PROTEGER TU PRIVACIDAD Y CONTROLAR TUS DATOS

Un recurso para el profesorado

Elaborado por la Oficina del Comisionado para la Protección de Datos de Irlanda

An Coimisinéir Cosanta Sonraí / Data Protection Commissioner

Adaptado por las Agencias / Autoridades de Protección de Datos de España y de las Comunidades Autónomas de Madrid, Cataluña y Euskadi.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Agencia de Protección de Datos de la Comunidad de Madrid

apdcat
Autoritat Catalana de Protecció de Dades

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

De la obra original

Redacción y edición:
Oficina del Comisionado
para la Protección de Datos
Canal House, Station Road, Portarlington, Co.
Laois, Ireland
LoCall: 1890 252 231
Tel: +353 57 868 4800
Fax: +353 57 868 4757
E-mail: info@dataprotection.ie
Web: www.dataprotection.ie

Publicado por:
Oficina del Comisionado
para la Protección de Datos
ISBN: 978-0-9557 187-0-0

De esta obra adaptada

Redacción, Edición adaptada y Publicación:
Agencia Española de Protección de Datos:
www.agpd.es
Calle Jorge Juan, 6
28001 Madrid
Teléfono: + (34) 901 100 099
Fax: + (34) 912 663 517
ciudadano@agpd.es

Agencia de Protección de Datos de la Comunidad de Madrid:
www.apdcm.es
Gran Vía 43, plantas 3 y 10
28013 Madrid
Teléfono: + (34) 917 209 738
Fax: + (34) 917 209 745
apdcm@madrid.org

Autoridad Catalana de Protección de Datos:
www.apd.cat
Calle Llacuna, 166, 7ª pl.
08018 Barcelona
Teléfono: + (34) 935 527 800
Fax: + (34) 935 527 830
apdcat@gencat.cat

Agencia Vasca de Protección de Datos:
www.avpd.es
www.kontuzdatos.info
Calle Beato Tomás de Zumárraga, 71, 3º
01008 Vitoria - Gasteiz
Teléfono: + (34) 945 016 230
Fax: + (34) 945 016 231
avpd@avpd.es

Diseño, Maquetación e Ilustraciones:
Hélice creativos, Vitoria-Gasteiz

Contenidos

AGRADECIMIENTOS[0]

La Oficina del Comisionado para la Protección de Datos quiere agradecer a las siguientes instituciones por su colaboración y por permitir la reproducción del material:
La sección irlandesa de Amnistía Internacional, el Fondo Ana Frank en Basilea, la Oficina Central de Estadística, el Consejo Irlandés para las Libertades Civiles, el Consejo Nacional de Tecnología en la Educación, la Oficina del Comisionado de Información, el Consejo de Prensa de Irlanda, el periódico The Scotsman.

Asimismo, la Oficina del Comisionado para la Protección de Datos quiere dar las gracias a Deirdre Phelan, profesora del centro docente de enseñanza secundaria St. Kieran's College de Kilkenny, por la elaboración de algunos de los materiales y ejercicios prácticos, y también a Conor Harrison, coordinador nacional para la CSPE (Educación Cívica, Social y Política) del Servicio de Apoyo de Segundo Grado (Departamento de Educación y Ciencia).

Asimismo, queremos dar las gracias a los siguientes centros docentes que aceptaron poner en práctica aspectos del programa de comunicaciones de esta oficina con alumnos de 12-18 años durante un periodo de prueba en 2007:
Coláiste Íosagáin, Portarlington, Co. Laois.
Coláiste Naomh Cormac, Kilcormac, Co. Offaly.
Patrician College, Ballyfin, Co. Laois.
St Mary's Secondary School, Edenderry, Co. Offaly.
Mountmellick Community School, Co. Laois.
Ard Scoil Chiaráin Naofa, Clara, Co. Offaly.
Ardscoil Rath Iomgháin, Rathangan, Co. Kildare.

[0] Estos agradecimientos ya están presentes en la edición original de este material educativo de la Oficina del Comisionado para la Protección de Datos de Irlanda.

Respecto a la edición adaptada de este recurso educativo, las Agencias y Autoridades de Protección de Datos que han participado en la adaptación desean mostrar su agradecimiento a las siguientes instituciones:
Al Gobierno Vasco y, en particular, al Departamento de Educación, Universidades e Investigación por su colaboración revisando y valorando la adecuación de los materiales educativos.

SOBRE ESTE RECURSO FORMATIVO

Este programa educativo está diseñado como un recurso para la sensibilización y la reflexión acerca del valor de la privacidad y la importancia de la protección de datos personales, y cabe su utilización en aquellas materias o asignaturas en las que se considere adecuado introducir estos conceptos, así como en las sesiones de tutoría y de orientación escolar.

El profesorado no tiene necesariamente por qué aplicar este recurso en su totalidad, de principio a fin, con sus alumnos y alumnas. El programa trata aspectos relacionados con los conceptos de Derechos y Responsabilidades y con la Legislación. La intención es que el profesorado seleccione elementos de este recurso, junto con otros recursos educativos, durante los cursos de la Educación Básica, Primaria y Secundaria, en los que se imparten las asignaturas de Educación ético-cívica, Educación para la Ciudadanía y los Derechos Humanos, Tecnologías o Informática, entre otras.

No obstante, animamos a que se dé a este recurso un uso intercurricular, ya que se puede adaptar para ser utilizado en otras asignaturas de cursos de secundaria y bachillerato, indistintamente.

INTRODUCCIÓN

La toma de conciencia respecto a la privacidad y a la necesidad de proteger los datos personales como un aspecto de la ciudadanía está relacionada con el fomento de otros valores y actitudes positivas, tales como la preocupación por los derechos humanos, la preocupación por el bien común y el respeto al imperio de la ley. Asimismo, uno de los objetivos principales consiste en ser conscientes de cómo la tecnología puede influir en la privacidad de las personas.

El concepto de la protección de datos está vinculado al surgimiento del derecho a la privacidad tras la Segunda Guerra Mundial. En aquel momento, se empezó a prestar atención a los derechos humanos básicos y a las libertades fundamentales, lo cual dio lugar a la elaboración de una serie de declaraciones y cartas internacionales como, por ejemplo, la Declaración Universal de los Derechos Humanos (DUDH).

Desde entonces, se han producido rápidos avances tecnológicos y, en consecuencia, una creciente atención al procesamiento de datos personales en grandes cantidades. La protección de datos se centra en implantar medidas necesarias para salvaguardar el tratamiento de datos personales a través de una variedad de medios (por ejemplo, archivos manuales, bases de datos, circuitos cerrados de televisión, bancos de imágenes y telecomunicaciones móviles). En la actualidad, la protección de datos consiste en un marco de leyes establecido, tanto a nivel nacional como mundial, que recoge los principios básicos que regulan la protección de datos personales.

En vista de las tecnologías emergentes, muchos países del mundo han constituido autoridades de control encargadas de vigilar el desarrollo de lo relacionado con la protección de datos personales. Así, La Agencia Española de Protección de Datos (AEPD) supervisa el cumplimiento de la ley de Protección de Datos en España mediante la orientación y la investigación de posibles violaciones de las leyes, y ofreciendo un espacio en el que los particulares puedan presentar sus quejas en relación con el uso de sus datos personales en situaciones específicas. En el ámbito de sus competencias, las Agencias de Protección de Datos de la Comunidad de Madrid (APDCM), Cataluña (APDCAT) y País Vasco (AVPD), controlan que las administraciones públicas cumplan la normativa de protección de datos cuando en el ejercicio de sus funciones gestionan datos de carácter personal.

Asimismo, estas Agencias de Protección de Datos colaboran en el ámbito europeo e internacional participando en una amplia variedad de foros, grupos de trabajo y seminarios. Es de especial importancia la existencia de un grupo de trabajo de la UE, compuesto por Comisionados para la Protección de Datos de la Unión Europea, junto con una persona representante de la Comisión Europea. Este grupo de trabajo, conocido como el Grupo de Trabajo del Artículo 29, es un órgano independiente y dispone de competencias de asesoramiento a la Comisión Europea.

En este recurso se aborda el nacimiento de la protección de datos como fenómeno independiente dentro del tema de la privacidad en general. No obstante, con el fin de estimular el interés en torno a la noción básica de la privacidad, muchas de las actividades y trabajos de curso que contiene este material se centran en los aspectos fundamentales de la privacidad.

CONCEPTOS CLAVES

Este recurso está estructurado alrededor de un enfoque conceptual que pretende conseguir que los estudiantes lleguen a ser ciudadanos y ciudadanas activas, conscientes y responsables. La ciudadanía es el concepto central del curso y el material que contiene este recurso está ligado con dos conceptos claves de la misma, en particular: los conceptos de "**Derechos y Responsabilidades**" y la "**Legislación**". Al abordar los conceptos de "Derechos y Responsabilidades" y "Legislación" desde la perspectiva de la privacidad y la protección de datos, se espera conseguir que el alumnado adquiera una nueva visión del concepto de ciudadanía activa.

Este recurso está distribuido en cuatro unidades principales. En cada unidad se describe cuáles son los objetivos, los conceptos, las actitudes, los conocimientos y las habilidades correspondientes y se ofrecen actividades a modo de ejercicios opcionales. Los apartados "Actividades de Seguimiento" e "Ideas para la Acción" se incluyen como opciones complementarias, junto con las actividades que pueden realizarse en clase.

- **Unidad 1**: su objetivo es servir de introducción a la idea general de privacidad, comenzando en un entorno familiar para ir avanzando hacia situaciones menos convencionales, tales como el Gran Hermano de la novela de George Orwell y las relaciones entre fama y privacidad.
- **Unidad 2**: se muestran los antecedentes sobre cómo la privacidad fue considerada como un derecho humano.
- **Unidad 3**: trata sobre la legislación relacionada con la protección de datos en un contexto nacional y global.
- **Unidad 4**: traslada la atención a la tecnología y a las consecuencias de la innovación en la privacidad.

ACTIVIDADES

Se utilizan una serie de metodologías para el aprendizaje activo entre las que se encuentran las siguientes:

- Discusión estructurada
- Estudios de caso
- Gráficos
- Debates
- Representaciones
- Escritura creativa
- Estímulos visuales

PÁGINAS PARA ESTUDIANTES

El símbolo de fotocopia (véase más abajo) se utiliza para indicar las páginas que deberían ser fotocopiadas y distribuidas entre el alumnado.

UNIDAD 1

OBJETIVOS

- 1. Comprender el concepto de privacidad.
- 2. Examinar la clásica situación de "Gran Hermano" de la novela de George Orwell.
- 3. Analizar la idea de la privacidad y la gente joven, utilizando un contexto no convencional.
- 4. Tomar conciencia acerca de unas orientaciones de buenas prácticas en relación con la privacidad y los medios de comunicación.

CONOCIMIENTOS

- Cómo puede definirse la privacidad.
- Peligros de interferir o de violar el derecho a la privacidad de la persona.
- Consecuencias de la supresión de la privacidad para aquellas personas que, por lo demás, son materialmente privilegiadas.
- La privacidad es un derecho humano.

CONCEPTOS

- Derechos y Responsabilidades.
- Legislación.

HABILIDADES

- Comunicación – discusión, debate, trabajo en grupo, juego de roles, ejercicio de escucha.
- Análisis – medios de comunicación, tiras dibujadas, imágenes y situaciones.
- Escritura creativa.

ACTITUDES Y VALORES

- Desarrollo del sentido de por qué la privacidad es importante y por qué debería ser respetada.
- Conciencia de los derechos.

UNIDAD 1.1

PROFESORADO

¿QUÉ ES LA PRIVACIDAD?

Explore los siguientes aspectos con sus estudiantes

EL DERECHO A QUE TE DEJEN EN PAZ

La privacidad es el derecho a que te dejen en paz. A medida que se acerca la noche, corremos las cortinas de nuestros hogares para impedir la entrada de la oscuridad y encendemos las luces. Una vez que corremos las cortinas, nuestras actividades y movimientos quedan fuera de la vista de otras personas. Lógicamente, sentimos que este espacio está reservado para la familia, las amigas y los amigos. Es nuestro espacio privado.

DOCUMENTOS PERSONALES

Asimismo, también queremos que algunos de nuestros documentos personales sean privados –la mayoría de las familias tienen una caja o archivo donde almacenan documentos pertenecientes a los diferentes miembros de la familia como, por ejemplo, certificados de nacimiento, resultados académicos, escrituras de la casa o documentos de matriculación del coche. No hay razón alguna para que otras personas vean estos documentos y preferimos guardarlos en un lugar seguro.

PERTENENCIAS PERSONALES

Otros objetos que poseemos contienen un valor sentimental. En algunas ocasiones, nos gusta colocarlos en el hogar familiar, por ejemplo, fotos familiares, tarjetas de cumpleaños, los dientes de leche, mechones de pelo o títulos académicos enmarcados. Exhibimos esos objetos por satisfacción propia y para compartirlos con la familia, parientes y visitas.

La privacidad es el derecho a que te dejen en paz, a vivir tu propia vida con las mínimas interferencias. Este derecho implica la facultad de disponer sobre el uso que se hace de tus propios datos.

UNIDAD 1.2

PROFESORADO

PRIVACIDAD EN EL HOGAR

Fotocopie la página siguiente y distribúyala a las alumnas y alumnos. Inicie una discusión estructurada sobre la privacidad utilizando los estímulos visuales del diagrama.

OBJETIVO

Introducir al alumnado en el tema de la privacidad mediante el análisis de dos imágenes contrapuestas.

Utilizando la metáfora de correr las cortinas al anochecer, pida a la clase que reflexione sobre una situación en la que hubiera gente mirando qué hacemos dentro de casa continuamente, sin poder impedir esa vigilancia constante.

Asimismo, pida a las alumnas y a los alumnos que examinen las dos escenas opuestas (exterior / interior) representadas en la página siguiente.

Pida que reflexionen sobre cómo se sentirían si se tratara de su propia casa y una persona ajena pudiera conocer todo lo que sucede dentro de ella. Y si esa persona pudiera...

- Escuchar la conversación telefónica entre Xabier y su novia.
- Observar y hacer una lista de todos los programas de televisión y DVD que ven los miembros de la familia.
- Echar un vistazo y hacer una copia electrónica de los álbumes de fotos familiares almacenados en el ordenador.
- Copiar las claves y los nombres de usuarios que permiten acceder a la cuenta bancaria de la familia.
- Enterarse del secreto de Beatriz.
- Saber exactamente la cantidad de dinero en metálico que tiene la familia en casa al alcance de la mano, por ejemplo en algún lugar de la cocina.

¿Cuál es el aspecto más preocupante de esta situación para los alumnos y las alumnas?

Finalmente, pídales que comparen esta situación de vigilancia con un robo con allanamiento de morada.

Observe lo siguiente con su alumnado

Los ladrones se cuelan en las casas y roban pertenencias físicas o destrozan objetos. Pero también inmiscuirse en la vida privada de alguien y descubrir sus hábitos, vigilar sus actividades y escuchar sus conversaciones puede resultar igualmente perjudicial a largo plazo.

CONCLUSIONES

Pregunta: ¿qué es la privacidad?

Respuesta: el derecho a que te dejen en paz.

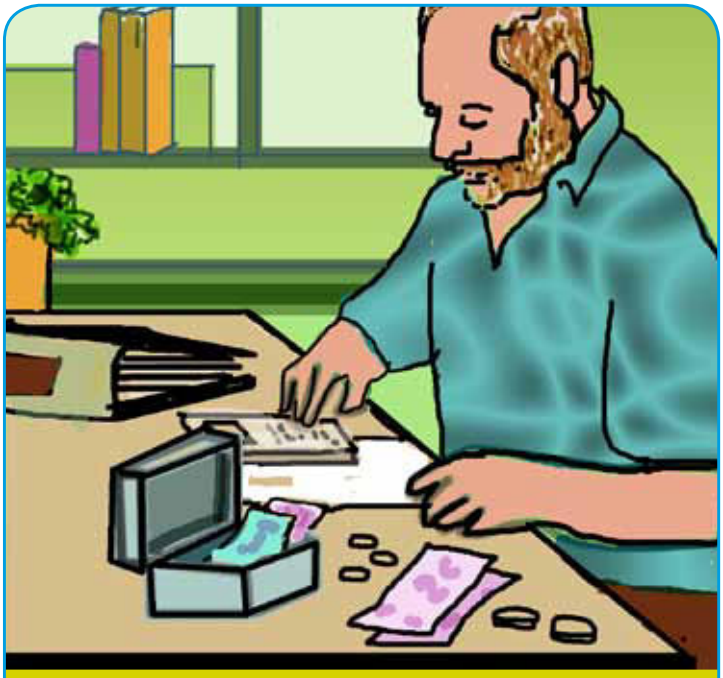
Pregunta: ¿quién debería preocuparse por su privacidad?

Respuesta: todas las personas.

FOTOCOPIABLE

UNIDAD 1.2. ALUMNADO

Mamá está cargando en Internet fotos familiares y, después, piensa realizar algunas operaciones bancarias en la red.



Como tesorero del club de fútbol local, papá está contando el dinero recaudado durante la última colecta.

Beatriz, de 13 años, está susurrando un secreto a su hermana mayor Ane, de 17 años. Beatriz fue acusada de robar en una tienda pero, finalmente, los cargos fueron retirados. Beatriz todavía está preocupada porque la gente de la tienda podría ponerse en contacto con sus padres.

Xabier, de 16 años, habla con su novia por teléfono mientras ve un partido de fútbol en la televisión.

UNIDAD 1.3

PROFESORADO

EL GRAN HERMANO EN LA NOVELA DE GEORGE ORWELL

Es importante explicar a los alumnos el término "Gran Hermano" y su origen. Para ello, la imagen visual de la página siguiente podría resultar útil. Puede fotocopiarla, y utilizarla en un retroproyector o como diapositiva de PowerPoint.

George Orwell reflejó un mundo dominado por el Gran Hermano en su famosa novela **1984**. En esta novela publicada en 1949, tras la Guerra Civil Española y la Segunda Guerra Mundial, George Orwell trató de mirar hacia el futuro y describir una visión de una sociedad en la que no existe la libertad individual para "la militancia del partido" y el Estado somete a la ciudadanía a una vigilancia constante utilizando tecnologías sofisticadas.

El término "Gran Hermano" tiene su origen en esta novela.

Imaginaos que nuestro país fuese como el Gran Hermano de George Orwell. Hay una vigilancia constante y el gobierno quiere saber todo sobre cada persona.

El "Ministerio de la Verdad" (un departamento del gobierno) difunde propaganda con el objetivo de inculcar el modo de pensar que el gobierno desea de los ciudadanos y ciudadanas. Por doquier hay carteles advirtiendo que "EL GRAN HERMANO TE ESTÁ MIRANDO", y llevar un diario en el que revelamos nuestros verdaderos sentimientos podría ser motivo de que nos condenaran a muerte... Vivimos en un país en el que podemos ser acusados de "crimen de pensamiento" por la "policía de control del pensamiento" y, además, es ilegal enamorarse...

FOTOCOPIABLE

UNIDAD 1.3. ALUMNADO

UNIDAD 1.3

PROFESORADO

EL GRAN HERMANO EN LA NOVELA DE GEORGE ORWELL

OBJETIVO

- Motivar al alumnado para que reflexione sobre las formas en las que un gobierno de otro tipo de sociedad o estado puede restringir las libertades individuales, incluido el derecho a la privacidad.

  Fotocopie la hoja de actividades de la página siguiente y repártala.

ACTIVIDAD RELACIONADA

- Pida a las alumnas y alumnos que indiquen por escrito cuál sería su mayor temor si el "Gran Hermano" estuviera observándoles continuamente.
- Pídales también que consideren si existen aspectos positivos en tener al "Gran Hermano" rondando cerca.

  Divida la clase en grupos para que intercambien sus opiniones y pensamientos.

ACTIVIDAD RELACIONADA / DEBERES

- Pida al alumnado que diseñe un póster o componga un poema en el que representen al "Gran Hermano". El póster puede ser un croquis, una imagen, un símbolo, una fotografía, una imagen de una revista, un gráfico, una tira dibujada...
- Localice pasajes de la novela **1984** (disponible fácilmente en Internet) y seleccione algunos capítulos para que los lean. Asimismo, pídales que reflexionen sobre las siguientes preguntas: ¿se da en nuestra sociedad actual alguna de las observaciones o predicciones de George Orwell? ¿Qué papel o función desempeña la tecnología en la novela **1984**?

FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Imagina que tuvieras que vivir en las condiciones que se describen a continuación. Califica en una escala de 1 a 10 las situaciones siguientes según el grado de rigor en el control que consideres existiría en cada caso. Por ejemplo, si crees que racionar el chocolate no es un problema grave, otorga sólo un 3 en la escala de rigurosidad. Todas las condiciones tipo Gran Hermano descritas en la siguiente tabla se han extraído de la novela **1984** de George Orwell.

CUESTIONARIO

Contexto: Gran Hermano	**Calificación (1-10)**
Un helicóptero patrulla por tu vecindario husmeando por las ventanas y en los jardines de las casas.	☐
Escribir un diario está prohibido.	☐
En cada una de las habitaciones de tu casa hay colocada una cámara que graba continuamente todos los movimientos de tu familia.	☐
El chocolate está racionado. Tienes que presentar el carné de identidad para comprar 15 gramos al mes (media barra de chocolate).	☐
Si tienes un pensamiento negativo sobre el gobierno, la "policía de control del pensamiento" podría arrestarte y condenarte sin juicio previo.	☐
Una televisión de pantalla plana colocada en tu salón emite propaganda del gobierno las 24 horas de los siete días de la semana. Se puede bajar el volumen un poco, pero no apagarla ni cambiar de canal.	☐
Enamorarse es delito.	☐
Te dan cupones de racionamiento para comprar ropa por un valor de 3.000 al año. Un pijama cuesta 600 cupones.	☐
El gobierno "controla la realidad". La historia se revisa continuamente. Si el gobierno decide "no, eso nunca sucedió", se modifican los registros históricos. A menudo te preguntas si tu memoria te engaña.	☐

ACTIVIDAD 1.4 PROFESORADO

FAMA Y PRIVACIDAD

OBJETIVO

- Estimular a los estudiantes a que reflexionen sobre la privacidad, eligiendo una situación que refleje la cultura moderna actual, pero que se centre en el derecho a la vida privada de los ciudadanos y las ciudadanas.

Las vidas privadas de las celebridades, la realeza y otras figuras públicas destacadas son a menudo el centro de atención de los medios de comunicación. Los paparazzi son la principal intrusión en la vida de algunas de estas celebridades. Cuando la intrusión se extiende hasta sus familiares más cercanos, éstos generalmente tienen que tomar medidas para proteger su privacidad.

Nota: fotocopie el caso de estudio de la página siguiente para distribuirlo en clase. Explíqueles que el suceso de la princesa Carolina es un caso que sienta precedente, no debido a la celebridad involucrada, sino porque el caso llegó hasta el Tribunal Europeo de Derechos Humanos, que falló a favor de la princesa. Quizá también les interese saber que existe otro caso similar en curso en el Reino Unido debido a unas fotos de JK Rowling, autora de las novelas de Harry Potter, su marido y su bebé, fotos sacadas mientras paseaban por una agencia de prensa especializada en celebridades. JK Rowling perdió el juicio contra la agencia de prensa en el Tribunal Superior pero está dispuesta a apelar contra esa decisión.

También pueden mencionarse otros casos relacionados con la fama o la celebridad y la protección de la vida privada. Así, Diana de Gales, ex mujer del príncipe Carlos de Inglaterra, perdió la vida a causa de un accidente de tráfico mientras era sometida a una persecución por parte de periodistas de la prensa rosa.

Nota: resoluciones de la Agencia Española de Protección de Datos (AEPD) ante reclamaciones de ciudadanos referidas a la difusión de información en Internet y en diversos medios de comunicación.

En España existen diversos pronunciamientos de los tribunales en lo referente a la colisión entre el derecho a la información y el derecho al honor, a la intimidad personal y familiar y a la propia imagen, todos ellos derechos fundamentales conforme a nuestra Constitución. Es particularmente destacable la doctrina del Tribunal Constitucional que viene considerando juzgar prevalente el derecho a la información, condicionándolo "a que la información se refiera a hechos de relevancia pública, en el sentido de noticiables y a que la información sea veraz".

Por su parte la AEPD ha tramitado diversos casos en los que ha tenido que pronunciarse sobre posibles colisiones entre el derecho fundamental a la protección de datos y la libertad de expresión y determinar cuál debe prevalecer. Para ello, analiza factores como la naturaleza y finalidad de la información, su veracidad, la existencia de intereses generales en la obtención de esa información y la proporcionalidad de la misma.

En este sentido, la AEPD ha venido otorgando la prevalencia del derecho a la información en muchas de sus resoluciones -esencialmente referidas a la difusión de datos personales por medios de comunicación- cuando la información comunicada se hubiera considerado proporcionada, veraz, y de relevancia pública y referida a asuntos públicos de interés general. No obstante, también se ha pronunciado en sentido contrario en casos en los que no han existido estos criterios para otorgar la prevalencia de la libertad de información. Son destacables algunos casos en los que la AEPD ha resuelto sancionar a quienes han publicado datos de terceras personas sin su consentimiento en diversos sitios Web, o aquellos en los que ha tutelado el derecho a cancelar imágenes y otros datos personales en servicios como foros, redes sociales, portales de vídeo y otros servicios de la sociedad de la información.

FOTOCOPIABLE

UNIDAD 1.4 . ALUMNADO

Lee el siguiente caso de estudio.

EL CASO DE LA PRINCESA CAROLINA

La princesa Carolina, princesa de Hannover y princesa de Mónaco, es la hija mayor de la estrella de cine americana Grace Kelly.

Cuando Grace Kelly contrajo matrimonio con el príncipe Rainiero III de Mónaco en 1956, abandonó su carrera de actriz y se trasladó a Mónaco. La princesa Grace estuvo permanentemente en el punto de mira público, hasta que falleció trágicamente en un accidente de tráfico en 1982. Para entonces, sus hijos (la princesa Carolina, la princesa Estefanía y el príncipe Alberto) ya se habían convertido en el centro de atención de los medios de comunicación europeos.

A finales de la década de los 90, la princesa Carolina llevó a una serie de revistas alemanas ante los tribunales, por la publicación de unas fotografías en las que aparecían ella, su marido y sus hijos realizando diversas actividades como compras, deporte y saliendo de un restaurante. Los tribunales de Alemania rechazaron la demanda interpuesta para prohibir a estos medios de comunicación fotografiar a la princesa, sin embargo, fallaron a favor de no publicar ciertas fotografías de sus hijos.

Después de la decisión de la judicatura, la princesa Carolina hizo hincapié en su derecho personal a la privacidad y llevó su caso ante el Tribunal Europeo de Derechos Humanos en Estrasburgo. Este Tribunal resolvió que se había infringido el derecho a la privacidad de la princesa Carolina, porque en el artículo 8 de la Convención Europea de Derechos Humanos (1950) se estipula que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

La legislación española:
La Constitución Española, en su artículo 18, garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen; reconoce la inviolabilidad del domicilio; garantiza el secreto de las comunicaciones; y, en particular, regula que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
Asimismo, el derecho a la privacidad está claramente recogido en la Declaración Universal de los Derechos Humanos (DUDH) redactada en 1948.

FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Escapar de los paparazzi

Lee la situación que se describe a continuación y completa el ejercicio de la página siguiente.

Imagina que eres el hijo o la hija de una pareja de celebridades. Los medios de comunicación constantemente os persiguen a ti y a tu familia para conseguir imágenes vuestras en lugares públicos. Publican fotografías tuyas en familia asistiendo a un estreno, de camino a la escuela con tus amigos y amigas, jugando al fútbol o saliendo por la noche al cine o con una cita. Es verdad que algunas veces tu vida es emocionante y glamourosa, pero la novedad enseguida se desvanece. Ahora crees firmemente que no deberías soportar la persecución de los paparazzi cuando estás realizando tus actividades cotidianas. Tampoco entiendes por qué tu familia y su equipo de abogados tienen que derrochar tanto tiempo y dinero en gastos legales intentando que los tribunales prohíban a los paparazzi sacaros fotografías. A pesar de que entiendes que hay gente a la que le gusta comprar revistas llenas de fotografías de celebridades y sus familias, deseas que reflexionen en cómo esto te afecta. Sin embargo, también reconoces que las hijas e hijos de algunas celebridades buscan por activa y por pasiva la atención de los medios de comunicación.

Durante el último año han aparecido publicadas en periódicos y revistas las siguientes fotografías tuyas y de tu hermana...

Los Oscar

Jugando al fútbol

¡Plantada!

El hijo adolescente de la estrella acude a expertos por causa del acné

FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Redacta una petición ingeniosa y graciosa a la prensa, solicitándoles que te dejen en paz. Esperas que tu declaración se publique en diversos periódicos serios con el objetivo de que las revistas de moda y la prensa rosa dejen de acosarte. Aceptarías que te fotografiaran únicamente cuando asistas a actos públicos. En la declaración puedes recordar a la prensa que legalmente eres una persona menor de edad y deseas que te dejen crecer cometiendo errores en cuestiones de indumentaria o moda, haciendo nuevas amistades y viviendo tu propia vida sin someterte a un examen riguroso y a una especulación constante por parte de los medios de comunicación.

A continuación puedes escribir tu petición en forma de canción, poema o carta.

ACTIVIDAD 1

PROFESORADO

FAMA Y PRIVACIDAD

IDEAS PARA LA ACCIÓN

- Tomando como base la situación descrita anteriormente, organice una competición con las declaraciones que cada estudiante ha escrito a la prensa para que le dejen en paz en formato de poema, canción o carta. Anímeles para que redacten escritos y los representen ante un jurado. Considere premios para varias categorías, así como un "premio absoluto".

ACTIVIDAD DE SEGUIMIENTO

- Lleve a clase una pequeña selección de revistas conocidas en las que aparezcan celebridades, cotilleos y cuestiones sobre moda. Divida la clase en grupos para que en cada uno se examinen las publicaciones conjuntamente en busca de fotografías de cantantes, modelos, actrices y actores, futbolistas famosos y de sus respectivas familias.

  Luego, hagan un debate en torno a los siguientes aspectos (tome nota de sus conclusiones para comunicárselas al final del debate):

- Algunas veces las caras de los hijos e hijas de las celebridades que aparecen en las fotografías se muestran borrosas (esto es, desenfocadas deliberadamente); en otras imágenes de publicaciones similares, en cambio, las caras aparecen nítidas. Según tu opinión, ¿cuál podría ser el motivo?
- ¿Todas las fotografías que se sacan a las celebridades y a sus hijas e hijos son tomadas como parte de apariciones oficiales en actos públicos?
- ¿Qué opinas de esos padres y madres que firman una exclusiva con una revista para permitir publicar fotografías en las que aparecen la familia completa en sus casas?
- ¿Muestra alguna revista mayor sensibilidad que las demás? O en general, ¿crees que todas las revistas se encuentran más o menos al mismo nivel?
- A menudo los retratos y las fotografías oficiales son la opción preferida de personalidades públicas destacadas, como por ejemplo de los políticos y políticas. ¿Por qué crees que la prensa no muestra gran interés en utilizar este tipo de imágenes?

UNIDAD 1.5

PROFESORADO

FAMA Y PRIVACIDAD

Información adicional que se puede utilizar o debatir en clase.

ESTÁNDARES DE PRIVACIDAD

En el sector de los medios de comunicación

En muchos países europeos industria periodística y periodistas se reúnen con el resto de agentes implicados y acuerdan actuar siguiendo unos Códigos de Conducta. En dichos Códigos se establecen normas para una serie de comportamientos, incluido lo relativo a fotografiar a menores. Estas normas no siempre se cumplen pero sirven como directrices.

Por ejemplo, la Federación de Asociaciones de Periodistas de España ha aprobado un Código Deontológico de la Profesión Periodística. En su artículo 4.d. habla del respeto al derecho a la intimidad de los menores y en el artículo 6 se recoge que, en particular, las personas que informan deberán abstenerse de entrevistar, fotografiar o grabar a menores de edad sobre temas relacionados con actividades delictivas o enmarcables en el ámbito de la privacidad.

Otro ejemplo lo encontramos en un Manual de Ética Comparada, producido por el Centro de Competencia en Comunicación para América Latina. Algunos de los valores y Principios ético-profesionales del Periodismo, convalidados por grandes diarios del mundo, abordan el tratamiento de menores (ver algunos fragmentos en la columna de la derecha).

MENORES

"Los medios de comunicación no deberían, por regla general, entrevistar o fotografiar a menores de 16 años sobre temas que se refieran a su situación personal, en ausencia de, o sin el consentimiento de los padres u otro adulto que esté a cargo de ellos. No se debe abordar a menores, ni hacerles fotografías cuando estén en la escuela, sin el permiso de las autoridades escolares". —BPRESS.

"Cuando los menores sean víctimas de un delito, sus nombres no serán publicados, excepto si las familias han dado su aprobación, o si fueran ampliamente conocidos por la opinión pública". —LE MONDE.

"Este periódico no publica en sus textos la identidad de personas menores de 18 años, cuando: a) son víctimas o autores de delitos o contravenciones, b) se encuentran en estado de abandono o en peligro material o moral". —CLARIN.

UNIDAD 1.5

PROFESORADO

FAMA Y PRIVACIDAD

Información adicional que se puede utilizar o debatir en clase.

IDEAS PARA LA ACCIÓN

Localiza y examina un caso de la AEPD sobre la Inserción de un vídeo en Youtube, tras la grabación sin consentimiento de imágenes de un menor discapacitado. La ruta para su localización es www.agpd.es (sección Resoluciones; Procedimientos Sancionadores y seleccionar **Inserción de un vídeo en Youtube**; el enlace acortado es http://bit.ly/mYkIXA).

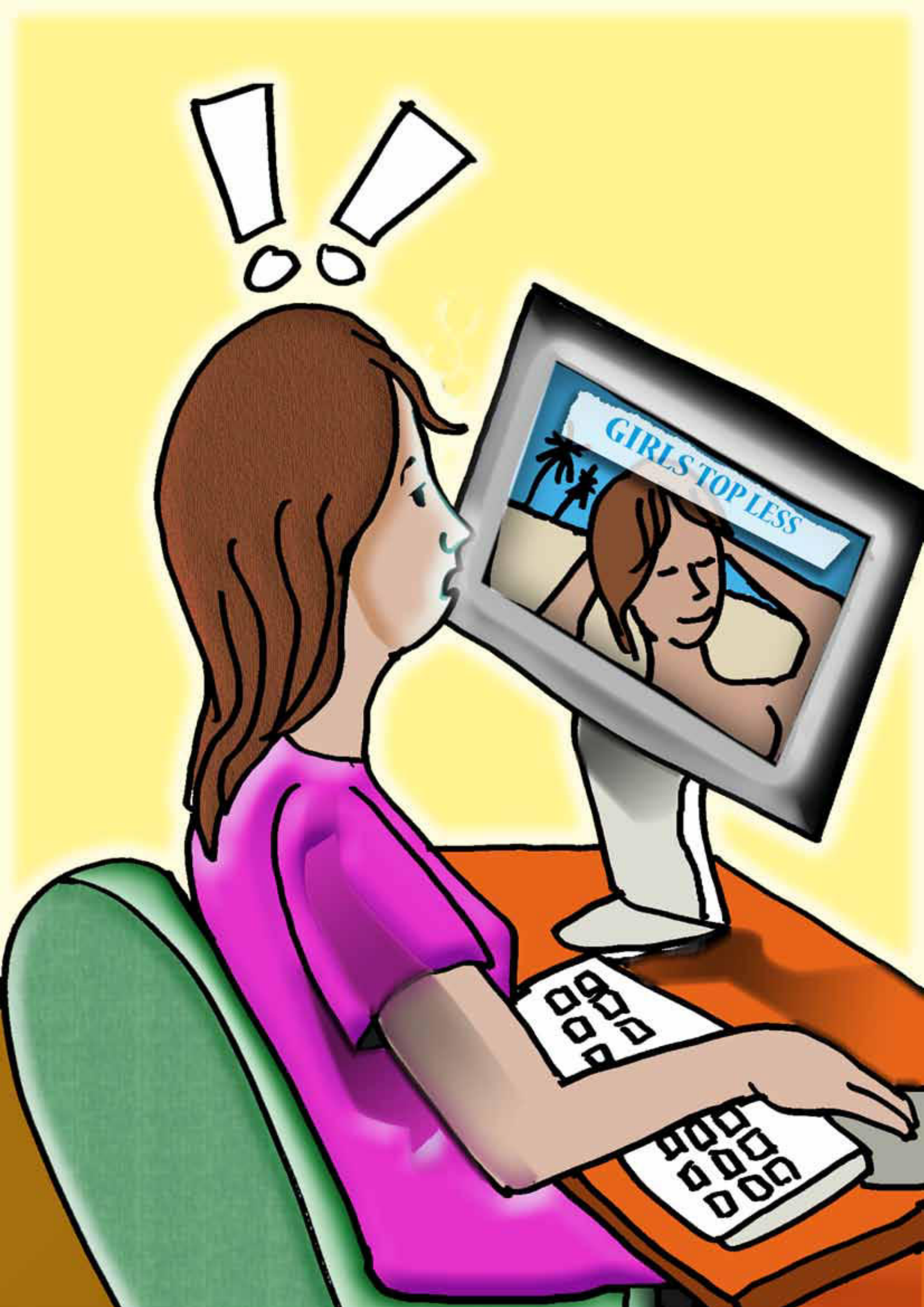
A iniciativa propia, la AEPD abrió una investigación a raíz de las informaciones publicadas en medios de comunicación, referidas a la captación y posterior difusión, a través de un conocido portal de videos, de imágenes en las que varios jóvenes se burlaban de un discapacitado psíquico (PS/00479/2008)

Las actuaciones investigadoras concluyeron con la declaración de una infracción grave de la Ley Orgánica de Protección de Datos, y la imposición de una multa de 1.500 euros, a los responsables de la grabación y posterior publicación de imágenes de una persona con discapacidad psíquica, sin su consentimiento.

En su resolución, la AEPD pone de manifiesto que la captación y reproducción de imágenes de personas y su publicación accesible para cualquier usuario de Internet están **sometidas al consentimiento de sus titulares**, siempre que permitan la identificación de las mismas y cuando no se encuentren amparadas por el ejercicio de las libertades de expresión e información.

ACTIVIDAD DE SEGUIMIENTO

- Un grupo de estudiantes representará una obra que tiene lugar en una sala de un juicio: los personajes son una pareja de celebridades que han demandado a la prensa por publicar unas fotografías en las que están de vacaciones con sus hijos e hijas.


GIRLS TOP LESS

UNIDAD 2


LA PRIVACIDAD
COMO DERECHO HUMANO
EL CENSO DE POBLACIÓN
PROTECCIÓN DE DATOS

OBJETIVOS

- Aprender cómo y por qué la privacidad se ha convertido en un aspecto muy valorado.
- Considerar la privacidad como un derecho humano.
- Aprender cómo surgió la legislación sobre la protección de datos.

CONOCIMIENTOS

- La difícil situación de los judíos en Alemania y en los territorios ocupados por los nazis durante la Segunda Guerra Mundial.
- La finalidad de un censo nacional y las garantías vigentes para proteger los datos de los ciudadanos y ciudadanas.
- El papel del cambio tecnológico en el surgimiento de la protección de datos como un conjunto específico de principios y corpus legal.

CONCEPTOS

- Derechos y Responsabilidades.
- La Dignidad Humana.
- La Ley.

HABILIDADES

- Análisis: organización, comparación, enumeración y evaluación de diferentes conjuntos de datos.
- Comunicaciones: discusión,role play, audición, representación, empatía.

ACTITUDES Y VALORES

- Mostrar interés por los derechos humanos desde el punto de vista de la privacidad.
- Desarrollar empatía hacia las personas necesitadas o en desventaja como resultado de los abusos contra la privacidad.
- Entender el valor de las grandes recopilaciones de datos, las garantías y derechos vigentes y las áreas de abuso potenciales.

UNIDAD 2.1

PROFESORADO

EL SURGIMIENTO DE LA PRIVACIDAD COMO UN DERECHO HUMANO

Explique a los alumnos y a las alumnas el contexto descrito a continuación

ANTECEDENTES

Poco después de que el régimen nazi de Hitler llegara al poder en Alemania en 1933, el gobierno comenzó a recopilar catálogos de fichas identificativas de enemigos políticos y raciales del Reich alemán (Estado). En la Alemania del siglo veinte los judíos y las judías estaban completamente integrados en la sociedad alemana y habían adquirido estatus en el mundo de los negocios, en los ámbitos científicos, como profesionales de la abogacía, la física, entre el profesorado y como escritores y escritoras. No obstante, una vez que Hitler se hizo con el poder, la comunidad judía se convirtió uno de los objetivos principales, ya que una de las obsesiones de Hitler era lograr la purificación de la raza alemana según el ideal tradicional de alemán ario, rubio y de ojos azules. Asimismo, el deseo de perfección y el "Movimiento de Higiene de la Raza Alemana" provocó que se persiguiera también a la gente con discapacidades.

Se calcula que durante el régimen de Hitler fueron asesinados unos cinco mil niños y niñas y ocho mil personas adultas con alguna discapacidad en hospitales estatales e instituciones mentales.

Durante la Segunda Guerra Mundial, mientras el ejército alemán luchaba contra las fuerzas aliadas y los civiles de toda Europa, el régimen nazi cometió crímenes terribles contra los judíos y los gitanos. Se cree que en Europa murieron seis millones de personas de ascendencia judía y quinientos mil gitanos como consecuencia de la Segunda Guerra Mundial, muchos de ellos asesinados por los nazis en campos de concentración.

UNIDAD 2.1

PROFESORADO

Organice un debate entre el alumnado en torno a los siguientes puntos clave antes de repartir la hoja informativa de la página 32.

¿Cómo se produjo un holocausto a tan gran escala?

¿Cómo sabían las autoridades nazis con exactitud quién era judío o judía?

Respuesta: DATOS

¿Cómo fueron capturadas personas judías?

¿Cómo identificó el Tercer Reich las zonas residenciales donde vivían más judíos?

LOS NAZIS UTILIZARON DATOS PARA CREAR SISTEMAS SOFISTICADOS DE IDENTIFICACIÓN DE LA POBLACIÓN

CENSO DE POBLACIÓN

El censo es un recuento oficial de la población de un país

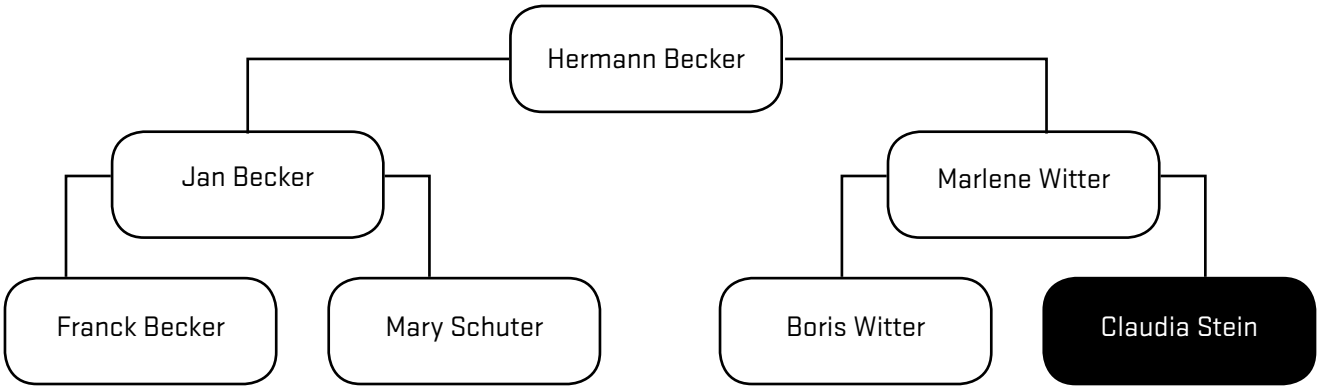
El Censo Nacional fue una de las principales herramientas utilizadas para identificar a los ciudadanos de raza o ascendencia judía.

El censo alemán de 1939 obligaba a la ciudadanía a identificarse, tanto por su filiación religiosa como por su raza. Asimismo, les exigía que indicaran la religión de sus cuatro abuelos y abuelas, con lo que se podía identificar a la gente con cualquier traza de ascendencia judía.

FOTOCOPIABLE

UNIDAD 2.1. ALUMNADO

Hoja informativa para el alumnado



En última instancia, el censo de 1939 se convirtió en la herramienta principal para crear un registro nacional de personas de ascendencia judía. En un periodo de tres años, el registro nacional completado proporcionó a los nazis la base para elaborar las listas de deportación de judíos y de judíos "Mischlinge" (judíos de razas mixtas).

Registro de la población

Nombre y apellido	Dirección	Religión	Judío de raza
Becker, Hermann	11 Weiss Strasse	Luterano Cabuela paterna: Claudia Stein. Judía)	25% Mischlinge

SISTEMAS DE IDENTIFICACIÓN DE LA POBLACIÓN: CARNÉS DE IDENTIDAD

Tras una recopilación de datos de diversas fuentes del gobierno, se distribuyeron a todos los habitantes del Reich tarjetas de identidad con foto, obligatorias según la ley de 10 de septiembre de 1939. Asimismo, en cumplimiento de lo estipulado en las disposiciones especiales de 27 de septiembre de 1939, se repartieron las tristemente famosas "tarjetas-J" para los judíos.

UNIDAD 2.2. ALUMNADO

Lee la situación descrita a continuación

DEPORTACIÓN

La mayoría de las personas deportadas a campos de concentración murieron en el Holocausto. En territorios ocupados como, por ejemplo, los Países Bajos, se utilizaron métodos similares para recopilar datos acerca de los judíos. Todas aquellas personas identificadas como judías fueron sometidas a una estricta restricción de su libertad en numerosos sentidos.

Ana Frank, una chica judía, tenía trece años cuando escribió lo siguiente en su diario:

Después de mayo de 1940 los buenos tiempos quedaron definitivamente atrás: primero la guerra, luego la capitulación [la rendición de Holanda ante los Nazis], seguida de la llegada de los alemanes, que fue realmente el comienzo del sufrimiento para la comunidad judía. Las medidas antijudías se sucedieron rápidamente. Las personas de ascendencia judía deben llevar una estrella amarilla; deben entregar sus bicicletas; no les está permitido viajar en tranvía; les está prohibido conducir; los judíos sólo pueden hacer la compra desde las tres hasta las cinco de la tarde en tiendas que tengan el cartel de "tienda judía". No pueden estar en la calle después de las ocho de la noche y ni siquiera pueden estar sentados en su propio jardín a partir de esa hora; no les está permitida la entrada en teatros, cines y otros lugares de ocio; no les está permitido tomar parte en ningún tipo de deportes públicos. Tienen prohibida la entrada en piscinas, pistas de tenis, campos de hockey y de cualquier otro deporte. Los judíos no pueden visitar a los cristianos, deben ir a colegios judíos. Y muchas más restricciones similares. Con lo que no podíamos hacer esto y nos prohibían hacer aquello.

Ana Frank: ***El diario de Ana Frank***

EN ALGÚN OTRO LUGAR...

Al otro lado del Atlántico, mediante investigaciones se ha demostrado recientemente el modo en que la Oficina del Censo de EE.UU. facilitaba información a las agencias de vigilancia americanas durante la Segunda Guerra Mundial. Los datos del censo se utilizaron para identificar a las personas con ascendencia japonesa.

UNIDAD 2.2

PROFESORADO

LECCIONES APRENDIDAS

La gente pudo ver el poder destructivo que podía tener la información en manos de un gobierno malvado y cómo la información recabada para un fin determinado puede reutilizarse para una amplia variedad de propósitos siniestros. Estos ejemplos extremos de mal uso del censo y de sistemas de identificación de la población para perseguir a las minorías y exterminarlas pesaron enormemente en las conciencias de aquellas personas que se encargaron de la reconstrucción de Europa y de redactar las declaraciones de derechos humanos.

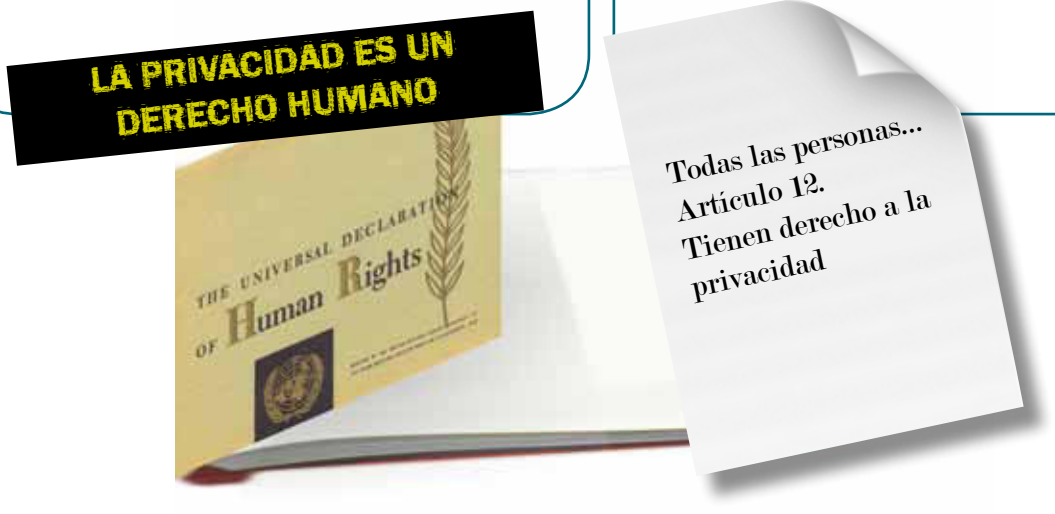
Estos antecedentes históricos nos ayudan a comprender la razón por la cual, en la actualidad, la privacidad se considera expresamente un derecho humano –el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948 y el artículo 8 del Convenio Europeo de Derechos Humanos (1950) recogen la lección de la posguerra y tienen como fin proteger a los ciudadanos y a las ciudadanas de injerencias externas–. Ambos artículos expresan el derecho de las personas a la privacidad.

IDEAS PARA LA ACCIÓN

Visite las páginas web de algunas organizaciones en pro de los derechos humanos que conozca.

Invite a una organización en pro de los derechos humanos a acudir al colegio para realizar una presentación sobre los derechos humanos y las libertades civiles. Solicíteles de antemano algunos ejemplos recientes en los que los derechos humanos relacionados con la privacidad hayan sido infringidos.

Nota u observación para el profesorado: un posible tema de discusión podría centrarse en los profesionales del periodismo que intentan hacer llegar informes a través de Internet desde países en los que no siempre se admiten la libertad de expresión o el derecho a opinar. En esos países, a menudo, las autoridades del gobierno piden los datos personales de los periodistas al proveedor del servicio de Internet, quien en ocasiones se los ha proporcionado, facilitando de ese modo la búsqueda y el arresto de los periodistas y las periodistas implicados.



FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Completa el siguiente ejercicio

ANTECEDENTES

Todo tipo de datos, incluso tu nombre, puede revelar aspectos sobre ti y tu pasado.
Así, por ejemplo, se consideran datos personales:

Nombre, dirección, fecha de nacimiento, nombres del padre y de la madre y sus profesiones, religión, orígenes étnicos o culturales, saldo bancario, historial médico, expediente académico, nº de carné de identidad, nº de la Seguridad Social, imágenes de video, fotografías, huellas dactilares, prescripciones facultativas como las recetas médicas, facturas de teléfono, resultados de exámenes, número del teléfono móvil, nóminas, afiliación a un partido político.

Rodea con un círculo los datos solicitados que consideres innecesarios e irrelevantes en la situación descrita en los siguientes casos:

1. Para solicitar trabajo como socorrista a tiempo parcial en una piscina local durante el verano:

Nombre: .....
Dirección: .....
Número de teléfono: .....
Fecha de nacimiento: .....
Profesión del padre y de la madre: .....
Aficiones:.....
Experiencia laboral: .....

2. ¡Una oferta de una funda para el teléfono móvil gratis! Simplemente completa la etiqueta que hay en la parte trasera de una conocida bebida mineral y te enviarán el soporte siempre que envíes el número correcto de etiquetas junto con tu solicitud:

Nombre: .....
Dirección: .....
Número de móvil: .....
Correo electrónico: .....
Bebida mineral preferida: .....

3. Una organización benéfica está vendiendo boletos para una rifa. Compras un boleto y te piden que rellenes la siguiente información en el propio boleto:

Nombre: .....
Dirección: .....
Nº de teléfono de contacto: .....
Nº de carné de identidad: .....
Origen étnico/cultural: .....
.....

4. Para trabajar como voluntario o voluntaria en la biblioteca del centro parroquial:

Nombre: .....
Dirección: .....
Nº de teléfono: .....
Religión: .....

UNIDAD 2.3

PROFESORADO

EL CENSO DE POBLACIÓN

OBJETIVO

- Capacitar al alumnado para evaluar desde un punto de vista crítico el modo en que se realiza en la actualidad el censo de población.
- Hacer hincapié en las garantías vigentes y en la obligación de confidencialidad y anonimato que se recoge en la legislación.
- Concienciar sobre los peligros de unas garantías inadecuadas y de los abusos que podrían producirse en situaciones en las que predominen las condiciones extremas.

La organización que elabora el Censo es el Instituto Nacional de Estadística (INE) [1].
La norma legal de aplicación es la Ley 12/1989, de la Función Estadística Pública.

Las estadísticas de población son necesarias y fundamentales para planificar la provisión de recursos para la asistencia sanitaria, la educación, el empleo o el desarrollo de infraestructuras básicas. Asimismo, el censo es el único medio para medir con precisión el alcance exacto de los fenómenos migratorios. Respecto a la información personal proporcionada, en la actualidad hay muchas garantías en vigor para proteger a las personas particulares y respetar la confidencialidad.

- Los datos recabados sobre personas particulares o familias no pueden transferirse a otros órganos o agencias públicas.
- Los datos únicamente pueden ser utilizados para los fines legalmente previstos.
- La información sobre tu persona y tu familia se carga en la base de datos del INE por separado, esto es, no se retienen nombres ni direcciones en la información guardada informáticamente.
- Preguntas en torno a la raza y la religión no se incluyen y ni han formado parte de los censos españoles ni están previstas para el Censo 2011; es más, con la legislación actual (art. 11.2. de la Ley 12/1989) difícilmente podrían incluirse, salvo como preguntas de respuesta estrictamente voluntaria y, en consecuencia, sólo podrían recogerse previo consentimiento expreso de los interesados.

[1] **Se puede comprobar si en su Comunidad Autónoma existe algún organismo público con funciones estadísticas que colabora con el INE en la elaboración del Censo.**

ACTIVIDAD 1

PROFESORADO

1. Fotocopie esta página y la siguiente y distribúyaselas a los alumnos y a las alumnas.
2. Examine el fragmento del impreso del censo mostrado a continuación y pídales que localicen el punto donde se indica:
a) La Ley 12/1989, de la Función Estadística, garantiza la confidencialidad.
b) La participación en el Censo es obligatoria.
3. Pídales que respondan a las dos preguntas resaltadas como si verdaderamente estuvieran rellenando el impreso del censo.
4. Pídales que cumplimenten el cuestionario.
Observación: no se les pide que escriban su nombre en la hoja de respuesta correspondiente a este ejercicio.
5. Pida a uno de los alumnos o alumnas que recoja todas las hojas de respuesta.
6. Designe a un grupo de alumnos y alumnas para que calcule el porcentaje de alumnado correspondiente a cada categoría seleccionada de acuerdo con las respuestas recogidas (España, esta Comunidad Autónoma, este Municipio, otro Municipio o país anteriormente).
7. Pida a un grupo que calcule el número de "sí" y "no" para cada pregunta del cuestionario (véase página siguiente), por ejemplo, el 60% de la clase respondió "sí" y el 40% "no" a la pregunta 1, etc.

Instituto Nacional de Estadística (INE)
Censo de Población de 2001

Sobre el censo

El censo de población se realiza junto al censo de viviendas con una periodicidad de diez años, por imperativo legal en los años terminados en 1 y recoge el cómputo de todas las personas y familias del país. Se aprovecha igualmente para obtener una serie de datos demográficos, económicos y sociales relativos a su población, considerada desde el punto de vista cuantitativo. Así, los resultados del censo ayudan a confeccionar una imagen global de las condiciones sociales y de vida de los habitantes y proporcionan información fundamental necesaria para planificar el futuro de nuestro territorio. Los métodos de recogida de información de los censos son una combinación de censos basados en registros (padrones municipales) y encuestas por muestreo.

La participación es obligatoria

El censo se desarrolla de conformidad con la Ley de la Función Estadística Pública (Ley 12/1989). Son una estadística de cumplimentación obligatoria. Si no se responde o si se dan a sabiendas datos falsos, se podrán aplicar las sanciones previstas en los artículos 50 y 51 de la Ley de la Función Estadística Pública.

Se garantiza la confidencialidad

La Ley de la Función Pública Estadística garantiza la confidencialidad de los datos del censo. Con la única excepción de los datos patronales, que el INE debe enviar al ayuntamiento que corresponda, la información solicitada no será publicada ni cedida a nadie, de manera que se pueda saber a quién corresponde, ni siquiera indirectamente. Además, el personal implicado en los trabajos censales tiene obligación expresa de guardar el secreto estadístico.

Agente censal

Su agente censal le ayudará en caso de que tenga alguna dificultad a la hora de rellenar el impreso o si deseara información adicional sobre el mismo.
Gracias por su colaboración.

FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Fragmentos del Censo de 2001

Cuestionario del hogar

5 ¿Desde qué año reside (aunque sea desde que nació) en:

España ☐☐☐☐

Esta Comunidad Autónoma ☐☐☐☐

Este Municipio ☐☐☐☐

Si antes residía en otro Municipio o país, escríbalo:

☐☐☐☐☐☐☐☐☐☐☐

☐☐☐☐☐☐☐☐☐☐☐

CUESTIONARIO

Pregunta	Sí	No
1. ¿Estás de acuerdo en que la declaración "Confidencialidad Garantizada" y la Ley de Función Estadística Pública te protegen?	☐	☐
Pregunta	**Sí**	**No**
2. ¿Te tranquiliza saber que todos los nombres y los detalles de las personas particulares no están vinculados con los datos sobre nacionalidad, situación de residencia, variables migratorias, condición socioeconómica, etc. que se conservan en los ordenadores?	☐	☐
Pregunta	**Sí**	**No**
3. ¿Reconoces que la sociedad necesita este tipo de información para planificar el futuro y establecer prioridades en los servicios?	☐	☐

ACTIVIDAD DE SEGUIMIENTO

Juego de roles: prepare una situación para presentarla en clase. Imagine que es la noche del censo y una persona está sentada rellenando el impreso del censo. Elija a un alumno o a una alumna para que represente a esta persona y a otro para que asuma el papel de responsable de recoger los impresos cumplimentados, esto es, de agente censal. La persona se muestra reticente a responder a cuestiones como la naturaleza del régimen de ocupación de la vivienda, es decir, si es de alquiler, propiedad de alguna autoridad local, o propia –véase Pregunta 2 del impreso del censo de 2001 facilitado más abajo–.

Cuando llega el o la agente censal para recoger el impreso, éste y la persona se enzarzan en un debate a la puerta de la casa. El primero deberá persuadir a la persona encuestada para que conteste a las preguntas restantes, recordándole sus obligaciones legales en este sentido y tranquilizándole con las garantías vigentes que protegen su privacidad.

2 Régimen de tenencia de la vivienda
Marque una única casilla

- ☐ En propiedad por compra, totalmente pagada
- ☐ En propiedad por compra, con pagos pendientes (hipotecas…)
- ☐ En propiedad por herencia o donación
- ☐ En alquiler
- ☐ Cedida gratis o a bajo precio por otro hogar, la empresa…
- ☐ Otra forma

ACTIVIDAD DE SEGUIMIENTO

En el ordenador del colegio, de la biblioteca o de casa, entre al sitio web del INE y descargue una copia del impreso correspondiente al Censo más reciente (2001, 2011):
http://www.ine.es/censo2001/cuestionarios.htm

- Pregunte a los alumnos cuáles serían las consecuencias si las personas dejaran de confiar en el INE y no facilitaran la información requerida.

UNIDAD 2.4

PROFESORADO

PROTECCIÓN DE DATOS

Las páginas siguientes contienen una serie de ejercicios. Elija una o varias actividades adecuadas para el alumnado

La Alemania nazi es un ejemplo del siglo pasado en el que se manipulaba y se hacía mal uso de la información sobre discapacidades e identidad racial, con el objetivo de segregar o tratar con crueldad a los ciudadanos y las ciudadanas vulnerables. Sin embargo, cuando en la década de los 50 surgieron las declaraciones de derechos humanos y el marco legal sobre la privacidad, la sociedad también comenzó a evolucionar a un ritmo vertiginoso en el ámbito tecnológico. La capacidad de procesamiento de información de los ordenadores y, en particular, de las bases de datos para almacenar, agrupar y manipular información trajo consigo finalmente la necesidad de promulgar legislación para poder ajustarse a la velocidad del progreso tecnológico. Sin lugar a dudas, las nuevas tecnologías pueden brindar muchas oportunidades y mejoras, pero también pueden crear oportunidades para intromisiones más frecuentes en las vidas privadas de los ciudadanos y de las ciudadanas.

Con el fin de contrarrestar tales amenazas para la privacidad, se tomaron medidas para controlar la manera en que las personas particulares y las organizaciones podían recopilar y procesar la información personal. En la actualidad, la ley que aborda la información personal es la Ley Orgánica de Protección de Datos de Carácter Personal (Ley 15/1999, de 13 de diciembre). La legislación española se introdujo a partir del desarrollo normativo del marco europeo –principalmente el Convenio 108/81, de 28 de enero, del Consejo de Europa y dos directivas clave de la UE de 1995 y 2002–.

La legislación sobre protección de datos no es de aplicación a los datos personales conservados por particulares para actividades personales o domésticas.

Ejemplos de aspectos **regulados** por la legislación	Ejemplos de aspectos **no regulados** por la legislación
Una empresa que posea una lista de nombres y números para fines comerciales.	La legislación no afecta a la posesión de una lista de nombres y números en un teléfono móvil de una persona en particular.
Una organización deportiva que tenga una hoja de cálculo con los nombres de todas las personas del equipo y sus datos de contacto.	La legislación no afecta a una lista de nombres en una hoja de cálculo que contenga una relación de las personas de tu equipo de fútbol y sus respectivos datos de contacto, para poder contactar con ellas y ellos y fijar las fechas de los encuentros.
Un anuario del colegio con nombres y fotos del alumnado.	La legislación no afecta a una lista de nombres en un diario personal en el se detallen nombres, fechas y comentarios sobre personas conocidas. [No obstante, una lista de nombres en una página web personal en la que se detallen nombres, fechas y comentarios sobre personas conocidas podría entrar en el marco de la legislación, puesto que un sitio web de redes sociales es un foro público].

FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Completa el siguiente cuestionario

¿QUIÉN TIENE MI INFORMACIÓN?

- Divida a la clase en grupos de cinco.
- Cada grupo tiene que imaginar de qué tipo de información relacionada con personas particulares dispone cada uno de los organismos y por qué.
- Cada grupo rellenará tantas columnas como le sea posible.

Organismo	Tipo de información	¿Por qué?
Compañía telefónica		
Banco o Caja de Ahorros		
Supermercado		
Asuntos Sociales		
Colegio		
Farmacia		
Educación		
Unidad de Impuestos sobre Vehículos		
Compañía de seguros		
Servicio Médico		
Ministerio de Interior (Policía Nacional) para expedición de pasaportes		
Salud e Infancia		
Policía de Tráfico		
Videoclub		

ACTIVIDAD 1 PROFESORADO

Las respuestas facilitadas a continuación son únicamente orientativas

OBJETIVO

El objetivo de la Actividad 1 consiste en que los alumnos y las alumnas se familiaricen con las instituciones que guardan un registro de sus datos personales e intenten imaginarse qué tipo de información tiene cada una de ellas y por qué.

Cuando comiencen a completar las columnas de sus respectivas hojas de ejercicios, puede ayudarles con la lista expuesta a continuación. Explíqueles que para que la sociedad funcione correctamente, de una manera organizada, es necesario que las organizaciones recopilen y almacenen información sobre las personas particulares.

Institución [4]	Tipo de información	¿Por qué?
Compañía telefónica	• Nombre • Dirección • Número de teléfono • Todas las llamadas realizadas y recibidas	Para emitir una factura y registrar todas las llamadas de teléfono.
Banco o Caja de Ahorros	• Detalles de las tarjetas de débito y de crédito. • Documento acreditativo de identidad • Dirección • Detalles de las transacciones	Los datos de contacto son necesarios para poder enviar los extractos bancarios. Además, el banco debe controlar las transacciones y aplicar la legislación contra el blanqueo de dinero.
Supermercado	• Tarjeta de fidelidad por puntos • Nombre • Dirección • Historial de compra	Para enviar cupones por correo. Cuestiones de marketing (para enviar información sobre productos que pudieran interesar al cliente).
Servicios de Asuntos Sociales	• Nombre • Dirección • Fecha de nacimiento • Número de carné de identidad o documento acreditativo	Para la solicitud de prestaciones (por ejemplo, la asignación por hijos e hijas).

[4] **El profesorado puede adaptar la denominación de las instituciones a su Comunidad Autónoma. Se han utilizado nombres genéricos de áreas, servicios, departamentos, etc.**

ACTIVIDAD 1 PROFESORADO

Las respuestas facilitadas a continuación son únicamente orientativas

Institución [4]	Tipo de información	¿Por qué?
Colegio	• Nombre • Dirección • Datos de contacto del padre, madre o tutores • Resultados académicos • Informes escolares • Registro de asistencia • Información sanitaria	Debe tener un registro de todos los alumnos y alumnas y disponer de los datos necesarios para contactar con las familias en caso de emergencia.
Hospital	• Detalles del nacimiento • Radiografías archivadas	Es importante conservar los detalles del nacimiento, incluyendo cualquier complicación surgida. El hospital debe archivar las consultas de los pacientes, con sus respectivos datos, para disponer de un expediente sanitario y realizar los diagnósticos.
Farmacia	• Recetas • Nombre • Dirección	Para controlar las recetas; podría resultar importante llevar un registro de las recetas en caso de reacción adversa.
Educación	• Nombre	Para mantener un registro del alumnado matriculado en los centros docentes y de los resultados académicos. En caso de pérdida, los registros podrían ser repuestos.
Unidad de Impuestos sobre Vehículos	• Nombre • Dirección • Tipo de vehículo y matriculación	Datos sobre el Permiso de Conducción y el Impuesto de Circulación.

[4] **El profesorado puede adaptar la denominación de las instituciones a su Comunidad Autónoma. Se han utilizado nombres genéricos de áreas, servicios, departamentos, etc.**

ACTIVIDAD 1 PROFESORADO

Las respuestas facilitadas a continuación son únicamente orientativas

Institución [4]	Tipo de información	¿Por qué?
Compañía de seguros	• Nombre • Dirección • Propiedad asegurada • Inscripción del vehículo, matrícula, marca y modelo • Historial de seguro • Tipo de vehículo y matriculación	La compañía debe poseer los datos de contacto, conocer el objeto asegurado y calcular el riesgo.
Médico	• Nombre • Dirección • Nombres del padre y de la madre	El médico tiene que poder identificar a cada paciente. El historial clínico ayuda a emitir un diagnóstico y proporcionar la asistencia sanitaria adecuada.
Ministerio de Interior (Policía Nacional)	Impreso de solicitud del pasaporte con los siguientes datos: • Nombre • Dirección • DNI • Fotografía En caso de solicitar el pasaporte por primera vez: • Fecha de nacimiento	Debe garantizar que los pasaportes se expiden sólo a las personas que realmente tienen derecho a ello.
Servicio de Salud e Infancia	• Nombre • Dirección • Médico	El servicio lleva un seguimiento del programa de inmunización.
Policía de Tráfico	• Matrícula del vehículo • Nombre • Dirección	Prevención y detección de infracciones y delitos.
Videoclub	• Tarjeta del videoclub • Nombre • Dirección • Número de teléfono	Para localizar los DVD.

[4] El profesorado puede adaptar la denominación de las instituciones a su Comunidad Autónoma. Se han utilizado nombres genéricos de áreas, servicios, departamentos, etc.

FOTOCOPIABLE

ACTIVIDAD 2. ALUMNADO

Lee los siguientes casos de estudio y, después, responde a las preguntas

CASO DE ESTUDIO (I)

Un centro escolar publicó en su página web fotos de una alumna realizando diversas actividades extraescolares, sin haberlo comunicado previamente a la alumna ni a su familia ni haber solicitado su consentimiento para ello.

La Agencia Española de Protección de Datos (AEPD) emitió un informe (Informe 194/2009 AEPD) acerca de esta publicación no consentida, en el que consideró que la imagen de la menor era un dato de carácter personal y, en consecuencia, era necesario recabar su consentimiento o el de sus tutores legales. La AEPD consideró también que el hecho de publicar las fotos en una página web de acceso libre a cualquier usuario de Internet suponía poner a disposición de un número indeterminado de personas la imagen de la niña. Aparte de considerar estos hechos por sí solos susceptibles de sanción por vulnerar el derecho a la protección de datos y privacidad de la menor, la AEPD recordó en su informe el derecho que asiste a los afectados a solicitar la cancelación de esos datos, por ser inadecuados y excesivos, dirigiéndose en primer lugar a quien ha tratado los datos, en este caso el centro educativo, y si éste ignorase la petición, reclamando la tutela de su derecho a la AEPD.

CUESTIONARIO

	Sí	No
¿Estás de acuerdo?	☐	☐
¿Se ha respetado el derecho a la privacidad de la niña?	☐	☐
¿Crees que la familia que denunció los hechos actuó correctamente o tuvieron una reacción exagerada?	☐	☐
¿Crees que la situación es especialmente grave por el hecho de que las fotos eran de una menor de edad?	☐	☐
¿Crees que habría sido mejor si el centro educativo hubiera pedido al alumnado y sus familias autorización para publicar fotos de los estudiantes en la web escolar?	☐	☐

FOTOCOPIABLE

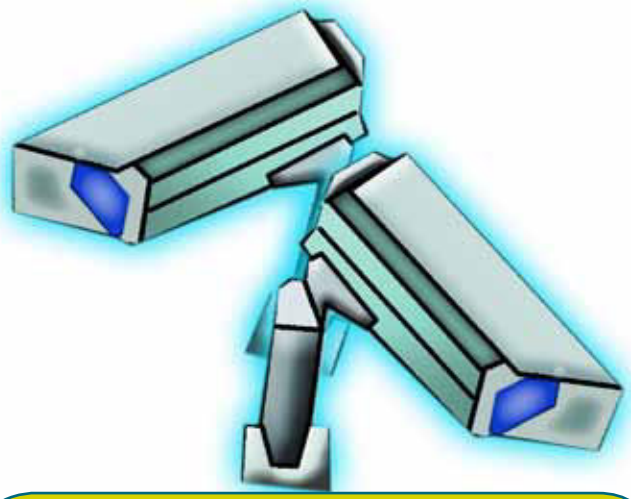
ACTIVIDAD 2. ALUMNADO

Lee los siguientes casos de estudio y, después, responde a las preguntas

CASO DE ESTUDIO (II)

Un Instituto de Enseñanza Secundaria implantó un sistema de cámaras de videovigilancia para prevenir actos vandálicos y un sistema de control de accesos con reconocimiento de huellas dactilares. Algunas de las cámaras de videovigilancia se hallaban situadas en los baños de los estudiantes.

La situación exigía ponderar dos derechos en conflicto, el derecho a la seguridad de las personas y sus bienes en el entorno del centro educativo y el derecho a la protección de datos y privacidad de los afectados. En todo caso se consideró que la vigilancia con cámaras debía ser una medida adoptada respetando el principio de proporcionalidad. Será aceptable si es lo menos intrusiva posible para la intimidad de las personas. Sin embargo, la instalación de las cámaras en los baños de los estudiantes se consideró una medida excesiva, no pertinente e inadecuada en relación con la finalidad de seguridad para la que se recogían las imágenes, una medida ni ponderada ni equilibrada al suponer un perjuicio de derechos de terceros más dignos de protección.
En conclusión, la AEPD declaró la instalación de cámaras de videovigilancia en los baños del Instituto una medida lesiva del derecho a la protección de datos y la privacidad. (Resolución 259/2010).



CUESTIONARIO

	Sí	No
¿Estás de acuerdo?	☐	☐
¿Se ha respetado el derecho a la privacidad de los estudiantes?	☐	☐
¿Crees que quienes denunciaron los hechos actuaron correctamente o tuvieron una reacción exagerada?	☐	☐
¿Crees que la situación es especialmente grave por el hecho de que las imágenes tomadas fueran de menores de edad?	☐	☐
¿Crees que habría sido mejor para el centro educativo si hubiera pedido al Consejo Escolar, que representa a la comunidad educativa, autorización para poner las cámaras en los baños?	☐	☐

FOTOCOPIABLE

ACTIVIDAD 3. ALUMNADO

Es posible que te sorprendas al descubrir que existen una serie de actividades de tu vida diaria en las que tu privacidad se ve afectada. Es importante saber distinguir entre una intrusión o una violación de la privacidad y una interacción social habitual.

- Primero divida la clase en grupos de cuatro personas. Cada grupo leerá las preguntas que encontrará a continuación y marcará las actividades que crea que son una violación de la privacidad y las actividades que considera normales (aunque puede que no sean deseadas). No hay respuestas correctas o erróneas; este ejercicio simplemente pretende que el alumnado reflexione sobre lo que, según su opinión, considera aceptable.

CUESTIONARIO

¿Qué actividades de las descritas en esta tabla crees que podrían considerarse una intromisión a la privacidad?	Sí	No
1. Una compañía telefónica te llama e intenta convencerte para que cambies de compañía y te des de alta con ellos.		
2. Una empresa de teléfonos móviles te envía mensajes intentando que te descargues tonos.		
3. La prima de un/a amigo/a te llama para preguntarte dónde has comprado tu nuevo top.		
4. Una cámara de circuito cerrado de televisión enfocando la entrada de los servicios de un restaurante de comida rápida.		
5. Un mensaje de tu padre preguntándote a qué hora volverás a casa.		
6. Una carta de un banco enviada a una chica de catorce años ofreciéndole una tarjeta de crédito.		
7. Un e-mail de un hotel en el que se alojaron tu madre y tu padre hace 6 años en el que informan de una oferta especial.		
8. Una norma de otro colegio, por la que se te piden las huellas dactilares cuando vas allí de visita.		
9. Una fotografía tuya publicada sin tu permiso en un cartel publicitario anunciando una carrera benéfica.		
10. Tu médico habla de tu historial médico en la recepción de la clínica.		
11. Alguien cuelga tu fotografía en Internet sin tu permiso.		
12. Tu jefe/a deja los datos de los sueldos de los trabajadores y trabajadoras encima de un mostrador al alcance de cualquiera.		
13. Tus datos personales (nombre, dirección, número de teléfono) aparecen en un sitio web como si tú los hubieras posteado.		
14. Una agencia de viajes proporciona los datos personales de tu familia a una empresa de tarjetas de crédito.		
15. Un mensaje de un/a amigo/a invitándote a una fiesta.		

ACTIVIDAD DE SEGUIMIENTO

Cuando corrija esta actividad, pida a los alumnos que piensen en ejemplos de actividades en las que su privacidad se haya visto afectada, aunque no se percataran de ello en el momento en el que se produjo.

UNIDAD 3

DERECHOS Y RESPONSABILIDADES

PROCESANDO DATOS PERSONALES

DATOS ESPECIALMENTE SENSIBLES

EDAD PARA DAR EL CONSENTIMIENTO

SOLICITUDES DE ACCESO
A LOS DATOS PERSONALES

CASOS DE ESTUDIO

OBJETIVOS

- Aprender cómo la legislación sobre la protección de datos confiere derechos e implica responsabilidades.
- Aprender cómo las personas particulares pueden presentar una solicitud de acceso.
- Aprender cómo las personas particulares pueden presentar una queja.

CONOCIMIENTOS

- Principios y leyes para la protección de datos.
- Tratamiento de datos.
- Datos sensibles.
- Edad para el consentimiento.
- Derechos de acceso.
- Derecho a acciones de reparación o compensación.
- Estudios de casos sobre la protección de datos en ámbitos relevantes para la juventud.

CONCEPTOS

- Derechos y Responsabilidades.
- Legislación.

HABILIDADES

- Análisis, organización, comparación, enumeración y evaluación de conjuntos de datos dispares.
- Comunicaciones: discusión, role play, audición, representación, empatía.

ACTITUDES Y VALORES

- Conciencia de los derechos.

UNIDAD 3.1

PROFESORADO

DERECHOS Y RESPONSABILIDADES

Explique a los alumnos y a las alumnas
el contexto descrito a continuación

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, otorga **derechos** individuales, y establece algunas medidas protectoras esenciales. Asimismo, la Ley crea obligaciones e impone **responsabilidades** para quienes recopilan y conservan información personal (responsables de ficheros).

En la mayoría de los casos, organizaciones (por ejemplo, colegios, hospitales, empresas, administraciones públicas, entidades de crédito, bibliotecas) y particulares (por ejemplo, profesionales de la medicina o de la farmacia) que manejan información personal relacionada con los individuos, actúan de forma responsable.

No obstante, es posible que:

- La información almacenada sobre tu persona sea errónea o no esté actualizada;
- La Información sobre ti sea transmitida a personas no autorizadas;
- Recibas "correos basura" o mensajes o e-mails que no has solicitado;
- Tu privacidad esté gravemente amenazada.

PROFESORADO

Antes de proceder a examinar exhaustivamente los "Derechos y Responsabilidades", el alumnado tiene que investigar más profundamente el concepto de "tratamiento". Fotocopie y distribuya a cada persona una copia del diagrama que aparece en la página 53 y pídales que lo analicen. Asegúrese de que entienden que el "tratamiento" es algo más que una operación electrónica.

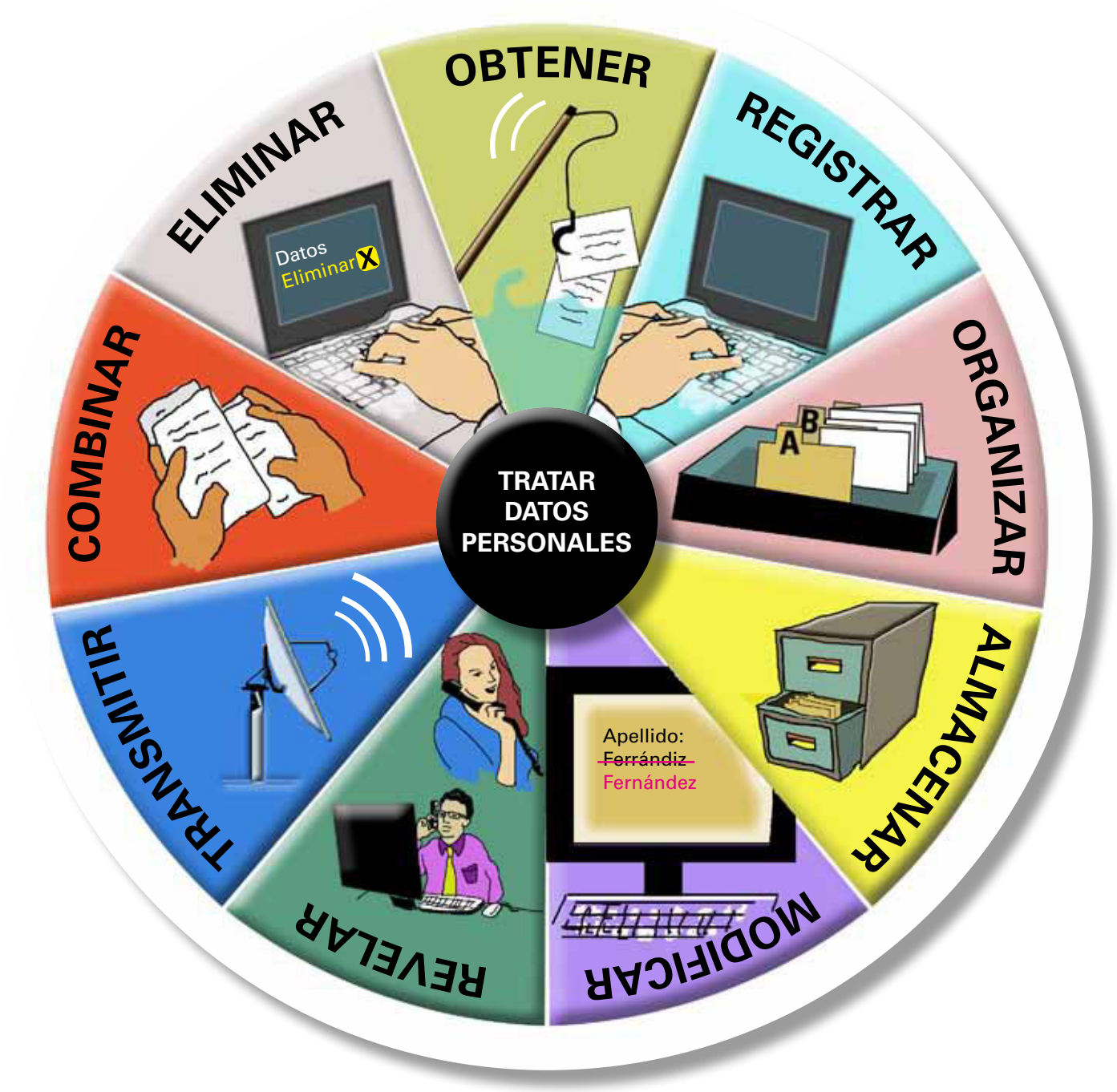
FOTOCOPIABLE

UNIDAD 3.1 . ALUMNADO

PROCESANDO DATOS PERSONALES

El diagrama circular de esta página nos ayudará a entender los diferentes métodos para tratar los datos personales

Tus datos personales deben ser tratados de acuerdo con la Ley de Protección de Datos.
El tratamiento de datos engloba una completa gama de actividades relacionadas con la información personal. La Ley de Protección de Datos afecta a todos los datos personales que se tratan manualmente en un sistema de clasificación o electrónicamente.



UNIDAD 3.1

PROFESORADO

PROCESANDO DATOS PERSONALES

Utilice el esquema de “Derechos y Responsabilidades” de la página siguiente. Coloque ese esquema en un lugar visible de la clase y lea en voz alta cada uno de los derechos y responsabilidades.

DERECHOS DE LAS PERSONAS A LAS QUE SE REFIEREN LOS DATOS

A menudo se solicita a las personas particulares (sujetos a los que se refieren los datos) que faciliten información personal sobre ellos mismos a diversas organizaciones y personas particulares (responsables de ficheros) para infinidad de finalidades.

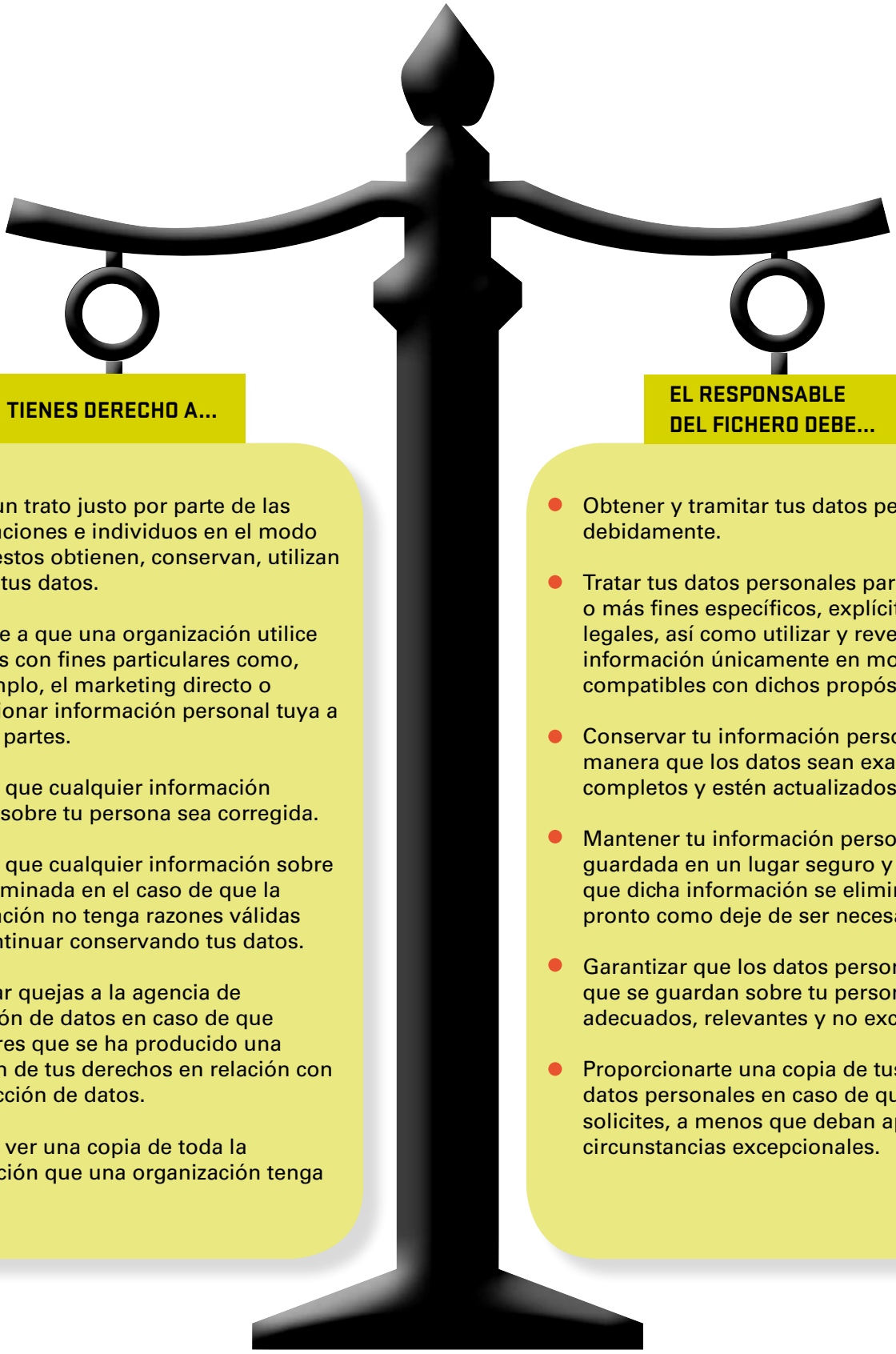
RESPONSABILIDAD DE LOS LLAMADOS RESPONSABLES DE FICHEROS

Los responsables de ficheros (organizaciones y particulares) recopilan datos personales que pertenecen a los individuos a los que se refieren.

UNIDAD 3.1

PROFESORADO

DERECHOS Y RESPONSABILIDADES



TIENES DERECHO A...

- Recibir un trato justo por parte de las organizaciones e individuos en el modo en que éstos obtienen, conservan, utilizan y ceden tus datos.
- Oponerte a que una organización utilice tus datos con fines particulares como, por ejemplo, el marketing directo o proporcionar información personal tuya a terceras partes.
- Solicitar que cualquier información errónea sobre tu persona sea corregida.
- Solicitar que cualquier información sobre ti sea eliminada en el caso de que la organización no tenga razones válidas para continuar conservando tus datos.
- Presentar quejas a la agencia de protección de datos en caso de que consideres que se ha producido una violación de tus derechos en relación con la protección de datos.
- Solicitar ver una copia de toda la información que una organización tenga sobre ti.

EL RESPONSABLE DEL FICHERO DEBE...

- Obtener y tramitar tus datos personales debidamente.
- Tratar tus datos personales para uno o más fines específicos, explícitos y legales, así como utilizar y revelar dicha información únicamente en modos compatibles con dichos propósitos.
- Conservar tu información personal de manera que los datos sean exactos, completos y estén actualizados.
- Mantener tu información personal bien guardada en un lugar seguro y garantizar que dicha información se eliminará tan pronto como deje de ser necesaria.
- Garantizar que los datos personales que se guardan sobre tu persona son adecuados, relevantes y no excesivos.
- Proporcionarte una copia de tus datos personales en caso de que lo solicites, a menos que deban aplicarse circunstancias excepcionales.

ACTIVIDAD 1 PROFESORADO

Fotocopie las dos páginas de la actividad "¿Necesitas tomar medidas?" de las páginas 58 y 59 y distribuya una copia de esas hojas de ejercicios a todas las personas de la clase. Deje a cada una unos 10 minutos para que analicen las primeras cuatro situaciones, y luego haga una pausa para revisar las respuestas. Utilice la información proporcionada a continuación para dirigir la conversación. Finalmente, vuelva a trabajar la actividad para que examinen las últimas cuatro situaciones.

VISIÓN GENERAL DE LAS SITUACIONES Respuestas que se sugieren

David/Artículos deportivos on-line: deben tomarse más medidas
David tendría que entrar de nuevo en el sitio web en el que ha comprado los artículos y localizar sus datos de contacto. Debería enviarles un e-mail o llamarles por teléfono para comunicarles que no quiere recibir e-mails con publicidad en el futuro. Como es posible que la lista se genere automáticamente desde una base de datos de clientes, David probablemente tendría que seguir las instrucciones para "borrarse" de la lista de e-mails. La empresa debería respetar los deseos de David de no ponerse en contacto con él; si siguiera enviando e-mails no solicitados a David, correspondería al país o a la jurisdicción legal en el que esté constituida la empresa perseguir o procesar a ésta. Si la empresa tiene su sede en la UE, debería haber incluido en cada mensaje detalles sobre cómo anular la suscripción.

La entrada de papá para un acto benéfico:deben tomarse más medidas
Es aconsejable que papá llame a la organización benéfica y se informe sobre sus comunicaciones. Papá puede decir que no recuerda que le comunicaran que continuarían contactando con él una vez que finalizara el evento. En primer lugar, es posible que la organización benéfica no le pidiera permiso. Por otra parte, podrían haberle informado que no marcó la casilla "borrarse", indicando que no quería que contactaran con él para informarle de futuros eventos/campañas. No obstante, incluso si sin darse cuenta no hubiera marcado esa casilla, papá tiene derecho a solicitar a la organización benéfica que eliminen sus datos de la base de datos de la organización y dejen de enviarle e-mails. La organización benéfica debe respetar esta solicitud.

Trabajo a tiempo parcial de Marta: no es preciso tomar más medidas
Uso legítimo. Las personas responsables de la empresa necesitan conocer los datos de afiliación a la Seguridad Social de los trabajadores para poder cumplir con sus obligaciones legales. Asimismo, también es posible que necesiten comprobar la edad de alguna persona pera verificar que supera la edad mínima legal para trabajar.

ACTIVIDAD 1 PROFESORADO

VISIÓN GENERAL DE LAS SITUACIONES Respuestas que se sugieren

La tarjeta de teléfono de David: deben tomarse más medidas

Esta práctica resulta difícil de verificar, puesto que existe un grupo selecto de empresas en el sector de las telecomunicaciones que se ganan la vida utilizando los datos personales de personas particulares para otros fines no especificados en el momento de la suscripción. A menudo, los clientes que se suscriben pueden haber aceptado inconscientemente recibir posteriores "ofertas". Las compañías están obligadas legalmente a ofrecer a sus clientes un modo de "borrarse" de este tipo de servicios. En cada comunicación debería indicarse el procedimiento para "darse de baja"; sin embargo, hay casos en los que se informa a los clientes que cancelar su suscripción les costará dinero. La Agencia Española de Protección de Datos ha combatido estas prácticas y sancionado a compañías de este ámbito y continuará haciéndolo, con el fin de garantizar que se respetan las leyes.

La experiencia de mamá en el supermercado: deben tomarse más medidas

Mamá debe contactar con las oficinas centrales del supermercado y volver a comprobar cuál es su política de marketing. Existe una tecnología emergente denominada RFID (identificación por radiofrecuencia) que implica colocar un dispositivo (o chip) a los productos para conocer el recorrido de los mismos, desde el almacén pasando por las estanterías del supermercado hasta que llegan a la caja. Algunos vendedores están analizando la posibilidad de colocar estos chips a las tarjetas de fidelidad del supermercado para saber cuándo un cliente se encuentra en la tienda y, en este sentido, poder dirigir la actividad del mismo. Las cuestiones de privacidad se concentran en que este tipo de tecnología se utilice de forma apropiada y en la necesidad de limitar claramente su alcance y el nivel de intrusión en los movimientos de las personas.

Carla y el videoclub: no es preciso tomar más medidas

Es muy probable que la tienda haya adoptado una política por la que se deban demostrar los datos de residencia presentando algún documento que acredite la información, por si se da el caso de que el cliente no devuelva los DVD o intente eludir el pago de la multa correspondiente al excederse en el plazo de devolución. Si algún cliente proporcionara una dirección falsa, tendría más oportunidades para hacer mal uso de su suscripción.

Prácticas de eliminación y retención de datos: deben tomarse más medidas

Marta debe informar inmediatamente a la dirección y sugerir que los documentos sean triturados y marcados para ser eliminados con total seguridad. Cuando las medidas de seguridad son inadecuadas o insuficientes se incrementa el riesgo de que los datos personales sean revelados a terceras partes, así como la posibilidad de fraude, abuso o robo de identidad.

Exactitud de los datos: deben tomarse más medidas

Papá debería contactar con la entidad de crédito para comprobar cuál es su historial de crédito y aclarar el malentendido. Muchas instituciones financieras investigan el historial de crédito de las personas. Si una persona no ha pagado un préstamo, este hecho queda registrado en las bases de datos. No obstante, pueden producirse errores a la hora de introducir los datos o introducirse nombres similares; por tanto, cualquier persona tiene derecho a solicitar una rectificación o corrección de sus datos personales cuando éstos sean erróneos o incorrectos.

FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Lee las siguientes situaciones y marca la casilla adecuada.

¿NECESITAS TOMAR MEDIDAS?

- ¿Consideras aceptable el tipo de datos solicitados?
- ¿Tendrías algún tipo de preocupación por el modo en el que se obtienen o utilizan los datos?
- ¿Crees que las personas de las que se han obtenido los datos (David, Marta, Carla, mamá y papá) deberían tomar medidas y plantear algunas preguntas o presentar objeciones?

No hay respuestas únicas para ninguna de estas situaciones, puesto que no se conocen todos los hechos, sin embargo, tu profesor o profesora os explicará las respuestas proporcionadas y observará si la mayoría de los miembros de la clase está de acuerdo en qué se considera como práctica aceptable.

Situación	Es preciso tomar más medidas	No hace falta tomar más medidas
David compró algunos artículos deportivos por Internet y ahora recibe todo tipo de e-mails sobre estos productos, equipo de fitness y vitaminas en pastillas. Sabe que no es spam o correo basura porque los mensajes proceden del proveedor al que compró los artículos deportivos. Además, su nombre aparece en el texto del mensaje y el contenido, relacionado con lo que compró por Internet, está directamente dirigido a él.		
Hace algunos meses, **papá** compró una entrada para un acto benéfico al que asistió dos semanas después. En el momento en que compró la entrada, papá facilitó sus datos de contacto para que pudieran confirmarle más adelante la hora y detalles sobre el recinto en el que se celebraba el evento. Desde entonces, ha estado recibiendo mensajes para animarle a contribuir en varias campañas.		
Marta tiene un nuevo empleo a tiempo parcial, y el empleador le pide que el primer día de trabajo presente su documento de afiliación a la Seguridad Social y su Documento Nacional de Identidad. El empleador introduce su número de afiliación en el sistema y, una vez comprobado el certificado de nacimiento, se lo devuelve a Marta inmediatamente sin hacer una copia del mismo.		
David acude a un concierto al aire libre y aprovecha la oferta de una tarjeta de teléfono gratis con un saldo de 15 € para realizar llamadas a móviles. Rellena algunos datos personales en la tarjeta para poder disponer del crédito gratuito ofertado. Ahora recibe mensajes sobre todo tipo de ofertas y oportunidades para vacaciones.		

FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Lee las siguientes situaciones y marca la casilla adecuada.

¿NECESITAS TOMAR MEDIDAS?

• ¿Consideras aceptable el tipo de datos solicitados?
• ¿Tendrías algún tipo de preocupación por el modo en el que se obtienen o utilizan los datos?
• ¿Crees que las personas de las que se han obtenido los datos (David, Marta, Carla, mamá y papá) deberían tomar medidas y plantear algunas preguntas o presentar objeciones?

No hay respuestas únicas para ninguna de estas situaciones, puesto que no se conocen todos los hechos, sin embargo, tu profesor o profesora os explicará las respuestas proporcionadas y observará si la mayoría de los miembros de la clase está de acuerdo en qué se considera como práctica aceptable.

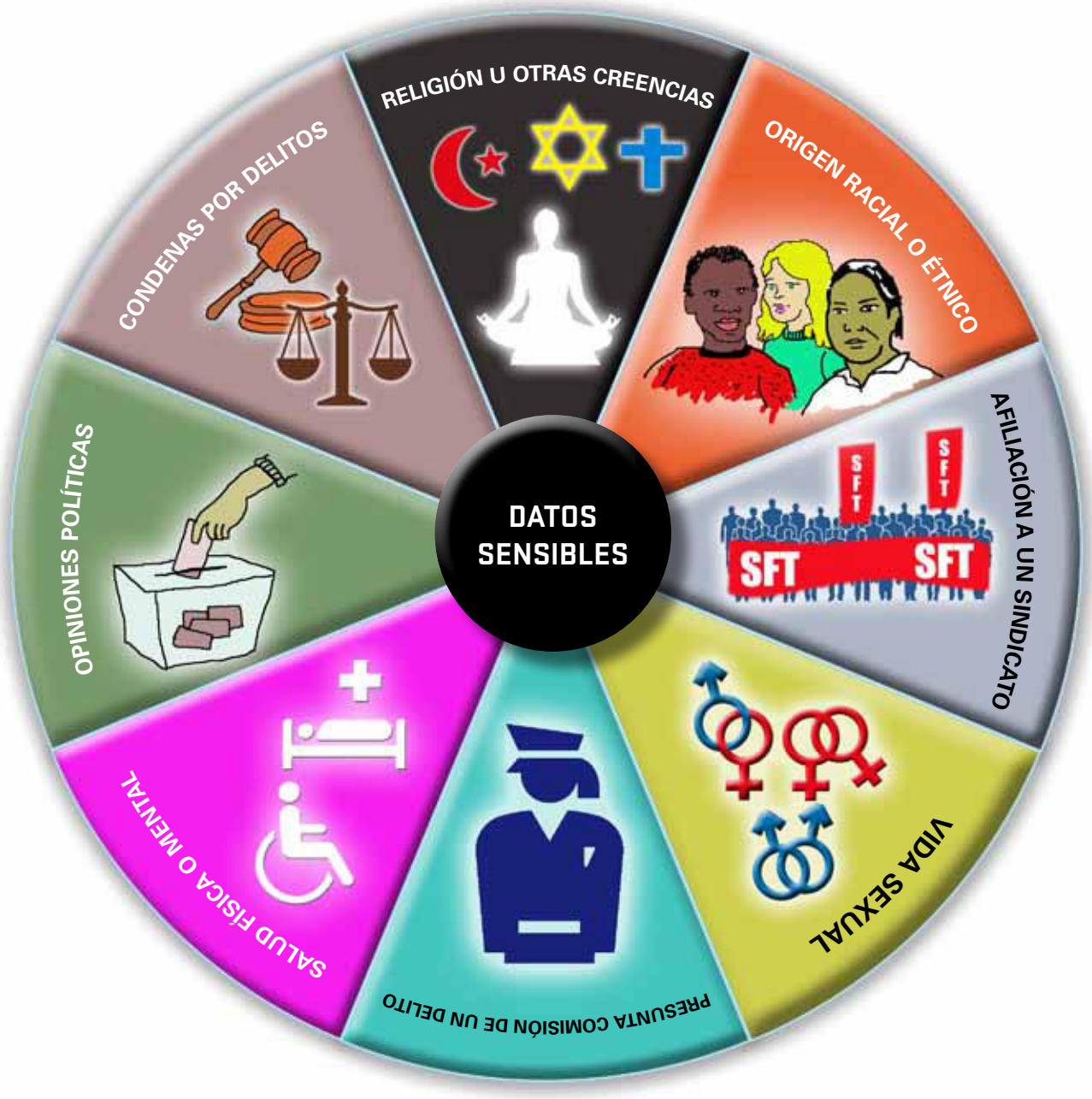
Situación	Es preciso tomar más medidas	No hace falta tomar más medidas
Mamá recibe un mensaje cuando está en el supermercado para informarle de una oferta especial de detergentes en el tercer pasillo. Mamá tiene una tarjeta de fidelidad, por lo que sabe que en su momento facilitó al supermercado su número de teléfono móvil, pero se siente confusa, ya que se pregunta cómo saben cuándo se encuentra en el supermercado o si simplemente ha sido una coincidencia.		
Carla se acerca al videoclub para hacerse la tarjeta de socia, pero rechazan su primera solicitud porque le exigen dos cartas que demuestren la dirección de su domicilio. Cuando Carla presenta las dos cartas, las examinan en el videoclub y se las devuelven.		
Un día, al fichar a la salida de su trabajo a tiempo parcial, **Marta** ve una pila enorme de archivos de clientes que se han desechado recientemente y que se han depositado en los contenedores de basura situados a un lado de las instalaciones, al alcance de cualquiera. Marta sabe que los archivos contienen detalles de tarjetas de crédito de los clientes.		
Papá solicita un préstamo a un banco para hacer una ampliación a la casa y se horroriza cuando el banco le informa de que su historial de crédito es negativo y de que tiene varias deudas pendientes. El banco rechaza la solicitud de préstamo de papá, pero éste sabe que no tiene deudas pendientes y nunca ha tenido problemas en el pasado a la hora de devolver los préstamos concedidos.		

FOTOCOPIABLE

UNIDAD 3.2 . ALUMNADO

DATOS ESPECIALMENTE SENSIBLES

La Ley de Protección de Datos ofrece mayor protección a las categorías de datos representadas en el diagrama circular. Los responsables de ficheros deben justificar la razón por la cual requieren este tipo de datos y, además, deben prestar atención especial a la hora de tratarlos.



FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Los siguientes titulares de prensa pueden ser ejemplos de violación de las leyes de protección de datos. Rodea con un círculo los titulares que creas que también pueden incluirse dentro de la categoría "datos sensibles".

EL DÍA A DÍA

El Ayuntamiento justifica la publicación de nombres y direcciones de los solicitantes de permisos de edificación en la web.

NOTICIAS

Una asociación médica reconoce que la publicación de datos sobre la raza y las creencias religiosas de médicos en prácticas en el sitio web de la asociación fue un error técnico garrafal.

LA HOJA DE LA SEMANA

Juicio suspendido después de que la acusación admitiera haber revelado al jurado una serie de imputaciones contra el acusado.

ECOS

Una cadena de tiendas reconoce que los hackers han conseguido acceder a los detalles de tarjetas de crédito de sus clientes.

TIEMPO

El personal universitario publica los nombres de los estudiantes junto con los resultados de los exámenes en el tablón de anuncios de la facultad.

GACETA DIARIA

Una compañía ferroviaria deduce del sueldo de sus empleados afiliados a sindicatos la parte correspondiente a los paros efectuados durante una huelga.

PERIÓDICO DE HOY

Un centro escolar publica en el tablón de anuncios la lista de alumnos y alumnas admitidos y no admitidos e incluye detalles como la discapacidad de una menor y la renta de su familia, junto con la puntuación de estos apartados para los efectos de la admisión.

AVANCE

Imágenes de una fiesta privada en casa de una estrella obtenidas con zoom.

ACTIVIDAD 1

PROFESORADO

Respuestas orientativas de la actividad sobre los titulares de prensa de la página 61.

El Ayuntamiento justifica la publicación de nombres y direcciones de los solicitantes de permisos de edificación en la web.

Según la Ley de Protección de Datos, estos datos no se consideran sensibles. Las autoridades locales podrían disponer de una legislación en materia urbanística que les permitiera exponer esa información al público, bien electrónicamente o de otro modo.

Una asociación médica reconoce que la publicación de datos sobre la raza y las creencias religiosas de médicos en prácticas en el sitio web de la asociación fue un error técnico garrafal.

La información sobre la raza o las creencias religiosas son datos sensibles, y así se indica en las leyes. El caso expuesto anteriormente es un ejemplo de revelación no intencionada de datos confidenciales. Se podrían plantear a la Agencia de Protección de Datos preguntas relacionadas con las prácticas de seguridad. También, en primer lugar, se podrían plantear preguntas acerca de la finalidad de solicitar este tipo de información.

Juicio suspendido después de que la acusación admitiera haber revelado al jurado una serie de imputaciones contra el acusado.

De acuerdo con la Ley de Protección de Datos, las acusaciones son datos sensibles. Si no se tratan adecuadamente, se infringen muchas leyes en materia de procedimiento judicial, confidencialidad y protección de datos.

Una cadena de tiendas reconoce que los hackers han conseguido acceder a los detalles de tarjetas de crédito de sus clientes.

Los detalles de las tarjetas de crédito no se consideran datos sensibles según las leyes. Los clientes afectados podrían presentar una queja ante la Agencia Española de Protección de Datos, sin embargo, lo ideal sería que la empresa en cuestión notificara la violación de la seguridad a la Agencia, quien procedería a examinar las prácticas de seguridad.

El personal universitario publica los nombres de los estudiantes junto con los resultados de los exámenes en el tablón de anuncios de la facultad.

Según la legislación, este tipo de información no entra en la categoría de datos sensibles. En nuestro ámbito, y específicamente desde 2007 , no es preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias (...).

ACTIVIDAD 1

PROFESORADO

Respuestas orientativas de la actividad sobre los titulares de prensa de la página 61.

Una compañía de transporte ferroviario deduce del sueldo de sus empleados afiliados a sindicatos la parte correspondiente a los paros efectuados durante una huelga.

La empresa conocía a qué organizaciones sindicales estaban afiliados sus trabajadores, ya que éstos facilitaban ese dato para que se descontara de su retribución la cuota sindical y se transfiriera a los sindicatos. En esta ocasión, la empresa utilizó esos datos de afiliación sindical para descontar la parte del sueldo correspondiente al día no trabajado. Los datos se utilizaron para una finalidad diferente de aquella para la que fueron recogidos y, en consecuencia, los datos fueron tratados de manera indebida. Además, los datos de afiliación sindical están especialmente protegidos por la legislación, que exige, para poder tratarlos, el consentimiento expreso y por escrito de la persona afectada (titular de los datos).

Un centro escolar publica en el tablón de anuncios la lista de admitidos y no admitidos e incluye datos como la discapacidad de una menor y la renta familiar, junto con la puntuación recibida para los efectos de la admisión.

Para garantizar el derecho a la igualdad de oportunidades en procesos de concurrencia competitiva, la AEPD considera más adecuada la publicación sólo del resultado global de la valoración, y que los datos de salud, renta, etc., se faciliten solamente a las personas interesadas, que compiten por una plaza, cuando lo soliciten ante posibles desacuerdos y comprobaciones. Así, se evita que estos datos sean conocidos por terceras personas no afectadas por el proceso.

Imágenes de una fiesta privada en casa de una estrella obtenidas con zoom.

Es poco probable que, según las leyes, se consideren datos sensibles; sin embargo, las imágenes son datos personales. Por tanto, la estrella podría presentar una queja indicando que se han obtenido datos personales de ella de forma ilegal.

UNIDAD 3.3

PROFESORADO

EDAD PARA EL CONSENTIMIENTO

Debata con la clase la información expuesta a continuación

Según la normativa de protección de datos las personas mayores de 14 años pueden consentir por si mismas el tratamiento de sus datos personales, salvo en aquellos casos en que la Ley exija la asistencia del padre, madre o tutor.

Por el contrario, si se quieren tratar datos de menores de 14 años, se necesita contar con el consentimiento del padre, madre o tutor. No está permitido solicitarles información sobre la profesión, la economía, los datos sociológicos o de cualquier otro tipo relativa a sus familiares si éstos no han dado su consentimiento. Únicamente se les puede pedir la identidad y la dirección del padre, madre o tutor para solicitarles el consentimiento. La normativa también determina que la información dirigida a ellos debe ser comprensible y obliga al responsable del fichero a establecer procedimientos que garanticen que se ha comprobado la edad del menor y la autenticidad de su consentimiento o del de su padre, madre o tutor.

Para instalar un sistema de vigilancia por circuito cerrado de televisión en el pasillo de la escuela, junto a las taquillas, **no se requiere el consentimiento de estudiantes y progenitores. Es necesario que se justifiquen problemas previos de seguridad que no puedan ser resueltos por medios menos invasivos.**

Se podría negar el acceso al padre o a la madre para examinar el historial médico de su hijo o hija **menor de edad, si por sentencia judicial firme se les ha privado de la patria potestad.**

UNIDAD 3.3

PROFESORADO

EDAD PARA EL CONSENTIMIENTO

Debata con la clase la información expuesta a continuación

En un centro de educación secundaria, la legislación sobre protección de datos permite que tanto las alumnas y alumnos como sus respectivos padres, madres o tutores jueguen su papel en lo relativo al consentimiento para el tratamiento de los datos personales de los estudiantes. Los profesores y profesoras también tienen derecho a solicitar examinar cualquier información personal que el centro educativo conserve sobre ellos.

14 AÑOS

Un alumno o alumna de 14 años podría firmar un documento en el que consienta la publicación de su fotografía en el anuario escolar.

Una escuela debería solicitar el consentimiento de los alumnos y de sus respectivos progenitores o tutores para utilizar un sistema diseñado para controlar la asistencia del alumnado, basado en la identificación de huellas dactilares. Cualquier alumno o alumna debería tener derecho a negarse a utilizarlo, así como sus respectivos padres, madres o tutores.

El consentimiento firmado de un alumno o alumna de 14 años de una escuela de educación secundaria debería ser suficiente para hacerse socio o socia de la biblioteca escolar o de un banco estudiantil.

15 AÑOS

Un estudiante de 15 años podría ser considerado suficientemente maduro para solicitar el acceso a los datos personales que conserva el médico sobre él.

16 AÑOS

Un alumno o alumna de 16 años podría presentar una queja ante la Agencia de Protección de Datos si considera que la escuela ha utilizado o revelado de manera inapropiada sus datos personales. Como alternativa, el padre o la madre de este estudiante de 16 años podrían presentar la queja en nombre de su hijo o hija.

FOTOCOPIABLE

ACTIVIDAD 3. ALUMNADO

Observa esta imagen y, después, responde a las preguntas de abajo.

CUESTIONARIO

1. Nombra algunos de los derechos principales que posees en relación con tus datos.
Mira el esquema de "Derechos y Responsabilidades" para responder esta pregunta (Unidad 3, página 55).

2. ¿Qué medidas podrías tomar para tener mayor control de tus datos?

3. ¿Has tenido alguna vez que reivindicar tus derechos por el modo en el que estaban siendo tratados tus datos?

FOTOCOPIABLE

UNIDAD 3.4 ALUMNADO

SOLICITUDES DE ACCESO

Una solicitud de acceso consiste en un impreso en el que tú (la persona de la que se obtiene información personal) realizas una solicitud formal, acreditando tu identidad, y la presentas a la persona responsable del fichero, al amparo de la Ley de Protección de Datos, solicitando que te faciliten información sobre si tratan datos personales tuyos, con qué finalidad los tratan, de dónde los han obtenido, y si los han comunicado y a quién o si tienen intención de comunicarlos.

La normativa prevé que en los casos de incapacidad o minoría de edad este derecho de acceso a los datos personales se pueda ejercer a través de un representante.

ASPECTOS QUE DEBERÍAS CONOCER SOBRE LAS SOLICITUDES DE ACCESO

- Sólo tú puedes solicitar el acceso a tus datos personales, por lo que debes acreditar tu identidad adjuntando una fotocopia del DNI. También lo puedes hacer a través de medios electrónicos, siempre que puedas acreditar tu identidad.
- El acceso a tus datos debe ser gratuito. No te pueden obligar a enviar cartas certificadas, a llamar a teléfonos con tarificación adicional o a utilizar medios que te supongan un coste excesivo.
- El responsable del fichero debe responder a tu petición en el plazo de 1 mes y te debe contestar aunque no tenga datos tuyos.
- En caso de que tu solicitud de acceso sea rechazada o no te respondan, puedes presentar una reclamación ante la Agencia o Autoridad de Protección de Datos.

FOTOCOPIABLE

UNIDAD 3.4 . ALUMNADO

SOLICITUDES DE ACCESO

A continuación se incluye una hoja informativa sobre el modo de acceder a la información personal que conservan sobre nosotros.

Cómo realizar una solicitud de acceso:

MODELO DE EJERCICIO DEL DERECHO DE ACCESO

Datos de la persona solicitante

Nombre y apellidos:

DNI (Hay que adjuntar una fotocopia):

Dirección:

Datos de la persona o entidad responsable del fichero o tratamiento

Nombre y apellidos o cargo u órgano administrativo:

Dirección:

Localidad:

(Si se desconoce la dirección, se puede solicitar al Registro de Protección de Datos.)

Asunto:

Solicitud de información sobre los datos personales incluidos en un fichero o tratamiento

De acuerdo con lo establecido en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, solicito que me indiquen si disponen de información sobre mis datos personales incluidos en sus ficheros.

En caso afirmativo, pido que me envíen esta información de forma clara e inteligible, así como los datos resultantes de cualquier elaboración, proceso o tratamiento, el origen de los datos, los cesionarios y los usos y finalidades para los que se almacenaron. Si no disponen de información sobre mis datos personales, solicito igualmente que me lo comuniquen.

En el plazo de un mes desde la recepción de la presente solicitud, debe contestarse a la misma, por lo que pido que se me comunique la información solicitada o bien el motivo por el que la persona o entidad responsable del fichero considera que el acceso no es procedente.

En caso de no atender esta solicitud de acceso en el plazo mencionado, se entenderá que es desestimada, por lo que podrá interponerse la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de los derechos.

(Localidad, fecha)

(Firma de la persona solicitante)

ACTIVIDAD 3

PROFESORADO

CASOS DE ESTUDIO

Fotocopie los siguientes casos de estudio descritos en las páginas siguientes.

En esta unidad el alumnado ya se ha familiarizado con la Ley de Protección de Datos. La competencia para vigilar el cumplimiento de esta normativa está atribuida a las Agencias de Protección de Datos, que actúan con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones y tienen una amplia gama de potestades legales, entre las que se incluyen las siguientes:

- Obligar a los responsables de ficheros mediante notificaciones legales a facilitar cualquier información necesaria para tramitar las solicitudes.
- Obligar a los responsables de ficheros a poner en práctica lo estipulado en las leyes.
- Examinar las quejas presentadas por el público general.
- Autorizar a sus funcionarios para que entren en las instalaciones e inspeccionen el tipo de información personal que se registra, el procedimiento para su tratamiento y las medidas de seguridad aplicadas.

Un responsable de fichero considerado culpable de una infracción tipificada en la Ley puede ser castigado con multas de hasta 600.000 € y/o se le puede ordenar que elimine toda o parte de la información contenida en la base de datos.

• Divida la clase en grupos de cuatro personas. Asigne un caso de estudio a cada grupo y pida que lean el caso de estudio correspondiente y nombren los aspectos relacionados con la protección de datos que crean que podrían ser cuestionados. Pueden volver a consultar el esquema de "Derechos y Responsabilidades" (Unidad 3, página 55).

• Cada grupo designará a una persona como portavoz. Deje unos 10 minutos para leer el caso y discutir sobre ello en el grupo.

• Una vez hayan terminado, pida al portavoz que se levante y describa brevemente la queja y el tema en cuestión, que se podrían anotar en la pizarra.

ACTIVIDAD DE SEGUIMIENTO

- Pida a los estudiantes que respondan a la siguiente pregunta: ¿qué haríais para concienciar a los jóvenes sobre la protección de datos?
- Que diseñen un cartel informativo para las Agencias de Protección de Datos para ser distribuido en centros de enseñanza secundaria.

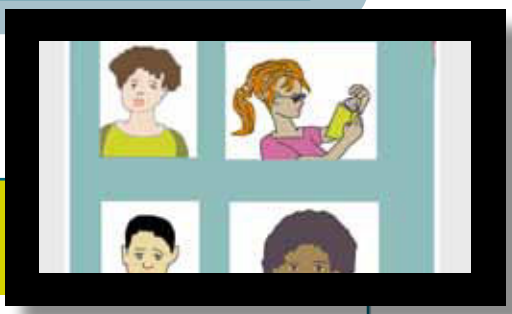
FOTOCOPIABLE

ACTIVIDAD 3. ALUMNADO

CASOS DE ESTUDIO

CASO DE ESTUDIO 1

Un hombre presentó una queja a **la Agencia de Protección de Datos** porque su hija de diez años había recibido una carta de un banco preguntándole si quería una tarjeta de crédito. El hombre también se puso en contacto con el banco y le contestaron que la lista de direcciones que utilizaron se la compraron a una empresa de marketing. La empresa de marketing le informó de que habían adquirido los datos a otra empresa. Esta otra empresa, a su vez, dijo que obtuvieron sus datos personales de una encuesta que él y su hija rellenaron tras unas vacaciones. En el impreso de la encuesta se indicaba claramente que la niña sólo tenía diez años. Esta empresa respondió que normalmente no utilizaban los datos de personas menores de 18 años, por lo que en este caso los datos personales de la niña se habían transmitido por error. La empresa corrigió su error y tomaron las medidas oportunas para que errores de este tipo no vuelvan a suceder.



CASO DE ESTUDIO 2

Una madre contactó con la Agencia de Protección de Datos para quejarse de que el centro de educación primaria había estado publicando datos sobre el alumnado en el sitio web de la escuela, sin pedir previamente permiso a los padres y a las madres. En las páginas de este sitio de Internet aparecieron fotografías y el nombre de los alumnos y alumnas, además de otro tipo de información relacionada con sus hobbies, qué les gustaba y qué no... La madre ya había planteado el asunto a la escuela pero no se quedó conforme con la respuesta que recibió.

La Agencia de Protección de Datos exigió a la escuela que eliminara todos los datos personales del sitio web. Luego, el director de la Agencia se reunió con la directora de la escuela, quien le explicó que todos los alumnos y alumnas estaban muy contentos con el nuevo sitio web, que incluso había ganado algunos premios. En cuanto a pedir permiso a los padres y madres, la directora señaló que se mencionó la iniciativa de crear un sitio web en una notificación escolar enviada a las familias recientemente y, además, se les invitó a que vinieran a la escuela y lo comprobaran por ellas mismas. A pesar de todo esto, la Agencia de Protección de Datos decidió que se debía obtener el consentimiento expreso de los padres, madres o tutores antes de utilizar de esta manera datos personales de menores de 12 años. La directora aceptó esta resolución y se comprometió a no colocar información personal en el sitio web sin el consentimiento de los padres, madres o tutores.

FOTOCOPIABLE

ACTIVIDAD 3. ALUMNADO

CASOS DE ESTUDIO

CASO DE ESTUDIO 3

Una empresa de investigación envió una encuesta por correo junto con sobres franqueados para devolverla, y pidió a las personas destinatarias que contestaran a las preguntas del impreso y lo enviaran de vuelta sin firmar, esto es, de manera anónima. Sin embargo, los sobres franqueados estaban identificados con un número de cuatro dígitos, lo cual sugería que la encuesta no era realmente anónima y que las respuestas enviadas se podían rastrear hasta conocer a las personas particulares que completaron la encuesta.

La Agencia de Protección de Datos organizó una reunión con la empresa. La empresa explicó que los números de los sobres se utilizaron para comprobar quién había respondido a la encuesta y para que la empresa pudiera enviar notas recordatorias a aquellas personas que todavía no habían devuelto la encuesta. Una vez que se sacaban las respuestas de los sobres, no había posibilidad de relacionarlas con las personas que las habían enviado. La Agencia de Protección de Datos se mostró satisfecha cuando supo que las respuestas de la encuesta no se podían rastrear para localizar a las personas remitentes.

CASO DE ESTUDIO 4

Una mujer quería comprar un frigorífico en una tienda y preguntó al dependiente si podría pagar el frigorífico a plazos. Entonces, el dependiente comprobó los datos de la mujer en el ordenador. Había otros clientes en el mostrador que pudieron ver perfectamente datos personales e información sobre la mujer, como por ejemplo, su fecha de nacimiento. La mujer presentó una queja a **la Agencia de Protección de Datos.** Cuando comenzó la investigación de este caso, se comprobó que la pantalla del ordenador estaba mal situada y que era posible que otros clientes pudieran ver los datos en la pantalla aunque el personal de la tienda intentara ser discreto.

Los propietarios remodelaron la tienda y colocaron la pantalla del ordenador en una posición mucho menos expuesta.

FOTOCOPIABLE

ACTIVIDAD 3. ALUMNADO

CASOS DE ESTUDIO

CASO DE ESTUDIO 5

Hace algunos años un hombre joven fue condenado en primera instancia por un delito menor. Apeló la sentencia y resultó absuelto. Al cabo de un tiempo, el hombre decidió emigrar a un país que le exigía no disponer de antecedentes policiales, para lo que necesitaba una certificación por parte de la policía. Presentó una solicitud de acceso a la policía acogiéndose a la Ley de Protección de Datos de carácter personal. Cuando la policía le respondió, el ciudadano se inquietó al comprobar que las diligencias policiales seguían constando en la base de datos. Entonces, el hombre contactó con **la Agencia de Protección de Datos** porque estaba preocupado por el hecho de que la acusación original siguiera figurando en las bases de datos policiales. Finalmente, la policía entregó al hombre una certificación acreditando la cancelación de sus antecedentes.

CASO DE ESTUDIO 6

Una mujer acudió al servicio de urgencias de un hospital público. Unos meses más tarde, una empresa que estaba realizando una investigación contactó con ella. Los investigadores sabían cuándo estuvo en el hospital y por qué, y le pidieron que respondiera a algunas preguntas. La mujer se molestó por el hecho de que el hospital hubiera informado a los investigadores sobre su estancia, por lo que acudió al hospital para aclarar este asunto. Sin embargo, no se quedó conforme con la respuesta del hospital y presentó una queja a la Agencia de Protección de Datos. El hospital dijo que habían colocado un aviso en la sala de espera de urgencias en el que se informaba a los pacientes que el hospital iba a proporcionar información sobre ellos a los investigadores, invitando a los pacientes que se opusieran a ello a comunicarlo en la recepción. **La Agencia de Protección de Datos** resolvió que el hospital debía haber preguntado a cada persona individualmente si querían o no participar en la investigación.

FOTOCOPIABLE

ACTIVIDAD 3. ALUMNADO

CASOS DE ESTUDIO

CASO DE ESTUDIO 7

La Agencia de Protección de Datos recibió una queja de una mujer que había cambiado los datos de su cuenta de teléfono, poniéndolos a su nombre tras separarse de su marido. El marido contactó con la compañía de teléfono y se las arregló para conseguir los códigos de acceso al buzón de voz. La mujer descubrió que su marido podía escuchar sus mensajes.

La compañía telefónica estudió minuciosamente esta queja y no consiguieron averiguar cómo se había producido exactamente esta situación; sin embargo, reconocieron que si el marido se inventó una historia para conseguir la información, en este caso, los procedimientos de la compañía para proteger los datos de los clientes no eran lo suficientemente eficaces. La compañía inició una revisión de los procedimientos de seguridad de sus centros de llamadas. Ahora, la compañía telefónica actúa de acuerdo con una serie de normas estrictas para gestionar la transferencia de los servicios telefónicos, sobre todo en situaciones de parejas que se han separado.

CASO DE ESTUDIO 8

Un grupo de trabajadores de cierta empresa se quejó a la **Agencia de Protección de Datos** porque se habían puesto sus evaluaciones particulares de "rendimiento laboral" a disposición de un gran número de directivos. Los trabajadores consideraban que sus datos confidenciales no debían ser facilitados a personas que no se encargaban de dirigirles.

Cuando el asunto se planteó con la empresa, ésta explicó que la directora de un departamento en particular había creado un archivo en el ordenador con los índices de rendimiento laboral de la plantilla que tenía a su cargo. No obstante, accidentalmente, los "permisos de acceso" a este archivo se configuraron de modo que otras personas ajenas a su equipo directivo pudieran verlo. Un miembro de la plantilla dio parte del problema a la dirección y el archivo en cuestión fue destruido. La empresa solicitó una investigación formal para analizar el asunto y adoptó medidas inmediatas para resolver los aspectos afectados en este caso, concretamente se aseguró de que las medidas de seguridad fueran adecuadas en lo sucesivo.

ACTIVIDAD DE SEGUIMENTO / DEBERES

PROFESORADO

- Fotocopie la hoja de reclamaciones de la página siguiente para repartirla en clase.
- Haga varias copias de cada uno de los casos de estudio y pida a los alumnos que elijan un estudio de caso que no hayan debatido en su grupo. Pida que lean de forma individual el nuevo caso de estudio que han seleccionado y rellenen la hoja de reclamaciones después de haber analizado la situación. Pueden elaborar o inventar detalles que no figuren en su caso de estudio.
- Consulte los informes anuales en los sitios web de las Agencias de Protección de Datos (www.agpd.es; www.madrid.org; www.apd.cat; www.avpd.euskadi.net) para conocer el desglose del tipo de consultas y reclamaciones que se reciben cada año.

Nota informativa:

De acuerdo con el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que la presentación de la denuncia da lugar a la inclusión de los datos de carácter personal en el fichero de registro de entrada y salida de documentos y en el fichero de expedientes de ejercicio de derechos, de inspección y sancionadores, cuya entidad responsable es la Autoridad de Protección de Datos.

Puede ejercer los derechos de acceso, rectificación, cancelación y oposición ante esta institución, calle ....

Le informamos de que sus datos pueden ser cedidos a otras autoridades que tienen competencias en procedimientos de garantía del derecho a la protección de datos, así como a otras instancias competentes en la garantía de los derechos de los particulares, para la resolución de su denuncia.

FOTOCOPIABLE

ACTIVIDAD DE SEGUIMIENTO / DEBERES

ALUMNADO

MODELO DE DENUNCIA ANTE LA AGENCIA DE PROTECCIÓN DE DATOS

Datos de la persona denunciante

Nombre y apellidos

DNI

Dirección

Datos de la persona o entidad denunciada

Nombre

Dirección

Localidad

Denuncio, por haberse vulnerado lo que dispone la normativa vigente en materia de protección de datos, los hechos siguientes:

(Hay que enumerar los hechos que se denuncian.)

1.

2.

3.

[...]

A fin de justificar los hechos denunciados, aporto la documentación siguiente:

(Hay que indicar la documentación que corresponda.)

1.

2.

3.

[...]

(Localidad, fecha)

(Firma de la persona denunciante)


12/10/1995
04/05/2001
12/01/2010

UNIDAD 4

ADOLESCENTES QUE FACILITAN SUS DATOS

UN DÍA EN LA VIDA DE HELENA

VIGILANCIA

TV DIGITAL INTERACTIVA

COMPRAS: CIELO O INFIERNO

SITIOS WEB DE REDES SOCIALES

RFID: GENERANDO ONDAS

BIOMETRÍA

OBJETIVOS

- Subrayar el papel que juega actualmente la tecnología en nuestras vidas y sus consecuencias en nuestra privacidad.

CONOCIMIENTOS

- Perfiles.
- Innovación tecnológica.
- Técnicas de vigilancia.

CONCEPTOS

- Democracia.
- Desarrollo.
- Privacidad en las redes sociales.

HABILIDADES

- Análisis crítico.
- Comunicaciones: discusión, role play, audición, representación, empatía.

ACTITUDES Y VALORES

- Concienciar al alumnado de las ventajas y los posibles riesgos de la tecnología.
- Aprendizaje de actitudes sobre el control de la información en el uso de las tecnologías de la información.

FOTOCOPIABLE

UNIDAD 4.1
ACTIVIDAD 1

ALUMNADO

ADOLESCENTES QUE FACILITAN SUS DATOS

A continuación se muestra el perfil de un adolescente. Realiza una tabla similar con los datos de tu perfil.

Nombre:	J. P. (Adolescente que facilita sus datos)
Edad:	16 años
Dirección:	Calle Mayor, 3, Villanueva
Hermanos:	2 hermanos, uno mayor y otra menor que él.
Resultados en las calificaciones globales de 3º de la ESO:	1 sobresaliente; 4 notables; 3 aprobados; 1 insuficiente; 1 muy deficiente.
Desayuno favorito:	Zumo de naranja y cereales.
Expediente disciplinario de la escuela:	Dos castigos en la escuela –uno por llegar tarde con frecuencia y otro por hacer trampas en un examen–. Fue suspendido durante dos días en 1º por comportarse maleducadamente con los profesores.
Grupo sanguíneo:	B +
Historial médico:	Apendicitis, sarampión, fractura de muñeca a los 5 años.
Antecedentes:	Fue sorprendido hurtando en una tienda con 14 años y posteriormente, una noche de julio el año pasado, tuvo que ser acompañado a casa por agentes de la Policía Local, porque se encontraba en estado de embriaguez.
Alergias / enfermedades:	Es asmático y lleva consigo un inhalador.
Ahorros:	Tiene 90 € en una cuenta de ahorro en el banco.
Correo electrónico:	JP@hotmail.com
Hobbies:	Lectura de novela fantástica medieval (necesita gafas para leer), ir al cine y los videojuegos.
DNI:	11111111z
Nº de teléfono móvil:	666 666 666
Mejor amigo/a:	Ruth
Deportes:	Juega al fútbol y al baloncesto.
Vacaciones:	Realiza un campamento todos los años en julio, pasa el resto del verano con sus abuelos en el pueblo de sus padres.

ACTIVIDAD 1

PROFESORADO

Debata en clase con los alumnos y alumnas los puntos descritos a continuación.

- ¿Qué tipo de información sobre J. P. consideran datos sensibles?
- Reflexionen sobre las consecuencias que pudieran producirse si todos los datos de J. P. se introdujeran en un ordenador y se creara un perfil.

Imagina que los siguientes tres datos sobre J. P. aparecieran en la pantalla de un ordenador:

Nombre: J. P.

Expediente disciplinario de la escuela: dos castigos en la escuela –uno por llegar tarde con frecuencia y otro por hacer trampas en un examen–. Fue suspendido durante dos días en 1º por comportarse agresiva y maleducadamente con los profesores.

Antecedentes: fue sorprendido robando en una tienda con 14 años y posteriormente, una noche de julio el año pasado, tuvo que ser acompañado a casa por agentes de la Policía Local, porque se encontraba en estado de embriaguez.

REFLEXIÓN

¿Creen los alumnos y alumnas que este perfil es injusto, puesto que se han omitido todos los logros y cualidades positivas de J. P.? ¿Sería adecuado que su escuela tuviera un enlace para acceder al sistema informático de la Policía Local con el fin de que los expedientes escolares pudieran actualizarse para reflejar cualquier altercado que el alumnado tuviera con la ley (ya sean inocentes o no)?

Imagina que los siguientes datos aparecieran en la pantalla de un ordenador:

DNI: 11111111z

Nº de teléfono móvil: 666 666 666

Ahorros: 90 € en una cuenta de ahorro en el banco.

E-mail: dteen@hotmail.com

REFLEXIÓN

¿Podría ser perjudicial para J. P. el hecho de que se revelen sus datos o que alguien acceda a ellos sin justificación alguna? ¿Podría alguien conseguir suplantar a J. P. gracias a esta información? ¿Creen los alumnos y alumnas que estos datos se podrían utilizar para hacer compras o gestiones bancarias por Internet?

Se puede diseñar el perfil de los intereses, movimientos, relaciones, logros, liquidez económica y salud de una persona recabando información personal de una gran variedad de fuentes como, por ejemplo, el bono-bus, la escuela, el médico y diversas instituciones financieras. El conjunto de datos resultante sería un perfil completo de detalles correspondientes a la persona en cuestión.

FOTOCOPIABLE

UNIDAD 4.2 . ALUMNADO

UN DÍA EN LA VIDA DE HELENA

Lee el siguiente diario:

07:30 Helena se despierta.

08:00 Después de desayunar, Helena enciende su ordenador y se conecta a Internet. Una vez conectada, entra en un sitio web de noticias. A Helena le gusta y se registra. Aunque le ofrecen leer la declaración de privacidad del sitio web antes de registrarse pulsa aceptar todo el tiempo para acabar cuanto antes. A Helena no le preocupa en qué se utilizarán sus datos personales.

08:15 Helena busca cosas que le interesan en Internet. Su PSI (proveedor de servicios de Internet) registra y guarda todas las búsquedas de Helena durante un periodo de tiempo indeterminado. El motor de búsqueda que utiliza también conserva la información de las búsquedas sin declarar ningún fin específico.

09:00 Helena llega a su lugar de trabajo y las cámaras de vigilancia del circuito cerrado de televisión registran su llegada. Antes de que se instalaran las cámaras, la jefa de Helena informó claramente a los trabajadores que las imágenes registradas en el sistema sólo se utilizarían para fines relacionados con la seguridad y que todas las imágenes se guardarían a buen recaudo. La jefa de Helena también colocó un sistema de fichaje con lector biométrico del pulgar [para más información sobre la biometría, ver la página 97]. El sistema registra todas las entradas y salidas del lugar de trabajo de cada trabajador. A Helena le preocupó que ese sistema fuera algo indiscreto, pero esto parecía no importarles a sus compañeros, por lo que decidió adaptarse al sistema. Helena no ha recibido más detalles sobre los demás usos que su jefa pueda hacer de esta información.

11:15 En la pausa para el café, Helena entra en su cuenta bancaria on-line. La noche anterior había hablado con su hermano pequeño y quedaron en que le mandaría algo de dinero. Su hermano está recorriendo Europa en plan mochilero. El banco de Helena, al igual que las demás entidades financieras principales, utiliza el sistema interbancario SWIFT para transferir cantidades económicas. El banco no le ha explicado claramente si el Gobierno estadounidense puede acceder a la información relativa a la transferencia y a sus datos personales, ya que controla todas las transacciones SWIFT como medida preventiva en la lucha contra el terrorismo.

13:00 Helena sale a comer y se acerca a su supermercado local para comprar algunos productos para el hogar porque tiene intención de hacer una limpieza general de primavera en casa. En la caja, Helena muestra la tarjeta del establecimiento para ganar puntos por fidelidad. Su supermercado utiliza la información registrada en su tarjeta de fidelidad para controlar sus hábitos de compra y para enviarle ofertas de productos afines en el próximo buzoneo. A Helena no le importa que el supermercado conozca sus hábitos de compra.

13:20 Helena va a la biblioteca local para devolver un libro de autoayuda titulado "Química entre hombres y mujeres" y coge otro libro sobre cómo aumentar la autoestima: "Bombas de amor humanas". Para ello utiliza su carné de la biblioteca que registra los datos de sus préstamos en la base de datos del Ayuntamiento.

FOTOCOPIABLE

UNIDAD 4.2. ALUMNADO

16:00 Helena tiene que salir antes del trabajo para ir al hospital porque tiene hora con el especialista. Hace tres años, en la granja familiar, accidentalmente recibió un disparo en la pierna y todavía sufre dolores de esa herida. Cuando llega al hospital, da sus datos personales. El especialista tiene todo su expediente y Helena es consciente de que todo su historial médico está registrado en el sistema electrónico del hospital. No le importa pero supone que solamente acceden a dicha información aquellas personas que necesitan ver su historial para después tratarla.

19:00 Helena va a ir a una clínica privada en Nueva York para que le practiquen una pequeña operación de cirugía plástica. Después de cenar, Helena se conecta de nuevo a Internet y reserva un vuelo. Para realizar la reserva, Helena tiene que dar una gran cantidad de datos personales. Antes de viajar, como medida preventiva en la lucha contra el terrorismo, el Gobierno estadounidense recibirá estos datos para evaluarlos y decidir si Helena supone una amenaza para la seguridad de Estados Unidos. El sitio web de la compañía aérea sí contiene información notificando esta práctica, pero Helena generalmente no lee todas las informaciones adicionales de ese tipo, por lo que no es consciente de ello.

20:00 Helena recibe una llamada en su teléfono móvil. No reconoce el número pero, aún así, decide contestar. La persona que llama cuelga inmediatamente y Helena se olvida de esa llamada. Sin embargo, Helena no sabe que la persona que ha marcado su número de teléfono accidentalmente es considerada por la policía sospechosa de realizar actividades delictivas. En breve, la policía solicitará comprobar todos los registros telefónicos de esta persona. Los registros mostrarán que ha marcado el número de Helena. Como consecuencia, la policía también requerirá comprobar todos los detalles del teléfono móvil de Helena de los últimos tres meses para decidir si esa información es relevante en sus investigaciones.

Helena termina el día viendo la televisión. Sus datos personales ya no se facilitan a nadie más durante el resto del día.

FOTOCOPIABLE

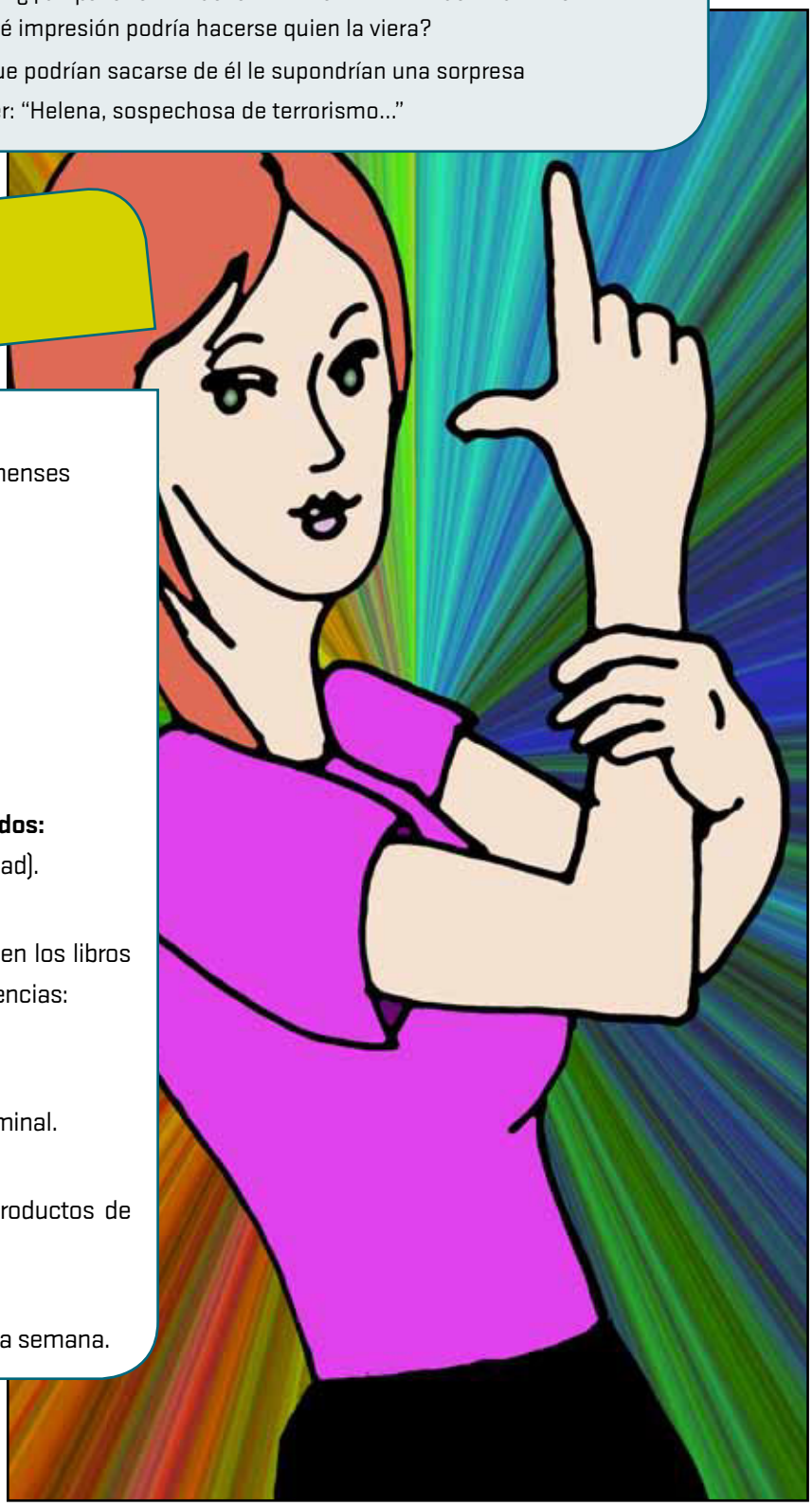
UNIDAD 4.2. ALUMNADO

¿SOCIEDAD DE LA VIGILANCIA?

Helena cree que no tiene motivos para preocuparse de si otras personas tienen acceso a su información personal. En realidad ella, que cumple con las leyes, ¿por qué debería preocuparse por eso? La tecnología ha hecho su vida cotidiana más fácil y ella ha compartido de buen grado sus datos personales para aprovecharse de esas ventajas.

Pero quizás Helena debería preocuparse. ¿Qué pasaría si toda la información retenida sobre ella se colocara en un único lugar central? ¿Qué impresión podría hacerse quien la viera?

El perfil resultante y las conclusiones que podrían sacarse de él le supondrían una sorpresa desagradable. Una conclusión podría ser: "Helena, sospechosa de terrorismo..."



HELENA:

Búsqueda de noticias en Internet:
Artículos de interés: Terroristas londinenses imputados (registros de Internet).

Búsquedas en la Web:
Cirugía plástica.

Transferencia de fondos:
A una persona en Hamburgo.

Historial médico:
Operada de una herida de bala.

Expediente delictivo/delitos cometidos:
Sí. (Dos multas por exceso de velocidad).

Archivos de la biblioteca municipal:
En una búsqueda de palabras clave en los libros prestados se produjeron dos coincidencias: "química" y "bomba".

Registros telefónicos:
Llamada recibida de un conocido criminal.

Hábitos de compra:
Compra de una gran variedad de productos de limpieza peligrosos.

Planes vacacionales:
Viaje en avión a Nueva York la próxima semana.

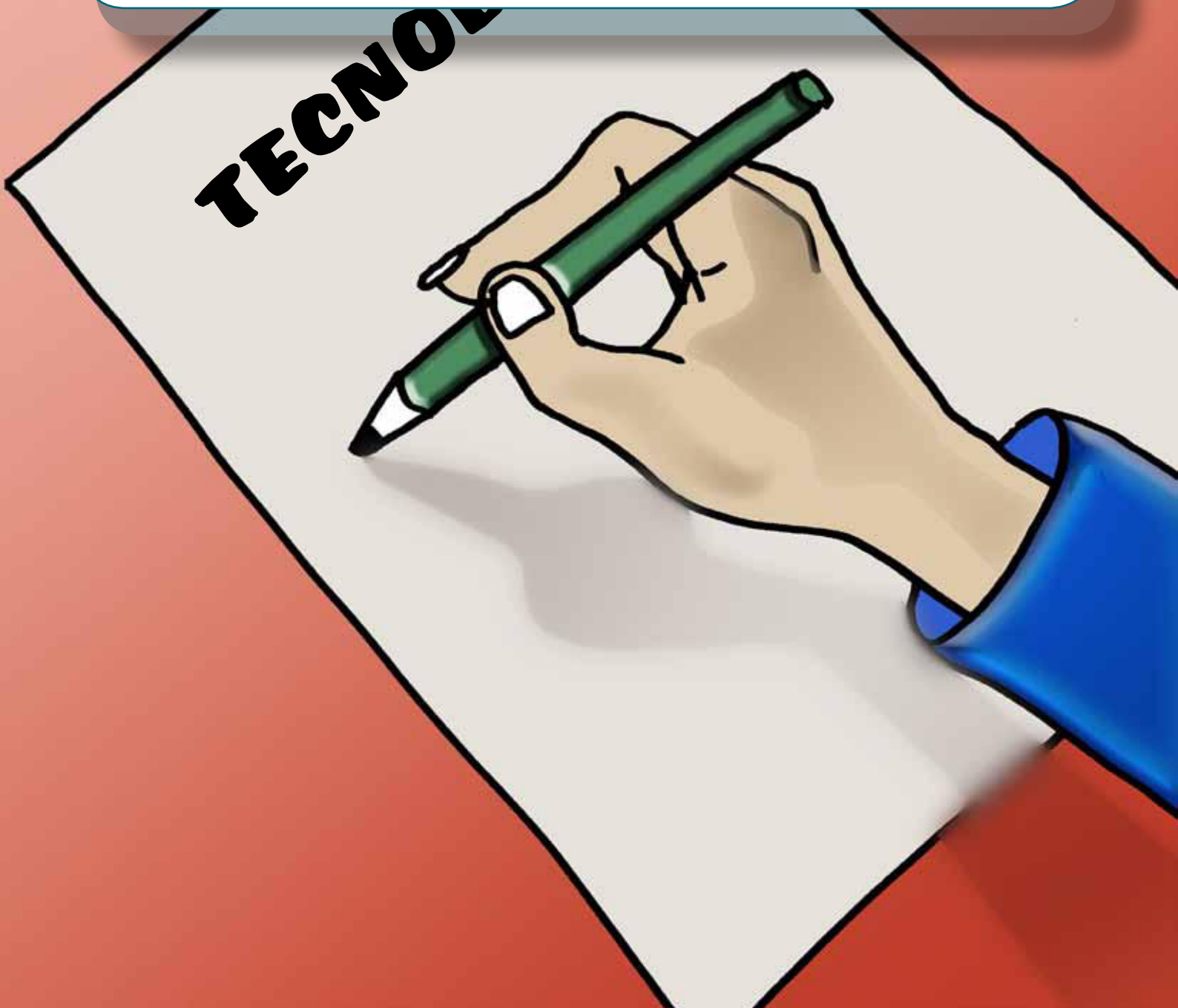
ACTIVIDAD 2

PROFESORADO

Tecnodiario

ACTIVIDAD DE SEGUIMIENTO

Al hilo de la situación descrita en las páginas anteriores "Un día en la vida de Helena", pida a los alumnos y alumnas que escriban un informe detallando sus interacciones con la tecnología. Las entradas pueden incluir transacciones como, por ejemplo, publicar comentarios o fotos en una red social, crear una entrada o post en un blog, subir vídeos a un portal determinado, utilizar abonos de transporte de autobús o tarjetas de préstamo de libros en una biblioteca, etc. Recuérdeles que piensen en el uso de sus teléfonos móviles o de Internet y en las zonas de su entorno donde hay instaladas cámaras de vigilancia. Los diarios podrían contener también un registro de las visitas al médico, libros prestados, DVD alquilados, competiciones en las que han participado, música descargada...



UNIDAD 4.3

PROFESORADO

VIGILANCIA

Fotocopie la actividad de la página 87 y distribúyala en clase. Utilice el material facilitado a continuación para presentar la actividad.
Las respuestas están en la página 88.

El predominio de la tecnología en nuestras vidas diarias es algo que ya se da casi por sentado.

Puede decirse que tenemos una huella electrónica que deja un rastro tras nosotros. Ya sea cuando encendemos nuestro teléfono móvil, pasamos el abono del autobús por el lector, fichamos al entrar al trabajo o en la escuela, compramos por Internet o somos grabados por las cámaras de vigilancia cuando andamos por la calle, muchos de nuestros movimientos y actividades pueden ser rastreados en términos de tiempo y espacio.

Parte de esa vigilancia se realiza abiertamente, como es el caso de las cámaras de vigilancia situadas a la vista, con una nota informativa al lado, explicando los fines para los que se graban las imágenes.

Cierto tipo de vigilancia es pasiva; por ejemplo, las imágenes grabadas por las cámaras de control de velocidad que uno se encuentra instaladas en determinados lugares de las carreteras de todo el país cuando pasa conduciendo por allí. Este tipo de vigilancia no exige nada a una persona en particular, a menos que el individuo se vea obligado a explicar ciertas acciones o comportamientos.
En ocasiones, es posible que la vigilancia por razones legítimas necesite ser encubierta, esto es, la vigilancia se lleva a cabo sin que las personas sometidas a vigilancia sean conscientes de ello. Sin embargo, deben examinarse más detenidamente muchos tipos de vigilancia posibles gracias a las tecnologías emergentes, y también es preciso que su uso sea justificado.

REFLEXIÓN

Pida a los alumnos y alumnas que decidan si piensan que los contextos descritos en la página siguiente son situaciones de “vigilancia abierta” en la que el uso de algún tipo de tecnología para vigilar a una persona es obvio y previsible. Por otro lado, la “vigilancia encubierta” se produce en una situación en la que el uso de la tecnología para vigilar las actividades de una persona no se muestra claramente. [Recordar que la vigilancia encubierta puede ser perfectamente legítima].

FOTOCOPIABLE

ACTIVIDAD 1. ALUMNADO

Decide si la vigilancia en los ejemplos siguientes es obvia (abierta) u oculta (encubierta).

Situación	Abierta √	Encubierta √
Fichar para entrar a trabajar con tu tarjeta de banda magnética.		
Una videocámara oculta instalada por la dirección de la escuela bajo la mesa de una profesora sin conocimiento de ésta. La cámara está colocada frente a la clase y graba las actividades de los alumnos y de la profesora.		
Dispositivos de seguridad en la ropa de una boutique. Si salieras de la tienda con una prenda que todavía lleva el dispositivo saltaría la alarma.		
Cámaras de control de velocidad.		
Cookies instaladas en tu ordenador para controlar todas las actividades que realizas en un sitio web determinado.		
El historial de un motor de búsqueda: registro de todas las búsquedas realizadas desde un ordenador concreto.		
Una cámara de vigilancia en una gasolinera.		
Marcar la casilla "Me gusta" en Facebook: esta información se registra y almacena en los bancos de datos de esta red social para ser utilizada posteriormente, generalmente con fines lucrativos.		
Un mensaje de voz dejado en tu teléfono móvil te vincula con una zona geográfica determinada a una hora y un día concreto del año pasado.		
Suscribirse en una red social a un juego o a una aplicación: la red social puede acceder a estos datos de actividad y utilizarlos para fines como la publicidad personalizada.		

ACTIVIDAD 1

PROFESORADO

Respuestas

Situación	Abierta √	Encubierta √
Fichar para entrar a trabajar con tu tarjeta de banda magnética.	√	
Una videocámara oculta instalada por la dirección de la escuela bajo la mesa de una profesora sin conocimiento de ésta. La cámara está colocada frente a la clase y graba las actividades de los alumnos y de la profesora.		√
Dispositivos de seguridad en la ropa de una boutique. Si salieras de la tienda con una prenda que todavía lleva el dispositivo saltaría la alarma.	√	
Cámaras de control de velocidad.		√
Cookies instaladas en tu ordenador para controlar todas las actividades que realizas en un sitio web determinado.		√
El historial de un motor de búsqueda: registro de todas las búsquedas realizadas desde un ordenador concreto.		√
Una cámara de vigilancia en una gasolinera.	√	
Marcar la casilla "Me gusta" en Facebook: esta información se registra y almacena en los bancos de datos de esta red social para ser utilizada posteriormente, generalmente con fines lucrativos.		√
Un mensaje de voz dejado en tu teléfono móvil te vincula con una zona geográfica determinada a una hora y un día concreto del año pasado.		√
Suscribirse en una red social a un juego o a una aplicación: la red social puede acceder a estos datos de actividad y utilizarlos para fines como la publicidad personalizada.		√

FOTOCOPIABLE

UNIDAD 4.4 . ALUMNADO

TV DIGITAL INTERACTIVA

La televisión digital interactiva se está expandiendo por todo el mundo. Se utilizan muchas palabras de moda para describir la TV digital: la revolución digital, gran oportunidad, control...

¿Qué es la TV digital interactiva?

La TV digital interactiva es aquélla en la que hay una interacción en la que la información fluye entre la persona espectadora y el proveedor del servicio (la compañía de la televisión digital que ofrece los canales de televisión). El proveedor del servicio de televisión hace preguntas y el espectador contesta utilizando el mando de la televisión. Según las respuestas, el contenido televisivo va cambiando.

¿Cómo funciona?

La televisión tiene un chip de memoria que enlaza con una base de datos central. Este chip controla las horas que pasas viendo la televisión al día y registra todos los programas vistos en cada televisión individual. Cada vez que se pulsan los botones del mando a distancia, el movimiento queda anotado en la base de datos. Este sistema se conoce como "flujo de clicks" del televisor y puede ser generalizado para crear un perfil muy sofisticado del espectador y sus preferencias. Las personas analistas que trabajan para el proveedor de televisión, con el paso del tiempo, pueden llegar a conocer cada vez mejor los gustos y hábitos de los espectadores y esta información podría venderse a las empresas de investigación de mercado y a anunciantes.

Opciones

Muchos paquetes nuevos que van apareciendo en el mercado ofrecen descuentos o más canales televisivos si registras tus datos en un registro central y aceptas que controlen todo lo que ves. La factura mensual que recibe tu familia podría rebajarse y, además, se podrían conseguir descuentos en productos relacionados. ¿Merece la pena? Tú decides...

¿Cómo te sentirías si en la pantalla de tu televisor aparecieran sugerencias sobre las próximas emisiones de programas que pudieran interesarte de acuerdo con tus preferencias? ¿Te importaría que te enviaran notas recordatorias a tu teléfono móvil o a tu cuenta de correo electrónico? ¿Cómo te sentirías si tu proveedor transmitiera tus datos a otras compañías y éstas contactaran contigo para informarte sobre productos y servicios relacionados con tus hábitos televisivos? Algunos materiales dirigidos a ti podrían revelar un aspecto sobre tu persona que preferirías mantener en privado, fuera del alcance de los demás, por ejemplo, información relacionada con dificultades financieras, cirugía estética, productos de culturismo, agencias matrimoniales, pastillas para adelgazar, enfermedades médicas embarazosas...

La TV digital interactiva podría ser un modo de intentar meterse en tu cabeza para descubrir tu opinión sobre todo tipo de cuestiones... Imagina lo útil que sería esta información para las empresas, los partidos políticos, los medios de comunicación, etc.

FOTOCOPIABLE

ACTIVIDAD DE SEGUIMIENTO / DEBERES. ALUMNADO

Escribe un diario con los programas de televisión que ves durante una semana y calcula las horas que pasas delante del televisor al día. La siguiente semana presenta los resultados en clase para debatirlos en grupo. ¿Qué revelan los resultados sobre tu personalidad e intereses? ¿Crees que las empresas de marketing pensarían que esta información es útil para conocer qué tipo de anuncios y mensajes personalizados les interesaría emitir en tu televisor? ¿Crees que las ventajas contrarrestan los aspectos negativos? ¿Hay programas que prefieres que nadie sepa que los ves?

FOTOCOPIABLE

UNIDAD 4.5 · ALUMNADO

COMPRAS: CIELO O INFIERNO

FOTOCOPIABLE

ACTIVIDAD DE SEGUIMENTO / DEBERES

ALUMNADO

ANTECEDENTES

Los supermercados pueden controlar nuestros hábitos de compra gracias a las tarjetas de fidelización. Con las ofertas y los descuentos de todo tipo que hacen a los clientes que han adquirido una tarjeta de fidelización, los supermercados consiguen información valiosa sobre las compras habituales y los productos para ocasiones especiales que adquieren las personas.

Los supermercados utilizan los datos de estas tarjetas de forma muy inteligente. Analizan estos datos para descubrir con qué frecuencia sus clientes compran determinados productos y si existen patrones comunes. Las compras se dividen en categorías: de lujo, económicas (ajustadas a presupuesto) o del hogar. Además, los datos también servirían para clasificar a los clientes en los diferentes grupos sociales o económicos. Cuando un cliente solicita la tarjeta de fidelización debería ser informado de que sus datos serán analizados y los supermercados deberían preguntarle si consiente que su información sea transferida a otras empresas, ofreciéndole la posibilidad de decir que "no" si no quiere que eso ocurra.

Mucha gente se sorprendería al ver los datos directamente relacionados con ella o si se enterara de que sus hábitos de compra se han transmitido a otras empresas sin su permiso. Por ejemplo, imagina que el supermercado te envía un mensaje de texto cada vez que añaden un nuevo producto en la sección de panadería porque el año pasado compraste muchos pasteles. ¿Te importaría que el supermercado informara de ello a otras empresas y te ofrecieran un descuento en pastillas para adelgazar mediante mensajes de texto?

¿Crees que el hecho de utilizar la información para otro propósito que no sea la finalidad inicial para la que se requirieron los datos supone un incumplimiento de las obligaciones del (responsable de tratamiento datos) supermercado? Un responsable de datos debe... conservar tus datos personales para uno o varios fines específicos, explícitos y legales. Asimismo, un responsable de datos debería...utilizar tus datos personales únicamente para esos fines.

Ver el esquema "Derechos y responsabilidades". (Unidad 3, pag. 55).

La próxima vez que vayas al supermercado o estés en una tienda de una cadena que te ofrece contratar una tarjeta de fidelización, solicita una copia del impreso de solicitud y lee el apartado "Términos y Condiciones".

Responde a las siguientes preguntas:

- ¿Existe claramente un límite de edad mínima para solicitar una tarjeta de fidelización?
- Después de leer los "Términos y Condiciones", ¿entiendes para qué se utilizarán tus datos o los de tu familia?
- ¿Puedes decir que "no" quieres que contacten contigo para otros servicios; por ejemplo, préstamos, seguros de coche o del hogar?
- ¿Puedes decir que "no" quieres que envíen tus datos a "una serie de empresas" asociadas con el supermercado?

FOTOCOPIABLE

UNIDAD 4.6 ALUMNADO

SITIOS WEB DE REDES SOCIALES

Los sitios web de redes sociales (por ejemplo, Tuenti, Facebook o Twitter) son un lugar extraordinario para charlar con amigos y amigas y conocer gente nueva. Aunque muchos sitios web de redes sociales permiten a los usuarios restringir el acceso, las encuestas demuestran que la mayoría de las personas no activan las opciones de privacidad o las medidas de seguridad.

Existen varios factores que podrían afectar a tus experiencias en los sitios de redes sociales, por ejemplo, tu actitud hacia la privacidad, la cantidad de información que compartes con otras personas, las opciones de privacidad disponibles y el sistema de seguridad del sitio en el que te has inscrito. Cuando creas una cuenta en un sitio de redes sociales, merece la pena recordarte a ti mismo que estás creando una huella electrónica o un registro de tu vida en un lugar y momento específicos. El hecho de revelar demasiados datos personales, información sobre tus relaciones y lo que haces en tu tiempo libre podría acarrear consecuencias en un futuro... el pasado puede volver sin previo aviso.

2020 GENERACIÓN Z

Según vas posteando mensajes y subiendo vídeos y fotos a tu sitio web de redes sociales, un buscador electrónico rastrea sin que tú lo sepas la Red Global Mundial (World Wide Web) capturando (guardando) tus páginas. Aunque elimines el contenido de tus páginas cada pocos meses, te aterrará saber que la colección de vídeos, fotos y posts que creaste cuando eras adolescente volverán a salir a la superficie en el año 2020, en un archivo colgado en la red con el título "La Generación Z: los años perdidos".

Situación 1:
Es el año 2020 y tienes una entrevista importante para tratar sobre un futuro ascenso. Cuentas con que vas a conseguir el ascenso y con el correspondiente aumento de salario para que te concedan la hipoteca para tu primera casa. Un antiguo compañero de clase te advierte de la existencia del archivo "Generación Z" y estás preocupado porque tu jefa puede echar mano de este material como parte del proceso de investigación. Algunas fotos y conversaciones grabadas de aquella época resultan ahora bastante impactantes.

Situación 2:
Eres un político local ambicioso y trabajador y tienes pensado presentarte como candidato al Parlamento en las elecciones generales de 2020. Uno de tus rivales descubre el archivo "Generación Z" y avisa al periódico local. El periódico publica comentarios sobre ti de otras páginas de la misma comunidad virtual, donde te describen como impopular, vago y egocéntrico. Intentas reírte de ello, porque es un instante aislado de la primera etapa de tu vida adulta pero, a medida que vas haciendo campaña en la localidad, no puedes evitar observar que se ha producido un cambio en la actitud de las personas hacia ti.

FOTOCOPIABLE

UNIDAD 4.6 ALUMNADO

SITIOS WEB DE REDES SOCIALES

CASO DE ESTUDIO 1

Menores de edad enviaban sus fotos a un portal especializado en servicios de contactos personales, que carece de medidas que aseguren la certeza de la edad y en el que se podía acceder a las fotografías y comentarios sin restricciones. La AEPD investiga los hechos y constata que el tratamiento de los datos personales se realiza sin el necesario consentimiento de los padres de los menores y sin haber sido previamente informados, por lo que se acuerda sancionar al portal.

CASO DE ESTUDIO 2

Alumnos que en clase toman la fotografía del profesor con un teléfono móvil y la distribuyen a través de una red social en la que se vuelcan comentarios. La AEPD investiga los hechos, pues se trata de la difusión de un dato de carácter personal, como es la imagen, realizada sin el consentimiento de la persona afectada y que, por tanto, da lugar a responsabilidad de conformidad con la legislación sobre protección de datos.

CASO DE ESTUDIO 3

La suplantación de la identidad de un menor en una red social, al que se le atribuyen determinados comentarios que no ha realizado. La AEPD investiga los hechos, así como la línea telefónica desde la que se ha llevado a cabo para la determinación de responsabilidades.

FOTOCOPIABLE

ACTIVIDAD DE SEGUIMIENTO / DEBERES

ALUMNADO

Sitios web de redes sociales: ¿Una trampa para robar identidades?

Los llamados ladrones de identidades reúnen información personal de la red esperando conseguir datos suficientes para robar temporalmente la identidad de una persona y cometer un fraude.

Se pueden adivinar las claves de acceso de los usuarios documentándose sobre sus relaciones y pasatiempos. A veces la gente facilita en sus páginas web los detalles suficientes y esto permite que otras personas se hagan pasar por ellas o incluso acosarlas.

Medidas preventivas

• Publicar en Internet tu fecha de nacimiento, el número de teléfono móvil, el lugar de residencia, cuándo te vas de vacaciones, o datos médicos (grupo sanguíneo, etc.) podría resultarte perjudicial. Realmente, nunca es una buena idea dar a conocer esta información en una página web, una red social o un blog; únicamente deberías compartirla con personas en las que puedas confiar plenamente.

• Al entablar amistades virtuales, hazlo sólo con gente que conozcas y si tuvieras dudas sobre su verdadera identidad, ponles a prueba para comprobarlo.

• Ten cuidado al cargar imágenes en Internet. Nunca cargues una imagen de otra persona sin su consentimiento.

• Evita utilizar máquinas de acceso público para conectarte a Internet (cibercafés, etc.), y si lo haces, desconéctate como es debido.

En el ordenador de la escuela, de la biblioteca o de casa, entra en algunas de las siguientes direcciones electrónicas:

• Agencia Española de Protección de Datos: "Recomendaciones a usuarios de Internet". Puedes consultar los Capítulos XI "La web 2.0", (pág. 38) y XII "La responsabilidad de los internautas", (pág. 43).

• Agencia de Protección de Datos de la Comunidad de Madrid . Consulta Jóvenes e Internet, dedicado a los jóvenes.

• Autoridad Catalana de Protección de Datos. Consulta el área joven Privacidad para Jóvenes.

• Agencia Vasca de Protección de Datos. Donde puedes consultar Privacidad en redes sociales, Vídeos formativos y el Portal para adolescentes y educadores Kontuzdatos.

Si tienes una cuenta en un sitio web de redes sociales, responde a las siguientes preguntas según tu opinión y tu propia experiencia en la materia.

• En general, los perfiles que diseñáis tú y tus amigos y amigas, ¿son públicos o privados?

• ¿Facilitas datos como el nombre, la fecha de nacimiento y el número del teléfono móvil?

• ¿Sabes si personas que conoces "añaden" amigos que no conocen? ¿De qué manera te afectaría si uno de tus amigos añadiera a un extraño a su grupo de amigos on-line?

• ¿Etiquetas fotos de tus amigos y amigas sin su permiso?

• ¿Haces comentarios en tu muro o en el de tus amigos sin pensar en si lo que escribes es privado o lo que dices puede resultar molesto?

• ¿Puedes aplicar alguna de las recomendaciones a la experiencia que tú y tus amigos habéis tenido en relación con los perfiles web?

IDEAS PARA LA ACCIÓN

Analiza el tema del "robo de identidad" utilizando diferentes medios de comunicación (prensa/televisión/radio/ Internet) durante un periodo de tiempo determinado. Céntrate especialmente en los datos estadísticos disponibles sobre el robo de identidad en cualquier ámbito en el que se produzca. Investiga con qué frecuencia se menciona que los sitios web de redes sociales son fuentes potenciales para el robo de identidad. Finalmente, redacta un informe y prepara una exposición/ presentación para explicar tus conclusiones principales.

UNIDAD 4.7 . ALUMNADO

RFID: GENERANDO ONDAS

Identificación por radiofrecuencia (RFID)

La Identificación por Radiofrecuencia (RFID) es un tipo de sistema de identificación automática que utiliza frecuencias de ondas de radio. La información se transmite a través de un dispositivo portátil denominado etiqueta o tag, cuya señal es captada por un lector de RFID. Los datos transmitidos por la etiqueta pueden contener información relacionada con su identificación o localización.

Las etiquetas de RFID son muy utilizadas en los sectores de almacenamiento y transporte porque ayudan a identificar el paradero de las mercancías. Asimismo, los supermercados y el comercio minorista han mostrado un gran interés por estas etiquetas de RFID. Los grupos de libertades civiles y los activistas en pro de la privacidad han expresado sus preocupaciones y cuestionado en qué momento debería dejar de funcionar la etiqueta de RFID colocada en el producto: ¿al pagar el producto en caja (punto de compra) o al abrirlo en casa (consumo)? Al igual que los artículos, las tarjetas de fidelización son un objeto obvio para colocar etiquetas de RFID porque el lector de RFID del supermercado alertaría de tu presencia si entras en el establecimiento con la tarjeta de fidelización en tu cartera...

¿Las compras del futuro?

Cuando una persona entra en un establecimiento de una conocida cadena de tiendas de moda y lleva consigo su tarjeta de fidelización con una etiqueta de RFID, en ese mismo instante el dependiente del establecimiento, gracias al lector de RFID manual que tiene, conoce las preferencias del potencial comprador, las compras anteriores y estadísticas fundamentales antes incluso de que el comprador empiece a echar un vistazo. Una vez en el probador, el lector de RFID sugiere al cliente otras prendas que podrían combinar con las que ha elegido mostrándoselas en una pantalla de video instalada en el probador. En algunos casos, los lectores de RFID pueden incluso leer las etiquetas colocadas por otras empresas. Escaneando el resto de las bolsas de tus compras o las tarjetas de fidelización que llevas en la cartera, se hará una imagen más amplia de tus hábitos de compra que se añadiría al perfil que diseñó la tienda sobre ti.

FOTOCOPIABLE

UNIDAD 4.7 ALUMNADO

RFID: GENERANDO ONDAS

LAS ETIQUETAS DE RFID Y LOS NIÑOS Y NIÑAS

En algunos países están probando dispositivos de RFID diseñados para "identificar y localizar" niños. Las soluciones son varias:

Etiquetas para bebés: a los bebés se les coloca una pulsera que transmite una señal de radio a un auricular que lleva consigo el padre, la madre o la persona que cuida al bebé. Se genera un anillo protector y la alarma se dispara cuando el niño gatea fuera de esa zona.

Teléfono i-Kids: los padres regalan a sus hijos teléfonos i-Kids. Si los padres quieren saber dónde está su hijo, envían un mensaje de texto a un número determinado y reciben la señal del teléfono i-Kids de su hijo indicándoles su localización.

Cinturones rastreadores: en estos cinturones se coloca una etiqueta con un Sistema de Posicionamiento Global (GPS), para que los padres puedan entrar en Internet y obtener una imagen de satélite de la localización de sus hijos. La imagen se actualiza cada 15 segundos.

Implantes: en realidad, los chips se implantan debajo de la piel. En la actualidad, las mascotas ya llevan microchips, pero los planes de implantar chips en los niños se han encontrado con oposición debido a cuestiones éticas.

ACTIVIDAD DE SEGUIMIENTO

El Consejo Escolar de un colegio de primaria de tu zona quiere probar una instalación de "identificación y localización" de niños para un radio de 50 metros. Como secretario o secretaria de la Asociación de Madres y Padres de alumnos (AMPA), debes escribir una carta a la dirección del colegio para solicitar información sobre la iniciativa y sus motivos. Solicita una reunión para hablar sobre el tema.

ACTIVIDAD DE SEGUIMIENTO

Tus padres están pensando en comprar un dispositivo con etiqueta RFID para tu hermano de seis años. De este modo, ellos estarían más tranquilos, pero tú estás preocupado porque piensas que se están pasando. Escribe una lista con argumentos a favor y en contra de que los padres compren dispositivos para "identificar y localizar" a sus hijos. Reflexiona sobre lo siguiente: ¿qué pasaría si cuando los hijos e hijas crecieran y fueran adolescentes los padres decidieran que deben continuar llevando esos dispositivos? ¿Deberían los adolescentes tener voz y voto en el asunto?

FOTOCOPIABLE

UNIDAD 4.8 . ALUMNADO

BIOMETRÍA

Los sistemas informáticos que generan información biométrica identifican automáticamente las características fisiológicas como las huellas dactilares, la retina, la cara, los patrones vocales e incluso el olor corporal como características únicas del individuo. **Lee este artículo de prensa y responde a las preguntas de la página siguiente.**

Escáneres biométricos en un comedor escolar

Kevin Schofield, *The Scotsman*, 27/10/2006

Los alumnos de una escuela de primaria de Escocia han sido los primeros del mundo en pagar sus comidas pasando la palma de la mano por un escáner en lugar de hacerlo con dinero en efectivo.

La escuela de primaria Todholm en Paisley ha introducido la tecnología biométrica que permite identificar a los alumnos y alumnas a través de los patrones únicos de las venas de sus manos.

Esto significa que se acabó el perder el dinero para el comedor –y este sistema protege la identidad de los alumnos o alumnas que tienen derecho a recibir comidas gratis en la escuela–. Asimismo, identifica a aquellas personas con alergias alimenticias y fomenta la dieta equilibrada entre el alumnado, proporcionándoles una lectura de las comidas que han elegido durante la semana.

Ahora, aquellas personas relacionadas con este sistema pretenden expandirlo por toda Escocia y aseguran que se podría utilizar para permitir la entrada y la salida de los chicos y chicas en la escuela, para registrar su asistencia y para sacar libros de la biblioteca. No obstante, los opositores del sistema argumentan que es innecesario y que posiblemente supone una violación de las libertades civiles.

Pat Swanson, vicedirector de la escuela Todholm, dijo que el sistema nuevo es mucho mejor que el anterior. "A los niños les gusta porque es nuevo y emocionante, y además, fácil de usar", y añadió que "esto significa que no tienen que andar trayendo dinero a la escuela, que además suelen perder a menudo, y así no tenemos que enviar cartas a las familias reclamando el pago de las comidas".

Muchas escuelas ya utilizan tarjetas de banda magnética para evitar utilizar dinero en efectivo en los comedores. Sin embargo, Grant Henderson, director de contratación de Amey, empresa encargada del escáner de manos, aseguró que este sistema es mucho más fiable. Dijo que "el problema consiste en que los alumnos pueden perder las tarjetas de banda magnética, especialmente los más jóvenes" y garantizó que "con este sistema, los más pequeñas sólo tienen que acudir al comedor y pasar la palma de la mano por el escáner. A continuación, un dispositivo muestra a la encargada del comedor la cantidad de dinero restante en la cuenta del alumno correspondiente y las comidas del menú que ha seleccionado en ocasiones anteriores, y de este modo tiene la opción de elegir algo más saludable."

"Incluso se le puede comunicar a la empresa de catering las alergias que cualquier alumno pueda tener para que sepan el tipo de alimentos que no pueden comer". Mr Henderson predijo que la tecnología biométrica podría aplicarse en otros ámbitos de la vida escolar. Dijo que "por ejemplo, en vez de pasar lista cada mañana, los alumnos y alumnas únicamente tendrían que pasar la palma de la mano por el escáner cuando llegan a la escuela."

"Este sistema también podría utilizarse para cuestiones de seguridad, es decir, podría ser una manera de mantener alejadas de la escuela a las personas que no deberían estar allí." No obstante, Patrick Harvie, miembro del Parlamento escocés perteneciente al partido verde, dijo que le preocupaba mucho el uso de la tecnología biométrica en las escuelas. "Cualquiera de estos sistemas podría potencialmente acarrear como consecuencia el tratamiento erróneo de la información o que la información llegara a quien no debiera."

FOTOCOPIABLE

UNIDAD 4.8 . ALUMNADO

BIOMETRÍA

PREGUNTAS

1. ¿Cuál es el objetivo principal del nuevo sistema biométrico?
2. Según el artículo, también se podría reunir información para otros muchos fines, ¿cuáles son?
3. ¿Te sorprenderías si al elegir el menú te recomendaran que cogieras algo más saludable porque ya has comido patatas fritas esa semana?
4. ¿Te preocuparías si tus padres pudieran solicitar una copia detallada de todas las comidas o los tentempiés que has comprado en el comedor de la escuela?
5. ¿Crees que la escuela consultó a los alumnos y a sus familias las opiniones sobre este nuevo sistema antes de implantarlo?
6. ¿Crees que existe algún modo de que los padres y las madres permitan a sus hijos utilizar un comedor en el que no se pague con dinero en efectivo pero tampoco se registre ningún dato (excepto la cantidad total gastada)?
7. ¿Para cuales de estos fines crees que se podría utilizar la biometría? Puedes elegir todos, alguno o ninguno. Argumenta tu respuesta.

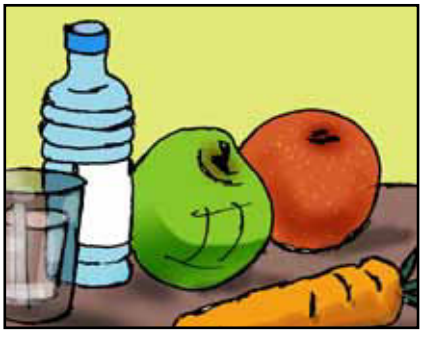
FINES DE SEGURIDAD

ASISTENCIA / PASAR LISTA

COMIDAS GRATUITAS EN LA ESCUELA

ALERGIAS

PRÉSTAMO DE LIBROS DE LA BIBLIOTECA



DIETA / ALIMENTACIÓN

UNIDAD 4.8 ALUMNADO

BIOMETRÍA

ACTIVIDAD DE SEGUIMIENTO

Registro escolar de las huellas dactilares:

En este momento tu escuela está considerando instalar un sistema de identificación mediante huellas dactilares que avisaría a las familias de que sus hijos o hijas no han asistido a clase en cuestión de segundos. Los alumnos colocan su dedo en un escáner que lee la huella dactilar y registra la asistencia en un ordenador. Si un alumno o alumna no se registra al comienzo del día, se envía inmediatamente un mensaje de texto de alerta al teléfono móvil del padre o de la madre. Esa información también podría ser remitida a los inspectores de educación que quieran utilizar los datos para localizar a los alumnos que hacen novillos.

Imagina que te han encargado escribir un artículo para la revista de la escuela sobre la propuesta de implantación del sistema biométrico, descrito en la página anterior, para controlar la asistencia de los alumnos. Trata de encontrar un equilibrio entre los derechos de los alumnos y alumnas y las necesidades de la escuela.

ACTIVIDAD DE SEGUIMIENTO

Imagina la siguiente situación: en el Parlamento se someterá a debate una ley que regulará las disposiciones sobre los sistemas de etiquetas electrónicas en el transporte público.

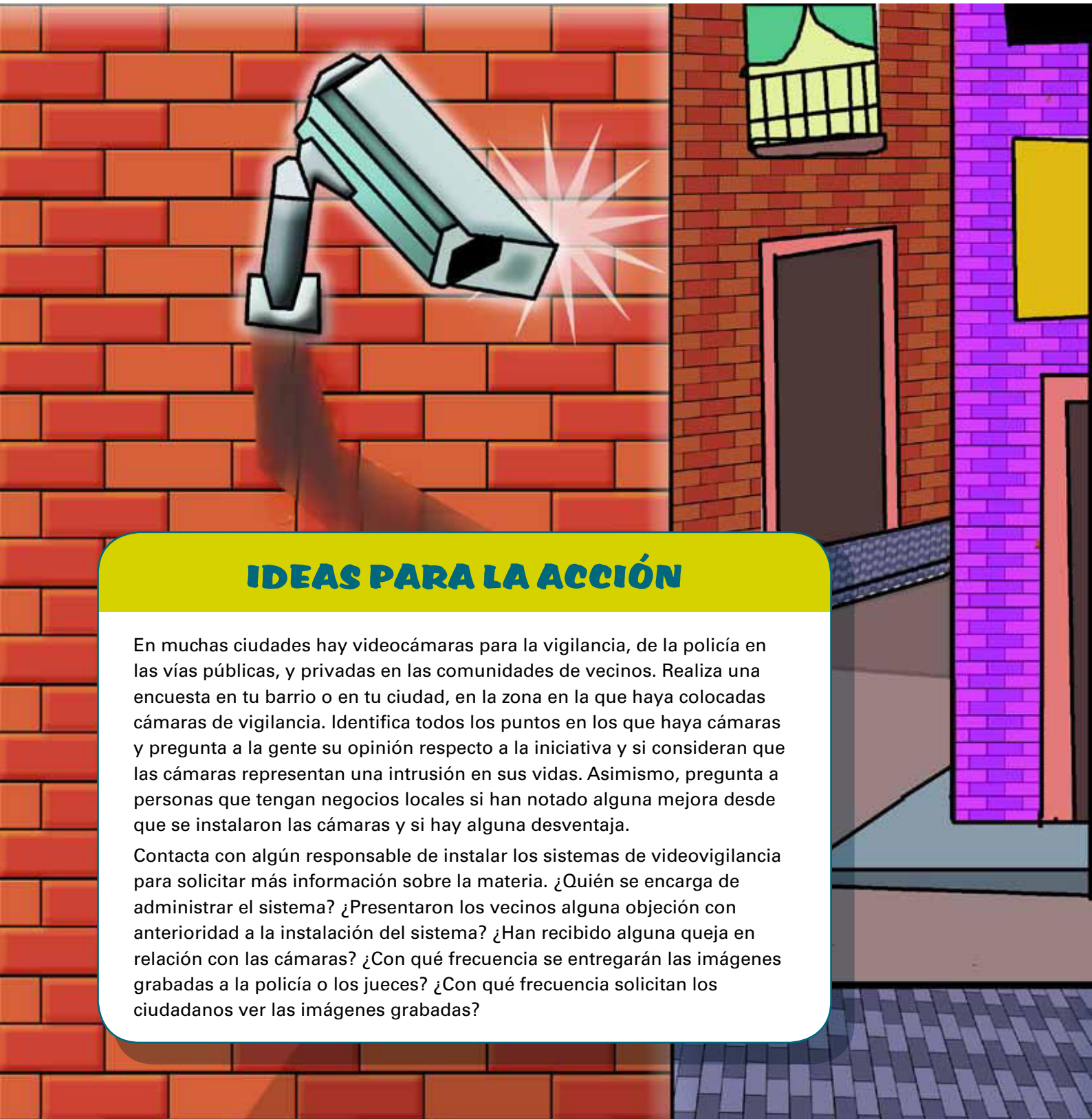
En caso de que se aprobara la ley, todos los bonos de los transportes públicos llevarían una etiqueta electrónica. La etiqueta transmitiría datos como el nombre de la persona titular de la tarjeta de viaje y el destino a una base de datos central administrada por una agencia de transporte del gobierno. La etiqueta sería válida durante dos semanas. Los defensores de la nueva ley defienden que este sistema resultaría extremadamente útil a la hora de localizar a los autores de los crímenes y ayudaría a determinar los últimos movimientos de las personas desaparecidas. Los opositores, en cambio, argumentan que este sistema no sólo supone una intrusión injustificada en el derecho a la privacidad, sino que también afecta gravemente al derecho a la libertad de movimiento.

Debatan en clase el sistema de etiquetas propuesto en los bonos de transporte, y que los alumnos y alumnas investiguen sobre este tema para averiguar si en otros países europeos han implantado sistemas similares, por ejemplo, la tarjeta de transporte “Oyster Card” en Londres. Divida la clase en dos grupos (uno representará al Gobierno y otro a la oposición) para generar un debate en torno a la ley y presentar sugerencias para posibles enmiendas. Organice una votación sobre la ley y las enmiendas que hayan podido aceptarse. Analicen el significado del resultado final en lo que a funcionamiento y gestión del nuevo sistema se refiere.

FOTOCOPIABLE

UNIDAD 4.8 . ALUMNADO

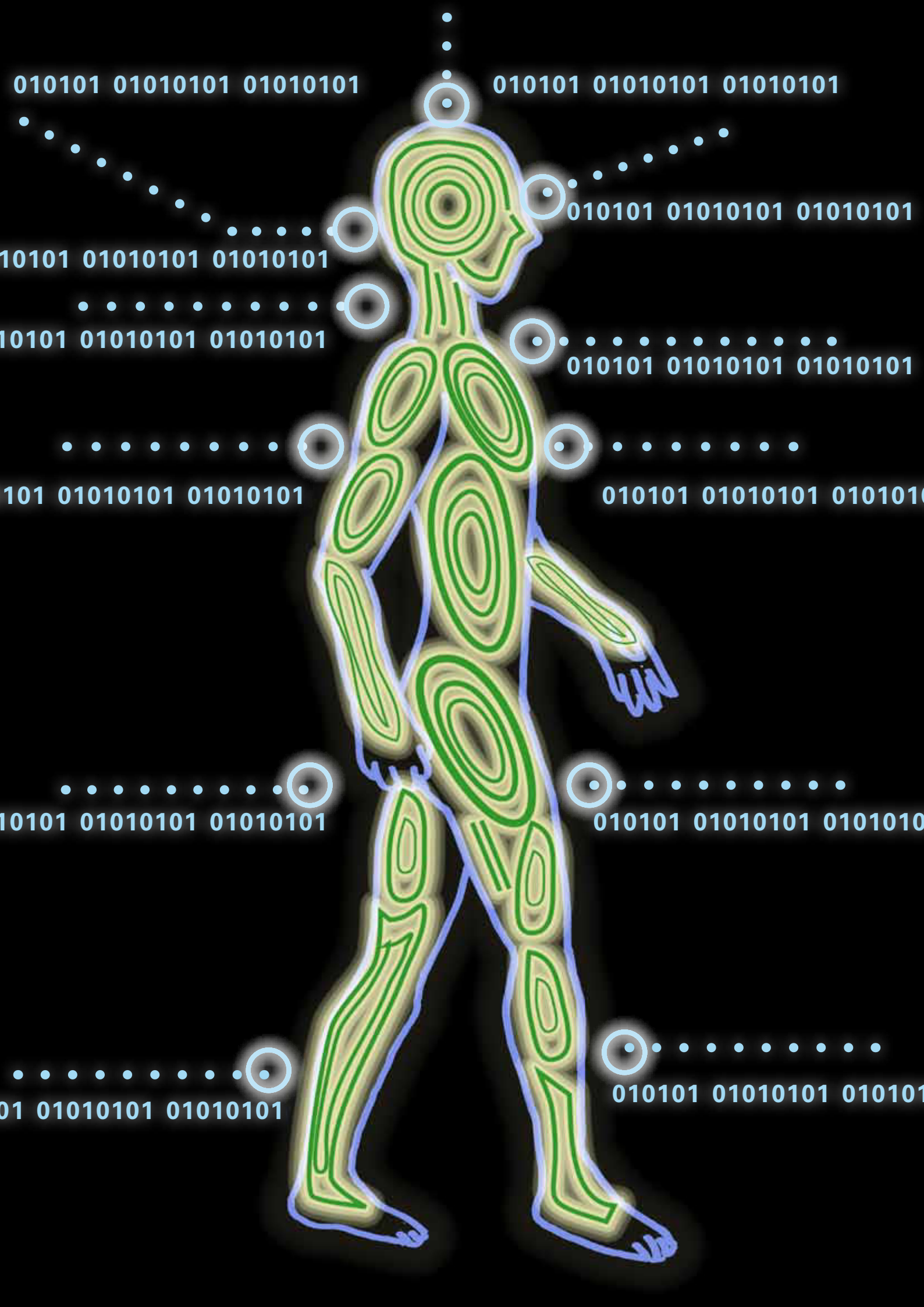
BIOMETRÍA



IDEAS PARA LA ACCIÓN

En muchas ciudades hay videocámaras para la vigilancia, de la policía en las vías públicas, y privadas en las comunidades de vecinos. Realiza una encuesta en tu barrio o en tu ciudad, en la zona en la que haya colocadas cámaras de vigilancia. Identifica todos los puntos en los que haya cámaras y pregunta a la gente su opinión respecto a la iniciativa y si consideran que las cámaras representan una intrusión en sus vidas. Asimismo, pregunta a personas que tengan negocios locales si han notado alguna mejora desde que se instalaron las cámaras y si hay alguna desventaja.

Contacta con algún responsable de instalar los sistemas de videovigilancia para solicitar más información sobre la materia. ¿Quién se encarga de administrar el sistema? ¿Presentaron los vecinos alguna objeción con anterioridad a la instalación del sistema? ¿Han recibido alguna queja en relación con las cámaras? ¿Con qué frecuencia se entregarán las imágenes grabadas a la policía o los jueces? ¿Con qué frecuencia solicitan los ciudadanos ver las imágenes grabadas?


010101 01010101 01010101
010101 01010101 01010101
010101 01010101 01010101
10101 01010101 01010101
10101 01010101 01010101
010101 01010101 01010101
101 01010101 01010101
010101 01010101 010101
10101 01010101 01010101
010101 01010101 010101
01 01010101 01010101
010101 01010101 010101

APÊNDICE


GUÍA
DE
CONTENIDOS
LEGALES

INTRODUCCIÓN

El 10 de diciembre de 1948, la Asamblea General de las Naciones Unidas aprobó y proclamó **la Declaración Universal de Derechos Humanos**. Tras este acto histórico, la Asamblea pidió a todos los Países Miembros que publicaran el texto de la Declaración y dispusieran que fuera "distribuido, expuesto, leído y comentado en las escuelas y otros establecimientos de enseñanza, sin distinción fundada en la condición política de los países o de los territorios".

La Declaración Universal de Derechos Humanos en su **artículo 12** dice:

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Asentados en esta declaración se basan los **artículos 18.1 y 18.4 de la C.E.** y la **Carta de los Derechos Fundamentales de la Unión Europea**.

En nuestro país, la **Constitución Española de 1978** reconoce en el **art. 18** el derecho al honor, a la intimidad personal y familiar, a la propia imagen, el derecho a la inviolabilidad del domicilio y al secreto de las comunicaciones. El principal desarrollo legislativo que se ha producido hasta ahora del derecho a la intimidad, reconocido en el art. 18.1 de la Constitución, ha sido la **Ley Orgánica 1/1982, de 5 de mayo**, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. El artículo 18.4 de la C.E. se encuentra incluido dentro de la norma constitucional que reconoce y proclama distintos derechos relativos a la privacidad de las personas. Así, esta norma dicta un derecho nuevo a controlar la propia información personal sea íntima o no, un derecho general frente a las tecnologías de la información.

El desarrollo de las tecnologías de la información presenta también algunos aspectos de inseguridad y alarma. Son varios los derechos fundamentales que pueden verse amenazados o vulnerados por un uso indebido de las tecnologías de la información, existe el peligro de que las tecnologías de la información entren en conflicto con el derecho a la intimidad. El tratamiento automatizado de información relativa a las personas físicas, facilita un número indeterminado de posibilidades que permite recoger datos personales, conservarlos y transmitirlos. La tecnología es capaz de tratar un gran volumen de información y de relacionarla entre sí, de forma que da la posibilidad de crear perfiles de nuestra personalidad, perfiles que pueden llegar a justificar decisiones públicas o privadas y que puedan limitar nuestra libertad o condicionar nuestro modo de actuar.

La STC 292/2000, de 30 de noviembre representa el pronunciamiento del **Tribunal Constitucional** más claro en relación a la existencia de un derecho fundamental a la protección de datos personales, a partir del art. 18.4 de la C.E., con autonomía respecto del derecho a la intimidad.

El derecho fundamental a la protección de datos personales es un derecho autónomo, con un contenido concreto que permite a la persona un control de sus datos personales, sean o no íntimos. Este derecho fundamental no protege únicamente la información íntima del individuo, sino cualquier información referida a una persona; incluso la información conocida por toda la sociedad. La definición de datos

de carácter personal hace referencia a datos atribuibles a una persona, que la identifiquen, que puedan facilitar la configuración de un perfil, aunque no pertenezcan al reducto de la intimidad de la persona.

Respecto a la legislación europea relativa a este derecho, destacamos que en la **Carta de Derechos Fundamentales de la Unión Europea**, se reconoce este derecho con naturaleza propia e independiente del derecho a la vida privada y del derecho a la intimidad.

Al reconocimiento de este derecho ha contribuido, en parte esencial, la normativa del Consejo de Europa y el Derecho de la Unión Europea. Especial consideración merece el **Convenio 108, de 28 de enero de 1981, del Consejo de Europa**, para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales, los principios de los derechos y libertades. Es de resaltar la **Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995** relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Otro precepto a subrayar, es la **Directiva 2002/58/C del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997**, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, donde se hace mención expresa a la necesidad de respetar en las comunicaciones electrónicas y en el comercio electrónico este derecho fundamental a la protección de datos personales. Esta Directiva, pretende hacer compatible el desarrollo del sector de las telecomunicaciones, que supone el tratamiento y almacenamiento masivo de datos de abonados y usuarios, y la protección de los derechos y las libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas.

Dentro de la legislación sectorial y entrando más en el ámbito que nos afecta, es importante señalar la **Ley Orgánica 2/2006, de 3 de mayo, de Educación**, donde en su disposición adicional vigesimotercera describe claramente el tratamiento de datos personales de los alumnos en las distintas ramas educativas.

Las nuevas tecnologías de la información y las comunicaciones han contribuido de manera inequívoca a evolucionar los sistemas de tratamiento de la información respecto a los medios tradicionales, a través de los cuales, y hasta fechas recientes, se canalizaba la información derivada de la actividad de los centros docentes y de la Administración educativa. Todo centro escolar para poder realizar su función educadora necesita recabar datos de carácter personal, tanto de los alumnos, como de sus empleados públicos –administrativos y docentes-, y sobre ellos gestiona ficheros y/o tratamientos de datos, bien en soporte informático, bien en soporte papel, o bien una parte automatizada y otra manual formando un soporte mixto. A su vez, la Administración educativa trabaja diariamente con datos de carácter personal. Estos datos se refieren fundamentalmente a los indicados anteriormente, pero también pueden hacer referencia a terceras personas que, como consecuencia de su actividad, entran en contacto tanto con los centros docentes como con los propios Órganos administrativos.

En este contexto, tanto la Administración educativa como los propios centros escolares deben adaptarse a las exigencias de la **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)**, habida cuenta que la sociedad actual demanda que las innovaciones tecnológicas se adecuen al respeto a la intimidad y a la protección de este importante derecho.

Debe recordarse que la aplicación de la Ley Orgánica de Protección de Datos se extiende a todos los ficheros de titularidad pública y privada que contengan datos de carácter personal, con las únicas excepciones que la propia Ley establece, por lo que difícilmente puede excusarse el cumplimiento de dicha obligación legal por parte de ningún centro educativo que mantenga y/o realice tratamiento de ficheros con datos de carácter personal.

Otro aspecto importante a tratar en el ámbito educativo, es el uso de las nuevas tecnologías por parte de los alumnos. Es mucha la información, opiniones y propuestas presentadas que tratan este tema en diferentes medios, tanto especializados como no. Si bien, en algunos casos es importante la diferencia de cifras sobre los peligros, acoso y falta de seguridad de los jóvenes en el tratamiento de información en Internet, prácticamente todas las cifras coinciden, entre otros, en los siguientes términos.

- Los escolares navegan por Internet sin ningún control ni medida de seguridad.
- No son conscientes del peligro que supone no aplicar estas medidas.
- Chatean con personas a las que no conocen.
- Facilitan datos personales suyos y en algunos casos de sus familiares, así como otra información del ámbito familiar.
- Cuelgan imágenes de terceras personas sin su consentimiento, así como comentarios y frases que afectan al honor e intimidad de terceros.

Estas circunstancias junto a otras, en algunos casos de mayor trascendencia, son las que han impulsado a las diferentes Agencias y Autoridades de Protección de Datos del Estado, a estudiar, elaborar y proporcionar unos medios que ayuden a los educadores para tratar de divulgar e inculcar el uso responsable de Internet a los alumnos de los centros educativos.

Por último, informar que el objetivo de esta Guía de Contenidos Legales, es facilitar a los educadores una relación de preceptos que, consideramos, puede ayudar al desarrollo de su actividad. La Guía está dividida en varios apartados dependiendo del ámbito territorial, normativa Europea, Estatal (incluida la jurisprudencia), autonómica y sectorial (educativa y menores).

LEGISLACIÓN EUROPEA

- **Carta de los derechos fundamentales de la Unión Europea (arts. 7 y 8).**
- **Tratado de Funcionamiento de la Unión Europea (art. 16).**

  El título II, artículo 16, reconoce el derecho de toda persona a la protección de datos de carácter personal.
- **Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.**

  Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- **Directiva 1999/93/CE, del Parlamento Europeo y del Consejo de 13 de diciembre de 1999.**

  Por la que se establece un marco comunitario para la firma electrónica.
- **Directiva 2000/31/CE, del Parlamento Europeo y del Consejo de 8 de junio de 2000.**

  Relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.
- **Directiva 2002/20/CE, del Parlamento Europeo y del Consejo de 7 de marzo de 2002.**

  Relativa a la autorización de redes y servicios de comunicaciones electrónicas.
- **Directiva 2002/21/CE, del Parlamento Europeo y del Consejo de 7 de marzo de 2002.**

  Relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.
- **Directiva 2002/58/CE, del Parlamento Europeo y del Consejo de 12 de julio de 2002**.

  Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.
- **Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006.**

  Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.
- **Directiva 2009/136/CE, del Parlamento Europeo y del Consejo de 25 de noviembre de 2009.**
  Por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.
- **Reglamento (CE) nº 45/2001, del Parlamento Europeo y del Consejo de 18 de diciembre de 2000.**

  Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.
- **Decisión Marco 2008/977/JAI, del Consejo de 27 de noviembre de 2008**.
  Relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

LEGISLACIÓN ESTATAL

- **Constitución Española de 27 de diciembre de 1978.**
- **Ley Orgánica 15/1999, de 13 de diciembre,** de Protección de Datos de Carácter Personal, modificada por la **Disposición Adicional Quincuagésima Sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.**
- **Real Decreto 1720/2007, de 21 de diciembre,** por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- **Real Decreto 3/2010, de 8 de enero,** por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (Disposición adicional cuarta. Modificación del Reglamento de desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre).
- **Real Decreto 428/1993, de 20 de marzo,** por el que se aprueba el estatuto de la Agencia de Protección de Datos.

INSTRUCCIONES

- **Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos,** sobre el tratamiento de datos personales con fines de vigilancia a través de sistema de cámaras o videocámaras.
- **Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos,** sobre publicación de sus Resoluciones.
- **Instrucción 2/1995, de 4 de mayo, de la Agencia Española de Protección de Datos,** sobre garantía de los datos personales recabados en la contratación de seguro de vida de forma conjunta con un préstamo hipotecario o personal.
- **Instrucción 1/1996, de 1 de marzo, de la Agencia Española de Protección de Datos,** sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a edificios.
- **Instrucción 2/1996, de 1 de marzo, de la Agencia Española de Protección de Datos,** sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.

LEGISLACIÓN AUTONÓMICA

AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID

- **Ley 8/2001, de 13 de julio,** de Protección de Datos de Carácter Personal en la Comunidad de Madrid.
- **Decreto 40/2004, de 18 de marzo,** por el que se aprueba el Estatuto de la APDCM.
- **Decreto 99/2002, de 13 de junio,** de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales.
- **Decreto 67/2003, de 22 de mayo,** por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.
- **Resolución de 9 de enero de 2007,** del Director de la APDCM, por la que se establecen los modelos de impresos y los medios por los que debe procederse a la notificación de inscripciones de creación, modificación o supresión de ficheros, al Registro de Ficheros de Datos Personales.
- **Instrucción 1/2007, de 16 de mayo,** de la APDCM, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid.
- **Instrucción 1/2009, de 17 de diciembre de 2009**, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales de los recién nacidos en los centros asistenciales que integran la red sanitaria única de utilización pública de la Comunidad de Madrid.
- **Instrucción 2/2009, de 21 de diciembre de 2009,** de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales en la emisión de justificantes médicos.
- **Tratamiento de datos personales en la emisión de justificantes médicos.** NOTA ACLARATORIA
- **Recomendación 1/2004, de 14 de abril,** de la APDCM, sobre la utilización y tratamiento de datos del padrón municipal por los Ayuntamientos de esta Comunidad Autónoma.
- **Recomendación 2/2004, de 30 de julio,** de la APDCM, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas.
- **Recomendación 1/2005, de 5 de agosto,** de la APDCM, sobre Archivo, Uso y Custodia de la Documentación que compone la Historia Social no informatizada por parte de los Centros Públicos de Servicios Sociales de la Comunidad de Madrid.

LEGISLACIÓN AUTONÓMICA

AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID

- **Recomendación 1/2006, de 3 de abril,** de la APDCM, sobre cesiones de datos de empleados públicos de la Comunidad de Madrid a las secciones sindicales, comités de empresa y juntas de personal.
- **Recomendación 1/2008, de 14 de abril,** de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el Tratamiento de datos personales en los Servicios Sociales de la Administración de la Comunidad de Madrid y en los Servicios Sociales de los Entes Locales de la Comunidad de Madrid.
- **Recomendación 2/2008, de 25 de abril,** de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios webs institucionales y en otros medios electrónicos y telemáticos.
- **Recomendación 3/2008, de 30 de abril,** de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre tratamiento de datos de carácter personal en servicios de administración electrónica.

LEGISLACIÓN AUTONÓMICA

AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS

- **Estatuto de Autonomía de Cataluña: artículos 31, 156 y 182.3.**
- **Ley 32/2010, de 1 de octubre,** de la Autoridad Catalana de Protección de Datos.
- **Decreto 48/2003, de 20 de febrero,** por el que se aprueba el Estatuto de la Autoridad Catalana de Protección de Datos.
- **Instrucción 1/2009, de 10 de febrero,** sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.
- **Recomendación 1/2008,** sobre la difusión de información que contenga datos de carácter personal a través de Internet.
- **Recomendación 1/2010,** sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña.
- **Recomendación 1/2011,** sobre la creación, modificación y supresión de ficheros de datos de carácter personal de titularidad pública.
- **Resolución de 4 de abril de 2011,** por la que se aprueba la modificación de los soportes normalizados para formalizar las inscripciones de los ficheros en el Registro de Protección de Datos de Cataluña.

LEGISLACIÓN AUTONÓMICA

AGENCIA VASCA DE PROTECCIÓN DE DATOS

- **Ley 2/2004, de 25 de febrero,** de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.
- **Decreto 308/2005, de 18 de octubre,** por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos.
- **Decreto 309/2005, de 18 de octubre,** por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos.
- **Resolución de 21 de julio de 2005,** del Director de la Agencia Vasca de Protección de Datos, por la que se establecen los modelos normalizados y los medios por los que debe procederse a la solicitud de las inscripciones de creación, modificación o supresión de ficheros en el Registro de Protección de Datos de la Agencia Vasca de Protección de Datos.
- **Resolución de 28 de noviembre de 2005,** del Director de la Agencia Vasca de Protección de Datos, por la que se desarrolla la estructura orgánica de la Agencia Vasca de Protección de Datos.

JURISPRUDENCIA

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

- **Sentencia de 24 de noviembre de 2011** que declara la aplicación directa del artículo 7 f) de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

JURISPRUDENCIA TRIBUNAL CONSTITUCIONAL

- **Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional.**

  Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

JURISPRUDENCIA TRIBUNAL SUPREMO

- **Sentencia de 2 de julio de 2007 de la Sala de lo Contencioso-Administrativo del Tribunal Supremo,** que legitima el uso de la huella para el control horario de los trabajadores.
- **Sentencia de 26 de septiembre de 2007, de la Sala de lo Social del Tribunal Supremo,** para la unificación de la doctrina sobre el acceso al correo electrónico del trabajador por parte del empresario.
- **Sentencia de 6 de octubre de 2009, de la Sala de lo Contencioso-Administrativo del Tribunal Supremo,** que deniega la legitimación del denunciante para impugnar en vía judicial las resoluciones de la AEPD.
- **Sentencia de 26 de enero de 2010, de la Sala de lo Contencioso-Administrativo del Tribunal Supremo,** sobre el ejercicio de forma desleal del derecho de acceso.
- **Sentencia de 15 de julio de 2010, de la Sala de lo Contencioso-Administrativo del Tribunal Supremo,** que anula varios artículos del Reglamento de la LOPD.

JURISPRUDENCIA

JURISPRUDENCIA AUDIENCIA NACIONAL

- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 29 de octubre de 2009,** sobre publicación de los datos de deportistas sancionados por dopaje en una página web.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 25 de febrero de 2010,** sobre la vulneración de las medidas de seguridad y del deber de secreto.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 20 de mayo de 2010,** sobre tratamiento de datos personales y cesión de los mismos sin consentimiento.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 27 de mayo de 2010,** sobre tratamiento de imágenes sin cumplir la LOPD.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 29 de octubre de 2010,** sobre un fichero que estaba "colgado" en Internet al cuál se podría acceder usando el programa "e-mule".
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 12 de noviembre de 2010,** sobre el uso de los datos del menor para una finalidad distinta de la que motivó su entrega.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 3 de enero de 2011,** sobre cesión de datos personales sin consentimiento del afectado.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 1 de abril de 2011,** sobre publicación de datos de menores en una página web.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 25 de marzo de 2011,** sobre documentos judiciales aparecidos en la basura.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 20 de mayo de 2011,** sobre la instalación de cámaras en la vía pública.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 16 de junio de 2011,** sobre el ejercicio del derecho de oposición en relación con la publicación de las actas de los Plenos de las Corporaciones Locales.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 30 de junio de 2011,** sobre el contenido del ejercicio del derecho de acceso.
- **Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 30 de junio de 2011,** sobre el ejercicio del derecho de cancelación ante un fichero de la Guardia Civil.

DATOS DE CONTACTO

INFORMACIÓN DE CONTACTO DE LAS AGENCIAS O AUTORIDADES DE PROTECCIÓN DE DATOS EN ESPAÑA

Agencia Española de Protección de Datos (AEPD)

Sitio web principal **www.agpd.es**

Calle Jorge Juan, 6

28001 Madrid.

Teléfono: + (34) 901 100 099

+ (34) 912 663 517

Correo electrónico: ciudadano@agpd.es

Agencia de Protección de Datos de la Comunidad de Madrid (APDCM)

Sitio web principal **www.apdcm.es**, específicamente para jóvenes el apartado "Jóvenes e Internet"

Agencia de Protección de Datos de la Comunidad de Madrid (APDCM)

Gran Vía 43, plantas 3 y 10

28013 Madrid

Teléfono: +(34) 917 209 738

Fax: +(34) 917 209 745

Correo electrónico: apdcm@madrid.org

apdcat
Autoritat Catalana de Protecció de Dades

Autoridad Catalana de Protección de Datos (ACPD)

Sitio web principal **www.apd.cat.** Apartado del sitio web "Privacidad para jóvenes":
http://www.apd.cat/es/contingut.php?cont_id=305&cat_id=251
Autoridad Catalana de Protección de Datos (APDCAT)
Calle Llacuna, 166, 7ª pl.
08018 Barcelona
Teléfono: + (34) 935 527 800
Fax: + (34) 935 527 830
Correo electrónico: apdcat@gencat.cat

Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

Agencia Vasca de Protección de Datos (AVPD)

Sitio web principal **www.avpd.es**
Micrositio con programas para Jóvenes y la Comunidad Educativa:
www.kontuzdatos.info
Agencia Vasca de Protección de Datos (AVPD)
Calle Beato Tomás de Zumarraga 71, 3º
01008 Vitoria - Gasteiz
Teléfono: + (34) 945 016 230
Fax: + (34) 945 016 231
Correo electrónico: avpd@avpd.es

En caso de necesitar más información sobre nuestras actividades para la sensibilización y capacitación para la protección de la privacidad, no dude en enviarnos un e-mail a **avpd@avpd.es**, indicando en el asunto del mensaje Sensibilización y Capacitación.

REGISTRARSE

ENTRAR

DARSE DE BAJA

PROTEGER TU PRIVACIDAD
Y CONTROLAR TUS DATOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Agencia de Protección de Datos de la Comunidad de Madrid

apdcat
Autoritat Catalana de Protecció de Dades

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

01

Los Datos Personales y la Privacidad.

Nuestros Derechos y Obligaciones.

Principales Riesgos en la Red.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ÍNDICE

I. OBJETIVOS

- Conocer qué es un dato personal y algunos ejemplos de tipos y categorías de datos personales.
- Conocer cuándo, cómo y qué datos personales se deben proporcionar a quienes los piden.
- Valorar la importancia de proteger nuestros datos personales como medio para salvaguardar nuestra privacidad.
- Conocer los derechos que la ley nos otorga para proteger nuestros datos personales.
- Conocer algunas de las situaciones de riesgo más frecuentes que pueden poner en riesgo nuestra privacidad en Internet.

II. CONCEPTOS

1. LOS DATOS PERSONALES Y LA PRIVACIDAD

a) ¿Qué es un dato de carácter personal?

La Ley Orgánica 5/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) establece que un dato de carácter **personal es cualquier información concerniente a personas físicas identificadas o identificables.**

Persona identificable es aquella cuya identidad puede determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

b) ¿Cuáles son los datos personales?

Entre muchas otras, se pueden mencionar las siguientes categorías:

- El nombre y los apellidos.
- El domicilio.
- El número de DNI.
- El número de teléfono.
- El número de la Seguridad Social.

- La imagen (videos, fotografías,...).
- La voz.
- Datos de salud: enfermedades, pruebas médicas, diagnósticos, tratamientos,...
- Datos financieros: cuentas corrientes, tarjetas de crédito,...
- Datos laborales: salario, categoría profesional, afiliación sindical,...
- Datos biométricos: huellas dactilares, iris, huella palmar,...
- La información genética.
- Las direcciones de correo electrónico.
- Las direcciones IP.
- La matrícula de los vehículos.

c) ¿Por qué es importante proteger los datos?

- Porque dicen quién eres.
- Porque dicen cómo eres.
- Porque pueden revelar una forma de contactarte.
- Porque pueden sugerir tu procedencia u orígenes.
- Porque pueden revelar tus aficiones, preferencias y hábitos de consumo.
- Porque pueden revelar información de tu entorno o familia.
- Y, por ello, pueden ser utilizados para finalidades que no has previsto y que pueden perjudicarte o resultarte desagradables.

d) Hay algunas categorías particulares de datos que gozan de una especial protección. ¿Cuáles son?

Son los datos que hacen referencia a los orígenes raciales o étnicos, opiniones políticas, creencias religiosas o filosóficas, afiliación a un sindicato o los datos relativos a la salud o la vida sexual.

En todos estos casos, para su tratamiento o cesión se requiere el consentimiento expreso - y en algunos casos incluso por escrito - de los afectados y, además, los ficheros donde se registren dichos datos deberán incorporar unas medidas de seguridad del nivel más alto de los tres legalmente previstos (básico, medio y alto).

e) ¿Y los datos relativos a los menores?

El tratamiento de los datos de los menores de 14 años requerirá el consentimiento de los padres o tutores.

f) ¿Qué debemos tener en cuenta cuando nos piden los datos?

Todo tratamiento de datos personales comienza con su recogida, que puede realizarse de muy diversas formas:

- Verbalmente: Por ejemplo, en la contratación telefónica o cuando damos nuestros datos en un comercio.
- Por escrito: Cuando rellenamos impresos de admisión o de alta.
- Usando formularios online: Por ejemplo, cuando nos damos de alta en una red social.
- Mediante la captación de nuestras imágenes por cámaras de vigilancia o a través de una webcam.

En estos casos, quien recoge los datos - llamado "responsable del fichero o del tratamiento"-, debe cumplir con dos obligaciones básicas:

- Informarnos de la finalidad de su recogida (para qué nos los piden) y
- solicitar nuestro consentimiento, salvo que la ley autorice u obligue a entregar los datos.

› ¿Qué otras cuestiones son importantes para proteger nuestros datos personales?

Calidad de los datos.

› Sólo podrán solicitarnos nuestros datos para ser tratados si son "adecuados, pertinentes y no excesivos" en relación con las finalidades para los que se piden. (proporcionalidad).

› No podrán usarse para otros fines que sean diferentes de aquellos para los que los datos hayan sido recogidos.

› Los datos deberán ser exactos y estar actualizados de forma que reflejen con veracidad la situación real de la persona afectada.

› Está prohibida su recogida por medios fraudulentos, desleales o ilícitos.

Seguridad de los datos.

› El responsable del fichero deberá garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida o acceso no autorizado, para lo que deberá adaptar las medidas técnicas y organizativas necesarias.

› Según sea el tipo de datos, existen diferentes niveles de medidas de seguridad (básico, medio y alto) que deberán establecerse en el llamado "documento de seguridad".

› La pérdida o el acceso no autorizado a los datos personales constituyen las llamadas "brechas o fugas de seguridad".

Deber de secreto.

› Todas las personas que tengan acceso a datos de carácter personal están obligadas a guardar secreto sobre los mismos.

› El secreto es esencial para garantizar el derecho fundamental a la protección de datos.

› Por ejemplo, las personas que legalmente tienen acceso al expediente psicopedagógico de un menor, no pueden revelar datos del mismo a otros padres.

Consentimiento.

› Con carácter general, siempre que pidan nuestros datos, o vayan a ser objeto de tratamiento o de cesión, deberán pedirnos el consentimiento.

› Pero hay determinados casos en que no se requiere el consentimiento, sin que por ello se vea afectado nuestro derecho fundamental a la protección de datos personales. Así ocurre cuando lo autoriza una Ley, o su tratamiento sea necesario para el ejercicio de las funciones propias de las Administraciones Públicas, o se produzca en el ámbito de una relación laboral o contractual, o se trate de documentos para ser aportados en un proceso judicial, o cuando exista un "interés legítimo" y no se vulneren los derechos del interesado (por ejemplo, el tratamiento de datos que se produce para la expedición de un título académico).

2. NUESTROS DERECHOS Y OBLIGACIONES.

a) Mis derechos:

¿Qué es el derecho a la protección de datos de carácter personal?

Es un derecho fundamental que reconoce a las personas la facultad para controlar, disponer y decidir sobre sus datos personales.

¿Cuáles son mis derechos para poder proteger mejor mis datos?

Derecho de información.

Es el derecho que tengo a que, siempre que se vayan a registrar y tratar mis datos personales, me informen previamente:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de su recogida (para qué nos los piden) y de sus destinatarios (para quién).
- De las consecuencias de la obtención de los datos o de la negativa a darlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento.

Cuando se utilicen cuestionarios u otros impresos (incluso si son en formato electrónico) para la recogida, figurará en ellos, en forma claramente legible, la referida información.

Esta información estará disponible en la web de la organización que recoge los datos (responsable del tratamiento) en la llamada "política de privacidad", o "cláusula de privacidad".

Derecho de acceso.

Es el derecho a obtener información sobre si mis datos personales están siendo tratados y, si es así, qué datos están siendo tratados y con qué finalidad, así como toda la información disponible sobre el origen de dichos datos.

Derecho de rectificación.

Es el derecho a que mis datos personales se modifiquen cuando sean inexactos o incompletos.

Derecho de oposición.

Es el derecho a que no se lleve a cabo el tratamiento de mis datos personales, o se cese en el mismo, por existir un motivo legítimo y fundado que lo justifique y siempre que una Ley no disponga lo contrario.

Derecho de cancelación.

Es el derecho a que mis datos personales se supriman cuando resulten inadecuados o excesivos. Por ejemplo, podemos solicitar a una red social que suprima nuestros datos cuando nos demos de baja en su servicio.

1. No han respetado mis derechos. ¿Qué puedo hacer?

Primero tengo que reclamar mis derechos dirigiéndome al responsable del fichero o tratamiento de mis datos personales. Y sólo en el caso de que mi reclamación no haya sido atendida por dicho responsable, podré dirigirme a la Agencia Española de Protección de Datos mediante el procedimiento de Tutela de Derechos. Los modelos para solicitar la tutela de la Agencia Española de Protección de Datos están disponibles en la web de la AEPD (www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos).

b) Mis deberes.

La idea básica es que debemos hacer un uso responsable y seguro de los datos personales, especialmente en el entorno de Internet (redes sociales, chats, servicios de mensajería instantánea, etc.), lo que significa:

- Que hay que **ser precavido y usar el sentido común** cada vez que nos soliciten tanto nuestros datos personales como el de otras personas (familiares o amigos). Sabed que no os pueden pedir información sobre la actividad profesional o información económica de los padres, sin el consentimiento de ellos.

- Que debéis **informaros bien de a quién dais vuestros datos y para qué**, y en caso de duda preguntad a vuestros padres, profesores o personas de confianza.
- Que se debe **pedir permiso a la persona afectada** cada vez que subimos a Internet una foto o cualquier documento que contenga sus datos personales.
- Que se deben **adoptar unas elementales medidas de seguridad** para evitar que alguien pueda apropiarse indebidamente de nuestros datos, como configurar nuestra privacidad en los perfiles de las redes sociales o establecer contraseñas fuertes y seguras.
- Que debemos **ser respetuosos con los demás** y no hacer un uso de Internet que pueda perjudicar a los demás, como, por ejemplo, haciéndose pasar por otro, suplantando su identidad.

3. PRINCIPALES RIESGOS PARA LA PRIVACIDAD EN INTERNET. CONSEJOS PRÁCTICOS.

a) En las redes sociales.

- Si no se limita el acceso a nuestros datos, la información estará disponible para cualquiera, incluidos los buscadores. Es fundamental, pues, que configuremos bien la privacidad de nuestro perfil en una red social.
- Publicar información o imágenes de otros sin su consentimiento da lugar a que se violen los derechos de terceros.
- El robo o la suplantación de identidad es otro de los riesgos si no tomamos ciertas precauciones, especialmente en la configuración y uso de las contraseñas. Una contraseña segura sería la que incluye números, mayúsculas y minúsculas y símbolos.
- La publicación de excesiva información personal en un perfil puede permitir identificarnos e incluso localizar nuestra ubicación física.

b) En los correos electrónicos (e-mails).

› El correo electrónico (e-mail) es el cauce más habitual por el que se difunden virus, gusanos y malware en general.

› La dirección de correo es también la forma más común de registrar la "identidad" de una persona en Internet y puede utilizarse como base para acumular información sobre ella. Por ejemplo, no debemos incluir en la dirección información que revele el año de nacimiento o que dé a entender los años que tenemos.

› Cuando remitamos correos a múltiples destinatarios debemos tener un especial cuidado para garantizar su confidencialidad utilizando el campo "Con Copia Oculta" (CCO), para evitar que las direcciones de todos los destinatarios queden a la vista. Hay que tener en cuenta que el que nosotros tengamos esas direcciones no significa que puedan acceder a ellas todos los demás que reciben nuestro mensaje.

c) En los servicios de mensajería instantánea y chats.

› Las conversaciones que se mantienen en las salas de chat (lugares virtuales en los que los participantes escriben mensajes que aparecen en los equipos del resto de usuarios al instante) están al alcance de cualquier usuario que esté participando en esa misma sesión.

› En los chats es muy difícil conocer la identidad real de los usuarios que contactan a través de estos servicios.

› Hay que evitar, pues, ofrecer demasiada información que pueda identificarnos y localizarnos de forma precisa, incluso físicamente.

d) En los buscadores.

› Los buscadores pueden indexar la información contenida en páginas web y otros servicios de Internet, como redes sociales, otorgándoles una difusión masiva y universal. Pueden incluso guardar en la memoria caché el contenido textual de una página que ya no esté accesible en Internet.

› Para la prestación de sus servicios, los buscadores manejan un amplio abanico de datos: direcciones IP, información que registran las cookies o la información que el propio usuario aporta. Con el tratamiento de esos datos pueden realizarse perfiles de hábitos de los usuarios.

e) En los smartphones (geolocalización).

› Un dispositivo móvil inteligente o *smartphone* está íntimamente relacionado con un individuo específico. Normalmente estos dispositivos se llevan siempre encima, lo que permite a los proveedores de servicios de geolocalización tener una visión muy cercana de los hábitos y patrones de movimiento del titular de ese teléfono.

› Con la ayuda de las tecnologías de geolocalización (GPS y puntos con acceso *wifi*) estos dispositivos móviles pueden permitir el seguimiento de los mismos y, dado que están particularmente vinculados a sus propietarios, ofrecer una visión muy íntima de la vida privada relacionada con su situación geográfica y hábitos de desplazamiento.

› Uno de los riesgos de la utilización de estos dispositivos es que los propietarios no son conscientes de que pueden estar transmitiendo su ubicación y a quién.

4. PARA SABER MÁS.

› El derecho fundamental a la protección de de datos. Guía para el ciudadano – AEPD:

› https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf

- Recomendaciones a usuarios de Internet – AEPD:
- https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_recomendaciones_internet_052009.pdf

- Derechos de los niños y niñas y deberes de los padres y madres – AEPD:
- http://www.agpd.es/portalwebAGPD/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf

- Guía de Menores en Internet para Padres y Madres – INTECO:
- http://cert.inteco.es/extfrontinteco/img/File/intecocert/Proteccion/menores/guiapadresymadres.pdf

Seguridad

- Proyecto Intypedia. Vídeos sobre seguridad de la información – Universidad Politécnica de Madrid:
- http://www.intypedia.com/
- Navegación segura – INTECO
- http://www.navegacionsegura.net/
- Vidente. (subtítulos en inglés)
- http://www.youtube.com/watch?v=F7pYHN9iC9I

III. ACTIVIDADES

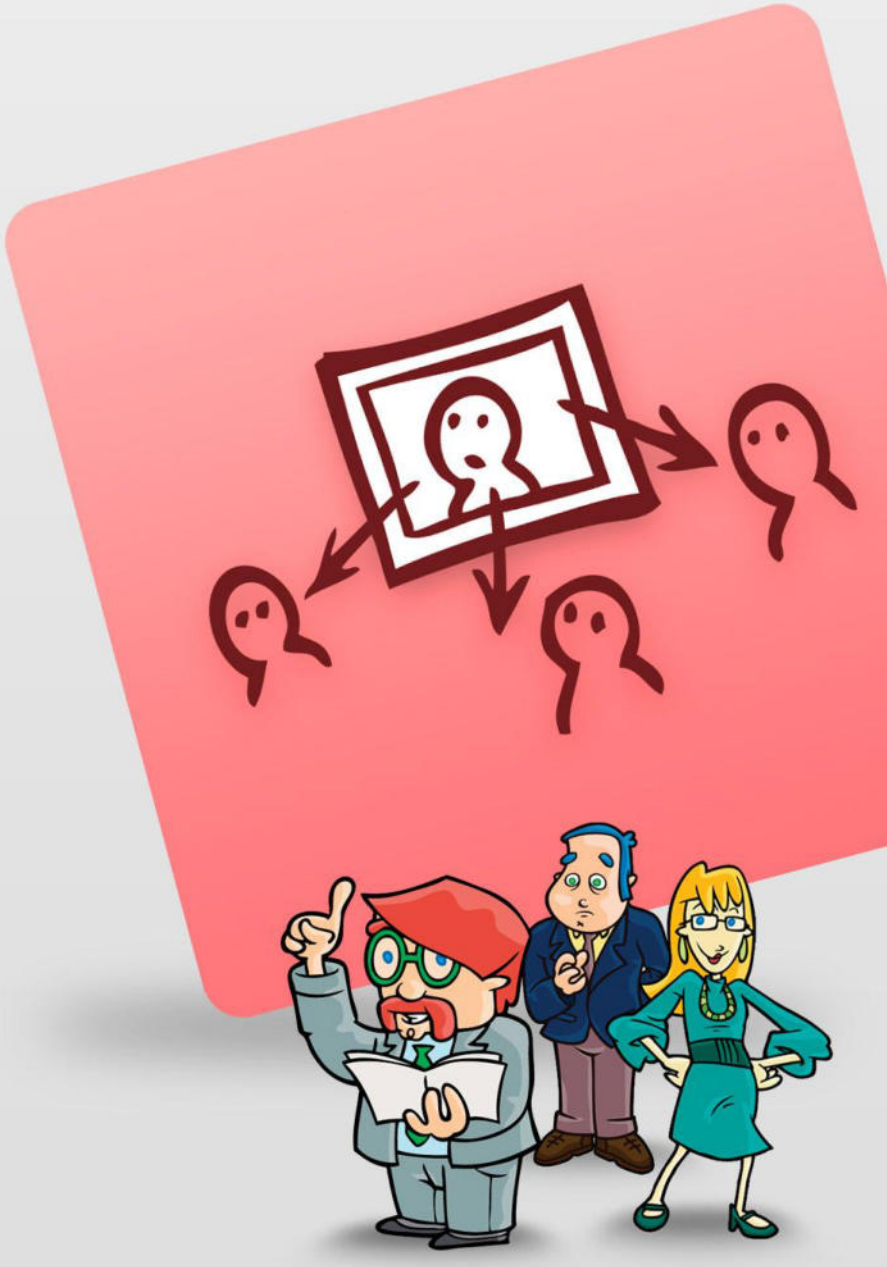
El educador propone el siguiente test a los alumnos. Pueden contestarlo en pequeño grupo:

1. Una imagen grabada ¿es un dato personal?
2. Di tres datos personales.
3. Con respecto a la protección de datos, ¿es necesario mi consentimiento para que los puedan utilizar? ¿Y si soy menor de 14 años?
4. ¿El consentimiento para el tratamiento de mis datos personales lo puedo dar verbalmente?
5. ¿Tengo derecho a conocer e incluso eliminar mis datos personales de un fichero de datos?
6. Para reclamar la rectificación de mis datos personales, ¿me tengo que dirigir directamente al responsable del fichero o bien a la Agencia Española de Protección de Datos?
7. ¿Es aconsejable configurar bien el apartado de privacidad en nuestro perfil de una red social?
8. ¿Es posible conocer mi "identidad" a través de mi cuenta de correo electrónico?

02

Identidad Digital y reputación Online.

Redes sociales.



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ÍNDICE

I. OBJETIVOS

Concienciar del uso adecuado de los servicios que componen el entorno Web 2.0 (buscadores, plataformas colaborativas, redes sociales, imágenes en la red: webcams, fotografías, videos en la red, etc.) y sus consecuencias. Al utilizar estos servicios el usuario muestra atributos de la personalidad que escapan de su control debido a la estructura de participación de las nuevas tecnologías. Por tanto, dependiendo de su utilización construiremos una identidad "digital" que se proyecta en los demás construyendo así una determinada reputación.

II. CONCEPTOS

1. EL WEB 2.0: NUEVO PARADIGMA DE INTERNET.

A diferencia de sitios web tradicionales, donde los usuarios se limitan a la observación pasiva de los contenidos, el término Web 2.0 está asociado a servicios que fomentan la interoperabilidad, el diseño centrado en el usuario y la colaboración. Los servicios del entorno Web 2.0 son canales multidireccionales que ofrecen nuevas posibilidades de colaboración, expresión y participación.

La Web 2.0 supone el nacimiento de un universo social poblado de comunidades que pueden ir de lo más cercano a cualquier tipo de agrupación horizontal - grupos profesionales o sociales -, vertical, - espacios de trabajo en grupo -, e incluso "informal" sin límites de espacio o tiempo. Posibilita a los usuarios interactuar y colaborar entre sí como creadores de contenido generado por usuarios en una comunidad virtual. Ejemplos de la Web 2.0 son las comunidades Web, los servicios Web, las aplicaciones Web, los servicios de red social, los servicios de alojamiento de videos, las wikis, blogs, etc.

a) Identidad digital y reputación online.

Cuando el usuario utiliza los servicios de la Web 2.0 va creando respecto de su actividad un conjunto de atribuciones que conforman su identidad digital. Las Tecnologías de la Comunicación y la Información (TIC) consiguen crear una **"identidad expandida"** en la mayoría de sus usuarios: potencian sus habilidades y les permiten estar en contacto con otros usuarios manteniendo diferentes niveles de relación, intimidad, compromiso, etc.

Hasta ahora la identidad la conformaban el nombre y apellidos, un número de identificación y, a lo sumo, un domicilio físico, pudiendo denominarse identidad tradicional o analógica.

La identidad digital será aquella información sobre un individuo o una organización expuesta en Internet (datos personales, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona.

Para entender verdaderamente en qué consiste la **identidad digital** resultan especialmente clarificadoras sus características definidas por la Organización para la Cooperación y Desarrollo Económicos (OCDE):

- **Es esencialmente social**. A medida que el individuo proyecta su personalidad en la Red, sus vecinos digitales lo caracterizan y reconocen de forma efectiva, incluso en ocasiones en que no se ha producido una verificación presencial de la identidad.
- **Es subjetiva**. Tanto la percepción del "yo" como del "nosotros" están basadas en la experiencia que personas diferentes construyen y que les permiten reconocerse.
- **Es valiosa.** La actividad de los sujetos genera capital informacional que puede ser empleado para establecer relaciones personalizadas y para tomar decisiones en las relaciones con las personas, con un mayor grado de confianza.
- **Es referencial**. De hecho, una identidad no es una persona o un objeto, sino una referencia a dicha persona u objeto.
- **Es compuesta**. Mientras que algunas informaciones son suministradas de forma voluntaria por los propios usuarios, otras informaciones sobre los mismos son construidas por terceros, sin la participación del sujeto en cuestión.

- **Produce consecuencias.** La divulgación de la información en ocasiones puede generar efectos y, en otros casos, es la no divulgación la que constituye una amenaza por sí misma.
- **Es dinámica.** Se encuentra en cambio y modificación permanente. Se debe ver como un flujo de informaciones.
- **Es contextual.** La divulgación de la información puede generar un impacto negativo empleada en un contexto erróneo, o sencillamente ser irrelevante. Mantener las identidades segregadas entre sí permite tener más autonomía.

Si el **uso** de los servicios Web 2.0 conforma la identidad digital, el **modo** en que se utilicen conformará la **Reputación Online**. Es decir, el modo en que se utilicen dichos servicios tendrá consecuencias que afectarán directa e indirectamente al usuario, teniendo especial sensibilidad cuando la reputación se construye respecto de menores de edad, por ser un colectivo de especial vulnerabilidad.

La **Reputación Online** no es tanto lineal sino acumulativa. Es decir, no pierde o gana solidez en el tiempo. Cada acción en la red deja rastros fácilmente detectables que pueden almacenarse y reutilizarse hasta el infinito. Así, cualquier persona puede dar información y opiniones en el entorno Web 2.0, que a su vez es susceptible de ser localizada, indexada, copiada y enlazada, alcanzando una elevada difusión. Lo que dificulta enormemente el control sobre la propia información, hasta casi hacerlo imposible.

Los elementos determinantes de la reputación Online se pueden clasificar en actuaciones llevadas a cabo por el propio sujeto (el modo en que un usuario se muestra, trasladando aspectos de su vivencia personal al entorno Web 2.0, siendo un elemento importante en cuanto a cómo nos ven los demás); la información generada por servicios de Internet (la utilización de buscadores, la navegación en determinadas páginas, etc., deja un registro que asociado a un usuario crea un perfil determinado, por ejemplo, un aficionado del deporte visitará páginas Web de clubes deportivos, de periodismo deportivo, comprará entradas para dichos eventos, etc., toda esa actividad creará un perfil) y, finalmente, otro factor serán las actuaciones emprendidas en el ámbito relacional del usuario (por ejemplo, en redes sociales basadas en el seguimiento de usuarios, de sus comentarios, las veces que se hace clic en "me gusta", los amigos online que se hagan, etc.)

Por eso podemos afirmar que todos tenemos una reputación online, en mayor o menor medida, siendo muy importante la gestión que hagamos de ella sobre todo teniendo muy presente el concepto y la importancia de la Privacidad.

b) Privacidad: parámetro de la identidad digital.

Según la Real Academia de la Lengua Española, se considera privacidad al "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".

En el ámbito concreto del entorno **Web 2.0**, la privacidad se refiere al control de quiénes son las personas que pueden tener acceso a la información que posee o que se refiere a un determinado usuario que se conecta a la Red. Es un término amplio, formado por aquella información que tomada por sí misma puede no ser relevante, pero que analizada en un momento o contexto concretos puede llevarnos a formar un perfil de una persona bastante acertado.

La privacidad de los usuarios se puede ver comprometida en muchos momentos de la experiencia online, ya sea en la utilización de buscadores, de redes sociales, de servicios de plataformas de videos online, de suscripciones a servicios publicitarios, de compras en la red, etc.

c) Buscadores, páginas Web, cookies y privacidad.

Los buscadores de Internet son servicios de provisión de búsqueda de contenidos o, dicho de otro modo, es un enorme sistema informático programado para rastrear la red, organizando y registrando su contenido, de tal forma que los usuarios pueden encontrar resultados de su interés al realizar búsquedas con ciertas palabras clave.

Al utilizarlos aportamos diversa información asociada que conduce a la creación de perfiles de usuarios, muchas veces sin conocimiento y, por tanto, sin consentimiento del mismo. Esta información va desde la propia consulta realizada, almacenada en el registro del buscador en forma de URL, la dirección IP, la fecha y hora exacta en que se realiza la búsqueda, las preferencias, el navegador, el sistema operativo, el idioma, etc., hasta los anuncios en que se ha mostrado interés a través de los clic que se hayan hecho.

Esta información es fácilmente asociada por los responsables de los buscadores y páginas Web a través de las cookies que dichos servicios Web instalan en el dispositivo que utilice la red Internet. **Las cookies son archivos que se crean cuando el navegador del usuario carga alguna página Web en particular y que identifican unívocamente dicho navegador ante el sitio Web que se visita o el de terceros**. Se utilizan para reconocer las actividades del usuario en un sitio o red de sitios Web.

También es importante destacar la correlación de servicios "sugerida" por los prestadores de servicios Web, porque también puede comprometer la privacidad del usuario sin su consentimiento. La correlación entre servicios no es siempre necesaria para la utilización independiente de éstos, por ejemplo, en ocasiones los prestadores de servicios responsables de los buscadores "sugieren" al usuario el registro o alta de un determinado perfil para "mejorar" la experiencia de usuario. Cuando el usuario acepta la correlación entre su cuenta de correo electrónico y la utilización del buscador se añaden más datos y se facilita aún más la creación de un perfil de usuario de servicios Web, pudiendo ser amenazada la privacidad del usuario. Por eso es importante informarse adecuadamente de las consecuencias y finalidades de la correlación entre servicios y sobre todo de su necesidad, pues debe tenerse en cuenta que en la mayoría de los casos se puede utilizar un servicio de forma independiente de otro.

Una adecuada información y una gestión responsable de las cookies puede proteger en mayor medida la privacidad del usuario. Todos los navegadores tienen opciones de configuración de las cookies. Asimismo, las reformas legislativas llevadas a cabo obligan a los responsables de las páginas Web, buscadores, etc., a informar de la utilización de las mismas y a posibilitar al usuario su aceptación o rechazo.

d) Redes Sociales y privacidad.

Las redes sociales en Internet son tan atractivas porque son capaces de superar con enorme facilidad parámetros que condicionan al ser humano: espacio y tiempo. Las relaciones sociales tradicionales tienen estos límites. El lapso del tiempo y la lejanía mitigan y llegan a hacer desaparecer relaciones personales que se entablan en principio como eternas, pero

que poco a poco van enfriándose. Los amigos desaparecen, no vuelve a tenerse noticias de ellos. El tiempo y la distancia lo borran todo. Sin embargo, las redes sociales en Internet permiten recuperar y mantener relaciones que se consideraban finalizadas. Incluso a través de las redes sociales pueden entablarse relaciones que de otro modo se harían enormemente complejas.

Son un ejemplo más del entorno Web 2.0 o Web colaborativa, en la que Internet deja de ser un foco de información para convertirse en un espacio virtual retroalimentado en el que los usuarios consumen, pero también aportan información.

Posibles riesgos de las Redes Sociales en Internet. ¿Cómo pueden verse afectados los datos personales de los usuarios?

El primer momento crítico para la privacidad del usuario se encuentra en la fase inicial de registro del usuario, cuando éste proporciona la información personal necesaria para poder operar en la red social:

- **Que el tipo de datos solicitados en el formulario de registro, aunque no obligatorios, sean excesivos.**
  - Con frecuencia, las redes sociales solicitan a los nuevos usuarios datos relativos a su ideología política, orientación sexual y preferencia religiosa. Deben considerarse las implicaciones que puede conllevar para su vida y las personas de su entorno, ya que estos datos serán visibles por sus contactos y, dependiendo de la configuración, por todos los usuarios de la red. **Será necesario por tanto controlar el grado y la trascendencia de los datos publicados para que no resulten excesivos.**

- **Que el grado de publicidad del perfil de usuario sea demasiado elevado.**
    - Es en el momento inicial del registro como usuario cuando éste debe configurar debidamente el grado de publicidad de su perfil, de tal forma que **determine desde el comienzo quiénes podrán tener acceso a toda la información que el usuario publique**. La mayoría de las redes sociales tienen activado por defecto el mayor grado de publicidad, lo que supone un grave riesgo para la seguridad de los datos personales de los usuarios, en la medida en que éstos serán accesibles por parte de cualquier usuario de la plataforma.
- **Que la finalidad de los datos no esté correctamente determinada.**
    - Con frecuencia las políticas de privacidad recogidas en este tipo de plataformas determinan las finalidades para las que se recaban y tratan los datos personales, pero de forma generalista y sin aclarar completamente para qué pueden o no tratar los datos personales, lo que supone un grave riesgo para el tratamiento de los datos de los usuarios.

El segundo momento considerado crítico para la protección de datos personales se sitúa en la fase intermedia, es decir, en la que el usuario desarrolla su actividad en la plataforma y utiliza los servicios y herramientas que ésta le ofrece. En este momento los aspectos que pueden poner en riesgo la privacidad de los usuarios son:

- **Los amigos en las redes sociales:**
    - **Es primordial que el usuario**, y más concretamente el menor de edad, **distinga el concepto de amigo en la "vida real" del concepto de amigo en la "vida virtual"**. Normalmente a un desconocido no se le proporciona información determinada de la vida privada y en la "vida virtual" un amigo puede ser un desconocido. Es importante destacar que los menores piensan a veces que su lista de amigos en

una red social es un reflejo de su popularidad, por lo que agregan a personas que no conocen o conocen muy superficialmente para potenciar esa imagen.

- Las redes sociales tienen configuraciones de privacidad que pueden impedir que desconocidos accedan a los perfiles, pero si añaden a personas que no conocen a su lista de amigos les están permitiendo que accedan a su información personal.
- En este sentido algunas redes sociales permiten saber cómo se muestra el perfil a otros usuarios, con opciones de "ver como...". Es importante utilizar este servicio de vez en cuando, para que el usuario pueda ver qué información muestra a un tercero determinado.

› La publicación excesiva de información personal (propia o de terceros).

- En esta fase se mantiene el posible riesgo que conlleva la publicación excesiva de información personal.
- Además, se debe tener en cuenta la posibilidad de que se publiquen también datos de terceros, lo que puede conllevar el tratamiento y la cesión pública de datos de personas que no han prestado el consentimiento para ello.
- La idea tradicional de privacidad estaba vinculada a la idea de informaciones de datos personales que salían de la esfera privada. Hoy **el problema capital de los menores usuarios de los servicios Web 2.0 son las informaciones entrantes.** Los menores pueden, sin duda, ser productores de informaciones sobre ellos mismos, pero son particularmente sensibles a la información de entrada: con **las posibilidades de añadir metadatos (*etiquetado, tags,...*) a las publicaciones de éstos y a sus perfiles, pueden modificar la gestión de su privacidad.** Por ejemplo, se pueden publicar fotos de un partido de

fútbol donde el menor o adolescente haya participado y que un "amigo", o incluso otro usuario de la red social, incluya el lugar, la fecha del evento, incluso el nombre de los jugadores.

› **Alteración de la privacidad derivada de la sincronización con otros servicios de la Web 2.0.**

- El uso de aplicaciones, juegos o sitios Web vinculados a plataformas colaborativas puede implicar un cambio en las opciones de privacidad configuradas en los perfiles o páginas personales que, a su vez, es susceptible de derivar en la divulgación de información sensible.
- Esta amenaza está ligada al uso de aplicaciones sociales en dispositivos móviles: **al instalar estas aplicaciones se puede otorgar permiso para que se modifiquen las opciones de privacidad previamente configuradas.** Por ejemplo, al instalar una app para utilizar Facebook en nuestro smartphone, ésta nos solicita el uso de nuestros datos de geolocalización y los muestra en el muro. Por eso, es importante que revisemos la configuración de privacidad, tanto desde la plataforma, como desde la aplicación.

› **La instalación y uso de "cookies" sin conocimiento del usuario.**

- **Las redes sociales utilizan este tipo de ficheros almacenando determinada información sobre el usuario y su tipo de navegación a través de un sitio web**, de forma que resulta posible detectar el lugar desde el que accede el usuario, el tipo de dispositivo empleado (móvil o fijo) para el acceso, el tipo de contenidos accedidos, los lugares más visitados y las acciones habituales realizadas durante la navegación, así como el tiempo empleado en cada una de las páginas, entre otras muchas funcionalidades.

- **Otros sistemas de seguimiento y enriquecimiento de perfiles. (Web beacons, Me Gusta, Compatir,...)**
  - **Los *"Web Beacons"* son una diminuta imagen en una página Web o en un mensaje de correo electrónico que se diseña para controlar quién lee el mensaje.** Su tamaño es inapreciable, pudiendo ser un píxel en formato GIF y transparente. Se representan como etiquetas HTML. Permiten al sitio Web conocer quién y qué contenido online ha sido visitado. Normalmente estas imágenes son incluidas en correos electrónicos, anuncios, etc.
  - Asimismo, existen otros sistemas de enriquecimiento de perfiles como son las opciones para mostrar preferencias al hacer clic en banners que muestran la opción *"Me Gusta"*, o "+1", o las que permiten *"Compartir"* contenidos a través de la utilización del correo electrónico, sistemas de mensajería instantánea, etc. Al utilizar estas posibilidades se añaden más atributos de la personalidad del usuario que permiten conocer más aspectos de su privacidad.

- **La indexación automática del perfil del usuario por los buscadores de Internet.**
  - Poniendo el nombre y apellidos de una persona en un buscador puede llevarnos a su perfil de la red social. En algunos casos dicha indexación incluye el nombre del usuario registrado, su fotografía del perfil y el nombre y fotografías del perfil de los amigos o contactos con los que cuenta en la red social, así como una invitación general a entrar a formar parte de la plataforma. **Este hecho supone una amenaza para la protección de datos personales de los usuarios, en la medida en que sus datos básicos y principales contactos se exponen públicamente en la Red,** accesibles por parte de cualquier usuario, **pudiendo llegar a ser empleadas esas informaciones de forma descontrolada por terceros,** sin que éstos queden en el "círculo cerrado" de la red social.

- **La recepción de comunicaciones comerciales electrónicas no solicitadas (spam).**
  - Cada vez más, **las redes sociales están siendo empleadas por spammers como fuentes para recabar información y datos personales a los que posteriormente se dirigirán comunicaciones comerciales no deseadas.** Caben varios tipos de spam dentro de las redes sociales:
    - Cuando el usuario se da de alta en varias aplicaciones o grupos y, posteriormente, decide enviar una invitación a todos sus contactos, sobre el registro en dichas herramientas, estará remitiendo a sus contactos una serie de comunicaciones que reportan importantes cantidades económicas para las plataformas y desarrolladores de este tipo de aplicaciones, cuyo valor aumenta en la medida en que existan más o menos usuarios registrados en las mismas.
    - Cuando el usuario permite que la aplicación o red en concreto acceda a su libreta de direcciones de correo electrónico para remitir a todos sus contactos un correo electrónico comercial animando a que se registren en la red.
    - Cuando el usuario admite que se envíen invitaciones a usuarios no registrados en la plataforma para convertirse en nuevos miembros, esta actuación podría llegar a ser interpretada como una forma de comunicación comercial electrónica no deseada, aunque habría que atender a las circunstancias concretas de cada caso.

› **La suplantación de identidad de los usuarios de la red social.**

- Con la suplantación de identidad una persona se hace pasar por otra diferente. Se puede definir como la **apropiación indebida de la identidad de un tercero y la actuación en su nombre**. Es uno de los riesgos que se pueden producir en la utilización de los servicios del Web 2.0. En estos casos una persona utiliza el nombre y demás datos personales de otra persona haciéndose pasar por ella. Son pues datos de carácter personal los que se utilizan.
- Ejemplos de estas conductas:
  - Crear un perfil de un tercero en una red social.
  - Utilizar el perfil real de un tercero en una red social, previa obtención ilegítima de las claves de acceso.
  - Utilizar la cuenta de correo de un tercero, previa obtención ilegitima de las claves de acceso.
  - Utilizar el teléfono móvil de un tercero sin su consentimiento, enviando mensajes.

El tercer momento crítico para la protección de la privacidad del usuario se sitúa en la fase en la que éste pretende darse de baja del servicio:

› **La imposibilidad de realizar la baja efectiva del servicio.**

- En algunos casos, a pesar de solicitar la baja del servicio conforme a las políticas de privacidad recogidas en las plataformas, la baja no se lleva a cabo de manera efectiva, manteniéndose los datos personales de los usuarios a disposición de los responsables de la red social.

- Es frecuente que el usuario que intenta darse de baja del servicio se encuentre con procedimientos complejos, que nada tienen que ver con el procedimiento automatizado y electrónico de alta en la plataforma. Este hecho implica un riesgo para la seguridad y protección de datos personales de los usuarios.

› **La conservación de datos y el cumplimiento del principio de calidad de los datos.**

- Muchos prestadores de servicios conservan los datos de tráfico generados por los usuarios en el sistema para, posteriormente, utilizarlos como herramientas a través de las que sectorizar y conocer las preferencias y perfiles de los usuarios para realizar publicidad contextualizada con el medio y contenido de sus comunicaciones a través de la Red, afectando de esta forma al principio de calidad de los datos.

2. CONSEJOS.

› Al registrarse en una Red Social, **dar los datos estrictamente necesarios** para dicho registro y configurar la privacidad. Escoger qué información del perfil es pública y qué usuarios pueden acceder a ella, estableciendo distintos niveles de privacidad según el contenido y usuarios que se traten. Ser cuidadoso con los datos que se publican. No más de los necesarios y datos como correo o teléfono, hacerlo de la forma más privada posible.

› En cada publicación que se haga en una red social, **configurar la visibilidad de la misma por terceros.** Asimismo, debes medir bien las críticas que se publican. Expresar la opinión o una burla sobre otras personas puede llegar a vulnerar sus derechos e ir en contra de la ley. **La libertad de expresión termina donde comienzan los derechos de los demás.**

- Cuando se sincronicen varias plataformas del entorno Web 2.0, **revisar la configuración de la privacidad**. Puede haberse modificado. También debes hacerlo cuando utilices estas plataformas desde distintos dispositivos. Por ejemplo, cuando utilizas una red social desde un ordenador portátil y cuando la utilices desde tu Smartphone, en ambos casos debes revisar la configuración de la privacidad para evitar posibles alteraciones.
- Al descargarse e instalar aplicaciones Web en los dispositivos móviles se deben **analizar los permisos que dicha aplicación solicita** y, ante la duda, no aceptar su instalación.
- **No aceptar ni agregar como contacto a desconocidos.** Tanto para amigos en redes sociales como para contactos en la lista de contactos de su cuenta de correo. No hay problema en ignorar solicitudes de amistad, invitaciones a eventos, grupos, etc. Es mejor tener menos amigos, pero conocerlos realmente. Una medida de prudencia es preguntar a amigos reales si conocen a esta persona que nos solicita amistad. En caso de discrepancias entre perfil declarado y real, bloquéalo.
- **Revisar la configuración del navegador respecto del uso de cookies**, realizar un borrado periódico de las mismas y de los archivos temporales de Internet en el dispositivo desde el que se acceda a la red.
- **Antes de publicar información que te han remitido de manera privada pregunta si lo puedes hacer.** En las redes sociales la información circula con demasiada velocidad de un lado a otro y lo que es privado se puede convertir en un secreto a voces.
- Si se utilizan programas para compartir música, películas, etc., hay que **comprobar las carpetas que utiliza el programa para compartir archivos**, debe recordarse que esas carpetas quedan a la disposición de millones de usuarios.
- **Leer atentamente las políticas de privacidad de los servicios del entorno Web 2.0.** Es muy importante saber qué datos son necesarios para la utilización de un determinado servicio, quién los va a tratar, para qué y hasta cuándo van a ser tratados. En caso de duda respecto del tratamiento que se vaya a dar a nuestros datos valorar la posibilidad de no utilizar dicho servicio.

› **Utilizar los servicios de Internet con sentido común,** y valorar las consecuencias que en otra época o contexto pueden tener. Lo que hoy resulta atractivo e incluso gracioso puede que con el paso del tiempo no sea positivo para la reputación del usuario. El conocimiento de uno mismo y el contexto considerado adecuado puede variar en función de la situación en que se encuentre el usuario.

3. PARA SABER MÁS.

› AEPD:

http://www.agpd.es/portalWebAGPD/CanalDelCiudadano/menores/Videos/index-ides-idphp.php

› Guía legal sobre las redes sociales, menores de edad y privacidad en la Red:

http://www.inteco.es/Seguridad/Observatorio/guias/guiaManual_redes_menores

› Guías de ayuda para la configuración de la privacidad y seguridad de las redes sociales:

http://www.inteco.es/Seguridad/Observatorio/guias/guia_ayuda_redes_sociales

› Proyecto Intypedia – Lección 15 sobre Redes Sociales – Universidad Politécnica de Madrid:

http://www.youtube.com/watch?v=nlfUhKijHCg

› Seguridad Web 2.0:

www.seguridadWeb20.es

› Vidente. (subtítulos en inglés)

http://www.youtube.com/watch?v=F7pYHN9iC9I

› Ciberbullying - Amanda Todd (subtítulos en español)

http://www.youtube.com/watch?v=NaVoR51D1sU

III. ACTIVIDADES

1. REPUTACIÓN ONLINE.

Esta actividad está dirigida a conocer qué significa la reputación digital y el valor y trascendencia que ésta tiene para nuestra vida futura.

Pedro tiene un perfil en una red social donde comparte comentarios y fotos sobre sus gustos y aficiones. No ha revisado sus opciones de privacidad y está permitiendo que todo el mundo pueda ver dicha información. Pedro se ha cambiado de centro educativo y ahora muchos de sus compañeros de clase conocen aspectos de su vida privada que no querría que se supieran

1. ¿Creéis que todo el mundo tiene que saber todo de vuestra vida?

2. ¿Cómo podría Pedro haber evitado esto que le ha ocurrido?

2. CONFIGURACIÓN DE LE PRIVACIDAD EN REDES SOCIALES

El educador preguntará a los chicos y chicas:

1. ¿Tenéis alguna cuenta abierta en una red social?

2. ¿Sabíais que las opciones de privacidad pueden ser cambiadas automáticamente sin que lo sepáis? ¿Alguna vez habéis revisado vuestra privacidad?

3. ¿Sabéis como se hace? (De manera opcional se puede entrar en una cuenta de una red social y revisar entre todos la privacidad).

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
red.es

"Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad"

[Red.es]

MONOGRÁFICO

NETIQUETA: COMPORTAMIENTO EN LÍNEA

MONOGRÁFICO: NETIQUETA: COMPORTAMIENTO EN LÍNEA

1. Objetivo del monográfico

«Sensibilizar sobre las principales normas de comportamiento en la red, cuya finalidad es respetar a los demás y transmitir la importancia de conductas ciberresponsables por parte de los menores; incidiendo en los procesos de comunicación online».

2. Conceptualización y descripción

¿Qué es la Netiqueta?[1]

Netiqueta es el código social de Internet basado en un principio fundamental, la *Regla de Oro de la Humanidad*:

> *"Nunca obres con los demás lo que no quieras que obren contigo."* Confucio.

Este término surge para establecer unas normas de buenas maneras a tener en cuenta en el uso de Internet. Estas normas se pueden comparar con las reglas de etiqueta del mundo real. Si se hace una comparación con los protocolos que se utilizan en la vida real la netiqueta establecería el protocolo al establecer "contacto" electrónico.

Historia del término Netiqueta

Si bien en el comienzo las redes estaban limitadas a uso militar, investigaciones científicas y universidades, con el tiempo se diseñaron sistemas para la discusión de temas. De este modo gente de diferentes lugares podían entrar en sitios de discusión y compartir información sobre diferentes temas.

Los problemas aparecieron cuando en estos "lugares de encuentro en red" se empezaron a dar desencuentros entre los participantes que entorpecían las conversaciones, llegando incluso recibirse insultos y comentarios ofensivos. En uno de estos foros por primera vez apareció la palabra netiqueta.

[1] Chiles, D. (2014). *Los principios de la Netiqueta.* Amazon: Amazon.

En los noventa, aparecieron los primeros Blogs, llamados entonces “web-log”. Esto significo el comienzo de la producción de información y la participación interactiva en Internet. Es en este momento cuando comienzan a publicarse y difundirse las reglas de la netiqueta. Si bien actualmente la página web NetworkEtiquette[2] es considerada como el referente en definir los estándares de la etiqueta de la red, existen numerosos libros y artículos en los que se habla de las reglas básicas de netiqueta.

Entre todas las publicaciones una destacable es el libro de Virginia Shea, *Netiquette* de 1.994. Su introducción nos da una clara idea del propósito del libro:

> *“Cuando entras en una nueva cultura, y el ciberespacio es una de ellas, te expones a cometer algunos errores. Puedes ofender sin proponértelo. O puedes malinterpretar lo que otros dicen y ofenderte cuando no era esa la intención. Para hacer las cosas todavía más difíciles, el ciberespacio hace muy fácil olvidar que se está interactuando con personas reales, no propiamente con caracteres ASCII [2] en una pantalla, sino con seres humanos.*
>
> *El libro Netiqueta tiene un doble propósito: por un lado, minimizar los errores de los principiantes y, por otro lado ofrecer recursos a los veteranos, a los usuarios del ciberespacio, para que puedan ayudar a estos principiantes. Las personas prefieren hacer amigos a ganar enemigos. Conocer unas reglas básicas que pueden evitar errores que nos impedirán hacer amigos.”*[3]

La Regla de Oro (The Golden Rule). La necesidad de netiqueta y su relación con las normas sociales y el contexto

La Regla de Oro, **«trata a los demás como quieres ser tratado»**, es el principio de la sociedad tal y como la conocemos hoy. Se basa en el intercambio, la persona tiene una conducta que busca la reciprocidad.

La gran mayoría de las religiones hacen referencia a este intercambio recíproco que se establece entre las relaciones personales: el Cristianismo habla de esta regla en la

[2] www.networketiquette.net

[3] Virginia Shea. (1.994). Introduction. En *Netiquette*(160). Albion.com: Albion Books.

Biblia, también el Confucionismo, el Hinduismo y el Budismo aunque entendido de una manera pasiva. Es por tanto una regla universal, que rige el comportamiento social tanto en la vida personal como en la laboral, no es un concepto nuevo creado a partir de las TIC, pero si se traslada al día a día de cualquier persona (niño, joven o adulto) por el protagonismo de las nuevas tecnologías en la vida diaria.

En la escuela y en casa los niños/as aprenden en mayor o menor medida una serie de reglas morales y éticas que aplicarán en su día a día, en la base de las cuales está la Regla de Oro.

> "*Para aplicar la Regla de Oro, tienes que imaginarte a ti mismo en el lugar de la persona que recibe el acto. Esto requiere que cada uno, dedique un instante en su ocupada vida, para ocupar de manera real y precisa el lugar de la otra persona.*"[4]

Internet es comunicación. Intercambio de datos de un ordenador a otro, pero también es la herramienta de intercambio de datos e información entre personas en un contexto concreto, por lo que no está exento de los principios morales y éticos que rigen nuestra sociedad. Al igual que en la vida real se establecen una serie de normas sociales necesarias para que la convivencia sea posible, la netiqueta se instaura en Internet.

Por otra parte, las normas sociales o principios básicos que regulan la sociedad se establecen de forma general y es necesario adaptarlas a las particularidades de cada contexto. Del mismo modo en la red hay que saber situarse en el contexto en el que se está en cada momento, por lo que el comportamiento según el lugar concreto en el que uno se encuentra es diferente. Lo que puede ser correcto en un contexto social o virtual determinado en otro puede ser inapropiado. Esto obliga, como buenos internautas a ser conocedores de estas reglas de netiqueta y aplicarlas en función de la audiencia y del medio.

El problema que se encuentra en Internet es que no es fácil limitar la audiencia y la permanencia en el tiempo de los mensajes. Se puede publicar un *tweet* o mensaje en el tablón de Facebook, pensando que sólo llegará a nuestra lista de seguidores o amigos, sin ser conscientes de la difusión exponencial que podría tener esa

[4] Putnam, MS. (2006). *Reflections on the Golden Rule*. 2006, de Global Ethics University Sitio web: http://www.globalethicsuniversity.com/articles/thegoldenrule.htm

información y por lo tanto, lo incontrolable que resulta establecer los destinatarios exactos (amigos, padres, profesores…) y el tiempo que el mensaje permanecerá en la red, ya que podría volver a la luz años después.

Por lo tanto, no se debe perder de vista la multiplicidad que genera la cadena de amigos en redes sociales. En muchos casos el emisor de la información no es consciente de la repercusión que puede tener la información publicada, aunque en redes sociales, como Facebook o Twitter tengamos una audiencia limitada, y por lo tanto los jóvenes así se comportan, no son consciente de que ese público se convierte en ilimitado, de forma que la información, fotos, comentarios… se pueden multiplicar como la espuma a través de las cadenas de amigos. En el apartado 5 de este monográfico se profundizará en más detalle sobre las pautas a tener en cuenta en los diferentes contextos.

La necesidad que el ser humano tiene de empatizar con los demás junto con las creencias, la ética y el criterio moral, lleva a la sociedad a comportarse de manera más o menos correcta con las personas que le rodean. Este hecho, en la vida física, queda entendido e interiorizado en cada persona desde edades tempranas. Por el contrario, este criterio moral, esta ética, e incluso las creencias religiosas de cada uno, se separan del mundo digital; se les resta importancia o, directamente, se pasan por alto. En Internet el individuo se desvincula de esta moralidad porque siente que en el mundo digital, las consecuencias de sus actos no son inmediatas ni reales, al contrario de lo que ocurre en el mundo físico.

Principios de la netiqueta

Los principios de la netiqueta están descritos para que los usuarios de Internet se sientan cómodos relacionándose entre ellos. Hoy en día la ciudadanía digital la componen las personas con acceso a Internet, correo electrónico y cuentas en redes sociales. Esto requiere el conocimiento de los siguientes **«principios generales»** para poder relacionarse de manera apropiada (extraídos del libro de Virginia Shea, *The Core Rules of Netiquette*[5]*,* anteriormente citado):

[5] Virginia Shea. (1.994). Introduction. Netiquette(160). Albion.com: Albion Books.

Recordar el lado humano

Al igual que se pide respeto, se debe respetar la privacidad de los demás en Internet. La información privada y datos personales de terceros deben ser manejados con precaución.

De igual modo, no se deben leer los mensajes privados de una persona al igual que no se puede entrar en su casa sin su permiso.

No sólo es falta de netiqueta, publicar información personal de terceros o leer mensajes privados puede constituir delito. Todos tenemos derecho a proteger nuestro honor, intimidad e imagen en la red.

Conocer dónde estás en el Ciberespacio

Cuando se entra en una web, foro, chat… la persona debe situarse. Es imprescindible saber dónde se encuentra uno, de qué se habla y quien habla. Las normas de comportamiento varían de un dominio a otro, en función de dónde se encuentre la persona en el entorno virtual, el mismo mensaje podría ser aceptable en un área (entorno familiar y social) e inapropiada en otra (entorno laboral).

En todos los casos es importante tener en cuenta los siguientes puntos:

- Se debe ser reservado a la hora de enviar mensajes, es decir, enviarlos por alguna razón. De este modo, se puede pedir a los demás que nos envíen mensajes por alguna razón concreta. Si se envían y reciben mensajes de manera correcta, con reserva, tolerancia y generosidad, todas las partes se benefician de una buena comunicación. De este modo se evitará perder el tiempo (tanto emisor como receptor) con mensajes no solicitados ni necesarios.

- Es importante enviar los mensajes en un horario apropiado, durante la noche el receptor está durmiendo por lo general. Se debe tener en cuenta que los mensajes profesionales tienen prioridad frente a los personales. Si se recuerda esto, se entiende que el tiempo de respuesta de los mensajes dependerá de la persona, del contenido y del tipo de mensaje. Una persona, cuando envía un mensaje, debe entender que aunque esté despierta trabajando o en un momento de ocio, no significa que el receptor del mensaje también lo esté.

Cuidar la imagen

En la comunicación electrónica es muy posible que no se juzgue por el físico, el tono de voz o la ropa que se usa, principalmente porque hay contacto personal con las personas con las que intercambiamos mensajes escritos. Se debe, entonces cuidar la imagen de estos mensajes. No sólo se debe revisar la gramática y la ortografía, también el contenido de lo que se comunica a la otra persona debe ser atractivo y tener sentido.

Algunos aspectos que se deben tener en cuenta para cuidar la imagen de nuestras comunicaciones online son las siguientes:

- No se debe mentir. La comunicación online debe basarse en la honestidad, evitar las declaraciones engañosas o confusas, independientemente del motivo o el objetivo que se persiga. La verdad debe estar por encima de cualquier intención.

- Se debe ser agradable y educado.

- En realidad, de este modo se conseguirá ser tomado con seriedad. Actuar de manera diferente da lugar a problemas en la comunicación.

- Se debe revisar la ortografía y la gramática en los mensajes. Textos con errores ortográficos y gramaticales son difíciles de entender, causan muy mala impresión y son inapropiados en cualquier contexto.

MAL

BIEN

- Se debe evitar escribir todo en mayúsculas. Escribir un texto en mayúscula equivale a gritar y esto se considera una grosería no sólo en las telecomunicaciones, sino también en la vida.

MAL

BIEN

Esto no quiere decir que se deba comenzar una frase o un nombre propio con minúsculas; las normas gramaticales son las mismas en la realidad y en las telecomunicaciones.

Mostrar conocimiento

Internet es comunicación, es intercambio de información. Se nutre del conocimiento de los usuarios. Se realizan cuestiones y son contestadas por los expertos. Compartir los conocimientos que uno tiene sobre un tema determinado es positivo así como lo es cuando se pide información y se recibe respuesta.

Respetar la privacidad de otras personas

Cuanto se interactúa con los demás en Internet, ya sea a través de un foro de discusión, una clase online, un grupo de Facebook o por mensajería instantánea, se está expuesto a información privada y datos personales de terceros que deben ser manejados con precaución.

Al igual que se pide respeto, se debe respetar la privacidad de los demás. No se puede leer los mensajes privados de una persona al igual que no se puede entrar en su casa sin su permiso. No solo es falta de netiqueta, leer mensajes privados puede constituir delito. Para ampliar información se puede consultar el monográfico “Gestión de la privacidad e identidad digital”.

- **Derecho a la protección de la imagen en Internet.** Todo ciudadano tiene el derecho a impedir que una imagen suya sea reproducida o dada a conocer públicamente. Por tanto, nadie sin nuestro consentimiento puede publicar una fotografía nuestra en redes sociales a excepción del caso de personas que, por cuya relevancia pública, su imagen sea habitual en los medios de

comunicación, siempre que se trate de imágenes tomadas en lugares o momentos de la vida pública. Ante la publicación de una imagen o dato íntimo sin nuestro consentimiento (como datos personales, dirección, teléfono…) uno está en su derecho de solicitar su retirada a la persona o grupo de personas que lo han publicado. En caso de que la imagen o dato privado no sea retirado se recomienda acudir al gestor de la Red Social o página web y, en última instancia, a los Tribunales y, en este caso, reclamar indemnización por "el daño moral" ocasionado.

- **Protección del Derecho al Honor en Internet.** El Derecho al Honor en redes sociales, foros y similares protege en los casos en los que uno es víctima de injurias y calumnias en redes sociales, foros y similares. No puede considerarse que toda expresión crítica atente contra el Honor, pero muchas veces la línea divisoria entre la crítica, el insulto, la injuria o la calumnia no está muy clara. La libertad de expresión no puede en ningún caso entenderse como derecho para insultar.

No abusar de nuestro poder

Del mismo modo que en las situaciones reales, hay personas que en el entorno virtual tiene más "poder" que otros, bien por tener más experiencia y conocimiento en el manejo de herramientas informáticas o por el desarrollo de una determinada habilidad o materia. Por ejemplo, ser administrador de sistemas, foros, grupos, etc., es una ventaja que uno tiene en beneficio de todos, para comunicar, informar y resolver problemas o dudas, pero esa ventaja nunca significa que uno pueda abusar de su posición (por ejemplo, violando la privacidad de los que están a su cargo).

Ser flexible con los errores de los demás

No todas las personas que navegan en la red tienen la misma experiencia ni conocen las normas de netiqueta. Cualquier persona puede cometer errores, bien por despistes, por ser principiante, por no conocer las normas, etc. En algún momento todos hemos sido principiantes y debemos tener empatía hacia los nuevos internautas. Algunos ejemplos de estos errores son: preguntas inadecuadas, respuestas muy extensas o palabras mal escritas. Se debe ser flexible y empático antes de corregir a alguien, quizás no sea tan importante y si se hace, que sea de una manera educada, asertiva, con el objetivo de ayudarle.

Mantener las discusiones sin sentido bajo control

- **¿Qué es un *Troll* en Internet?** Un *troll* en Internet es una persona agitadora e instigadora que encuentra placer creando una discordia general. El relativo anonimato de la red hace que las comunicaciones en Internet sean su lugar elegido para "jugar". Los usuarios no son considerados como humanos por lo que no sienten remordimientos ni compasión por la persona o el grupo destino de sus insultos. Su mayor logro consiste en infligir el mayor sufrimiento en los demás. No es posible razonar con ellos para hacerles cambiar. Los *trolls* no siguen la etiqueta de la red.

  > *"Los trolls ansían atención, y no les preocupa si ésta es positiva o negativa. Ven Internet como un espejo en el que pueden mirarse en un éxtasis narcisista".* Profesor Timothy Campbell.

  Un *troll* que quiere atacar un foro o grupo, por lo general envía numerosos mensajes. Puede que estos no contengan nada negativo pero son tan numerosos que no dejan a los demás que se comuniquen. También utilizan la suplantación de identidad, haciéndose pasar por otra persona para manifestar sus quejas.

- **¿Qué es flamear o *flaming* en Internet?** Flamear (*flaming*) significa atacar a alguien en Internet mediante insultos, apodos ofensivos, publicar mensajes deliberadamente hostiles e insultantes sin ningún propósito constructivo en un contexto social, como un foro o una lista de correo electrónico. En resumen, mostrar una total intolerancia hacía el otro. Estos mensajes se denominan *flame* y la persona que los envía se conoce como *flamer*. Es frecuente que se publiquen como respuesta a un cebo, un mensaje provocativo, pensado para generar esas respuestas insultantes.

  La diferencia con el *troll* es que el *flamer* se dirige a una persona específica y como consecuencia de una discusión sobre un tema concreto.

  Las principales causas de este comportamiento son, por un lado, la incorrecta interpretación de los mensajes escritos por la ausencia de escuchar la voz y/o ver los gestos de la otra persona, por otro lado, el relativo al anonimato hace que se utilicen expresiones y palabras "encendidas" que cara a cara difícilmente se utilizarían. Como tercera causa y, en el contexto de los chats de

videojuegos, se establece el estrés que la partida produce en la persona; se está jugando para ganar.

Hay usuarios a los que los *flameos y los trolls* no les afectan y asumen que este fenómeno es uno de los riesgos de Internet. Por el contrario, hay personas que se desaniman y abandonan grupos, foros o redes sociales por estas causas. Los adolescentes pertenecen en su mayoría a este último grupo sencillamente por su momento de desarrollo hasta la madurez, momento en el que todo adquiere una importancia vital, en el que necesitan reivindicarse, tener amigos y ser aprobados por los demás jóvenes de su entorno.

En definitiva los *flameos* y los *trolls* son una amenaza para la comunicación en Internet, sobre todo entre adolescentes.

Por último conviene resaltar que la netiqueta es un código social para las comunicaciones en red que no invalida la libertad de expresión. Esto tiene que estar claro pues cuando un *troll* ve que se le opone resistencia su queja es que tienen derecho a la libertad de expresión. Este derecho es universal pero hay que saber utilizarlo con respeto.

Respetar el tiempo y trabajo de los demás

La mayor parte de las personas llevan una vida ocupada y valoran en qué ocupan su tiempo, incluido el tiempo que pasan a la red, el tiempo para leer y para responder a través de las diferentes medios (mensajería instantánea, e-mail, redes sociales…). Este punto se debe tener en cuenta al compartir información con otros, procurando siempre que sea de su interés.

Por otro lado se debe valorar el tiempo y trabajo invertido en publicar contenidos. A continuación se explican aspectos a tener en cuenta cuando utilizamos publicaciones de otros.

- **Fuentes y autoría.** Uno de los errores más comunes en la comunicación en la red es usar contenidos de otras personas sin citar su autoría. Cuando se comparten imágenes, citas, artículos o videos, que no son propios se debe hacer referencia al autor o autores. Existen unas normas generales para, nombrar las referencias bibliográficas, que no se deben olvidar en la red.

Las citas textuales (texto de menos de cuarenta palabras) deben ir siempre entre comillas. Una vez finalizado el texto hay que escribir el nombre del autor y el contexto.

Cuando se utiliza contenidos de un libro, hay que hacer referencia al autor, año de publicación, título del libro, lugar de publicación y editorial. Cuando se utiliza un artículo de una revista hay que hacer referencia al autor, año de publicación, título del artículo, nombre de la revista y página o páginas donde se encuentra dicho artículo. Si el artículo procede de la web entonces, además, debemos añadir la dirección de la página o revista digital.

Es recomendable leer el Manual de estilo de la American Psychological Association, denominado APA, cuya dirección facilitamos al final del monográfico para la elaboración de Referencias Bibliográficas. Este manual nos permitirá elaborar las Referencias Bibliográficas en nuestros trabajos académicos y profesionales.

Relación entre netiqueta y c*iberbullying*

Si la red se convierte en un campo de batalla y nadie apuesta por los valores y normas sociales es normal que los menores reproduzcan estos comportamientos derivando en incidentes más o menos molestos en Internet entre amigos y compañeros o entre menores y adultos. Entre los incidentes más graves destaca el *ciberbullying*.

El *ciberbullying* es un tipo concreto de ciberacoso aplicado en un contexto en el que únicamente están implicados menores. Se puede definir de una manera sencilla y concisa 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».

La falta de netiqueta, al igual que la falta de normas sociales predispone al acoso escolar tradicional, puede dar lugar a conductas de ciberacoso entre los menores. Acciones como dar información de terceros sin su consentimiento, contar mentiras sobre alguien, mostrar fotos inapropiadas e hirientes de otra persona, constituyen falta de netiqueta y son situaciones propias del *ciberbullying*.

El menor que acosa ve esta falta de etiqueta en la red inofensiva, en primer lugar porque no ve la reacción del acosado, únicamente tiene una pantalla de ordenador o dispositivo móvil frente a él. En segundo lugar, como se ha comentado anteriormente,

porque no cree o no es consciente de que las consecuencias de sus actos en línea sean reales.

La etiqueta en la red es necesaria para reducir el riesgo de ser víctima de *ciberbullying*. Es necesario crear entornos agradables en los que se minimicen los comportamientos hostigadores, para ello se hace necesario que los jóvenes conozcan los mecanismos de interacción social y que estén al tanto de las consecuencias en caso de ejecutar comportamientos que no las cumplan. Explicar cómo debe ser nuestra relación con los demás en el ciberespacio y, sobretodo, hablar de que el mundo digital es tan real como el mundo físico, debe ser una tarea que se lleve a cabo de forma conjunta en el hogar y el centro educativo.

3. Datos de situación y diagnóstico

Situación de los menores en Europa[6].

La organización EU Kids Online publicó en 2014 un estudio elaborado a partir de las entrevistas realizadas a menores de 9 a 16 años de toda Europa. En estas entrevistas hablaron tanto de sus experiencias positivas como de las negativas menores de diferentes países europeos, Bélgica, República Checa, Grecia, Italia, Malta, Portugal, Rumanía, España y Reino Unido.

De esta publicación se extraen las siguientes experiencias online problemáticas:

- La más común es el envío de contenido vulgar, violento o con connotación sexual.
- Mensajes de odio en grupos, por ejemplo mientras juegan online.
- Extraños que les envían solicitudes de amistad, haciéndose pasar por jóvenes y luego no tienen la edad que decían tener en un principio.
- Contenidos vulgares en anuncios.

[6] Smahel, D. & Wright, M.. (2.014). *The meaning of online problematic situations for children*. 2015, de EUKidsOnline Sitio web: http://www.ehu.eus/es/web/eukidsonline/hasiera

- Menores que comparten fotografías privadas y comprometidas de alguien sin su permiso.
- Contenido sexual encontrado por error.
- Compartir contraseñas con los demás sin pensar que conlleva un riesgo importante.
- Información falsa o de contenido racista o de odio.

Netiqueta y menores en España

Los menores, nativos digitales, se mueven en la red. Están rodeados de numerosas formas de comunicarse e intercambiar información. Desde edades tempranas comienzan a crear su imagen digital y a moverse en Internet. Entran en diversas redes sociales y la relación con las personas de su entorno ha cambiado en el modo en el que los adultos las vivían.

La mayoría de los menores se conectan para hablar con compañeros y amigos con los que interactúan también fuera de Internet, por lo que el número de contactos con personas desconocidas es bajo[7]. La mayoría de los adolescentes saben una serie de normas básicas y lógicas aprendidas en casa o en la escuela y que aplican en la red. Pero eso no es suficiente, hace falta que, al igual o en mayor medida que los adultos sean educados en la etiqueta de la Red, netiqueta.

Los principios de la netiqueta anteriormente citados no han sido enseñados a los adolescentes con lo cual el resultado es una inadecuada netiqueta en su comunicación online:

- No se muestran en ocasiones como son en realidad.
- A veces se comportan de manera grosera, insultante y agresiva con los demás.
- Violan la privacidad de los demás.
- No son prudentes.

[7] Dra. Rapado, M. & Dr.Chiclana, C.. (2011). *los adolescentes y sus formas de comunicación: Redes Sociales.* 2015, de Fundación Alia2 Sitio web: http://www.alia2.org/index.php/es/blog/17?view=blog

- Buscan la provocación.

¿Se puede encontrar una razón a este comportamiento? En Internet se tiende a perder la empatía hacia los demás pues no vemos la reacción del otro. Virginia Shea nos decía que debemos recordar que el que está al otro lado es humano. Se resta pues importancia a la repercusión que en el otro puede tener su falta de etiqueta.

Es pues tarea de la comunidad educativa (padres, madres y docentes) transmitir estas normas básicas, conocer los riesgos que conlleva el uso incorrecto de la red y hacer las recomendaciones oportunas y necesarias para una navegación positiva, segura, satisfactoria.

4. Estrategias, pautas y recomendaciones para promover la netiqueta

Ordenadores, tabletas, *smartphone*… a través de todos ellos es posible comunicarnos en Internet. Se pueden visitar páginas para recopilar información, leer noticias, entrar en foros sobre temas concretos, jugar en línea, entrar en redes sociales, en chats de mensajería instantánea, enviar correos, ver videos de nuestros ídolos… las posibilidades son extraordinariamente grandes. Por ello, no se puede dejar de describir una serie de recomendaciones según el uso que le se está dando a la Red; según el lugar donde la persona se encuentre dentro del ciberespacio. Unos principios dentro de cada contexto para que la navegación sea satisfactoria.

E-mail

Una vez que se tiene cuenta de correo electrónico la persona se convierte en usuario de Internet. Ya tiene su identificación, su dirección desde la cual enviar y recibir. El Email da la entrada a la comunicación social de la red.

En la comunicación vía email se debe ajustar el estilo, no se está escribiendo una carta en el sentido tradicional. Por tanto, hay una serie de puntos a considerar a la hora de utilizar email.

- Cuando se envía un correo electrónico uno debe saber en qué lugar colocar a los destinatarios según convenga a la finalidad del mensaje. Así la “A ó Para” es para la dirección a la que va dirigido el mensaje y del que se espera

respuesta. “CC” es para las direcciones a las que se quiere hacer llegar el correo porque necesita ver el contenido pero puede o no responder o actuar sobre este. “CCO” se utiliza para enviar un mensaje a varias personas, de este modo se protege la privacidad de los destinatarios en envíos masivos.

- Existe un término para nombrar un estilo periodístico, la pirámide invertida que consiste en estructurar el contenido del mensaje según la importancia que la información tenga para el receptor. Es recomendable poner en primer lugar la información más importante.

- Se debe incluir la firma al final del email con tu nombre o cargo, dirección y teléfono, de este modo el receptor tiene otra manera de contactar contigo si lo necesita además de ser el sello de autenticidad de la cuenta de correo. Es fácil hacerlo, la mayoría de los programas tienen funciones para configurar esta firma. En el caso de adolescentes es bueno que se acostumbren a configurar su cuenta de correo al menos con su nombre de pila. Es importante que comiencen a firmar aquellos correos en los que envían trabajos de clase, esto les servirá para el futuro.

- No se da por hecho que un email es privado. Es bueno evitar enviar algo que uno no querría hacer público. Si se quiere que un mensaje continúe siendo privado se debe comunicar al receptor de dicho mensaje.

- Cuando se adjuntan archivos o videos hay que ser prudente con los envíos. Un archivo demasiado pesado puede resultar molesto al receptor.

- Se debe poner especial cuidado a la hora de utilizar demasiados colores ya que a muchos receptores les resulta molesto.

- Al recibir correos en los que hay varios destinatarios, se debe pensar antes de contestar. Si la respuesta es para el emisor no se pondrá en copia a todos los demás.

Redes sociales[8]

Aunque en redes sociales se deben repetir las mismas premisas de la netiqueta general, es necesario recordarlas y ampliarlas en este contexto concreto, pues los menores tienen a olvidar toda etiqueta en este entorno. Por su importancia y uso en jóvenes, a continuación se presentan recomendaciones específicas para redes sociales:

- Hay que pedir permiso antes de etiquetar fotografías en las que aparecen otras personas. Del mismo modo hay datos íntimos, privados de personas que no se deben hacer públicos sin preguntarse si a esa persona le importa. Hay que poner mucho cuidado en el derecho a la privacidad de las personas.

- Hay que dejar claro a los demás como quiere uno llevar y manejar su privacidad, así se evitarán situaciones incómodas y desagradables en redes sociales.

- Utilizar las etiquetas en positivo, pueden ayudar a crear un entorno agradable, nunca utilizando insultos, humillaciones y burlas.

- Medir bien las opiniones que se van a publicar. El Derecho al Honor de toda persona recogido en la Ley conlleva que un insulto o una injuria sea constitutivo de delito. No hay que confundir la libertad de expresión con otros comportamientos.

- Hay redes sociales que dan la oportunidad de denunciar una publicación que atente contra uno mismo pero no ha de usarse sin justificación.

- Preguntarse qué información de otras personas se expone y asegurarse de que no les importa. En ocasiones se publican aspectos de la vida con otras personas o de la vida de los demás sin tener en cuenta cómo les puede afectar que eso se sepa. Respetar la privacidad de los demás y pedir respeto por la de uno.

[8] Jorge Flores. (2010). *Netiqueta joven para redes sociales*. 2015, de Pantallas Amigas Sitio web: http://www.netiquetate.com/

- Cuando se etiqueta a otras personas se debe hacer sin engaño, la etiqueta debe transmitir una información cierta y siempre asegurarse de que no les molesta que se haga. Cuando se etiqueta a alguien se aporta mucha información que además, en muchos casos, se propaga de forma inesperada e incómoda.

- Se debe recordar que escribir todo en mayúsculas puede interpretarse como un grito.

- Es muy recomendable utilizar los recursos que se ofrecen (dibujos, símbolos, emoticonos…) para evitar malentendidos y poder expresar sentimientos o estados de ánimo.

- Se debe pensar antes de reaccionar de una manera equivocada ante algo que ha molestado. Puede ser una acción no intencionada. Si es una provocación lo peor que se puede hacer es contestar a ella pues entonces esa persona seguirá porque eso le divierte y se está entrando en el juego.

- El respeto a la hora de corregir a alguien es imprescindible tanto si se hace en público como en privado.

- No todas las redes sociales (Tuenti, Facebook, Hi5, Bebo, Orkut, Fotolog…) son iguales; hay que examinarlas, investigarlas, conocerlas… en definitiva saber dónde estamos.

Dispositivos móviles

Este término se refiere a tabletas y a teléfonos *smartphone.* Las reglas básicas de netiqueta móvil prohíben su uso en el aula, la conducción y en la mesa. En las demás situaciones no existe problema en utilizarlo siempre que no se interrumpa a nadie. Utilizarlo en la calle no es recomendable pues se puede sufrir algún percance sobre todo si se está cruzando la calle.

Es interesante resumir la netiqueta móvil en los siguientes puntos[9]:

[9] Abogacía española. (2013). *Netiqueta móvil: código de buenas maneras.* 2015, de RedAbogacía Sitio web: http://www.abogacia.es/2013/04/22/netiqueta-movil-codigo-de-buenas-practicas/

- Disfrutar del tiempo que pasas con otras personas. Internet no puede sustituir a los momentos reales que se pasan con los demás. Escribir mensajes o estar pendiente del teléfono en compañía de otras personas es un hábito extendido entre todos los usuarios que hace que no se preste atención a nuestros acompañantes.

- En la escuela, en medios de transporte y en lugares públicos silencia el móvil. Cuando se viaja en tren cada vez es más frecuente encontrar vagones en los que hablar con el teléfono está prohibido. De cualquier modo es educado buscar fuera del vagón un lugar para hablar.

  En algunas escuelas está prohibido su utilización pero cada vez son más las provincias que creen que bien gestionado su uso dentro de las aulas, el teléfono móvil puede ser muy útil para según qué actividades.

- Utilizar tonos de llamada y de notificaciones discretos, que no resulten molestos a los demás. Ser discreto también cuando se habla con el teléfono. En público es recomendable acortar las conversaciones y mantener un tono de voz adecuado.

- Apagar el móvil en cines, comidas, clases, reuniones con amigos… En ese momento uno está disfrutando de una película o de una comida, trabajando o atendiendo una clase. Hay personas al alrededor que merecen atención así como uno merece la de los demás.

- No se debe poner el móvil encima de la mesa. Si se espera una llamada urgente uno puede avisar de esa situación a la familia y/o amigos, y si se debe atender una llamada sin remedio se atiende pero antes hay que excusarse con los comensales.

- Cuando se llama a alguien puede que en ese momento el otro no pueda contestar. Los teléfonos móviles sobre todo permiten visualizar la llamada entrante. Esa persona en cuanto pueda devolverá la llamada.

- Del mismo modo, cuando se escribe un mensaje en chat de mensajería instantánea hay que entender el receptor o receptores pueden estar ocupados; cruzando una calle, en el cine, en clase… o simplemente que no tengan el móvil a mano, por lo tanto contestarán más tarde. Se debe ser paciente.

Blogs

A continuación se detallan algunos aspectos a tener en cuenta a nivel de netiqueta en cada una de las secciones de un blog.

- Autoría: los blogs son una herramienta para establecer conversaciones. Se recomienda identificarse al publicar las entradas para generar una sensación de transparencia y cercanía que favorezca la participación de los lectores. No tiene por qué ser el nombre real, pero si es necesario que no sea como "Editor", "Autor" o similares.

- Escritura: no escribir en mayúscula, respetar normas básicas de escritura (ortografía, gramática…), se debe ser conciso (valorando el tiempo de los lectores) de modo que un tema extenso lo podemos partir en varios post, se debe atender a una norma clásica de redacción "un párrafo, una idea", no abusar del énfasis (resaltando demasiados aspectos en negrita o subrayado) y evitar la redundancia.

- Enlaces: muy frecuentes en la globosfera, ahorran tener que explicar un concepto a la vez que reconocer la autoría y el esfuerzo de a quién enlazamos.

- Comentarios: son la herramienta de comunicación entre el autor del blog y los lectores, por eso se deben cuidar especialmente. No se recomienda dejar comentarios sin contestar, el autor tiene legitimidad para determinar qué comentarios lo complementan y cuáles no, pudiendo eliminar los que considere oportuno. Al igual que las entradas del blog, los comentarios deben ir firmados por el autor. Nunca deberían ser más largos los comentarios que el post al que hacen referencia. Se deben mantener las normas básicas de ortografía, gramática, no escribir en mayúsculas, entre otras, del resto de comunicaciones en la red.

- Imágenes: se recomienda establecer un criterio respetuoso del uso de imágenes, manteniendo la misma línea en todos los post (mismo tamaño, posición…).

- Vídeos: aunque son una herramienta muy valiosa a nivel de comunicación, se debe tener en cuenta que harán más lenta la web.

- Gestión del canal RSS: se debe animar a los lectores a suscribirse al blog, por ejemplo, a través de comentarios en los post. Nunca debe utilizarse esta suscripción para saturar de mensajes e información a los lectores.

Ideas para reconocer un *troll* y no caer en su juego

En el Apartado 2 se ha hablado de los *trolls*, a continuación se desarrollarán pautas que nos permitan reconocerlos. Generalmente se puede decir que "ha entrado un *troll*" cuando ese internauta:

- Escribe un mensaje contundente y obvio para asegurarse de que recibe respuestas enfadadas.
- Escribe un mensaje fuera de tema. Ejemplo: el tema puede ser de fútbol y él hablará de política.
- Inserta una imagen grande para hacer ilegible el mensaje anterior.
- Escribe un mensaje sexista, racista, con contenido que manifieste fanatismo religioso….un mensaje "incendiario".
- Escribe con fallos de manera deliberada. Ejemplo: "Es estupendo el papel de Will Smith en 'Los Juegos del Hambre'".

Twitter es una Red Social muy utilizada por los jóvenes por lo que se debe prestar atención a estos comportamientos en algunos usuarios:

- No buscan diálogo: sólo provocación para llamar la atención. Suelen escribir mensajes al otro usuario para enfadarle y, lo que les da más placer, que los seguidores del usuario entren en su juego. Suelen dirigir sus ataques contra cuentas con muchos seguidores y pueden tener fijación por ciertos usuarios concretos, a los que llegan a acosar.
- Perfiles con pocos seguidores y muchos usuarios a los que siguen. Son principiantes en Twitter y buscarán perfiles concretos para lanzar sus ataques.
- Se sienten crecidos cuando alguien les entra en su juego, y lo manifiestan. Cuando un *troll* consigue que una de sus víctimas se enzarce con él, a menudo lo comenta en su perfil porque para él es un logro.

Se presentan algunas recomendaciones, claras y fácilmente comprensibles que se deben tener en cuenta cuando se sospecha que podríamos iniciar un contacto con un *troll*:

- Si se tiene dudas de si el interlocutor busca provocar, es interesante revisar su perfil, puede facilitar información.
- Si insulta no hay que contestar.
- Ignorarle y, aunque se acceda a ver sus comentarios, nunca hay que seguirle.
- Bloquearle para que no sea seguidor.
- Si es necesario, denunciarlo en la red social.

Una vez analizados los diferentes contextos en los que se debe tener presente la etiqueta en Internet y presentadas las recomendaciones para cada uno de ellos, se pueden establecer una serie de pautas a seguir para que Internet sea satisfactorio, desde el entorno familiar, el entorno escolar y directamente a los menores.

Es importante en primer lugar que los adultos conozcan la etiqueta de la red, netiqueta, para que se pueda educar a los menores en el uso correcto de Internet. Porque Internet es el presente, tan real y cotidiano como levantarse todas las mañanas para ir a trabajar o a la escuela. No se puede prohibir, es imposible, pero si educar en ese uso correcto y hacer las recomendaciones precisas dentro de cada contexto.

Estrategias, pautas y recomendaciones para prevenir el riesgo desde el entorno familiar

Es responsabilidad padres, madres y tutores hablar sobre netiqueta a los hijos. No hace falta ser un experto para fomentar la ciberconvivencia como prevención a posibles problemas. Minimizar los errores que puedan cometer los menores.

1. Los padres, madres y tutores deben ser un ejemplo para sus hijos/as. No sólo explicar cuál es el principio de la netiqueta, la Regla de Oro: “Trata a los demás como quieres ser tratado”, sino llevarla a cabo. Se debe hacer entender a los jóvenes que Internet es un intercambio de información, es comunicación entre

las personas, por tanto hay que seguir unas normas básicas de buen comportamiento y no desvincular la vida digital de la vida física.

2. Fomentar el respeto y la tolerancia hacia los demás. Este respeto incluye no distribuir información privada de otras personas sin su consentimiento. No etiquetar a nadie en redes sociales sin su consentimiento. No dar información de otra persona sin su permiso. Hablar sobre el derecho a la protección de imagen y el derecho al Honor.

   Una persona respetuosa con los demás no utilizará mensajes de provocación, molestos, burlas y ni atentará contra el honor del otro.

3. De forma discreta, se debe hacer desde el entorno familiar un seguimiento de la actividad en línea del menor.

4. Los padres, madres y tutores deben estar atentos a cualquier comportamiento inadecuado en línea y trasladar al menor la forma correcta de proceder.

5. Cuando se realiza una recomendación no debe hacerse en forma de reproche o castigo.

6. Al igual que para el resto de conductas que queremos fomentar en el menor, es importante el componente motivacional. Será necesario mostrar al joven las ventajas de la netiqueta haciendo que el mismo esté motivado para llevar a cabo un adecuado comportamiento en línea, por los beneficios que aporta su uso y no por la imposición u obligación por parte de un adulto con castigos o reprimendas.

7. Haciendo uso del aprendizaje vicario, ya que en los jóvenes es muy frecuente que aprendan al ver lo que ocurre en los demás, siendo observadores. Se pueden mostrar al menor ejemplos de un uso inadecuado de la netiqueta para enseñar lo que no se debe hacer en la red.

8. Se debe ser acertado en el modo y forma de realizar recomendaciones al menor, evitando que perciba que desde la familia se quiere controlar su conducta, no olvidemos la etapa del desarrollo en la que se encuentran, cualquier prohibición puede tener el efecto contrario.

9. Incentivar la autoestima y explicar que en Internet hay que ser uno mismo, la misma persona que en la realidad y ganarse así la confianza de los demás. No se debe mentir en Internet del mismo modo que moral y éticamente no hay que mentir en el mundo físico.

Estrategias, pautas y recomendaciones para prevenir el riesgo desde el entorno escolar

Del mismo modo desde el entorno educativo es importante que se fomente la netiqueta y algunas recomendaciones pueden ser:

1. Se incorporarán pautas sobre netiquetas en asignaturas como: informática (seguridad, contraseñas…), lengua (uso de mayúsculas, ortografía…, ética (Regla de Oro, respeto, privacidad…), así como en tutorías tanto individuales como grupales (autoestima, honor…) y el proyecto TIC del centro.

2. Fomentar el respeto y la tolerancia en los demás, haciendo referencia a la importancia de tener en cuenta estos valores también en la red. Este respeto incluye no distribuir información privada de otras personas sin su consentimiento. No etiquetar a nadie en redes sociales sin su consentimiento. No dar información de otra persona sin su permiso. Hablar sobre el derecho a la protección de imagen y el derecho al Honor.

3. Trabajar desde el aula el sentido del honor y la privacidad. El aula es un entorno inmejorable para hablar sobre este punto, proponer diferentes situaciones y debatir ya que los adolescentes tienen un sentido del honor y la privacidad que difiere del de los adultos.

4. Incentivar la autoestima y explicar que en Internet hay que ser uno mismo, la misma persona que en la realidad y ganarse así la confianza de los demás. No se debe mentir en Internet del mismo modo que moral y éticamente no hay que mentir en el mundo físico.

5. Establecer normas (que deben redactar el propio alumnado para una mayor implicación) en las que se incluyan netiquetas: como por ejemplo no tener móvil en clase.

6. No es recomendable que un profesor tenga a sus alumnos en su lista de amistades si no es por un trabajo académico puntual.

También señalar que los centros educativos tienen la posibilidad de participar en el **Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos**[10], que pretende potenciar actuaciones preventivas en relación con los riesgos a los que se ven sometidos los menores y los jóvenes, en temas tan importantes como el uso de Internet y las nuevas tecnologías, entre otros. En el marco de este Plan los miembros de las Fuerzas y Cuerpos de Seguridad realizan charlas, visitas y actividades en centros escolares, dirigidas tanto al alumnado como al resto de la comunidad educativa (directivos, personal docente y Asociaciones de Madres y Padres de Alumnos). Como medidas adicionales, se contemplan acciones de sensibilización y formación dirigidas a concienciar sobre el "uso responsable de las nuevas tecnologías y los riesgos que las mismas pueden implicar, promoviendo, a su vez, la comunicación a su entorno familiar, educativo o a las Fuerzas de Seguridad de los hechos de los que pueden ser víctimas o testigos"

5. Mecanismos de respuesta y soporte ante un incidente

En algunos casos, tal y como se ha visto en el apartado de descripción de este monográfico, la falta de netiqueta puede derivar en incidentes realmente graves. Pero en la mayoría de los casos la falta de netiqueta no tiene por qué tener esas consecuencias. A continuación se presenta el protocolo que pueden seguir desde los dos entornos principales en los que se desenvuelve el menor.

Protocolo de respuesta en caso de incidente de falta de netiqueta para padres, madres y tutores

Como protocolo para padres, madres y tutores se establecen varios pasos:

[10] Ministerio del Interior. Instrucción nº 7/2013 de la Secretaría de Seguridad, sobre el "Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos". Recuperado de: http://www.interior.gob.es/documents/642012/1568685/Instruccion_7_2013.pdf/cef1a61c-8fe4-458d-ae0d-ca1f3d336ace

1. Diagnosticar el incidente o problema. Es necesario conocer en qué consiste la falta de netiqueta por parte del menor. Como hemos visto en el monográfico, la ausencia de netiqueta se puede manifestar de diferentes formas, para actuar frente a un caso concreto es necesario que el padre, madre o tutor del menor implicado delimite cuál ha sido el acto llevado a cabo por el menor.

2. Hablar con el menor para saber si es consciente de la ausencia de netiqueta en su comportamiento. Es importante conocer si sabe que lo ha hecho mal o lo está haciendo sin conocimiento de las consecuencias.

3. En caso de que no sepa que su conducta ha sido inapropiada, será necesario explicarle la manera correcta de actuar. En este caso habrá que personalizar la información facilitada en función del comportamiento inadecuado en concreto.

4. Se debe hacer responsable al menor de sus actos, debe saber que cumplir la netiqueta en la red está en su mano. Se debe transmitir como padre, madre o tutor que debe de pensar el daño que hace antes de actuar en la red y pensar qué consecuencias tienen sus actos. Cuando el daño ya está hecho debe pedir disculpas si ha sido el causante de alguna situación incómoda o molesta. Y, por supuesto, evitar que vuelva a ocurrir.

5. Se debe buscar asesoramiento jurídico cuando el comportamiento del menor ha desembocado en una denuncia por daños morales o de imagen. Del mismo modo se debe buscar este asesoramiento cuando es el menor la víctima. Hay que dirigirse a los titulares del foro, página web o red social, para informarles de que lo que publican o no es lícito porque no cuenta con el consentimiento ni de sus tutores legales en primera instancia ni del propio menor.

Protocolo de respuesta en caso de incidente de falta de netiqueta para educadores

1. Diagnosticar el incidente o problema. Es necesario que desde el centro educativo se detecte en qué ha consistido la ausencia de netiqueta que ha cometido el joven, ya que puede ser muy variada en tipo y gravedad.

2. Hablar con el menor para establecer el grado de consciencia que el menor tiene sobre el daño causado. Es importante conocer si el joven es consciente

de la ausencia de netiqueta o no. Es posible que no sepa que ha actuado de forma incorrecta.

3. En caso de que no sepa por qué su conducta ha sido inapropiada, explicarle la manera correcta de actuar. En este caso habrá que personalizar la información facilitada en función del comportamiento inadecuado en concreto. Se aprovechará para ello las horas de tutoría individualizada, si es el/la tutor/a el que le transmita la información.

4. El/la tutor/a del alumno/a implicado en un acto de falta de netiqueta podrá comunicarlo al departamento de orientación y/o al/la alumno/a mediador, que podrán hablar directamente con él/ella.

5. Según la gravedad de la ausencia de netiqueta será conveniente comunicarlo a la familia, al equipo directivo del centro educativo o a la persona responsable de llevar a cabo en el centro protocolos frente a riesgos relacionados con las TIC. Sobre todo para llevar a cabo las mismas pautas desde el centro educativo y el entorno familiar.

6. El/la alumno/a debe conocer la responsabilidad de sus actos, debe saber que cumplir con la netiqueta en la red está en su mano y es su obligación cumplirla. Como educador se debe transmitir este papel activo que el alumnado tiene en el cumplimento de netiquetas, tanto a través de sesiones de tutoría, como en asignaturas como Tecnología, Informática, Ética y horas de tutoría, tanto grupal como individual.

7. Cuando el daño ya está hecho debe pedir disculpas si ha sido el causante de alguna situación incómoda o molesta. Y, por supuesto, evitar que vuelva a ocurrir.

Protocolo de respuesta en caso de incidente para el menor implicado.

1. En casos en los que el menor sea víctima de daño moral o de imagen debe avisar al padre, madre o tutor legal para informar de la situación.

2. En el caso en el que el menor se vea involucrado en un incidente por su falta de netiqueta debe buscar ayuda y asesoramiento en la figura de un docente, padre, madre, tutor u otro familiar adulto cercano.

3. Cuando el daño ya está hecho debe pedir disculpas si ha sido el causante de alguna situación incómoda o molesta. Y, por supuesto, evitar que vuelva a ocurrir.

4. Ante la sospecha de que alguien es un *troll* se puede responder educadamente; puede que no lo sea y simplemente es alguien enfadado. Si por el contrario continúa con su comportamiento la mejor solución es no responder, cualquier otra reacción por nuestra parte como intentar razonar con él o insultarle, es su alimento para continuar. Enviar al administrador del sistema un mensaje sobre lo que está ocurriendo es siempre una buena idea. Esta persona le informará de que no es bien recibido en ese lugar, por lo que el *troll* ya no tiene derecho a permanecer en el sitio. En el caso de la suplantación de identidad, públicamente desmentiremos con un simple "ese no era yo" sin entrar en cómo te has sentido pues el *troll* quiere saber que causa dolor, de este modo se evita que se sienta satisfecho y a la vez se crea escepticismo en el resto de los contactos para que estén pendientes. Siempre que se encuentre un *troll* se publicará "alerta *troll*" para que él sepa que se le ha identificado y, al mismo tiempo, alerte a los demás.

Para resolver esta situación se debe hablar abiertamente y con respeto. Pedir un cambio de tono y que se ciña al tema de la discusión con argumentos y sin descalificaciones. Otra opción es ignorar los comentarios pero nunca se debe contestar directamente a los insultos y de igual manera, pues de este modo no se conseguirá parar. Si se le ignora, esta persona acaba perdiendo interés por la conversación.

6. Marco legislativo aplicable a nivel nacional y europeo

La falta de netiqueta como tal no constituye delito. Sin embargo, los daños morales y de imagen que vulneran el Derecho al Honor y la imagen en Internet están contemplados y el incidente puede ser llevado a los tribunales.

Protección de la imagen en la Red

El artículo 18.1 de la Constitución garantiza el Derecho al Honor, a la intimidad personal y familiar y a la propia imagen, concretándose su protección jurídica en el

artículo 7.5 de la Ley Orgánica 1/1.982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, según el cual tendrán la consideración de intromisiones ilegítimas "La captación, reproducción o publicación por fotografía, film o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo 8.2."; ahora bien, "No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso" (art. 2.2 de la citada Ley).

En el caso en el que la fotografía o el hecho lo haya publicado alguien que no se puede identificar, La Ley 34/2.002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico establece una responsabilidad de los prestadores de servicios de intermediación de la sociedad de información, en los que podemos incluir comentarios en los foros abiertos o redes sociales. Esta ley establece que los responsables de la web no son responsables siempre que no tengan conocimiento efectivo de que la actividad o la información es ilícita o lesiona bienes o derechos de un tercero susceptible de indemnización o, si es que lo tienen, actúen con diligencia para retirar los datos o inhabilitar el acceso a ellos.

Protección del Derecho al Honor en Internet

El artículo 7.7 de la anteriormente citada Ley Orgánica 1 / 1.982 define el derecho al honor desde el punto de vista de considerar que hay intromisión por la imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

La indemnización que se puede solicitar varía en función de la gravedad de la lesión a la reputación y la proyección pública que se tenga. Además de indemnización por vía civil, el Código Penal castiga la injuria y la calumnia.

El artículo 208 la define como la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

El artículo 209 establece un agravante si se hace con publicidad, como es el caso de redes sociales.

Según el artículo 205, la calumnia es imputar un delito a sabiendas de la falsedad de la imputación.

Es importante resaltar que el código 510 del Código Penal está siendo revisado para reflejar como agravante la propagación de odio cuando los hechos se hayan llevado a cabo a través de un medio de comunicación social, en Internet, de manera que el daño se hiciera visible y accesible a un muy elevado número de personas.

7. Organismos, entidades y foros de referencia

ORGANISMO / DETALLE
Chaval.es (www.chaval.es) Iniciativa del Ministerio de Industria, Energía y Turismo, puesta en marcha por Red.es para responder a la necesidad de salvar la brecha digital entre padres, madres, tutores y educadores respecto al avance de los menores y jóvenes en el uso de las TIC. Ofrece recursos de sensibilización y formación sobre la netiqueta.
Pantallas Amigas (www.pantallasamigas.net) Pantallas Amigas página que promociona del uso saludable de las tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia. En ella se pueden encontrar consejos y recomendaciones de netiqueta para los menores.
The Alberta's Teachers Association (www.teachers.ab.ca) Organización de profesores que promociona la educación pública. En ella se puede encontrar pautas y recomendaciones para docentes.
European Schoolnet Organización europea clave y referencia en la transformación de la enseñanza y el aprendizaje utilizando la integración de las Tics.

8. Más información

RECURSO / DETALLE

Fundación Alia2 (www.alia2.org)

Fundación dedicada a la protección del menor en Internet. En la página, padres, menores y docentes encontrarán ayuda y asesoramiento para un uso correcto y seguro de la Tecnología.

Words Wound (www.wordswound.org)

Página creada sobre el libro del mismo nombre escrito casi en su totalidad por adolescentes. Es un libro en el que se promueve la amabilidad y las buenas maneras en el mundo físico y en el digital especialmente. En él los menores encontrarán consejos sobre buenas maneras online.

RedAbogacía española (www.abogacia.es)

RedAbogací-a es un portal de servicios telemáticos para los abogados y los colegios de abogados. En esta página padres y docentes pueden informarse sobre cuestiones legales en situaciones provocadas por la falta de netiqueta.

EUKidsOnline (www.ehu.eus)

Universidad del País Vasco. Trabajos de investigación para EUKidsOnline. En esta página padres y, sobretodo, docentes pueden informarse de la situación de los menores europeos. También pueden recoger una serie de actividades y formas de trabajo con los adolescentes para una navegación satisfactoria.

9. Bibliografía

Abogacía española. (2013). Netiqueta móvil: código de buenas maneras. 2015, de RedAbogacía Sitio web: http://www.abogacia.es/2013/04/22/netiqueta-movil-codigo-de-buenas-practicas/

Chiles, D. (2014). Los principios de la Netiqueta. Amazon: Amazon.

Dra. Rapado, M. & Dr.Chiclana, C. (2011). los adolescentes y sus formas de comunicación: Redes Sociales. 2015, de Fundación Alia2 Sitio web: http://www.alia2.org/index.php/es/blog/17?view=blog

Hinduja, S. (2014). Natural Day – Love Yourself Before You Can Love Others. 2015, de Cyberbullying Research Center Sitio web: http://cyberbullying.us/natural-day-love-can-love-others/

Jorge Flores. (2010). Netiqueta joven para redes sociales. 2015, de Pantallas Amigas Sitio web: http://www.netiquetate.com/

La Instrucción de la Fiscalía General del Estado 10/2005, de 6 de octubre, sobre el tratamiento del acoso escolar desde el sistema de justicia juvenil.

La Ley Orgánica 1/1.982 sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen

Putnam, MS. (2006). Reflections on the Golden Rule. 2006, de Global Ethics University. Sitio web: http://www.globalethicsuniversity.com/articles/thegoldenrule.htm

S. Park et al. (2.014) Children and Youth Services Review 42 (2014) 74–81

Smahel, D. & Wright, M.. (2.014). The meaning of online problematic situations for children. 2015, de EUKidsOnline. Sitio web: http://www.ehu.eus/es/web/eukidsonline/hasiera

Virginia Shea. (1.994). Introduction. En Netiquette(160). Albion.com: Albion Books.

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es

"Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad"

[Red.es]

MONOGRÁFICO ACCESO A CONTENIDOS INAPROPIADOS

MONOGRÁFICO ACCESO A CONTENIDOS INAPROPIADOS

1. Objetivo del monógrafico

«Sensibilizar sobre los riesgos del acceso de menores a contenidos inapropiados en Internet, así como ofrecer recomendaciones para su prevención y para saber cómo actuar en caso de que suceda.»

2. Conceptualización y descripción del riesgo

En primer lugar, es importante delimitar aquellos conceptos relacionados con los contenidos inapropiados:

Contenidos inapropiados

Por **contenido inapropiado** entendemos todo material percibido por el menor de edad que sea dañino para él. Son las imágenes y estímulos que provocan un perjuicio en el menor, estos son, aquellos peligros que circulan por la Red, y las características de la información que contienen. Dentro de esta acepción, conviene distinguir entre contenidos *ilícitos*, que son aquellos que no están legalmente permitidos; y los contenidos *nocivos*, que sí están permitidos por Ley pero se consideran dañinos en el desarrollo personal y social de los menores.

Cualquier persona con un mínimo de conocimientos es capaz de encontrar cualquier tipo de información en la Red, y expresarse libremente gracias al amplio canal de comunicación que ofrece. Esto ha favorecido la proliferación de todo tipo de webs, con múltiples y diversos contenidos, muchos de los cuales no son apropiados para el grupo de edad que estamos abordando. A través de Internet, la televisión, el cine, la música o los videojuegos, a los que se accede por dispositivos como el ordenador, los *smartphones,* las tablets, videoconsolas o reproductores de audio y video, los menores tienen a su alcance multitud de contenidos inapropiados.

De este modo, los contenidos inapropiados pueden provocar graves perjuicios en el desarrollo de niños y adolescentes. Haciendo uso de las TIC (ya sea navegar por Internet, ver la televisión, jugar a la videoconsola etc.) los menores de edad, pueden encontrar información no adecuada especialmente para ellos. Son imágenes, actitudes y/o comportamientos que manifiestan y fomentan valores negativos y moralmente

reprobables. Hablamos de contenidos que, bien pueden ser ilegales desde el punto de vista jurídico y han escapado al control de los Cuerpos de Seguridad del Estado, o bien tratarse de contenidos no recomendables para las edades tempranas y reservados para población adulta. Estos son los ejemplos más comunes:

- **Contenidos pornográficos.** Todo el conjunto de obras que contienen imágenes sexuales explícitas con el fin de provocar la excitación del receptor. Debido a sus características, estos materiales no son adecuados para menores de edad por su falta de madurez para asimilar lo que están viendo. Además, los contenidos pornográficos ofrecen una visión distorsionada de las relaciones sexuales, categorizando a hombres y mujeres como meros objetos de deseo. A su vez, pueden generar ilusiones falsas sobre la naturaleza del cuerpo, provocando que el menor se obsesione con una apariencia física estereotipada o un ideal de belleza concreto como requisito indispensable para la satisfacción sexual.

- **Contenidos violentos.** Los menores de edad pueden acceder, a través de diferentes medios digitales, a contenidos de violencia (contra personas, animales u objetos) como son, por ejemplo, los casos de imágenes y videos referentes a peleas, palizas (a una o varias personas), insultos o amenazas a educadores en la escuela, maltrato animal, destrozo de mobiliario urbano etc., **grabados por ellos mismos, o a través de archivos compartidos** y/o difundidos en la Red. Igualmente, los menores pueden acceder, a través de los periódicos e informativos, a contenidos violentos, por ejemplo cuando tratan noticias sobre guerras; ataques terroristas; maltrato y/o asesinatos machistas; manifestaciones y protestas político-sociales que derivan en enfrentamientos; accidentes de tráfico; peleas en deportes colectivos como fútbol; ataques xenófobos, homófobos y discriminatorios, masacres, etc.[1]

  En plataformas de entretenimiento, como las **videoconsolas o juegos online**, los menores también pueden encontrar contenidos violentos: enfrentamientos armados, violencia sexual explícita, violaciones, peleas, colisiones con vehículos, batallas bélicas, agresividad verbal, humillaciones, destrucción de

[1] Bottero M.; Escoto L. y Goncálvez S. (2006) Educación Social y Cívica. Montevideo: Colección Estudiantil.

bienes u objetos, atracos, coacción a la autodeterminación de otros, y suicidios[2].

- **Contenidos falsos o faltos de rigor**. Se refieren a informaciones erróneas o visiblemente falsas que circulan por Internet y llegan fácilmente a un gran número de receptores debido a la naturaleza del contenido y la tendencia a propagarse rápidamente. Esta clase de información puede ser nociva e inapropiada para los menores, ya que podrían ser engañados al dar como ciertas imágenes y contenidos falsos o faltos de rigor, y fomentar en ellos actitudes y conductas inadecuadas. Como ejemplos destacamos:

    - Leyendas urbanas: son historias extravagantes pero verosímiles, que supuestamente han ocurrido, dadas siempre como verdaderas. Suelen arraigarse rápidamente en la cultura, como una verdad indiscutible[3]. Para hacerlas verosímiles, el narrador las cuenta como algo que a su vez le contó y/o sucedió a un amigo cercano. Se trata pues de historias contadas en cadena, a través de servicios de mensajería instantánea o redes sociales, con un contenido extraordinario, morboso, entretenido etc. que las hace atractivas para los receptores.

    - Mensajes en cadena: son tipos de correo basura cuyo fin es la propagación y coacción de alguna manera a los receptores para que los reenvíen a otro grupo de personas. Como ejemplos destacamos los mensajes del tipo:

        "WhatsApp pasa a ser de pago, envía este mensaje a otras 10 personas para que tu cuenta sea gratuita para siempre".

        ¡Atención! Tu teléfono Android ha sido gravemente infectado por un virus que puede conducir a un fallo total. Pulsa en OK para comenzar el proceso de reparación".

      Pueden darse situaciones donde el objetivo del emisor sea engañar o crear alarma en el receptor, transmitiendo información falsa, y

[2] Krug, E.G.; Dahlberg, L.L; Mercy, J.A.; Zwi, A.; Lozano, R. (Ed.) (2002).*World report on violence and health.* Washington: World Health Organization

[3] Orti A.; Sampere J. (2006) Leyendas urbanas. Barcelona: Ed. Martínez Roca

solicitando incluso datos personales que después utiliza de forma fraudulenta o maliciosa[4].

- Videos virales: es el nuevo fenómeno TIC que causa sensación especialmente entre la población más joven. Se trata de grabaciones, que bien pertenecen al ámbito privado de una persona, bien pertenecen a un ámbito público y célebre, difundidas a una enorme cantidad de personas, y compartidas a través de Internet, mensajería instantánea como *Whatsapp*, blogs, redes sociales, correos electrónicos y otros sitios web. Se plantean como retos o desafíos en cadena, y su contenido varía enormemente, lo cual supone también un riesgo potencial para la población menor de edad. Humor, cine, televisión, sexo, violencia, o cualquier contenido que pueda vulnerar la dignidad humana, hace de los virales un elemento a tener en cuenta[5]. Ejemplos de retos virales son el *eye-balling*, que consiste en introducir bebida alcohólica en los ojos para obtener un efecto más inmediato e intenso. Es una práctica altamente peligrosa, que puede causar daños en la vista. Otro ejemplo es el *reto de la pimienta* y el *reto de la canela*, que consiste en tragar pimienta o canela en polvo en el menor tiempo posible, sin beber ningún líquido, lo cual provoca tos, vómitos, irritación de garganta, dificultad para respirar, llegando incluso a la asfixia o el colapso pulmonar.

- El fomento de hábitos que dañan la salud física y psicológica. Durante las últimas décadas, las imágenes y mensajes en medios de comunicación asociados al aspecto corporal ha aumentado de forma notable. Es común encontrar ideales de belleza en medios TIC como la televisión, Internet, cine, prensa, ocio, etc. La mediatización del cuerpo realza los estereotipos imperantes que son asimilados por los ciudadanos. En este punto, damos especial relevancia a los **Trastornos de la Conducta Alimentaria**, caracterizados por comportamientos alterados ante la ingesta alimentaria y en el control del peso. Se trata de alteraciones mentales que conllevan problemas físicos, psicológicos y

[4] Gómez A. (Ed.) (2011) *Beyond good and evil the Spam.* RevistaModmex PC. Num. Septiembre 2011. pp.12-14 http://revistamodmex.wordpress.com

[5] Sánchez Herrera J. (2012) Nuevas tendencias en comunicación. Madrid: ESIC Editorial

sociales de las personas que lo padecen y de su entorno[6]. La información orientada a la búsqueda de ideales de belleza culturalmente establecidos (incluyendo métodos y consejos para perder peso, productos para adelgazar etc.), que en muchas ocasiones no está contrastada ni se acoge a los criterios vigentes de las Ciencias Médicas, lo cual supone un **riesgo para la salud** del menor. La cultura del culto al cuerpo, de los cánones de belleza pre-establecidos, también invade el mundo TIC, de lo cual se empapan forzosamente los más jóvenes, condicionando sus emociones, valores, forma de ver el mundo que les rodea, creencias y comportamiento. En multitud de páginas web podemos encontrar información de riesgo, en tanto en cuanto ofrece imágenes y pautas que pueden causar un daño severo a la propia salud. Tal vez el ejemplo más claro son las direcciones web, blogs etc. que tratan el tema del aspecto físico, y que contienen, entre otros, tablas de ejercicios físicos y dietas para perder peso que no se ajustan a los criterios médicos para el cuidado de la salud y el bienestar. Una de las consecuencias más destacadas del acceso a este tipo de contenidos inapropiados son las alteraciones mentales y emocionales, que conllevan graves problemas físicos y afectan al funcionamiento psicológico y social del individuo y su entorno[7]. Otro ejemplo es el referido al **blanqueamiento dental**. El interés estético y social por lucir dientes más blancos provoca la reproducción de incontables direcciones web, que ofrecen consejos y productos 'milagrosos' para conseguir blanquear los dientes fácil y rápidamente. Según los expertos en medicina, aclarar el color de los dientes supone el uso de productos capaces de eliminar el esmalte dental superficial, lo cual es un riesgo para los tejidos que rodean al diente, causando en muchos casos quemaduras en el tejido gingival, incluso la muerte del diente. De ahí la importancia de acudir a odontólogos profesionales[8].También destacar la proliferación de intervenciones de **cirugía estética**, con especial atención al grupo de edad adolescente. La percepción de la propia

[6] Trinidad Ayela M.R. (2010) Adolescentes: Trastornos de alimentación. Valencia: Editorial Club Universitario

[7] Fundación Imagen y Autoestima (2013) Trastornos de la Conducta Alimentaria. http://www.f-ima.org/es/prevencion/trastornos-relacionados-con-el-peso-y-la-alimentacion

[8] López Andrade M. (2015) El Lado Oscuro del Blanqueamiento Dental. En Europa Press http://www.infosalus.com/estetica/noticia-lado-oscuro-blanqueamiento-dental-20150318092359.html

imagen, o la necesidad de proyectar un aspecto que se adecúe a los cánones imperantes son algunos de los efectos de la cultura de la imagen, y afecta muy especialmente a los menores de edad. El **fomento del consumo de drogas** es otro de los contenidos inapropiados que pueden encontrar los menores en el uso de las TIC, fuertemente vinculados a la cultura del ocio.

- **Los juegos de azar**. Cada vez más presentes en las TIC, se basan en la posibilidad de ganar o perder dinero dependiendo de la capacidad del jugador así como también del azar. En su mayoría son juegos de **apuestas** donde la búsqueda de beneficio económico trae consigo el riesgo de ser engañado, o de perder cantidades considerables de dinero. Estos modelos de negocio que han invadido Internet y demás plataformas tecnológicas se basan en un modelo de 'captación', ofreciendo a los jugadores atractivos premios a cambio de juegos y apuestas sencillas, con lo que es fácil, especialmente en los menores de edad, caer en comportamientos adictivos.

- La afición de los menores de edad a los **videojuegos y juegos online** puede convertirse en un riesgo grave cuando pasan de la afición a la adicción. Los expertos señalan que el porcentaje de jóvenes que emplean largas horas del día a estas actividades se va multiplicando en poco tiempo. El aislamiento en la propia habitación del menor (o en la casa de un amigo) durante horas, encadenando partidas de diferentes partes del mundo, lleva a estos jóvenes a una desconexión total del entorno (no comer con la familia, dejar de interactuar con padres y/o compañeros, descuidar la higiene personal…). El riesgo de los juegos online es que poseen un potencial adictivo, porque da la posibilidad de jugar en casa, con un acceso sencillo. El llamado *Internet GamingDisorder* es un trastorno cuyo tratamiento se ha extendido en nuestro país y a nivel internacional. Los afectados manifiestan problemas asociados a este uso inapropiado como trastornos de conducta, personalidad o depresión. La baja autoestima también parece ser un factor de riesgo importante.

  Estas situaciones de afición y adicción a juegos de azar y/o videojuegos online se traducen en: alteraciones emocionales y conductuales, alteraciones familiares, del humor, irritabilidad, o ansiedad. Además, en muchos casos, la adicción lleva asociada la pérdida de contacto social, problemas económicos

derivados de las apuestas (juegos de azar y páginas de apuestas deportivas), y fracaso académico[9].

- La **publicidad en línea**, cuyo medio de difusión principal es Internet, permite a las compañías dar a conocer sus productos y servicios llegando fácilmente a un gran número de personas de cualquier parte del mundo. Este tipo de publicidad es tomada como contenido inapropiado debido a la ausencia de filtros hacia los destinatarios, corriendo el riesgo de incluir temas no recomendados para los menores de edad[10]. Como ejemplo, la publicidad referente a las bebidas azucaradas, tan demandadas por los jóvenes, ignorándose (incluso por un elevado porcentaje de padres y educadores) los perjuicios que pueden tener para la salud. Las bebidas azucaradas son azúcar líquido, y contienen una cantidad de dulce mayor de la que los profesionales de la Salud recomiendan que pueden consumir niños y jóvenes en todo un día.

- **Contenidos fraudulentos y virus.** Para infectar los sistemas y embaucar a los internautas los delincuentes se apoyan en técnicas de ingeniería social, que se refiere al uso de la manipulación psicológica sobre las personas para conseguir, teniendo en cuenta la tendencia general de éstas a la confianza, que realicen determinadas acciones en su provecho. Por ejemplo, obtener información que le permita un acceso no autorizado a un sistema y, por lo tanto, a la información que resida en el mismo. A pesar de que los objetivos generales de la Ingeniería Social suelen implicar actividades y contextos en los que habitualmente se relacionan adultos, también es posible encontrar situaciones en las que pueden verse implicados los menores: buscar contraseñas en redes sociales, correo electrónico y plataformas de juegos en línea. Para ampliar información, recomendamos la lectura del monográfico “Protección ante virus y fraudes”.

Perfiles psicosociales de los menores con acceso a contenidos inapropiados

Las tecnologías de la información y comunicación aumentan el grado de autonomía y acción de las personas. El mundo virtual se convierte en una extensión del mundo

[9] Unidad de Conductas Adictivas del adolescente. Hospital Sant Joan de Deu de Barcelona (2014) En http://www.lavanguardia.com/vida/20140413/54405725221/triplican-adolescentes-adictos-videojuegos.html

[10] Rodríguez del Pino D.; Miranda J.A.; Olmos A.; Ordozgoiti R. (2012) Publicidad online. Las claves del éxito en Internet. Madrid: ESIC Editorial

físico, lo que supone estar inmerso en un ambiente inteligente que responde a las necesidades, gustos y conocimiento de los menores.

Los niños y adolescentes suelen ser muy recelosos a la hora de abordar cuestiones que pueden llegar a considerar un ataque contra su intimidad. En concreto, aquellos temas referentes a su círculo de amigos, al tipo de contenidos al que acceden en el uso de TIC, el número de horas que emplean con el ordenador, el teléfono móvil o la videoconsola, o con quién establecen conversaciones y envío de mensajes a través de Internet.

Los estudios y análisis centrados los menores usuarios de TIC apuntan a la creciente autonomía de aquellos jóvenes que utilizan a diario la tecnología. Así, a medida que los menores usan más la tecnología, crece de forma sustancial el acceso a servicios y el intercambio de contenidos (apropiados e inapropiados) relacionados con los intereses y gustos de su grupo de iguales, lo cual favorece la interacción entre ellos, pero también se extiende el riesgo que conlleva el acceso a los contenidos inadecuados.

El multiacceso a través de diversos dispositivos, en múltiples lugares, es un rasgo típico y acentuado en los menores. Su vida social, expresada a través de estos medios exige un mayor acceso a Internet y demás tecnologías con mayor intensidad, lo cual explica la cantidad de dispositivos diferentes que poseen y manejan[11].

Por otra parte, algunas características que pueden influir en los hábitos de acceso a Internet que pueden propiciar el acceso a contenidos inapropiados son:

- **Pérdida de control,** que hace alusión al tiempo invertido y a la pérdida de los objetivos de conexión inicial.

- **Evasión,** uso TIC puede proporcionar sensación de evasión de la realidad y bienestar, de modo que la funcionalidad práctica y objetiva de las herramientas pasa a un segundo plano, con el fin de buscar un mayor grado de estimulación y satisfacción, con el consiguiente riesgo de acceder a temáticas no recomendadas para su edad (sexo, violencia, juego, o drogas).

[11] Bringué X.; Sádaba C. (2011). *Menores y Redes Sociales en España.* Madrid: Colección Generaciones Interactivas - Fundación Telefónica

- **Ocultación** por parte del menor tanto del tiempo empleado en Internet y demás tecnologías, como de los objetivos de conexión y las actividades realizadas durante las diferentes sesiones.

- **Abandono de actividades**, para poder dedicar más tiempo al uso de las tecnologías, donde buscarán nuevos contextos de relación y/o actividades de ocio.

- **Chatear y quedar con desconocidos a través de Internet,** muy común sobre todo en las fases iniciales del proceso madurativo, donde pueden tener lugar los comportamientos más inconscientes y de mayor riesgo para la socialización del menor[12].

Motivaciones de los menores para acceder a contenidos inapropiados

Los menores de edad que acceden a contenidos inapropiados en el uso TIC piensan en las tecnologías como un medio óptimo para construir y reconstruir su identidad social en los diferentes escenarios de su vida cotidiana, saciar su curiosidad y morbosidad acerca de temas 'tabú' para su edad, desafiar las prohibiciones y/o recomendaciones de los adultos cercanos a ellos (padres, madres, tutores y educadores), buscar respuestas e información sobre temas delicados que les afectan directa o indirectamente y participar de los sistemas más modernos de comunicación interpersonal. Los más jóvenes consideran normal el compartir información sensible en la Red (un alto porcentaje no ve riesgo en ello), acceder a contenidos 'de moda' pese a ser conscientes de los riesgos que contienen, o acceder a imágenes recomendadas para la edad adulta[13].

Motivaciones individuales

Hablamos de aquellas motivaciones basadas en las emociones, valores, creencias, sentimientos, percepciones, cogniciones, actitudes y conductas de los menores de edad:

[12] Instituto de adicciones, Madrid+Salud (2014) TIC. Prevención de usos problemáticos. http://www.madrid.es/UnidadesDescentralizadas/Salud/Publicaciones%20Propias%20Madrid%20salud/Publicaciones%20Propias%20ISP%20e%20IA/PublicacionesAdicciones/TIC.pdf

[13] United Nation Children´s Fund (UNICEF) (2011) Child Safety online. Global challenges and strategies. http://www.unicef-irc.org/publications/650

- En casos en que son protagonistas (como autores o víctimas) de alguna conducta reprobable (violencia, abuso, coacción) o perjudicial, recurren a los contenidos referidos a tales conductas como fuente de información, como búsqueda de respuesta y solución, etc.

- Buscan formas de evasión e independencia. El acceso a Internet sin filtro y sin supervisión. Es la búsqueda de sensaciones.

- Participar en páginas y redes sociales no recomendadas para menores de edad, representando identidades virtuales ficticias lo cual les permite mostrar una imagen deseable de sí mismos desde la que aspiran a ser percibidos, y a partir de la cual reciben respuestas de amigos y contactos virtuales. Es la posibilidad de cambiar la identidad (ser otro), y mantener el anonimato.

- La curiosidad del adolescente sobre temas socialmente controvertidos, como la violencia o la sexualidad, hace que busque esta clase de contenidos y en este sentido Internet proporciona una manera fácil de acceder a los mismos, bien para responder a sus dudas, bien por curiosidad, etc.

Motivaciones sociales

- Integrarse, formar parte de un grupo con el que poder identificarse. Es el sentimiento de pertenencia a algo común. Sentir que uno forma parte de la cultura imperante.

- Experimentar la sensación de anonimato, y la sensación de impunidad (poder acceder a contenidos castigados por Ley sin riesgo)

- Interés en experimentar con el sexo o con su sexualidad, presionados por una cultura sexualizada en exceso.

- Estar informado como una necesidad imperiosa. Estar al tanto de aquello que es tendencia (*trendingtopic*), a fin de integrarse en los usos y costumbres sociales imperantes.

Consecuencias del acceso a contenidos inapropiados

Llegados a este punto, resulta fundamental conocer el impacto que tiene el acceso a contenidos inapropiados en las emociones, actitudes, valores y comportamiento de los

menores. En los últimos años, los profesionales de la salud, la educación, y las tecnologías comparten preocupación acerca de la exposición de los más jóvenes a las representaciones explícitas y contenidos desagradables (violencia, sexo, drogas, etc.). Esta exposición temprana y sin filtro alguno les está convirtiendo, entre otros, en personas sexualmente activas a edades cada vez más tempranas. Por todo ello, los investigadores en estos campos constatan el aumento de la violencia y el abuso en las relaciones sexuales, la adicción a la pornografía, el aumento de la aceptación de los estereotipos sexuales y el aumento de la obsesión con la imagen corporal.

Los estudiosos constatan el gran impacto emocional que ciertos contenidos TIC provocan en los menores, sumado al aumento del porcentaje de jóvenes que, por el uso reiterado de las nuevas tecnologías, se han convertido en dependientes de las mismas. En los últimos años ha aumentado el número de menores de edad que abusan de las TIC, un perfil altamente influenciable y con riesgo de adicciones en diferentes ámbitos. Es uno de los principales motivos de preocupación, tanto para padres como educadores, la posibilidad de que aparezcan comportamientos adictivos que pueden alterar el desarrollo personal y social de los más jóvenes.

Entre las principales consecuencias del acceso a contenidos inapropiados en el uso tecnológico destacamos: el descuido de la vida personal y actividades de ocio de los menores, el aislamiento social, el desarrollo o empeoramiento de trastornos como la soledad o la depresión, la adicción a contenidos violentos y perversos (permanentemente asociados a los videojuegos trasgresores y realistas indicados para adultos), la pérdida de la privacidad, y el fomento del consumo inadecuado (drogas, juegos de azar, apuestas). La población adolescente y su entorno pueden verse afectados a causa de la posibilidad que ofrecen las TIC de obtener gran cantidad de información sobre sus usuarios, muchas veces sin que sean conscientes de ello (campañas de publicidad implícitas o persuasivas)[14].

Las TIC permiten la construcción de la identidad como base de la interacción *online* de los jóvenes, que además pueden inventar identidades y roles que en la vida real no tienen, gracias al anonimato que ofrecen las tecnologías. Esto también puede llevarles a tener vidas paralelas, una *online* y otra *offline*, al construir distintas identidades, que

[14] Naval C.; Sádaba Ch.; Bringué X. (2003) Impacto de las Tecnologías de la Información y la Comunicación (TIC) en relaciones sociales de los jóvenes navarros. Gobierno de Navarra. Instituto Navarro de Deporte y Salud.

tal vez puede llegar a tener efectos perjudiciales para su desarrollo[15].Partiendo de la premisa de que los grupos de población más jóvenes (niños y adolescentes) están en proceso de socialización y conformación de la personalidad e identidad, y por tanto son los más influenciables, una serie de estudios nacionales revelan que una de las consecuencias más peligrosas del efecto de los medios de información y comunicación sobre la imagen corporal es que, el éxito personal y social (sentido positivo de pertenencia a un grupo y una cultura), queda ligado a la imagen corporal de los individuos. Los medios tecnológicos de difusión son agentes poderosos en la transmisión de valores e ideas, y pueden llegar a condicionar o distorsionar la visión de la realidad de los menores. Así, por ejemplo, los personajes con más protagonismo en Internet, cine o televisión acaban convirtiéndose en referentes estéticos, individuales y sociales para la audiencia[16].

3. Datos de situación y diagnóstico

El uso cotidiano de las tecnologías, con Internet a la cabeza, implica una serie de riesgos a los que están expuestos los menores de edad, al ofrecer una tipología muy variada de contenidos. Multitud de estudios vienen abordando en los últimos años los principales problemas a los que se enfrentan padres y educadores en relación al acceso de los menores de edad a contenidos inapropiados. Por ello, existe una preocupación creciente acerca de la facilidad con que los menores pueden acceder a los mismos. En este sentido, se pone especial énfasis en buscar herramientas útiles para educar y concienciar a los más jóvenes en un uso responsable y seguro de las tecnologías[17].

Desde hace años, vienen proliferando investigaciones sobre el acceso a TIC de los menores de edad. La mayoría de los estudios iniciales, desde el año 2000, revelaron que un porcentaje alto de jóvenes no había recibido formación alguna sobre las normas básicas de seguridad a la hora de conectarse y navegar por Internet. Además, se observó que una mayoría de menores accedía a la Red desde dispositivos que no contaban con ningún sistema de seguridad ni filtrado de contenidos, con lo cual

[15] Castells M. (2001) Internet y la Sociedad Red. Lección inaugural del programa de doctorado sobre la sociedad de la información y el conocimiento (UOC). http://tecnologiaedu.us.es/revistaslibros/castells.htm
[16] Guerro-Prado D.; Barjau J. M.; Chinchilla A. (2001) *Epidemiología de los trastornos de la conducta alimentaria e influencia mediática: una revisión de la literatura*. Actas Españolas de Psiquiatría 29 pp. 403-410.
[17] Katz R. (2009). El papel de las TIC en el desarrollo. Madrid: Fundación Telefónica

alrededor de un 40% de los menores lograba acceder a contenidos inapropiados, elevándose el porcentaje según mayor edad[18].

En la actualidad, los menores disponen de mucha más información y conocimiento sobre manejo de TIC, y aun así, un porcentaje elevado sigue accediendo a contenidos no apropiados para su edad. Así, en los últimos años, varios estudios han tratado el acceso a contenidos inapropiados para menores, especialmente aquellos de carácter pornográfico[19], el ciberacoso, el *grooming* y la exposición de datos privados en la Red[20]. Del mismo modo, una reciente investigación en la que participaron una veintena de países europeos estudió la manera en que los más jóvenes utilizaban Internet, con el fin de identificar los factores de riesgo relativos a la seguridad en la Red. En ese estudio se puso de manifiesto la preocupación de los padres por el tipo de contenidos a los que tenían acceso sus hijos: imágenes explícitas de sexo o violencia (un 65%), que fuesen objeto de *grooming* (un 60%), o que pudiesen acceder a información dañina para su salud (55%)[21].

Además, tal como se ha podido comprobar, la actividad de riesgo más común entre los menores es relacionarse vía online con gente desconocida siendo el segundo riesgo más común la exposición a peligros potenciales al acceder a contenidos inapropiados (violencia, sexo, conductas dañinas para la salud). En este sentido, según las conclusiones de los estudios realizados por Media Smartsun elevado porcentaje de jóvenes reconoce consumir pornografía, si bien es más común entre los chicos que las chicas, y en los grupos de edad 14-17 años[22].

En cuanto a la reacción de los niños y adolescentes ante contenido inapropiado en la Red podemos decir que, aunque ésta varía en función de los grupos de edad, son pocos los menores que se mantienen al margen de las TIC tras una situación comprometida. Así, cuando acceden a una página web o reciben información que les resulta desagradable, en torno al 70% de ellos cambia de web, borra el correo o

---

[18] Instituto Nacional de Tecnologías de la Comunicación (2007).*Los controles parentales: cómo vigilar a qué contenidos de Internet acceden nuestros hijos.* Recuperado de: https://www.incibe.es/file/6CvtjRIY-9gkEhLjAz6BbA

[19] Mitchell K.; Finkelhor D.; Wolak J. (2003) *The Exposure of Youth to Unwanted Sexual Material on the Internet: A National Survey of Risk, Impact, and Prevention*. Youth & Society, 34(3), pp. 330-358.

[20]*Smith P.; Mahdavi J.; Carvalho M.; Fisher S.; Russell S.; Tippett N. (2008) Cyberbullying: Its nature and impact in secondary school pupils.* Journal of Child Psychology and Psychiatry, 49, pp.376-385.

[21]Hasebrink U.; Ólafsson K.; Štětka V. (2009) *Opportunities and pitfalls of crossnational research*. In S. Livingstone and L. Haddon (Eds.), Kids Online: Opportunities and Risks for Children (41-53). Bristol: ThePolicyPress

[22] Livingstone S.; Haddon L.; Gorzig A.; Olafsson K. (2011) Risks and safety on the internet: the perspective of European children. Full findings. EU Kids Online, LSE, London

abandona el chat. Un 20,3% continúa navegando y/o conversando. Y un 9,66% opta por comentarlo con un adulto de su confianza[23].

4. Ejemplos de casos reales

A continuación vamos a exponer una serie de ejemplos de casos reales referidos al acceso a contenido inapropiado por parte de menores de edad.

Noticia: "Tampodka, *eyeballing* y *oxy-shots*: las prácticas con alcohol más arriesgadas"[24]

> Beber alcohol con celeridad para que suba cuanto antes y coger un colocón instantáneamente se ha convertido en la prioridad para algunos adolescentes cuando salen de fiesta. Las prácticas son cada vez más peligrosas y dañinas (…) Las modas y tendencias importadas de países extranjeros en las que los grados etílicos tienen su preponderancia parecen alcanzar un nuevo cenit en las últimas semanas con varias experiencias irreflexivas que ponen a prueba la propia vida de los adolescentes. (…) El «tampodka» resulta de la fusión de los términos «tampón» y «vodka» y no es otra cosa que la introducción vía vaginal de un tampón impregnado en alcohol de alta graduación, normalmente whisky o vodka. Desde esta zona, muy irrigada, el alcohol pasa directamente a la sangre y los síntomas de la borrachera se producen con mayor intensidad y celeridad. (…)En el caso del «eyeballing», aún va más allá, puesto que introducen el alcohol en la córnea como si fuese un colirio, cogen una botella y se lo echan directamente en el ojo, lo que ocasiona no solo conjuntivitis en el menor de los casos, sino lesiones de córnea, en la mucosa (…) El «oxy-shots», que consiste en inhalar chupitos de alcohol a través de un sistema de inhalación como los asmáticos, para absorber el alcohol más velozmente por

[23] Miranda de Larra R. (2005) Los menores en la Red: comportamiento y navegación segura. Madrid: Biblioteca Fundación AUNA

[24] http://www.abc.es/sociedad/20130617/abci-tampodka-eyeballing-alcohol-adolescentes-201306111114.html

vía aérea. Esta práctica de ingerir alcohol en dispositivos de nebulización junto con oxígeno al igual que en los tratamientos broncodilatadores, como las anteriores, «daña el sistema nervioso» y esquiva el filtro hepático de la sustancia tóxica, además de que «podría acarrear patologías pulmonares graves.

Noticia: "El reto de la canela: los peligros de un chiste de adolescentes"[25]

El "reto de la canela", (Cinnamonchallenge, en inglés), ha sido el tema de muchos videos que circulan en las redes sociales, en los que se ve a adolescentes intentando tragar una cucharada de canela en polvo en 60 segundos sin la ayuda de agua. Las imágenes muestran que, poco después, la gente expulsa parte del polvo por la nariz, en lo que se conoce como "aliento de dragón". Puede parecer apenas una broma tonta, pero expertos médicos aseguran que puede causar problemas de respiración, inflamación, sarpullido, irritación, ataques de asma y cicatrices en el pulmón que pueden durar años, si no para siempre. (…) Sólo en 2012, en Estados Unidos se registraron más de 220 llamadas al centro de envenenamiento de jóvenes afectados tras ingerir canela en polvo sin agua. A más de 30 se les recomendó atención médica inmediata.

Noticia: "El 21% de los adolescentes españoles están en riesgo de ser adictos a Internet"[26]

El 21,3 % de los adolescentes españoles presentan indicios de desarrollar una conducta adictiva a Internet por el elevado tiempo que pasan conectados a la Red. Es decir, presentan indicios de aislamiento, irascibilidad y dejan de hacer cosas que antes hacían por estar en las redes sociales. Esta es la conclusión a la que ha

[25] http://www.bbc.co.uk/mundo/noticias/2013/05/130424_salud_cinnamon_challenge_canela_gtg
[26] http://sociedad.elpais.com/sociedad/2013/01/15/actualidad/1358257857_400678.html

llegado un estudio realizado sobre conductas adictivas en Internet, hecho en siete países europeos por la asociación Protégeles (…) El 58% de los jóvenes europeos ha accedido a imágenes pornográficas en la Red, aunque para un 33% esta ha sido una experiencia "desagradable". España se sitúa entre los porcentajes más bajos de exposición a este tipo de imágenes.

5. Estrategias, pautas y recomendaciones para su prevención

El papel de los padres/tutores y educadores en la educación de los menores en relación al uso responsable de las TIC es fundamental y necesario, de cara a la prevención de hábitos peligrosos para la salud y el bienestar por el acceso a contenidos inapropiados. El papel de la familia y los educadores es integrar los mensajes y actitudes hacia las nuevas tecnologías dentro del mismo estilo educativo positivo que emplean en otros ámbitos de la vida cotidiana, evitando los posicionamientos alarmistas.

En España la mayoría de políticas de protección de la infancia en el entorno audiovisual se basan en medidas de carácter restrictivo sobre la accesibilidad de determinados contenidos perjudiciales para públicos infantiles. En este sentido, resulta interesante que padres, madres, tutores y educadores conozcan la existencia de sistemas de clasificación de contenidos, entre los cuales podemos destacar los siguientes:

Criterios del Instituto de Cinematografía y de las Artes Audiovisuales (ICAA)

Los criterios del Instituto de la Cinematografía y de las Artes Audiovisuales (ICAA), organismo adscrito a la Secretaría de Estado de Cultura, sirven como principios orientativos para la Comisión de Calificación de Películas Cinematográficas, y permiten así la orientación de padres, madres, tutores y educadores de los menores de edad, además de posibilitar que los operadores/editores de televisión califiquen el resto de contenidos audiovisuales. El instrumento central del sistema de clasificación de contenidos en televisión es el Código de Autorregulación sobre contenidos televisivos e infancia, el cual considera que la clasificación del contenido audiovisual desempeña un papel primordial en la protección de los menores en el acceso a

medios como la televisión, el cine, los videojuegos e Internet. El ICAA establece unos criterios para poder calificar por grupos de edad los contenidos audiovisuales antes de su exhibición. El propósito es que los espectadores, especialmente aquellos que tienen responsabilidades educativas, formativas o de tutela sobre menores de edad, puedan tener conocimiento adecuado de lo que representa una determinada calificación atribuida a una película, y disponer así de información de calidad para responder de manera responsable con respecto a sus hijos o alumnos. De igual forma se examina el funcionamiento de la calificación por edades en otros países de nuestro entorno, y en otros contextos que presentan similitud con el sector audiovisual, como Internet y los videojuegos[27].

Clasificación PEGI y PEGI online

El sistema de clasificación por edades establecido por Información Paneuropea sobre Juegos (PEGI) se estableció en el año 2003, para ayudar a padres, madres y tutores a tomar decisiones responsables a la hora de adquirir videojuegos. Es un sistema que se utiliza en la mayor parte de Europa, respaldado por los principales fabricantes de videoconsolas así como por editores y desarrolladores de juegos interactivos. Además de los juegos de videoconsola, muchas direcciones web también contienen juegos, por lo que se diseñó la etiqueta, que indica que los jugadores de todos los grupos de edades pueden jugar porque no incluye ningún contenido de juego potencialmente inapropiado: violencia, actividad o insinuación sexual, desnudos, lenguaje soez, juegos de apuestas, fomento o consumo de drogas, y escenas de miedo. Si los videojuegos contienen alguno de estos elementos, son clasificados por edades según el sistema estándar de clasificación PEGI, consistente en etiquetas de clasificación por edad y descriptor de contenido.

[27] Fuente Cobo C. (Dir.) (2014) La protección del menor tras la Ley General de la Comunicación Audiovisual. ICmedianet
http://www.icmedianet.org/wp/ndog/wp-content/uploads/2014/01/Proteccion-Menor1.pdf

Por su parte, PEGI Online es un complemento del sistema PEGI, cuyo objetivo es ofrecer a los menores de edad una mejor protección frente a contenidos de juegos en línea inadecuados, así como mostrar a los padres, madres y educadores cómo garantizar un juego en línea seguro, y comprender los riesgos y el potencial daño que existe en el entorno online[28].

A continuación se presentan un conjunto de estrategias, pautas y recomendaciones que ayuden a padres y educadores a prevenir los riesgos en materia de seguridad TIC y el acceso a contenidos inapropiados:

- Hablar cotidianamente con los menores acerca de sus experiencias con el uso TIC para así conocer sus preocupaciones y poder ofrecerles la confianza para hablar de cualquier tema, resolver sus dudas o problemas relacionados con algún contenido. Así, se concluye que resulta más constructivo para el correcto desarrollo de los jóvenes que los padres y educadores intervengan con una actitud positiva y dispuesta al diálogo, con el fin de llegar a una utilización más beneficiosa de la tecnología[29].

- Fomentar un uso responsable de las tecnologías. Para ello resulta interesante hacer del uso de Internet y otras tecnologías una actividad familiar o escolar colectiva. Cuanto más tiempo se comparta con los menores en el uso de TIC más se aprenderá acerca de sus comportamientos, gustos e intereses.

- No amenazar a los hijos con “desconectarles”, pues eso puede traer el riesgo de que encuentren formas para seguir accediendo a esos contenidos sin el consentimiento de sus padres (saltándose los controles, usando el ordenador de algún amigo/a etc.).[30]

- Compartir el tiempo de navegación, enseñarles a controlar y manejar Internet de forma responsable. La tecnología es un medio importante de control, pero no puede sustituir completamente la tarea de padres y educadores. La educación, la supervisión y la implicación directa de los padres/tutores y educadores es la mejor manera de proteger a los menores.

---

[28] Pan European Game Information http://www.pegi.info/es/index/id/1397/

[29] Fundación Imagen y autoestima (2013) *La prevención desde los medios de comunicación.* Recuperado de: http://www.f-ima.org/es/prevencion/la-prevencion-desde-las-empresas

[30] Mc Lean S. (2013). *Inappropriate Content.* Victoria University. Recuperado de: http://www.education.vic.gov.au/Documents/about/programs/bullystoppers/sminappropriate.pdf

- El ordenador debe estar en un sitio visible de la casa, de manera que los adultos puedan supervisar para qué se utiliza.

- Los padres han de fijar (de acuerdo con sus hijos y atendiendo a la edad de éstos) unos límites de uso y tiempo para Internet.

- Los padres y los educadores deben familiarizarse y formarse en los peligros de los contenidos inapropiados.

- El uso de controles de filtrado y controles parentales (adaptados a cada grupo de edad) debe realizarse tanto en el entorno familiar como en el escolar.

- Los padres y los educadores tienen la tarea de enseñar a los niños la necesidad de llevar a cabo una adecuada gestión de privacidad desde edades tempranas, explicándoles por qué es importante que los niños respeten, y exijan el derecho a ser respetados[31].

Control parental y límites de uso

De cara a prevenir para que los menores de edad no accedan a contenidos inapropiados en el uso de las TIC, existen varias herramientas y sistemas de filtrado de contenidos para ayudar al control parental:

- Los **buscadores diseñados específicamente para los menores** de edad representan una herramienta altamente útil para la prevención y la navegación segura. Como ejemplos destacan *Yahoo! Kids, Ask Kids,* y *Kids Click*. Además de éstos, algunos buscadores generales también ofrecen configuraciones concretas que permiten filtrar determinados contenidos y direcciones inapropiadas para los menores de edad, los denominados *Safe Search* que pueden encontrarse en *Google, Yahoo, Bing…*

  La aplicación de video *YouTube,* ha estrenado recientemente una versión dedicada exclusivamente a los menores, llamada *YouTube Kids.* Es un programa gratuito cuyo contenido está centrado en temáticas e imágenes recomendadas para los más jóvenes. Así, se aconseja la utilización de

[31] Instituto de Adicciones. Madrid + Salud (2014). *TIC Prevención de usos problemáticos*. Recuperado de: http://www.madrid.es/UnidadesDescentralizadas/Salud/Publicaciones%20Propias%20Madrid%20salud/Publicaciones%20Propias%20ISP%20e%20IA/PublicacionesAdicciones/TIC.pdf

navegadores diseñados específicamente para menores de edad, los cuales presentan una serie de características que los hacen más seguros y accesibles. Entre las características que podemos destacar se encuentran:

- Diseño colorido e intuitivo, fácil de usar.
- Contenidos infantiles y juveniles, tales como recursos educativos, vídeos, juegos, etc.
- Filtros que impiden el acceso a contenidos inapropiados para su edad.
- Bloqueo de programas y aplicaciones que estén instaladas en el ordenador, pero cuyo empleo por parte del menor se quiera evitar.
- Protección para evitar que los menores borren archivos o modifiquen configuraciones del ordenador.
- Límite de tiempo de uso: bloquean la pantalla después de un determinado lapso.
- Posibilidad de personalizar los fondos y otras configuraciones con temas infantiles.

- Por otro lado, los **Proveedores de Servicio de Internet**, conocidos como ISP (Internet *Service Provider*), son compañías que, además de conexión a la Red, ofrecen a los usuarios programas informáticos con filtros incorporados para proteger a los menores de edad en el acceso a contenidos inadecuados. Además de este servicio útil para padres/tutores y educadores, también existen una serie de **aplicaciones recomendadas** expresamente para niños, como por ejemplo:
  - *El Búho Boo*: juego para preescolares con el que aprender a identificar los sonidos de cada animal gracias a sus primeras interacciones con una pantalla táctil.
  - *Temple run*: juego en el que correr por un laberinto esquivando obstáculos gracias a diferentes interacciones con la pantalla.
  - *Art of glow:* aplicación de dibujo con resplandor y animaciones configurables.

- *Paper:* aplicación para escribir y dibujar en una libreta con trazos realistas.
- *iCuadernos by Rubio:* los auténticos cuadernos de operaciones, escritura y problemas de Rubio llevados al iPad.
- *Toca Doctor*: aplicaciones dibujos y puzzles para que los niños jueguen a ser doctores.
- *En tus manos*: para aprender educación vial de forma divertida. Contiene un simulador para aprender a conducir un ciclomotor.
- *Toontastic:* permite crear historias propias, eligiendo personajes, diálogos, música y narración.
- *Kindle*.: lector de libros infantiles que además permite conexión con *smartphone* y Tableta.[32]

- En el mercado podemos encontrar diferentes **sistemas de control parental** de los contenidos, que van actualizándose en poco espacio de tiempo. Además, una multitud de programas, algunos gratuitos y otros bajo licencia de pago, permiten también diferentes métodos de filtrado. De este modo, los filtros de contenido son la más común de las herramientas tecnológicas de protección permitiendo a los usuarios decidir cuáles son los contenidos de Internet que considera inapropiados y, en función de ello, disponer a qué páginas se puede acceder y a cuáles no. La gran mayoría de filtros comerciales ofrece una serie de servicios adicionales como denegar el acceso a algunos servicios (chats, descargas de documentos, conexiones P2P, o comercio electrónico), o establecer distintos perfiles de usuario. Existen multitud de filtros comerciales, de fácil instalación y a precios asequibles.

De este modo, Internet presenta a los padres/tutores y educadores oportunidades únicas para tomar un papel más directo a la hora de decidir qué pueden ver y hacer sus hijos y alumnos. Pueden dirigir a los niños hacia contenidos beneficiosos, a la vez entretenidos, adaptados a la edad de cada niño/a, a su cultura, su capacidad intelectual o preferencias. También ofrece la oportunidad de educarles sobre un uso

[32] Chaval.es (2015) http://www.chaval.es/chavales/proteccion/las-diez-mejores-aplicaciones-para-menores

constructivo de Internet y proporcionar criterios para evitar un comportamiento de riesgo online y el acceso a contenidos inapropiados. Es muy importante que desde todas las esferas (padres, educadores, instituciones y gobiernos) se trabaje conjuntamente para crear los entornos seguros y accesibles para niños y jóvenes, ya se encuentren en casa, en la escuela o en instalaciones públicas como las bibliotecas o cibercafés. Es responsabilidad de todos fomentar estos entornos, de forma que los menores puedan disfrutar y aprovechar los contenidos positivos de Internet.[33]

Estrategias de prevención ante contenidos pornográficos

- Conversar con los hijos/alumnos sobre sexo y relaciones sexuales saludables desde una edad temprana adaptándonos al nivel de desarrollo y madurez de los mismos. No debemos olvidar que están expuestos a imágenes de contenido sexual a través de diferentes medios de información, por lo que es necesario establecer un diálogo abierto y honesto con los jóvenes, a fin de que ellos se sientan seguros y confiados de recurrir a los padres y educadores para resolver sus dudas.

- Fomentar el pensamiento crítico de los menores acerca de los estereotipos sexuales. Mostrar a los menores cómo los niños y niñas son representados en objetos de la vida cotidiana, como juguetes, catálogos de ropa, anuncios o películas. Debatir con ellos sobre cómo estos estereotipos se diferencian de su propia realidad.

- Usar software y/o suscribirse a servicios de Internet para controlar, filtrar y bloquear contenidos sexuales explícitos. En el caso de que esta medida sea poco práctica debido a que los menores quieran o necesiten mayor acceso a Internet, pueden utilizarse las opciones de filtrado disponibles en los motores de búsqueda.

- Si los menores encuentran de manera accidental un contenido pornográfico es fundamental mantener la calma. En muchos casos estos sitios aparecen accidentalmente a través de, por ejemplo, la publicidad en línea, siendo difíciles de eliminar. El objetivo es que los niños se sientan cómodos para recurrir a sus

[33] Internet Society (2013). Recuperado de: http://www.internetsociety.org/sites/default/files/bp-childrenandtheinternet-20129017-en_ES.pdf

padres o educadores en busca de ayuda y consejo cuando suceden estos incidentes. Hay que actuar con tranquilidad pero haciéndoles entender el carácter nocivo de tales contenidos para ellos.

Al alcanzar la adolescencia, aumenta el porcentaje de jóvenes que paga por acceder a contenidos pornográficos. Es natural en ellos ser curiosos acerca de la sexualidad e investigar antes de preguntar a sus padres o educadores cuestiones que puedan resultarles embarazosas. El problema de la pornografía es que es una respuesta a una preocupación poco saludable (por la visión tan grotesca y distorsionada de la sexualidad).

- A partir de cierta edad, los filtros dejan de ser una solución viable, ya que suelen bloquear de manera indiscriminada, tanto los sitios web pornográficos, como los sitios recomendados de educación sexual saludable. Desde aquí, el mejor enfoque para los padres es el diálogo permanente que reconoce el interés en las relaciones y el sexo como algo normal, ayudándoles a desarrollar las habilidades de pensamiento crítico que necesitan para tomar decisiones responsables en el uso TIC.

- Discutir sobre los mensajes sexuales que aparecen en diversos medios de información y comunicación. La alfabetización mediática ha resultado ser muy eficaz para ayudar a los jóvenes a comprender cómo las representaciones sexuales que aparecen en los medios de comunicación sexualizada pueden ser inexactas. Es fundamental ayudar a los hijos y alumnos a entender los efectos nocivos de las imágenes que degradan y explotan a las mujeres o a las niñas; de igual forma son nocivas las imágenes que promueven y presionan socialmente a los varones para ajustarse a un modelo masculino (centrado en el atractivo sexual y la destreza). Es importante atender a los estereotipos de género que pueden ser reproducidos por los medios de comunicación y que contribuyen a los roles sexuales retratados en la pornografía.

- Orientar a los hijos y alumnos para el acceso a direcciones web con contenido positivo que aportan información valiosa para una sexualidad saludable. Si la única fuente de información que los menores reciben acerca de la sexualidad son los sitios pornográficos, los padres y educadores se enfrentarán a un problema serio. Es necesario explorar junto a ellos y entender las diferencias

entre una expresión sexual saludable y normal, frente a la actividad de explotación tan frecuente en determinados sitios web[34].

Recomendaciones sobre contenidos de juegos y apuestas

Los juegos en línea pueden parecer inofensivos a simple vista. Sin embargo, la industria de los juegos de azar y casas de apuestas por Internet crece de forma exponencial. Es importante mantener conversaciones con los menores acerca de este tipo de ocio.

- Discutir con ellos cuáles son los principales riesgos de los juegos de azar (comportamientos adictivos, problemas económicos…)
- Recordar a los menores que si existen multitud de direcciones web de juegos y y apuestas es debido a que ingresan mucho más dinero del que regalan a los jugadores.
- Educar correctamente acerca de la estadística y las probabilidades, siempre presentes en los juegos de azar y apuestas.
- Tomar en consideración los propios hábitos de los padres, los cuales pueden influir y condicionar a los hijos (afición de los padres a los juegos online). Nunca hay que olvidar que lo que ve el niño en casa condiciona su manera de pensar y actuar[35].

Recomendaciones sobre contenidos dañinos para la salud

Es fundamental que los diferentes medios de información y comunicación participen activamente como promotores de salud, tanto física como mental, como potenciadores de valores positivos de nuestra cultura. Además, el papel de padres y educadores es primordial a la hora de encontrar pautas de actuación conjuntas:

- Promover la imagen de modelos corporales realistas que fomenten la salud.Mostrar a los menores modelos corporales más cercanos a la realidad de

[34] MediaSmart. Canada´s center for digital and media literacy (2014). *Responding to online pornography* http://mediasmarts.ca/digital-media-literacy/digital-issues/pornography/responding-online-pornography

[35] MediaSmart. Canada´s center por digital and media literacy (2014). *Gambling* http://mediasmarts.ca/digital-media-literacy/digital-issues/gambling

las personas puede contribuir a la mejora de su salud física y psicológica, debido a la importancia los más jóvenes atribuyen al físico y los riesgos de querer modificarlo a partir de dietas o conductas poco saludables.

- Advertirles sobre los riesgos que conllevan algunas informaciones que aparecen en la Red u otros medios de comunicación. Enseñarles a ser críticos y contrastar la información, ya sea con sus padres y educadores, o visitando sitios web de confianza (aprobados por los adultos).

- Fomentar la diversidad corporal y el respeto a ésta como un hecho y una riqueza. Cuando educamos a los hijos y a los alumnos en la diversidad corporal presente en la sociedad, contribuimos a evitar que desarrollen estereotipos asociados a la apariencia física.

- Promover estilos de vida y hábitos alimentarios saludables, enseñándoles cuáles son esas falsas creencias que pueden encontrar en la Red.La promoción de estilos de vida saludables relacionados con una buena alimentación, y el no consumo de drogas, debe ser el medio a través del cual padres y educadores fomenten la salud y ayuden a prevenir conductas de riesgo.

- Educarles en el desarrollo positivo de la autoestima, más allá del físico, y más allá de 'modas' (por ejemplo beber o fumar para sentirse integrado en el grupo social). Educarles en el pensamiento crítico, en la autonomía y capacidad de toma de decisiones.

- Fomentar en los jóvenes (desde edad temprana) estilos de vida saludables a través de mensajes que promuevan actitudes y hábitos propios de una alimentación saludable y equilibrada. Ayudarles a obtener por sí mismos información positiva sobre el cuidado de la salud en Internet (orientándoles sobre direcciones web). Facilitarles videojuegos que fomenten y eduquen en dichos estilos saludables y eviten otros relacionados con conductas de riesgo (personajes de videojuegos consumiendo drogas, o bebiendo alcohol).

- Proteger especialmente la población adolescente, más predispuesta a sentirse insatisfecha con el físico e incorporar conductas de riesgo. Los adolescentes son más influenciables a la hora de consumir drogas o llevar a cabo acciones

vistas en la Red que suponen un riesgo para su salud (reto de la pimienta, lanzarse desde un balcón a la piscina, etc.).

- Educarles en contenidos sobre las mujeres no centrados en su apariencia física. El bombardeo constante al que se ven sometidas las mujeres con mensajes que llegan desde los medios de información (la moda, la estética o la alimentación) contribuyen a favorecer la interiorización del modelo de delgadez como objetivo principal que deben alcanzar, además de reproducir los estereotipos sexuales.

- Mostrar sensibilidad a la hora de afrontar los trastornos de la conducta alimentaria o los problemas con el consumo de sustancias nocivas para la salud. Al hablar con los menores de este tipo de trastornos y conductas es básico fundamentar las informaciones con datos reales. Para ello, resulta útil el asesoramiento previo por parte de profesionales de la medicina o la psicología, expertos en los trastornos alimentarios.

- Enseñarles cuáles son las consecuencias de las conductas de riesgo relacionadas con la salud, como las dietas milagrosas, productos de adelgazamiento, productos bajos en calorías que encuentran en miles de sitios web o el consumo de alcohol y demás drogas[36,37].

También señalar que los centros educativos tienen la posibilidad de participar en el **Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos**[38], que pretende potenciar actuaciones preventivas en relación con los riesgos a los que se ven sometidos los menores y los jóvenes, en temas tan importantes como el uso de Internet y las nuevas tecnologías, entre otros. En el marco de este Plan los miembros de las Fuerzas y Cuerpos de Seguridad realizan charlas, visitas y actividades en centros escolares, dirigidas tanto al alumnado como al resto de la comunidad educativa (directivos, personal docente y Asociaciones de Madres y Padres de Alumnos). Como medidas adicionales, se contemplan

[36] Moreno J.L. (2010).*Moral corporal, trastornos alimentarios y clase social*. Madrid: Centro de Investigaciones Sociológicas

[37] Paricio M.P; Fernández C. (coord.) (2012).*Adicciones, estrategias de prevención y comunicación*. Barcelona: Erasmus Ediciones

[38] Ministerio del Interior. Instrucción nº 7/2013 de la Secretaría de Seguridad, sobre el "Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos". Recuperado de: http://www.interior.gob.es/documents/642012/1568685/Instruccion_7_2013.pdf/cef1a61c-8fe4-458d-ae0d-ca1f3d336ace

acciones de sensibilización y formación dirigidas a concienciar sobre el "uso responsable de las nuevas tecnologías y los riesgos que las mismas pueden implicar, promoviendo, a su vez, la comunicación a su entorno familiar, educativo o a las Fuerzas de Seguridad de los hechos de los que pueden ser víctimas o testigos.

Recomendaciones a trasladar a los menores

Para evitar el acceso de los menores a contenidos inapropiados para su edad, debemos recomendarles:

- Selecciona previamente los contenidos de blogs, foros, páginas etc. a los que vas a acceder, evitando aquellos de carácter violento, pornográfico o discriminatorio. Es fundamental que accedas sólo a aquellos contenidos recomendados y adaptados a tu edad.

- No ofrezcas información personal para evitar que alguien pueda rastrear tus datos. De igual forma no ofrezcas información personal de familiares, amigos y conocidos.

  Evita publicar fotos o conectar la webcam con desconocidos. Aun estando chateando con amigos, debes ser cauto y pensar qué es lo que vas a enviar y pensar cómo se sentirían otras personas que pudieran acceder a lo que estás dispuesto a enviar. Igualmente, ante cualquier duda sobre compartir o no ciertos datos o información, piensa si merece la pena correr el riesgo. Para ampliar información se recomienda la consulta del monográfico "Gestión de la privacidad e identidad digital".

- Debes ser consciente de la existencia de infracciones legales asociadas al uso de Internet así como de sus consecuencias, como por ejemplo delitos contra la propiedad intelectual, amenazas o coacciones, intimidación sexual, estafas o robos informáticos.

- Déjate ayudar cuando tengas un problema con la TIC, o te resulte violento o incómodo algún contenido. Ayuda que puedas dialogar con tus padres y educadores acerca de esos episodios[39].

6. Mecanismos de respuesta y soporte ante un incidente

Cuando se produce una situación de acceso a contenidos inadecuados, lo primero que debemos hacer es dialogar con el menor, con el fin de averiguar si el acceso ha sido accidental o voluntario. En el caso de que el acceso haya sido accidental es conveniente saber cómo se siente nuestro hijo/a o alumno/a al respecto y qué piensa después aclarar las posibles confusiones asociadas a la información recibida. Lo fundamental es dialogar con naturalidad adaptándonos a las necesidades del menor y a su proceso madurativo. A partir de aquí, podemos tomar medidas adecuadas como instalar un filtro parental de contenidos, explicando al menor por qué es conveniente hacerlo y de esa manera evitar acceder (por error o conscientemente) a esa clase de información no adecuada para su edad. A medida que los niños crecen y e inician el proceso madurativo, el filtro parental puede ir adaptándose a ese desarrollo para que finalmente la propia actitud crítica y selectiva del menor se convierta en herramienta de protección[40].

En otras ocasiones, los padres no son conscientes del acceso a contenidos inapropiados por parte del menor. En esos casos, observando la actitud y conducta de los niños y adolescentes, es posible intuir una acción de riesgo. Por ello se debe observar el tiempo que pasan usando TIC, si tienden a navegar o comunicarse a solas, si su estado anímico y/o físico ha cambiado o si reaccionan con nerviosismo al consultar un correo, leer un mensaje o consultar una página web. En definitiva, lo importante es conseguir que los niños confíen y cuenten lo sucedido. Para ello es fundamental promover en casa (y la escuela) un clima de comunicación, afecto y cohesión que facilite que los menores sientan la suficiente confianza para solicitar ayuda en caso necesario.

[39] Instituto de Adicciones. Madrid + Salud (2014). *TIC Prevención de usos problemáticos.* Recuperado de: http://www.madrid.es/UnidadesDescentralizadas/Salud/Publicaciones%20Propias%20Madrid%20salud/Publicaciones%20Propias%20ISP%20e%20IA/PublicacionesAdicciones/TIC.pdf

[40] Instituto Nacional de Tecnologías de la Comunicación (2007). Los controles parentales: cómo vigilar a qué contenidos de Internet acceden nuestros hijos. https://www.incibe.es/file/6CvtjRIY-9gkEhLjAz6BbA

De igual modo, como padres/madres/tutores o educadores debemos enseñarles qué deben hacer si acceden a un contenido inapropiado, como reportarlo y/o denunciarlo. Existen varias líneas de denuncia a disposición de padres, educadores y menores. Para denunciar contenidos inapropiados o ilegales en Internet, pueden recurrir a líneas de denuncia anónima, como las que ofrece *Google*, a través de su página *Google+*, que procede de acuerdo a su política de conducta y contenido, eliminándolos e incluso bloqueando a los usuarios que han infringido la normativa.

Igualmente desde las propias páginas donde aparece algún contenido inapropiado, se puede reportar accediendo a las opciones de configuración y herramientas disponibles para los usuarios[41].

7. Marco legislativo aplicable a nivel nacional y europeo

El actual marco legislativo a nivel nacional e internacional en materia de protección del menor de edad frente al acceso a contenidos inapropiados en el uso de las TIC establece lo siguiente:

Marco legislativo europeo

La Declaración de Derechos Humanos afirma en su artículo 19 que:

"Todo individuo tiene derecho a la libertad de opinión y expresión, este derecho incluye el no ser molestado a causa de sus opiniones; el de investigar y recibir informaciones y opiniones; y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."

El Comité de Derechos Humanos ha recordado en diversas ocasiones que los menores de edad gozan de todos los derechos civiles, lamentando que continúen prevaleciendo prácticas donde no se reconocen tales derechos, basándose en que los menores, al no haber alcanzado la madurez intelectual, no tienen la necesaria capacidad o competencia para ejercerlos. Con la incorporación de los derechos civiles a la Convención de los Derechos del niño se hace una declaración indiscutible de su

[41] Centro de Seguridad en Internet (2015) Contenido inapropiado en Internet: qué no debo hacer http://www.centrointernetsegura.es/noticias_interior.php?id=48

derecho y capacidad para gozar plenamente de estas libertades fundamentales. La Convención de los Derechos del niño establece en el artículo 13:

"El niño tendrá derecho a la libertad de expresión; ese derecho incluirán la libertad de buscar, recibir y difundir informaciones e ideas de todo tipo, sin consideración de fronteras, ya sea oralmente, por escrito o impresas, en forma artística o por cualquier otro medio elegido por el niño."

El derecho a la libertad de expresión está sujeto a ciertas restricciones que, según establece la Convención para los Derechos del niño, son aquellas que la Ley prevea y sean necesarias para el respeto de los derechos o reputación de los demás; y para la protección de la seguridad nacional o el orden público, o para proteger la salud o moral públicas.

Marco legislativo nacional

La Constitución española establece en su artículo 39 la obligación de los poderes públicos de asegurar la protección social, económica y jurídica de la familia, y en especial de los menores de edad, de conformidad con los acuerdos internacionales que velan por sus derechos.

De acuerdo a la vigente Ley Orgánica 1/1996, 15 enero, para la Protección del Niño y del Adolescente, se consideran contenidos no aptos, aquellos que promuevan, hagan apología o inciten a la violencia, a la guerra, a la comisión de hechos punibles, al racismo, a la desigualdad entre el hombre y la mujer; a la intolerancia religiosa y cualquier otro tipo de discriminación; al uso y consumo de cigarrillos y derivados del tabaco, de bebidas alcohólicas y demás especies previstas en la legislación sobre la materia y de sustancias estupefacientes y psicotrópicas, así como aquellos de carácter pornográfico, que atenten contra la seguridad de la Nación o que sean contrarios a los principios de una sociedad democrática.

La ley 7/2010 contempla, en su título II una normativa básica de la comunicación audiovisual, dentro de la cual se establecen los derechos del público, dedicándose el artículo 7 a los derechos del menor:

1. Los menores tienen el derecho a que su imagen y voz no sean utilizadas en los servicios de comunicación audiovisual sin su consentimiento o el de su representante legal, de acuerdo con la normativa vigente. En todo caso, está prohibida la difusión del

nombre, la imagen u otros datos que permitan la identificación de los menores en el contexto de hechos delictivos o emisiones que discutan su tutela o filiación.

2. Está prohibida la emisión en abierto de contenidos audiovisuales que puedan perjudicar seriamente el desarrollo físico, mental o moral de los menores, y en particular, programas que incluyan escenas de pornografía o violencia gratuita. El acceso condicional debe posibilitar el control parental. Aquellos otros contenidos que puedan resultar perjudiciales para el desarrollo físico, mental o moral de los menores solo podrán emitirse entre las 22 y las 6 horas, debiendo ir siempre precedidos por un aviso acústico y visual, según los criterios que fije la autoridad audiovisual competente. El indicador visual habrá de mantenerse a lo largo de todo el programa en el que se incluyan dichos contenidos. Asimismo, se establecen tres franjas horarias consideradas de protección reforzada tomando como referencia el horario peninsular: entre las 8 y las 9 horas y entre las 17 y las 20 horas en el caso de los días laborables y entre las 9 y las 12 horas sábados, domingos y fiestas de ámbito estatal. Los contenidos calificados como recomendados para mayores de 13 años deberán emitirse fuera de esas franjas horarias, manteniendo a lo largo de la emisión del programa que los incluye el indicativo visual de su calificación por edades (…) *Todos los prestadores de servicios de comunicación audiovisual televisiva, incluidos los de a petición, utilizarán, para la clasificación por edades de sus contenidos, una codificación digital que permita el ejercicio del control parental. El sistema de codificación deberá estar homologado por la Autoridad Audiovisual.* (…) *En horario de protección al menor, los prestadores del servicio de comunicación audiovisual no podrán insertar comunicaciones comerciales que promuevan el culto al cuerpo y el rechazo a la autoimagen, tales como productos adelgazantes, intervenciones quirúrgicas o tratamientos de estética, que apelen al rechazo social por la condición física, o al éxito debido a factores de peso o estética. (…)*

3. La autoridad audiovisual competente promoverá entre los prestadores del servicio de comunicación audiovisual televisiva el impulso de códigos de conducta en relación con la comunicación comercial audiovisual inadecuada, que acompañe a los programas infantiles o se incluya en ellos, de alimentos y bebidas que contengan nutrientes y sustancias con un efecto nutricional o fisiológico, en particular aquellos tales como grasas, ácidos transgrasos, sal o sodio y azúcares, para los que no es recomendable una ingesta excesiva en la dieta total".

Responsabilidad de la información

La información y comunicación que se encuentra en el uso TIC constituye una tarea global. Cada día son creados miles de blogs, son cargados a la Red miles de videos, se publican millones de comentarios, y entradas en páginas de elaboración colaborativa (por ejemplo *Wikipedia*). La responsabilidad por las infracciones que puedan cometerse en esos contenidos quedó fijada hace tiempo en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico:

La ley dice que el medio de información sólo será legalmente responsable cuando tenga "*conocimiento efectivo de que la actividad o la información almacenada es ilícita*" y no haya actuado con "*diligencia para retirar los datos o hacer imposible el acceso a ellos*".

No obstante, en algunos casos los jueces no alcanzan un consenso al aplicar la norma, haciendo recaer la responsabilidad sobre aquellos que aloja los contenidos, no sobre los autores reales de la información. Los tribunales, ante la dificultad que supone identificar a cualquier internauta, vienen adoptando una salida de compromiso consistente en la imputación de la responsabilidad a quienes alojan los contenidos. Algunos expertos coinciden en reconocer que el tema del anonimato es el problemático, y sugieren que para solucionarlo tendría que establecerse un régimen legal claro, que obligue a todo el que tenga sistemas automáticos de publicación a conservar y proporcionar la IP de sus usuarios en caso de ser solicitada por la justicia. La dirección IP es una dirección única que cada ordenador tiene en Internet, mediante la cual puede identificarse, a través del operador de telecomunicaciones, y mediante requerimiento judicial, a la persona, con nombre y apellidos, a la que pertenece un ordenador[42].

[42] Instituto Nacional de Ciberseguridad
https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Post_menores_contenidos

8. Organismos, entidades y foros de referencia

ORGANISMO / DETALLE

Chaval.es (www.chaval.es)

Iniciativa del Ministerio de Industria, Energía y Turismo, puesta en marcha por Red.es para responder a la necesidad de salvar la brecha digital entre padres, madres, tutores y educadores respecto al avance de los menores y jóvenes en el uso de las TIC. Ofrece recursos de sensibilización y formación sobre el ciberacoso.

UNICEF (www.unicef-irc.org/)

Portal web de UNICEF, un organismo de la Organización de las Naciones Unidas (ONU) que provee ayuda humanitaria y de desarrollo a niños y madres en países en desarrollo. UNICEF posee una Oficina mundial de investigación para mejorar la comprensión internacional de las cuestiones relativas a los derechos de los niños, y para ayudar a facilitar la plena aplicación de la Convención sobre los Derechos del Niño de apoyo a la promoción en todo el mundo.

Pantallas Amigas (www.pantallasamigas.net)

Iniciativa que tiene como misión la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia. Algunas de sus actividades principales son la creación de recursos didácticos, sesiones y jornadas formativas y estudios, con especial énfasis en la prevención del ciberbullying, el *grooming*, el *sexting*, la sextorsión y la protección de la privacidad en las redes sociales. Dispone de una línea de ayuda para niños y adolescentes ante situaciones de peligro en Internet.

INCIBE (www.incibe.es)

El Instituto Nacional de Ciberseguridad promueve servicios en el ámbito de la ciberseguridad que permitan el aprovechamiento de las TIC y eleven la confianza digital. En concreto, INCIBE trabaja en la protección de la privacidad de los usuarios, fomenta el establecimiento de mecanismos para la prevención y reacción a incidentes de seguridad de la información, minimizando su impacto en el caso de que se produzcan, y promueve el avance de la cultura de la seguridad de la información a través de la concienciación, la sensibilización y la formación.

9. Más información

Presentamos a continuación una relación de documentos y recursos para ampliar información sobre acceso a contenidos inapropiados:

RECURSO / DETALLE
EU Kids Online (www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx)
Proyecto de investigación financiado por la Comisión Europea a través del *Safer Internet Program,* red de 21 países europeos que tiene por objetivo examinar los aspectos culturales y contextuales y los riesgos del uso de las tecnologías online entre menores en Europa, identificar y evaluar hallazgos sobre el uso que las/los niñas/os hacen de Internet, así como huecos en las evidencias base; examinar cómo el marco en el que se realizan las investigaciones influye en la agenda de investigación, así como identificar los métodos con mejores prácticas; desarrollar recomendaciones de acciones de políticas públicas que promuevan el uso seguro de Internet basadas en evidencia.
Pew Research Center (www.pewinternet.org/topics/teens-and-technology/)
Centro de Estudios de referencia en los EEUU dedicado, entre otros, a la opinión pública, la investigación demográfica, el análisis de contenido de los medios de información, y el uso de Internet por parte de los menores.
Canal TIC (http://canaltic.com/internetseguro/manual/21_contenidos_inapropiados.html)
Entidad web cuyo objetivo es informar y formar sobre los beneficios, ventajas y contraventajas del uso de las Tecnologías de la Información y las Comunicaciones. Ofrece información y herramientas valiosas para utilizar las tecnologías con seguridad y responsabilidad, siendo una página útil para padres, tutores, educadores y menores de edad.
Madrid Salud (http://www.madrid.es/UnidadesDescentralizadas/Salud/Publicaciones%20Propias%20Madrid%20salud/Publicaciones%20Propias%20ISP%20e%20IA/PublicacionesAdicciones/TIC.pdf)
Guía para familias sobre la prevención de usos problemáticos de las Tecnologías de la Información y las Comunicaciones por parte de los más jóvenes. Otorga un papel primario a las familias, en el sentido

de integrar los mensajes y actitudes hacia las nuevas tecnologías dentro del mismo estilo educativo que emplean en otros ámbitos de la vida cotidiana. Es una guía para la educación en el uso adecuado de las tecnologías digitales, desde una actitud positiva y abierta hacia el conocimiento y manejo de las herramientas tecnológicas.

10. Bibliografía

Asociación Protégeles (2010). *Estudio sobre la utilización de la web 2.0 por parte de los menores.*

http://www.juntadeandalucia.es/observatoriodelainfancia/oia/esp/documentos_ficha.aspx?id=3618

Bottero M.; Escoto L. y Goncálvez S. (2006).*Educación Social y Cívica*. Montevideo: Colección Estudiantil.

Bringué X.; Sádaba C. (2011).*Menores y Redes Sociales en España.* Madrid: Colección Generaciones Interactivas - Fundación Telefónica

Castells M. (2001) Internet y la Sociedad Red. Lección inaugural del programa de doctorado sobre la sociedad de la información y el conocimiento (UOC). http://tecnologiaedu.us.es/revistaslibros/castells.htm

Centro de Seguridad en Internet (2015) Contenido inapropiado en Internet: qué no debo hacer http://www.centrointernetsegura.es/noticias_interior.php?id=48

EU Kids Online (2014) EU Kids Online: findings, methods, recommendations. EU Kids Online, LSE, London, UK. http://eprints.lse.ac.uk/60512/

Fuente Cobo C. (Dir.) (2014) La protección del menor tras la Ley General de la Comunicación Audiovisual. ICmedianet http://www.icmedianet.org/wp/ndog/wp-content/uploads/2014/01/Proteccion-Menor1.pdf

Fundación Imagen y Autoestima (2013).*Trastornos de la Conducta Alimentaria.* http://www.f-ima.org/es/prevencion/trastornos-relacionados-con-el-peso-y-la-alimentacion

Guerro-Prado D.; Barjau J. M.; Chinchilla A. (2001) *Epidemiología de los trastornos de la conducta alimentaria e influencia mediática: una revisión de la literatura*. Actas Españolas de Psiquiatría 29 pp. 403-410.

Gómez A. (Ed.) (2011) *Beyond good and evil the Spam.* Revista Modmex PC. Num. Septiembre 2011. pp.12-14. http://revistamodmex.wordpress.com

Hasebrink U.; Ólafsson K.; Štětka V. (2009) *Opportunities and pitfalls of crossnational research*. In S. Livingstone and L. Haddon (Eds.), Kids Online: Opportunities and Risks for Children (41-53). Bristol: ThePolicyPress

Hernández, I.; Limarquez M. (Eds.) (2008).*Glosario de términos de alcohol y drogas.* Madrid: Ministerio de Sanidad y Consumo Centro de Publicaciones. World HealthOrganization.

Instituto de adicciones, Madrid+Salud (2014).*TIC. Prevención de usos problemáticos.* http://www.madrid.es/UnidadesDescentralizadas/Salud/Publicaciones%20Propias%20Madrid%20salud/Publicaciones%20Propias%20ISP%20e%20IA/PublicacionesAdicciones/TIC.pdf

Instituto Nacional de Tecnologías de la Comunicación (2007) Los controles parentales: cómo vigilar a qué contenidos de Internet acceden nuestros hijos. https://www.incibe.es/file/6CvtjRIY-9gkEhLjAz6BbA

Internet Society (2013) Internet y los niños. Ginebra: Internet Society Ed. http://www.internetsociety.org/sites/default/files/bp-childrenandtheinternet-20129017-en_ES.pdf

Katz R. (2009).*El papel de las TIC en el desarrollo.* Madrid: Fundación Telefónica

Krug, E.G.; Dahlberg, L.L; Mercy, J.A.; Zwi, A.; Lozano, R. (Ed.) World report on violence and health (2002). Washington: World Health Organization

Livingstone S.; Haddon L.; Gorzig A.; Olafsson K. (2011).*Risks and safety on the internet: the perspective of European children. Full findings*. EU Kids Online, LSE, London.

López Andrade M. (2015) El Lado Oscuro del Blanqueamiento Dental. En Europa Press http://www.infosalus.com/estetica/noticia-lado-oscuro-blanqueamiento-dental-20150318092359.html

Mc Lean S. (2013).*Inappropriate Content.* Victoria University. Recuperado de: http://www.education.vic.gov.au/Documents/about/programs/bullystoppers/sminappropriate.pdf

MediaSmarts. Canada´s center for media and digital literacy: http://mediasmarts.ca

- (2014) *Responding to online ponography* http://mediasmarts.ca/digital-media-literacy/digital-issues/pornography/responding-online-pornography
- (2007) *Gambling* http://mediasmarts.ca/digital-media-literacy/digital-issues/gambling

Miranda de Larra R. (2005).*Los menores en la Red: comportamiento y navegación segura.* Madrid: Biblioteca Fundación AUNA

Mitchell K.; Finkelhor D.; Wolak J. (2003).*The Exposure of Youth to Unwanted Sexual Material on the Internet: A National Survey of Risk, Impact, and Prevention*. Youth & Society, 34(3), pp. 330-358.

Moreno J.L. (2010). Moral corporal, trastornos alimentarios y clase social. Madrid: Centro de Investigaciones Sociológicas

Naval C.; Sádaba Ch.; Bringué X. (2003) Impacto de las Tecnologías de la Información y la Comunicación (TIC) en relaciones sociales de los jóvenes navarros. Gobierno de Navarra. Instituto Navarro de Deporte y Salud

Organización de las Naciones Unidas (2008). Informe Mundial sobre las Drogas. UnitedNationsPublications

Orti A.; Sampere J. (2006). Leyendas urbanas. Barcelona: Ed. Martínez Roca

Pan EuropeanGameInformation (2015) http://www.pegi.info/es/index/id/1397/

Paricio M.P; Fernández C. (coord.) (2012). Adicciones, estrategias de prevención y comunicación. Barcelona: Erasmus Ediciones

Rodríguez del Pino D.; Miranda J.A.; Olmos A.; Ordozgoiti R. (2012). Publicidad online. Las claves del éxito en Internet. Madrid: ESIC Editorial

Ruiz San Román J. (2011) La protección de los menores en el artículo 7 de la Ley 7/2010 General de la Comunicación Audiovisual. Análisis y discusión crítica. *Nueva Época* No. 6. Junio-Agosto, 2011

Sánchez Herrera J. (2012) Nuevas tendencias en comunicación. Madrid: ESIC Editorial

Smith P.; Mahdavi J.; Carvalho M.; Fisher S.; Russell S.; Tippett N. (2008) *Cyberbullying: Its nature and impact in secondary school pupils*. Journal of Child Psychology and Psychiatry, 49, pp.376-385.

Trinidad Ayela M.R. (2010). Adolescentes: Trastornos de alimentación. Valencia: Editorial Club Universitario

Unidad de Conductas Adictivas del adolescente. Hospital Sant Joan de Deu de Barcelona (2014). http://www.lavanguardia.com/vida/20140413/54405725221/triplican-adolescentes-adictos-videojuegos.html

United Nation Children´s Fund (UNICEF) (2011). *Child Safety online. Global challenges and strategies*. http://www.unicefirc.org/publications/650

Venugopal K.R.; Patnaik L.M (Eds.) (2011) *Computer Networks and Intelligent Computing*. 5th International Conference on Information Processing, ICIP 2011, Bangalore, India, August 5-7, 2011. Springer Science & Business Media

Wilson J; Peebles R. et al. (2006).*Surfing for thinness: a pilot study of pro-eating disorder web site usage in adolescents with eating disorders.*Paediatrics 118(6). Pp. 1635-1643.

Referencias legales

- Ley Orgánica 1/1982, de 5 de mayo, de Protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Ley Orgánica 1/1996, de 15 de enero, de Protección jurídica del menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.
- Ley Orgánica 34/2002, de 11 de julio, de Servicios de la Sociedad de Información y Comercio Electrónico.
- La Ley General de la Comunicación Audiovisual 7/2010, de 31 de marzo
- Declaración de los Derechos Humanos http://www.un.org/es/documents/udhr/
- Convención de los Derechos del Niño

- Constitución Española