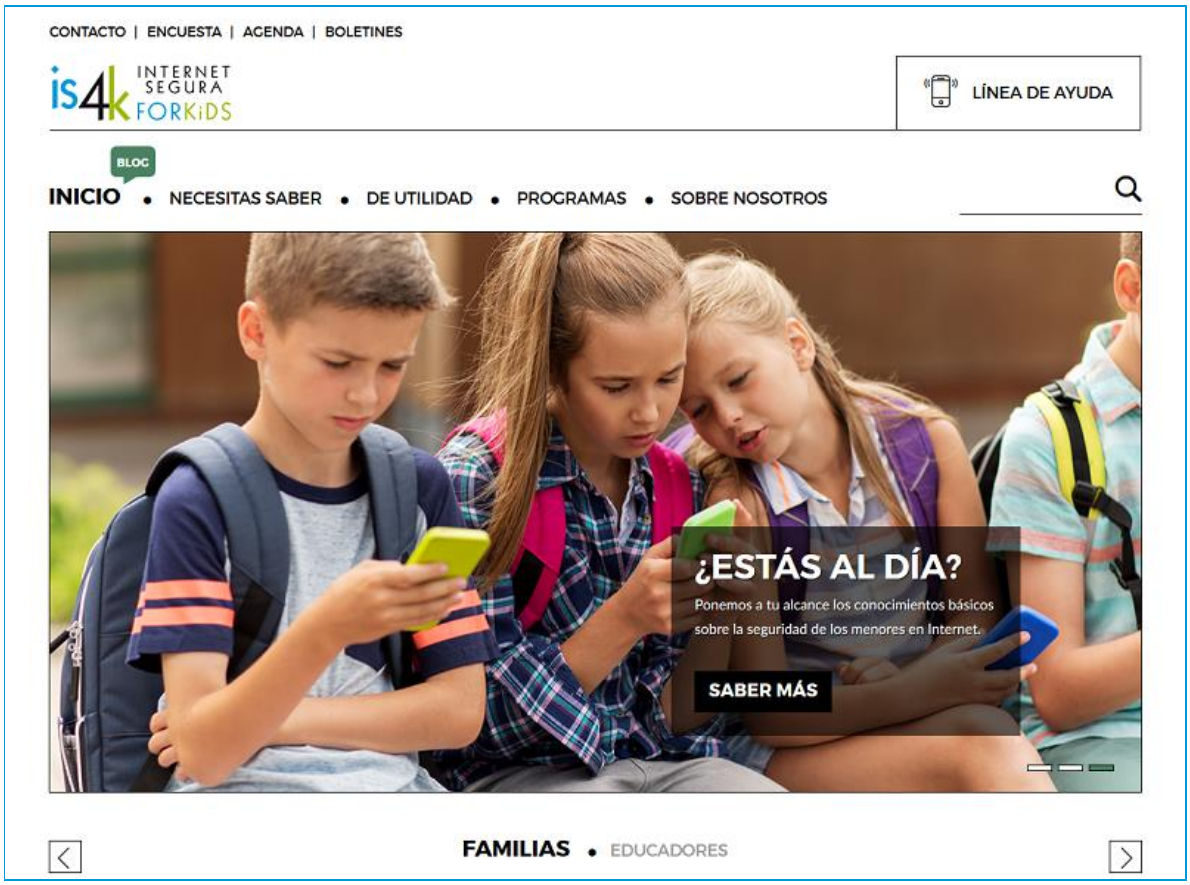
Netiqueta

- Monográfico "Netiqueta: comportamiento en línea". Red. es.
- Artículo "Conéctate y respeta – netiqueta". OSI Oficina de Seguridad del Internauta
- Artículo "Netiqueta, la educación en Internet también importa". OSI Oficina de Seguridad del Internauta.
- Vídeo "Reglas de Netiqueta".

Internet Segura for Kids http://www.is4k.es

Página web del Centro de Seguridad en Internet para menores en España. Incluye:

- La información que "**necesitas saber**" sobre privacidad, ciberacoso escolar, sexting, contenido inapropiado, uso y configuración segura, mediación parental.
- Artículos de interés y actualidad en el "**blog**".
- Guías, juegos, herramientas de control parental y otros recursos "**de utilidad**".
- Información de "**programas**" de sensibilización para un uso seguro y responsable de Internet por los menores.
- Una "**línea de ayuda**" con una serie de preguntas frecuentes y un contacto para resolver dudas.


CONTACTO | ENCUESTA | AGENDA | BOLETINES
INTERNET SEGURA FORKiDS
LÍNEA DE AYUDA
BLOG
INICIO • NECESITAS SABER • DE UTILIDAD • PROGRAMAS • SOBRE NOSOTROS
¿ESTÁS AL DÍA?
Ponemos a tu alcance los conocimientos básicos sobre la seguridad de los menores en Internet.
SABER MÁS
FAMILIAS • EDUCADORES

7. Anexo1. Test de autoevaluación

1.- Selecciona la opción más adecuada. Cómo debo actuar ante un contenido inapropiado en Internet, que me hace sentir realmente incómodo/a o asustado.
a. Comento la situación en mi entorno familiar (mis padres y/o hermanos mayores), esperando su consejo o recomendación, para poder enfrentarme a ello.
b. Comento la situación con mis compañeros/as de clase, para ver si alguno más se siente como yo.
c. No comento nada y espero a que le ocurra a alguien más y lo diga, para ver cómo reaccionan los demás.

2.- **Señala la opción correcta. Un hoax es:**
a. Un programa informático que utilizan los buscadores.
b. Un bulo o engaño que se difunde en Internet, frecuentemente a través de las redes sociales y correo electrónico.

3.- Las tabletas y smartphones no necesitan tener instalado un antivirus como medida de prevención, ante virus y fraudes.
❑ Verdadero
❑ Falso

4.- La identidad digital es el conjunto de información sobre una persona que podemos encontrar en Internet.
❑ Verdadero
❑ Falso

5.- **Es responsabilidad de las redes sociales configurar los perfiles de sus usuarios para reducir el riesgo de que la información se utilice con fines malintencionados.**
❑ Verdadero
❑ Falso

6.- Cual de estas características no define el ciberbullying o ciberacoso escolar:
a. Medios digitales: el acoso se realiza a través de ordenadores, teléfonos, y otros dispositivos digitales, lo que lo diferencia del acoso tradicional.
b. Causa daño: la víctima sufre un deterioro de su autoestima y dignidad personal dañando su estatus social, provocándole victimización psicológica, estrés emocional y rechazo social.
c. No es intencional: se produce accidentalmente.
d. Es repetido: no es un incidente aislado, refleja un patrón de comportamiento.

7.-En caso de ciberacoso ¿es correcto no contestar a las provocaciones y guardar las pruebas?
❑ Verdadero
❑ Falso

8.- ¿Hay un código escrito sobre la Netiqueta del que no te puedes salir?
❑ Verdadero
❑ Falso

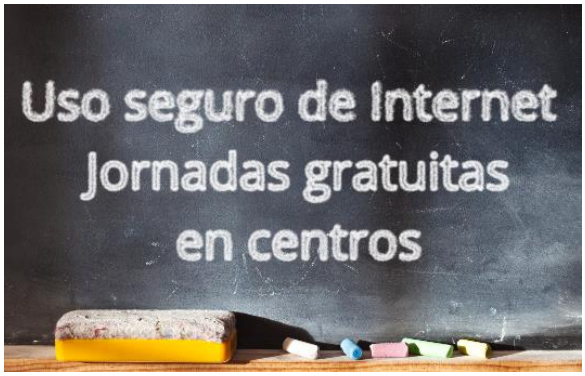
8. Anexo 2. Respuestas al Test de autoevaluación

1. **Opción A.** ¡Enhorabuena! Pareces haber interiorizado las buenas prácticas comentadas a lo largo de estas actividades y seguir las pautas y recomendaciones trabajadas. No olvides seguir solicitando el consejo de un adulto (familiar o profesorado) cuando tengas dudas, identificando y denunciando (si fuera el caso) aquellos contenidos que no son legales o que te hacen sentir incómodo/a o asustado/a. ¡Sigue así!
2. **Opción B.** ¡Perfecto! Un hoax es un bulo o engaño que se difunde en Internet, frecuentemente a través de las redes sociales y el correo electrónico. Una manera sencilla de detectarlos es introduciendo en un buscador alguna parte de la información que muestran y observa los resultados. Recuerda borrarlos y no contribuir a su difusión.
3. **Falso.** Aunque muchas personas siguen pensando que sólo los ordenadores deben protegerse con un antivirus, no es así, los virus pueden colarse perfectamente en nuestros smartphones y tabletas por lo que también debemos protegerlos.
4. **Verdadero.** La identidad digital es el conjunto de información sobre una persona que podemos encontrar en Internet. Se va construyendo, tanto con *nuestras* propias publicaciones, como con las publicaciones ajenas referidas a nosotros.
5. **Falso.** Has acertado, es nuestra responsabilidad no sólo configurar las opciones de privacidad más adecuadas para proteger nuestra privacidad, sino además, revisarlas periódicamente porque a veces las redes sociales actualizan las opciones de privacidad disponibles, lo que puede hacer que cambie la configuración que habíamos establecido previamente.
6. **Opción C.** No es intencional: se produce accidentalmente. Correcto, la respuesta C no forma parte de las características que definen el ciberacoso. En los casos de ciberacoso el comportamiento es deliberado, no accidental. Sin embargo, hay que tener en cuenta que la intención de causar daño de modo explícito no siempre está presente en los inicios de la acción agresora.
7. **Verdadero.** Junto a estas dos recomendaciones también es aconsejable informar o denunciar la situación de acoso a través del administrador del servicio web en el que se produce el ciberacoso (Twitter, Facebook, Instagram…) y pedir ayuda siempre a un adulto de referencia y confianza para ti. Y Si la amenaza es grave, pide ayuda con urgencia.
8. **Falso.** ¡Perfecto! Has entendido que *la* Netiqueta es una cuestión de actitud. En Internet existen determinadas reglas, no escritas, pero sí aceptadas por todos para hacer que la comunicación en la red sea posible, educada y respetan.

9. Anexo 3. Recursos asociados

Recursos asociados a esta unidad Didáctica disponibles para su futura utilización por los docentes:

- Presentación charla sensibilización dirigida al alumnado.
- Guía de preparación. Charla sensibilización dirigida al alumnado.



Toda la información del programa de Jornadas Escolares está disponible en la sección **programas** del portal **IS4K**.