

Uso seguro de Internet y las TIC

Guía para el profesorado

Lola Ramón Martínez



#Somos más

Uso seguro de Internet y las TIC

Guía para que el profesorado

Lola Ramón Martínez

Este material es propiedad de *#Somos más*, estando disponible en su página web. Se autoriza su reproducción siempre que se garantice la gratuidad de su distribución, así como la expresa referencia de *#Somos más*.

Autora

Lola Ramón Martínez

*Especialista en comunicación para el cambio social
y coordinadora de la agencia de publicidad y activismo digital
El Megáfono. ¡Siempre al acecho de nuevos proyectos!*
www.elmegafono.es

Ilustraciones de cubierta e interiores

Mauricio Maggiorini Tecco
www.mmaggiorini.com

Diseño, maquetación y edición de textos

Cyan, Proyectos Editoriales, S. A.

#Somos más



Contenido

INTRODUCCIÓN	5
1. LOS JÓVENES Y LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC). ¿Qué tiene Internet que tanto atrae?	7
2. HÁBITOS Y CONDUCTA. Aprendiendo a aprender	17
3. DERECHOS Y RESPONSABILIDADES DIGITALES. ¿A qué atenernos?	29
4. REDES SOCIALES, FOROS Y REPOSITORIOS DE VÍDEOS. Revolución social	43
5. APLICACIONES Y VIDEOJUEGOS. Mucho más que un juego	55
6. CIBERSEGURIDAD. Dando valor a nuestros datos	67
7. DECÁLOGO PARA EDUCAR EN EL USO SEGURO DE INTERNET. Kit de herramientas	77
8. DECÁLOGO PARA CHICAS Y CHICOS DE 12 A 18 AÑOS SOBRE EL USO SEGURO DE INTERNET	91
BIBLIOGRAFÍA	95

INTRODUCCIÓN

- Tanto las generaciones adultas como las menores estamos viviendo un cambio profundo en el paradigma social y en la manera en que consumimos información y entretenimiento.

Es innegable que Internet y la tecnología en general nos facilitan muchas tareas y nos dan considerables alegrías, pero debemos reflexionar sobre cómo nos afecta su uso y, sobre todo, cómo afecta a los y las menores. Debemos empezar a educar en consecuencia.

Este nuevo mundo que emerge, Internet, es como un continente hasta ahora desconocido, donde las oportunidades y riesgos nos son aún poco familiares. Todavía no hemos desarrollado un marco ético ni unas reglas razonables, según las cuales aprender a guiar a nuestros hijos, hijas y alumnado. Sin embargo, somos más que capaces de aprender y evolucionar en nuestro conocimiento de Internet y contribuir al desarrollo de estas “reglas”. Debemos hacerlo por las generaciones jóvenes.

Y es que este mundo nuevo que evoluciona y se transforma a tantísima velocidad no es inocuo; lo sabemos, no es inofensivo. Afecta a nuestra forma de pensar, de relacionarnos, de enfrentarnos a problemas complejos, y también a las toneladas y toneladas de basura electrónica que generamos cada año.

Es hora de que dejemos de mirar hacia otro lado. Internet lo creamos entre todos y todas y, conjuntamente, podemos lograr que se convierta

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

en un mundo positivo y seguro para nuestros hijos, hijas y alumnado. Empecemos por aprender y educar para lograrlo.

Esperamos que esta guía sea solo un principio para ponernos a trabajar en la construcción de un Internet mejor que potencie nuestras capacidades y las de nuestros hijos, hijas y alumnado en lugar de entorpecerlas. ¿Nos ponemos a ello?



LOS JÓVENES Y LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)

¿Qué tiene Internet que tanto atrae?

OBJETIVOS FORMATIVOS

Aprender a escuchar, comprender y asistir a los y las adolescentes en el descubrimiento y uso de Internet.

- I Comprender por qué les absorbe.
- I Priorizar el uso positivo y la seguridad.



CONTENIDOS FORMATIVOS

- I Adolescentes e Internet.
- I Postura de sus mayores.
- I Su papel en la construcción de un Internet seguro y positivo.



APUNTES

El salto generacional que supone la evolución tecnológica en este momento es innegable. Como personas adultas estamos siendo testigos de un cambio en los hábitos y conductas de nuestros hijos, hijas, alumnado y demás jóvenes a nuestro alrededor, que no nos recuerdan a los nuestros a su edad.

Mientras que, no hace tanto, disfrutábamos de la bicicleta, los castillos de arena y el pilla a pilla en las tardes de verano, ahora vemos a las nuevas generaciones pasar horas frente a la tablet o la consola portátil, mostrando poco o ningún interés por lo que no sea tecnología punta.

Dan ganas de cogerlos por los hombros y decirles: “pero ¿es que no veis el mundo que os estáis perdiendo fuera de la pantalla?”. El problema es que también ellos y ellas tienen una respuesta: “¿es que no ves tú que hay mucho más mundo dentro de la pantalla que fuera?”.

› LA MÚSICA COMO EJEMPLO

Históricamente, todos los cambios en el paradigma social han supuesto una brecha entre generaciones. Un ejemplo muy claro es la música.

Recordemos cómo casi todos los nuevos géneros que fueron surgiendo en el siglo XX eran criticados duramente por quienes defendían el estilo anterior. Así ocurrió con el *jazz* —desde finales del siglo XIX—, el *rock & roll*, el tango, el *blues*, el *soul*, etc. Uno tras otro, todos estos estilos musicales fueron vilipendiados y tildados de música maléfica. Frank Sinatra llegó a decir: “Yo a esa mierda de música llamada *rock and roll*, no le doy ni cinco años de vida” o “ [...] La música *rock* la hacen deficientes que cantan letras maliciosas, lascivas. Es la forma de expresión más brutal, nauseabunda, desesperada y viciosa que he tenido la desgracia de escuchar”.

¿Cuántas personas sentimos rechazo por el trap o el reguetón?

Las generaciones jóvenes de principios y mediados del siglo XX buscaban en el *jazz*, el *rock & roll* y demás formas musicales nuevas la **contraposición o el rechazo a lo establecido**. Ese fue el origen de los nuevos géneros musicales, y el miedo y la resistencia al cambio lo convirtieron también en el motivo de sus críticas.

Pero ¿qué manía tenemos como adolescentes de romper con lo establecido? ¿Por qué tiene que poner mi hija la música a todo trapo si sabe que no me gusta? ¿Cuántas veces le he dicho a mi hijo que no juegue con el móvil cuando estamos en la mesa?

Como adolescentes rompemos con lo establecido para **reivindicarnos como personas**.



› ADOLESCENTES Y REBELDÍA TECNOLÓGICA

Internet y tecnologías como los teléfonos inteligentes, las consolas, los vídeos, son el campo de rebeldía perfecto para la adolescencia. Por un lado, les permite confrontar directamente con la manera de entender el mundo de padres, madres y docentes (“cambia mi escala de valores y prioridades”); por otro, aislarse del entorno (“puedo pasarme horas en Internet construyendo una identidad ideal”); además, les permite ser expertos y expertas en campos (complejos) que las generaciones anteriores en muchos casos desconocemos: redes sociales, juegos *online*, etc.

Las generaciones adolescentes se rebelan en bloque no solo en los gustos, la forma de vestir, la música, sino en su **forma de vida que en algunos casos pasa a ser prioritariamente virtual.**

› ¿CÓMO HABRÍA VIVIDO YO LA ADOLESCENCIA DE HABER NACIDO EN LOS 2000?

Entendamos que los y las adolescentes están viviendo un momento de cambio sociológico sumamente complejo.

Internet, como herramienta, no está regulado. No existe un código ético común, no existe un camino seguro, no abundan los maestros ni maestras que entienden y consumen igual que yo las nuevas tecnologías.

Y, sin embargo, como adolescente, Internet me proporciona una ventana a la que asomarme a contrastar cada una de mis dudas existenciales: tengo pares en todo el mundo con los mismos problemas que yo, tengo distracción, sentimiento de pertenencia y una sensación de control mucho mayor que en el día a día fuera de Internet.

Cada vez que siento frustración o rabia, tengo cientos de alternativas para desconectar o sentirme a gusto conmigo; los mismos cientos de distracciones que surgen cuando quiero ponerme a estudiar.

Como adolescente, sé que Internet supone amenazas, pero aún no he aprendido necesariamente qué significa estar en riesgo y no tengo referentes adultos con el conocimiento suficiente para alertarme sobre los riesgos que supone el mundo virtual.

Vengo, además, de vivir una crisis económica profunda que ha derivado en la desafección política de mis mayores y la sensación de un futuro incierto para mí y mi generación. Leo, veo o digiero a diario la conmoción de una sociedad globalizada que se enfrenta a retos muy complejos, como el calentamiento global, la escasez de agua, el hambre, la migración, la violencia machista, para los que no hay una respuesta contundente.

He nacido en un momento de cambios profundos que ni puedo comprender en toda su complejidad ni mucho menos predecir. Y al mismo tiempo tengo un mundo virtual, rompedor en todos los sentidos, en el que sumergirme, explorar, fantasear y reivindicarme. **Para mí no existe frontera entre la vida real y la virtual;** solo una realidad común.

¿Qué hacen parte de mis mayores? En lugar de preguntarme y aprender a ponerse en mi lugar, me orillan al otro lado del debate y se olvidan de que sé bastante de este mundo virtual que tanto les asusta.

› NI PERSONAS NATIVAS NI ANALFABETAS DIGITALES

Como personas adultas tenemos que entender el efecto que las tecnologías de la información y la comunicación tienen sobre las nuevas generaciones, pero sobre todo tenemos que **comprender cómo las sienten** ellos y ellas. Tenemos que aprender a escuchar. Solo así podremos orientar y ayudar a evitar los riesgos y fomentar la participación positiva en Internet.

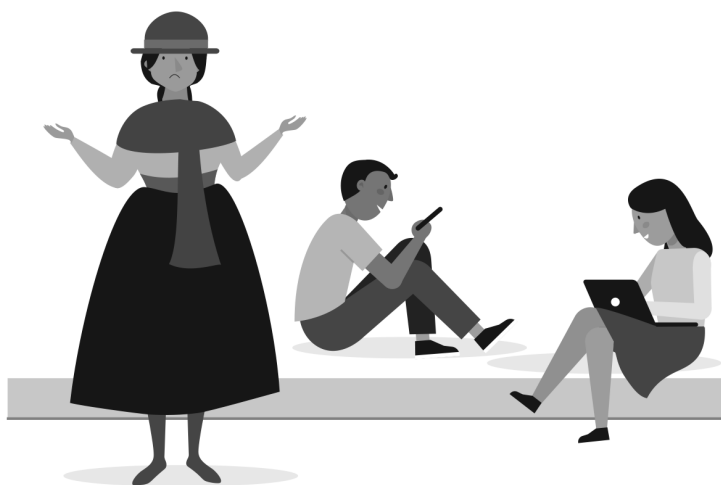
Hablar de generaciones nativas digitales es igual de poco relevante que hacerlo de generaciones analfabetas digitales. Ni todas las personas de entre 12 y 18 años hacen igual uso de Internet, ni las mayores de 40 son ineptas.

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

La brecha digital existe porque hay generaciones que han nacido y crecido con esta tecnología y han tenido que aprender de manera autodidacta a desenvolverse en el mundo virtual, mientras que gran parte de sus padres, madres, profesores, tutoras, conocen solo su visión de la tecnología o directamente desconocen el mundo digital.

Ocurre algo similar con los pueblos indígenas que son forzados a escolarizar a sus hijos e hijas en un sistema educativo ajeno: aparece una insalvable brecha cultural entre las generaciones adultas y las jóvenes, porque mientras las adultas mantienen su forma de vida indígena, a las jóvenes se les impone una educación basada en los conceptos de la sociedad dominante —la visión colonial, la globalización, el capitalismo—, que con frecuencia deriva en una visión de su propia cultura como primitiva y salvaje¹.



¹ <https://www.survival.es/escuelas-fabrica>

A diferencia de los pueblos indígenas, que necesitan apoyo internacional porque no comparten los códigos, nosotros y nosotras tenemos las herramientas para evitar o al menos disminuir la brecha digital.

Solo tenemos que aprender a escuchar a los niños, niñas y adolescentes, y mostrarnos como interlocutores válidos con conocimiento e interés para **aprender a afrontar los riesgos y oportunidades de Internet.**

› **POR LA SEGURIDAD Y EL USO RAZONABLE DE INTERNET EN CONJUNTO**

Y es que, además, Internet es tan joven todavía y tan mutable que desconocemos muchos de los efectos que produce en la sociedad. Efectos que pueden ser tanto negativos como positivos y que conviene esforzarse conjuntamente en conocer.

Como mencionábamos unos párrafos atrás, ni Internet ni las TIC tienen aún un marco ético ni una regulación definida. Por eso es tan importante que entre todas las personas nos preocupemos por sentar algunas de las bases fundamentales para construir un Internet donde todo el mundo pueda sentirse a gusto, a salvo y con espacio para participar.

En este sentido, las nuevas generaciones tienen un **papel esencial** porque son quienes han desarrollado mayor apego y, en muchos casos, habilidades hacia las nuevas tecnologías. Y es nuestra labor como personas a su cargo, que nos preocupemos por su bienestar y futuro, aprender a asistirles en este terreno tan inexplorado.

Si conseguimos trabajar de la mano de las generaciones jóvenes por un Internet más seguro y positivo, sin duda lograremos que este cambio histórico sin precedentes en la sociología humana sea mucho **más beneficioso que perjudicial.**

Cuestionario para la reflexión

PRÁCTICA PARA PADRES, MADRES Y TUTORES LEGALES

1. ¿Cuántos menores tienes a tu cargo?

1

2

3

4 o más

2. ¿De qué edad o edades?

3. ¿Cuántos dispositivos electrónicos inteligentes o con acceso a Internet (*smart TV*, ordenador/es, tableta/s, *smartphone/s*, *smartwatch/s*, consola/s, etc., tenéis en casa? Anótalos a continuación:

4. ¿A cuántos de ellos tiene/n acceso el/los menor/es?

5. ¿Están en un lugar común o en su habitación?

☐ Lugar común

☐ Habitación menor/es

6. ¿Sabes si tiene/n perfil en redes sociales?

☐ Sí ☐ No

7. ¿Sabes si accede/n a contenido no adecuado para su edad?

☐ Sí ☐ No ☐ Probablemente

8. ¿Habláis alguna vez del mundo virtual?

☐ Sí ☐ No

9. ¿Instalas controles parentales en los dispositivos?

☐ Sí ☐ No

10. ¿Habéis establecido límites en el uso de los dispositivos: límite diario, para qué se usan y para qué no, sitios donde no está permitido como la mesa a la hora de comer o la cama antes de dormir, etc.?

☐ Sí ☐ No

11. Si lo haces, ¿tratas de mostrar un buen ejemplo y cumplirlos también?

☐ Sí ☐ No

12. ¿Si tuvieras que puntuar tus conocimientos sobre seguridad y uso recomendado de Internet y los dispositivos inteligentes qué nota te pondrías?

1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	----

HÁBITOS Y CONDUCTA

Aprendiendo a aprender

OBJETIVOS FORMATIVOS



Aprender a inculcar hábitos y conductas positivos en Internet y el tiempo libre:

- I Comprender a qué responden y qué ocasionan los hábitos y conductas en Internet.
- I Entender el riesgo potencial de los malos hábitos en Internet.

CONTENIDOS FORMATIVOS



- I Cifras sobre consumo de Internet, *smartphones* y videojuegos.
- I ¿Cómo nos afecta la tecnología física y neurológicamente?

APUNTES

Como personas adultas tenemos una posición difícil. Por un lado, es vital que proporcionemos información y consejos sobre el uso de Internet y las nuevas tecnologías a los y las menores que tenemos a cargo, pero, por otro, en muchos casos tenemos muchos menos conocimientos al respecto que ellos y ellas mismas.

Es una situación paradójica, pero que tenemos que aprender a trascender: el uso de Internet, los *smartphones*, ordenadores y consolas está muy extendido y afecta de manera profunda a la socialización y el desarrollo de los y las menores.

› UN PAÍS HIPERCONECTADO

Repasemos algunas cifras:

- I La población española pasa más de **5 horas diarias** de media en Internet (informe de tendencias digitales y de redes sociales en todo el mundo de Hootsuite y We Are Social, 2019).
- I España es el **quinto país más enganchado al móvil** del mundo (*Estudio Digital Economy Compass* del Digital Market Outlook de Statista, 2017).
- I Los menores de entre 12 y 13 años pasan una media de entre **5 y 7 horas diarias** frente a alguna pantalla (*Estudio AIMC Niñ@s*, 2018).
- I El 85% de los menores de 10 años tienen **acceso a Internet** (INE, *Los hogares y la tecnología*).

El *Informe de la sociedad digital en España 2018*, de Telefónica, demuestra que la conectividad al móvil es casi universal:

- I Para el 91,9% de la sociedad española, el **dispositivo preferido** más usado es el *smartphone*.
- I En el caso de la **población de entre 14 y 19 años**, hablamos del 100%.

- Y el 81,9% de los **mayores de 64 años** también así lo indica.

En cuanto a la forma de comunicarnos, también de acuerdo con el *Informe de la sociedad digital en España 2018*:

- La **mensajería instantánea** es el canal de comunicación preferido para el 95,1% de la población española (incluso por encima de la comunicación en persona).
- El 93,6% de los y las usuarios utiliza diariamente **aplicaciones de mensajería instantánea**: el 98% de los menores de 34 años y el 88,2% de los mayores de 64 lo utilizan a diario.



El consumo de videojuegos, a partir del estudio *Descubriendo los eSports en España*, de Wink TTD, de 2019:

- Casi un 70% de la población española consume **videojuegos**.
- En el tramo de edad de entre los **14 y los 29 años**, un 89,2% juega.
- El 72,1% juega a través del **teléfono móvil**.
- La **media de tiempo semanal** es de 9,5 horas.

De acuerdo con el *Estudio de GAD3 para empantallados* con la colaboración de Orange y la Unión Europea en el 2018:

- I El 57,8% de los padres y las madres de menores **no establecen controles parentales.**
- I El 60% afirma que **echa de menos mayor formación** para asistir de manera adecuada a los y las menores en el entorno digital.

➤ NUEVOS HÁBITOS, NUEVOS DESAFÍOS

Como vemos, Internet y las nuevas tecnologías han entrado con fuerza en nuestra vida y la de los más pequeños. Nuestros hábitos han cambiado considerablemente y también el modo en que las personas más jóvenes crecen y se relacionan con el mundo que les rodea.

Esto no solo transforma nuestro día a día: la manera en que socializamos, nos informamos, consumimos, nos entretenemos; sino que además **nos afecta tanto a nivel físico como a nivel neurológico.**

A nivel físico representa un problema sobre todo para la **vista y para las dolencias y lesiones musculares.** Entre los expertos, se advierte de que un tiempo excesivo de exposición a las pantallas aumenta notablemente las probabilidades de que los y las menores desarrollen miopía y que, en general, a todas las edades, multiplica la aparición de una serie de dolencias incluidas en el síndrome visual informático (fatiga, irritación ocular, migraña y cefalea, sequedad ocular, visión borrosa y doble, vértigos, sensibilidad lumínica, dolor articular y muscular, etc.), que pueden degenerar en enfermedades o dolencias oculares y/o musculares como la cervicalgia o la hipertensión ocular.

Para el cerebro también supone un reto a tener muy en cuenta. El entorno y nuestros hábitos y conducta afectan a nuestro sistema neurológico. Según Nicholas Carr, un investigador estadounidense especializado en este tema, el uso de Internet y las nuevas tecnologías transforman nuestra neuroplasticidad y nuestra manera de producir dopamina.

La **neuroplasticidad o plasticidad cerebral** es una característica del cerebro que lo hace capaz de moldearse y cambiar en función de nuestras interacciones con el entorno. Es una función adaptativa que hasta los años sesenta se pensaba exclusiva de la infancia y adolescencia temprana, pero que más adelante se descubrió que seguimos teniendo en edades adultas, y que nos permite adaptar nuestras capacidades a los retos que nos impone el entorno. El problema es que, igual que nos permite cambiar cosas que no nos gustan de nosotros y nosotras mismas, hace que **nuestros hábitos modifiquen nuestras capacidades cerebrales sin que nos lo propongamos**.



Por otro lado, la **dopamina** es un neurotransmisor (una molécula mensajera que propaga información que recibe nuestro cerebro) responsable del placer, la motivación y el deseo. Internet y las tecnologías de la información y la comunicación están integrados por contenidos

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

y plataformas pensados para que generemos mucha dopamina de forma continuada. Los juegos, las redes sociales, los titulares, los anuncios *banner* están diseñados para ello.

En general, la información se nos presenta en formatos breves, inmediatos y simples, con recompensas simuladas que no son tangibles y que, en la mayoría de los casos, no suponen un beneficio real más allá del premio en sí mismo.

Esto nos genera dos problemas fundamentales: por un lado, por causa de la neuroplasticidad, **modificamos nuestra capacidad de obtener y retener la información**. Ganamos habilidades como las de escanear la información de la pantalla, leer textos por encima resaltando solo aquello que nos parece relevante, atender a más de un estímulo a la vez, es decir, la multitarea, o bloquear estímulos que no nos interesan, como los *banners*; pero **perdemos capacidad a la hora de hacer reflexiones profundas y desarrollar el pensamiento crítico**. Y esto es dramático, porque tanto las personas adultas, como sobre todo quienes aún están creciendo, necesitamos poder reflexionar y hacerlo de forma crítica para definir quiénes somos, quiénes queremos ser, y tener objetivos vitales que nos hagan sentir bien.

Por otro lado, como Internet y otros medios digitales como los videojuegos están plagados de estímulos que proporcionan recompensa, producen otra importante dificultad: al liberar mucha dopamina de forma continuada nos volvemos **insensibles a sus efectos**. Esto genera que cada vez nos resulte más difícil buscar recompensas que no estén vinculadas a los medios digitales porque son menos estimulantes y con ellas liberamos menos dopamina; perdemos el interés y la motivación. Y es trágico, porque la motivación es lo que nos arranca a buscar cosas que nos llenan y nos hacen crecer como personas.

Por supuesto, esto no significa que no podamos recuperar la capacidad reflexiva, el pensamiento crítico y la motivación, o que debamos

deshacernos de nuestros dispositivos y prohibírselos a nuestros hijos, hijas y alumnado; significa que, si queremos disfrutar de los medios digitales, tenemos que esforzarnos en que los **hábitos de los y las menores de edad en Internet estén demarcados y los beneficien en lugar de perjudicarlos.**

No hay que ser ilusos e ilusas: **Internet no es inofensivo.**

Además de estas cuestiones, Internet y las herramientas de la información y la comunicación generan algo parecido a la **adicción**. Tristemente, como estamos hablando de realidades muy recientes, no es común identificar un uso exagerado como tal, pero afecta a jóvenes y adultos de forma muy similar a otro tipo de adicciones. Es cierto que las causas suelen ser ajenas a Internet: aislamiento, depresión, baja autoestima; pero es igualmente importante que prestemos atención a los usos desmedidos de las tecnologías de la información y la comunicación.

Según el estudio de IKEA *¿Estamos hiperconectados?* publicado en 2018, el **25% de las personas por debajo de 25 años miran de media 150 veces el teléfono al día** (sin contar horas de sueño), es decir, una vez cada 7 minutos; y un tercio de las mayores cada 10 minutos o, lo que es lo mismo, 100 veces al día.

Estudios llevados a cabo por el Centro de Estudios Especializados en Trastornos de Ansiedad indican, además, que el 53% de quienes tenemos teléfono móvil sufre **nomofobia**. La nomofobia aparece cuando sentimos ansiedad o un miedo irracional al dejarnos el teléfono móvil en casa, quedarnos sin batería, sin cobertura o extraviarlo, por sentir que perdemos la conexión continua.

También existe otro término llamado **ningufoneo** que se refiere al acto de ignorar a la gente que tienes a tu alrededor físicamente para poner toda tu atención en tu dispositivo y que es muy común en adolescentes.

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC



Además de ser de mala educación, como la nomofobia, puede ser síntoma de un patrón adictivo a los dispositivos electrónicos y a la hiper-socialización.

Además de lo mencionado hasta ahora, es vital dar trascendencia a dos universos que preocupan especialmente a los y las profesionales expertas en pedagogía, sociología, psicología y desarrollo en el uso y conducta en Internet: **la ludopatía y la pornografía** y cómo afectan a jóvenes y adolescentes:

- I Juegos de azar y apuestas online:** a pesar de que el juego de azar y las apuestas está prohibido para menores de 18 años, se puede acceder a ellos *online*. A través del DNI y los datos bancarios de sus

parientes algunos menores encuentran cómo jugar en Internet sin tener que desplazarse ni sentirse juzgados gracias al anonimato. La publicidad en televisión, radio, redes sociales los seduce y las webs, sobre todo de apuestas deportivas, con frecuencia les regala dinero para que empiecen a jugar. Este hecho preocupa mucho a especialistas y asociaciones para la prevención del juego y la ludopatía, que están viendo cómo el consumo en menores aumenta y supone un importante factor de riesgo en el desarrollo de la adicción al juego.

- I Pornografía:** la pornografía *online* representa uno de los mayores problemas que Internet inflige en el desarrollo y la socialización de los y las menores, sobre todo por la carencia de una enseñanza afectivo-sexual en la educación formal y lo explícito de algunos contenidos. Hoy en día, es muy complejo regular las páginas web que ofertan contenido sexual porque están alojadas en servidores que se encuentran en países como Estados Unidos y Rusia que no tienen una regulación firme al respecto.

› MENORES MÁS VULNERABLES

El hábito y la conducta en Internet pueden afectar por igual a personas adultas y menores. Sin embargo, la mayoría de personas menores de entre 12 y 18 años aún no tienen claros sus objetivos vitales, son en general más confiadas y, por tanto, más vulnerables.

Además, como suele pasar en cualquier otro hábito que desarrollamos a edades tempranas, cuanto más joven eres al desarrollar un mal uso de Internet y la tecnología, **más difícil es reconducir el hábito y la conducta.**

Se suma que en la actualidad el uso de las tecnologías de la información y la comunicación entre la gente joven e incluso la menor de 12 años es prácticamente universal. Esto no es necesariamente negativo. Internet ofrece también considerables beneficios como el acceso a la información y la potenciación de capacidades de distinta

índole. Sin embargo, es más que nunca fundamental que como personas adultas nos preocupemos por educar activamente y combatir los malos hábitos y conductas negativas en Internet.

➤ **POSTURA QUE DEBEMOS TOMAR COMO REFERENTES ADULTOS**

Aunque pensemos que las generaciones jóvenes saben muchos más en lo que a “nuevas” tecnologías se refiere, no dejan de ser niños, niñas y adolescentes que nos necesitan. Necesitan tener modelos, maestros y guías. Necesitan límites, que les expliquemos qué está bien y qué está mal, hablar de lo que les inquieta y no saben cómo colocar. Y en Internet es normal que les surjan dudas; dudas que, al final, son mucho más humanas que digitales.

¿Cómo podemos, como referentes adultos, estar a la altura de las circunstancias? En primer lugar, siendo un buen ejemplo en el uso de Internet y la tecnología. Si nos ven pendientes del teléfono cada vez que pasamos tiempo juntos o en nuestro tiempo libre, lo demás va a ser poco eficaz. En segundo, como ya hemos comentado, tenemos que hablar con ellos y ellas y escuchar con atención, sin juzgar ni ser invasivos, tratando solo de construir el espacio necesario para que el o la menor pueda expresarse. Y en tercer lugar, para que puedan confiar en nosotros y nosotras como interlocutores válidos capaces de aportar a la conversación y a su experiencia, tenemos que estar al día de las tendencias, riesgos y oportunidades que Internet y las herramientas tecnológicas ofrecen.

Además de todo ello, veremos en el capítulo 7 de la guía consejos y pautas específicas para negociar y pautar mejores hábitos en Internet y la tecnología en general.

Cuestionario para la reflexión

PRÁCTICA PARA PADRES, MADRES Y TUTORES LEGALES

1. ¿Para qué puede(n) utilizar los dispositivos inteligentes tu(s) hijo(s) y/o hija(s) y para qué no? (jugar, deberes, redes sociales, vídeos, compras, mensajería, series, etc.).

2. ¿Cuánto tiempo de pantalla pueden dedicar al día a lo anterior?

_____horas

3. ¿Quién es responsable de que se cumpla ese límite diario?

_____ (nombre adulto) _____ (nombre menor)

4. ¿A qué tipo de contenidos no deberá(n) acceder?

☐ Páginas no recomendadas para menores de 18 años

☐ Páginas de descargas ilegales

☐ Otros: _____

5. ¿A qué tipo de contenidos deberá(n) acceder con permiso y supervisión de una persona adulta?

☐ Repositorios de vídeos

☐ Juegos *online*

☐ Otros: _____

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

6. ¿De qué manera comprobaremos mes a mes si se cumple nuestro acuerdo?

7. ¿En qué lugares y contextos no se pueden utilizar los dispositivos electrónicos?

☐ En la mesa cuando desayunamos, comemos, cenamos, etc.

☐ A la hora de dormir

☐ Cuando estamos hablando

☐ En tiempo de estudio o de hacer los deberes

☐ Otros (coche, visitando a los abuelos, etc.) _____

8. Definamos un horario de uso para Internet, el teléfono, las consolas, etc.:

Entre diario: __: __h a __: __h

En fines de semana: __: __h a __: __h

DERECHOS Y RESPONSABILIDADES DIGITALES

¿A qué atenernos?

OBJETIVOS FORMATIVOS



Conocer en qué consisten los derechos digitales:

- I Saber en qué se fundamentan nuestros derechos en Internet.
- I Entender la red como un lugar de expresión en el que ejercemos derechos fundamentales.
- I Aprender a identificar y evitar la difusión de las noticias falsas.

CONTENIDOS FORMATIVOS



- I Introducción al derecho digital.
- I Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- I Libertad de expresión, derechos sobre nuestra imagen.
- I *Fake news*, bulos y *clickbait*s.

APUNTES

Internet comprende tantas áreas, tantas realidades humanas, tantos países y se transforma de forma tan súbita que el planteamiento de los derechos vinculados a su uso no es tarea fácil, se encuentra en desarrollo y muchas veces nos es desconocido.

Para ser un poco más conscientes de qué derechos, responsabilidades y obligaciones tenemos tanto personas adultas como menores en Internet, vamos a **repasar las áreas de regulación que se han ido determinando**.

Algunos de estos derechos no son verdaderamente vinculantes, es decir, son más teóricos que prácticos, ya que dependen de la creación de políticas en base a ellos que no siempre tienen lugar o que están en desarrollo. Además, el ejercicio de regulación y establecimiento de los derechos vinculados a Internet es considerablemente complejo porque en ocasiones colinda con otros derechos previos, ya existentes para el mundo *offline*, y generan conflicto de intereses.

Como, además, en Internet todos y todas somos **tanto consumidoras de información como generadoras de ella**, la red no deja de ser un medio de expresión y debate en el que ejercemos varios **derechos democráticos fundamentales** que es importante proteger. Por todo ello, no es raro que en estos procesos surjan polémicas complejas, no por ello menos interesantes, que debemos conocer y formar parte para contribuir a una red global que potencie las oportunidades y minimice los riesgos de las personas.

› DERECHOS DIGITALES

Los derechos digitales son aquellos derechos humanos y/o legales referidos al **acceso, uso, creación y publicación** de contenidos digitales o al **acceso y uso** de los dispositivos electrónicos y las redes de telecomunicación por parte de las personas.

Están estrechamente relacionados con derechos ya existentes *offline*, como el derecho a la intimidad, a la privacidad, al acceso a la información o la libertad de expresión, pero enfocados en el uso de las tecnologías de la información y la comunicación, particularmente Internet.

Como el resto de los derechos individuales, el objetivo de su definición y ejercicio es **facilitar la convivencia y evitar la discriminación de las personas**. Para ello, sus focos principales son la privacidad e igualdad de los usuarios y usuarias de Internet, la supresión de los datos personales y la protección de los y las menores. Asimismo, los derechos digitales dan especial relevancia a la **libertad de expresión, reunión e interacción desde el respeto, la responsabilidad y la defensa de la intimidad**.



› DERECHOS EN INTERNET

En la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales desarrollada para adaptar la legislación española en esta materia al Reglamento General de Protección de Datos del reglamento de la Unión Europea, se enumeran los siguientes derechos:

Los derechos en la era digital: tanto los derechos como las libertades contempladas en la Constitución española y en los tratados internacionales que el Estado español haya ratificado son **derechos vinculantes** en el contexto de la red, y así deben garantizarlo las **empresas proveedores de Internet**.

Derecho a la neutralidad de Internet: sostiene que las empresas proveedoras de Internet tienen que tratar de la misma forma todos los **datos que viajan por Internet** independientemente de su contenido. Con ello, se pretende impedir que las empresas proveedoras puedan priorizar un tipo de datos sobre otros, por ejemplo, los de pago. Su objetivo es que la oferta sea transparente y se evite la censura derivada de los valores o intereses económicos de las empresas proveedoras.

Derecho de acceso universal a Internet: con la intención de combatir la brecha digital —haciendo hincapié en la generacional, la de género, la rural y la que afecta a personas con capacidades especiales—, este derecho hace referencia al **acceso a Internet como principio** de toda persona para poder ejercer derechos humanos fundamentales, como la libertad de expresión, y contribuir al crecimiento y progreso de la sociedad, independientemente de sus condiciones personales. La ONU estableció el derecho de acceso a Internet como un derecho humano en 2011.

Derecho a la seguridad digital: aunque ya aparece en la Constitución española el derecho a la privacidad de las comunicaciones con independencia del canal, en esta ley se especifica que los usuarios y

usuarias tienen derecho a la **seguridad en la transmisión de sus comunicaciones** a través de Internet. Se añade, además, que las empresas proveedoras de los servicios de Internet deben informarnos de nuestros derechos como internautas.

Derecho a la educación digital: por el aprendizaje en el uso seguro y respetuoso de las tecnologías digitales en todos los **planes educativos** en forma de módulos educativos. Establece, también, que los y las profesoras tendrán que recibir formación para poder impartir dichas competencias, y se refiere también a otras profesiones específicas que puedan necesitar de ella en el desempeño de sus labores.

Protección de los menores en Internet: hace referencia a la **responsabilidad de las familias, tutores y tutoras** para que el uso de los dispositivos por parte de los y las menores sea equilibrado y responsable para así “garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales”. La ley también se refiere a la publicación de sus imágenes que, aunque no especifica, establece podrá ser perseguida por el Ministerio Fiscal.

Derecho de rectificación en Internet: ya existente en la Ley Orgánica 2/1984, reguladora del derecho de rectificación, reivindica el **derecho a la libertad de expresión** en Internet para todas las personas, el derecho a rectificar cualquier información difundida de considerarla inexacta o perjudicial, o que atente “contra el derecho al honor, la intimidad personal y familiar en Internet” y “el derecho a comunicar o recibir libremente información veraz”. Establece que las empresas o responsables de las redes sociales y servicios similares tienen que proveer de protocolos necesarios para ejercer el derecho de rectificación.

Este derecho ha supuesto un importante debate por dos cuestiones: en primer lugar, el hecho de que ya exista en una ley orgánica anterior hace que se duplique la normativa que lo regula y esto, dicen algunas partes, puede derivar en inseguridad jurídica; y, en segundo lugar, grupos como la Plataforma de Defensa de la Libertad de Información (PDLI)

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

y la Federación de Sindicatos de Periodistas (FeSP) temen que, con la intención de regular y evitar las noticias falsas y el contenido erróneo, con la nueva ley se esté posibilitando la censura y dando el poder decisorio para eliminar, ocultar o transformar contenidos a empresas sin un criterio acreditado para ello, como son las empresas responsables de las redes sociales.

Esta regulación es tan compleja porque está estrechamente vinculada con el **derecho a la libertad de expresión y a la veracidad informativa** recogido en la Constitución, y fundamental para el desarrollo de una opinión pública plural y libre como base de un Estado democrático y de derecho.

En la actualidad, la proliferación de noticias falsas —o también llamadas *fake news*—, *clickbaits* y bulos en las redes sociales, los repositorios de vídeos y los servicios de mensajería instantánea es un problema alarmante que necesita ser abordado. Lo es hasta el punto de llegar a influir a los medios de comunicación digitales y el posicionamiento de las noticias e incluso al tono y veracidad de los discursos políticos. Este derecho pretende afrontar este problema, pero es vital que como internautas aprendamos a luchar contra este tipo de contenidos.

Fake news, bulos y clickbaits

Por eso vamos a aprovechar este apartado para conocer pautas para reconocer bulos y noticias falsas. Si queremos que nuestros hijos, hijas, alumnado y menores a cargo hagan uso de un Internet seguro, **es fundamental que no contribuyamos a la difusión del contenido falso o erróneo y que fomentemos que tampoco ellos lo hagan.**

Este tipo de contenidos falsos son perjudiciales porque propagan el miedo y la desinformación. Apelan a nuestra curiosidad, deseos

e ideología y al sentimiento de pertenencia, pero en realidad suelen estar vacíos de información relevante. El objetivo de quienes los originan suele ser económico (ganan dinero a través del número de clicks y el tráfico web) y/o ideológico. Veamos sus características:

- I **Los clickbaits:** son materiales diseñados para conseguir clicks y así generar ingresos publicitarios (la mayoría de campañas publicitarias se pagan por número de clicks). Un ejemplo claro son los textos escritos en formato de artículo con un titular sensacionalista como: “No creerás lo que esconde el tatuaje de Sergio Ramos”. Desgraciadamente, en la actualidad muchos medios de información digitales los utilizan para lograr tráfico web e ingresos. Tras abrirlos, el contenido no suele ser ni mínimamente interesante y muchas veces ni siquiera concuerda con lo anunciado en el titular. Son un ejemplo claro de cómo nos afectan las estrategias digitales que apelan al sentido de la curiosidad.
- I **Noticias falsas o fake news:** una noticia falsa es un tipo de bulo en el que se distribuye una noticia cuya información no es veraz, ya sea total o parcialmente.
- I **Bulos:** es un contenido falso que se propaga por Internet. Existen muchos tipos. Entre ellos el bulo informático por correo electrónico, la noticia falsa, el bulo propagado por las aplicaciones de mensajería instantánea, etc.
- I **Cadenas:** son bulos que tratan de convencerte de que los reenvíes o compartas.

¿Cómo identificar un bulo, una noticia falsa o una cadena?

1. **LEE AL COMPLETO:** no te limites a leer el titular. Si no lees el texto al completo, no podrás saber si es digno o no de tu atención, tus comentarios o —importante— de compartir. Sospecha también de las erratas y los titulares extremadamente efectistas con palabras tipo: “espectacular”, “inaudito”, “no imaginas [...]”, “nunca creerás [...]”.

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

Si el titular te causó una reacción fuerte, sorpresa, mucha curiosidad, incredulidad, enfado, reafirmación, desconfía. Están pensados para ello.

2. REVIS LA FUENTE Y LA URL: si está publicado en un medio o una página no fiable, no des crédito. Y revisa la URL porque muchas veces son dudosas y tienen caracteres de más.

Si no tiene fuente y es solo una imagen, un vídeo y un audio que te ha llegado por mensajería instantánea o por alguna red, ten en cuenta que las probabilidades de que la información que contiene sea falsa, errónea o imprecisa son muy elevadas. No compartas.

3. REVIS LA FECHA: con frecuencia los bulos vuelven a ponerse de moda repentinamente y mucha gente ni se fija en que se publicó equis años atrás. Esto suele ser indicativo de que o bien la información no es cierta o está descontextualizada.
4. COMPRUEBA LA AUTORÍA: ¿aparece el nombre de quien lo ha creado? Investiga si trabaja como profesional en alguna plataforma fiable sin sesgo ideológico.



5. **COMPRUEBA QUE NO ES UNA BROMA:** a veces nos tomamos muy en serio titulares que luego resultan ser un chiste.
6. **CONTRASTA:** utiliza el buscador para comprobar si la imagen se ha utilizado para otros bulos con anterioridad, o busca el titular para ver si alguien ha alertado de que es un bulo.
Existen medios y plataformas como www.maldita.es, la SER o las redes de la Guardia Civil, donde se publican algunos de los últimos bulos y noticias falsas.
7. **PREGUNTA** a quien te la envió si contrastó la información antes de hacerlo.

Derecho a la actualización de informaciones en medios de comunicación digitales: indica que cualquier persona puede pedir que los **medios de comunicación digital** actualicen una información publicada con anterioridad que le haya causado perjuicio.

Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral: concreta la **privacidad en el uso de los dispositivos tecnológicos** que necesitan los y las trabajadoras en su ámbito laboral, estableciendo que las personas empleadoras tendrán que detallar los criterios de utilización y solo podrán acceder a ellos con fines laborales y de garantía de los mismos.

Derecho a la desconexión digital en el ámbito laboral: detalla que los y las empleadoras no puedan contactar con quien trabaja a su cargo **fuera del horario laboral o en vacaciones.**

Derecho a la intimidad frente al uso de videovigilancia y de grabación de sonidos en el lugar de trabajo: especifica los escenarios en que se permite, previo anuncio, la utilización de **sistemas de vigilancia.**

Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral: permite el uso de sistemas para comprobar la **ubicación** de las y los trabajadores, previo anuncio.

Derechos digitales en la negociación colectiva: “Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con **el tratamiento de los datos personales** de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral”.

Protección de datos de los menores en Internet: tanto los centros educativos como otras personas que hagan uso de los datos de menores a través de Internet tienen que tener el **consentimiento expreso** de sus representantes legales o del menor. La edad mínima para dar el consentimiento se reduce a los 14 años (antes era a los 16).

Derecho al olvido en búsquedas de Internet: se refiere al derecho de toda persona a solicitar la **eliminación de los resultados que aparezcan en los motores de búsqueda** a partir de su nombre si son “inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo” según los fines para los que fueron recogidos.

Derecho al olvido en servicios de redes sociales y servicios equivalentes: profundiza en el anterior derecho pero en **redes sociales y similares**, estableciendo que cualquiera tiene derecho a que se eliminen los datos personales (incluyendo fotografías) que le afecten y hayan sido publicados en estos canales por terceros si son “inadecuados, inexactos, no pertinentes, no actualizados o excesivos”, “a su simple solicitud”. Si, además, quien lo solicita es menor, debe hacerse “sin dilación”.

El derecho al olvido también ha derivado en polémica porque puede colisionar con la libertad de información y de expresión.

Derecho de portabilidad de redes sociales y servicios equivalentes: protege el derecho a **trasladar los contenidos y datos propios** subidos a redes sociales y similares de una a otra plataforma, siempre que sea técnicamente posible. Recuerda a la portabilidad entre empresas de servicios telefónicos.

Derecho al testamento digital: contempla el derecho a crear un **testamento** para definir qué hacer con los perfiles de redes sociales, correo electrónico y servicios de mensajería instantánea propios tras el fallecimiento de la persona; y la posibilidad de dar acceso a los mismos a la familia.

Derechos sobre nuestra imagen en Internet

Además de los anteriores derechos recogidos en la Ley de Protección de Datos Personales y Garantía de los Derechos Digitales, es fundamental comprender cómo afectan los **derechos al honor, a la intimidad y a la propia imagen, y a la privacidad** en el contexto de Internet —en otros supuestos no contemplados en dicha ley—.

Los derechos sobre nuestra intimidad e imagen están recogidos en la Constitución, la Ley Orgánica 1/1982, la RGDP y el Código Penal, y afectan a toda persona física.

Según estos derechos, está **prohibido realizar una fotografía de cualquier persona y difundirla sin su consentimiento expreso, así como grabar en vídeo y/o audio y luego difundirlo**. Si lo hacemos, la persona en cuestión podrá no solo solicitar su retirada en caso de haberse publicado en una red social o plataforma con protocolo para el derecho al olvido, si no que además será denunciable.

Será este el caso de los y las menores que graben a docentes en el ejercicio de su profesión para publicarlo después en una red social o difundirlo por algún servicio de mensajería instantánea sin su consentimiento o contra su voluntad; estarán incurriendo en un delito si no tienen primero su permiso.

Los únicos supuestos en los que sí es legal difundir las imágenes y/o audio de alguien sin su consentimiento es si se trata de **un cargo público o tiene lugar en un acto o acontecimiento público, están autorizadas**

por un organismo competente o tienen un interés histórico, cultural o científico relevante.

En el caso de las grabaciones, grabar a alguien con quien estás manteniendo una conversación o en una conversación en la que tomes partido es legal tanto en audio como en vídeo, y puede usarse como prueba judicial, pero **difundir el material resultante es ilegal**. No se podrá publicar ni en redes sociales ni en otro servicio de comunicación o mensajería instantánea. En el caso de familiares que coloquen dispositivos de grabación a menores para recabar pruebas, por ejemplo, del trato de un o una profesional a sus menores a cargo, sería una grabación ilegal por ser una conversación ajena. A pesar de ello, hay ocasiones en que el tribunal hará una ponderación para determinar qué derecho debe primar.

Para **denunciar la publicación de fotos o vídeos propios sin consentimiento**, se puede hacer ante la policía, el grupo de delitos telemáticos o la brigada de investigación y ante la Agencia Española de Protección de Datos (AEPD). También, como se menciona, en la mayoría de redes sociales y servicios similares como foros y otras plataformas debe existir un formulario para solicitar la retirada de imágenes y vídeos.

Las sanciones varían en función de las infracciones, así como la posibilidad de indemnización.

Cuestionario para la reflexión

PRÁCTICA PARA PADRES, MADRES Y TUTORES LEGALES

Conversemos:

Tras estos tres primeros capítulos, es buen momento para tener una conversación con tus hijos, hijas o menores a cargo. Recuerda escuchar activamente y anota ideas claves que te sirvan para empezar o continuar construyendo ese espacio para que puedan expresarse y compartir sus conocimientos contigo respecto al uso responsable y seguro de Internet:

1. ¿Tiene o tienen redes sociales? Si continúas sin saberlo, es buen momento para preguntarlo:

☐ Sí ☐ No

Como veremos en el siguiente capítulo, la edad mínima para casi todas ellas es de entre 13 y 14 años.

2. ¿Se han sentido mal alguna vez porque alguien haya publicado una fotografía suya sin su consentimiento?

☐ Sí ☐ No

Si la respuesta es sí, ¿cómo se sintieron?; si es no, ¿cómo se sentirían?

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

3. Cosas que no debe(n) compartir en línea, a través de redes sociales o de mensajería instantánea:

- ☐ Imágenes y noticias cuya información no podemos contrastar
- ☐ Imágenes o vídeos de personas que no conozco
- ☐ Imágenes de personas que conozco sin su consentimiento
- ☐ Imágenes que pongan en ridículo o avergüencen a compañeros, compañeras, familiares o al cuerpo docente y administrativo del centro de estudios
- ☐ Imágenes de terceros sin su consentimiento
- ☐ Datos personales propios, de la familia y de terceros
- ☐ Información de seguridad como contraseñas, año de nacimiento, etc.
- ☐ Otros: _____

4. Como personas adultas, ¿es aconsejable que compartamos lo anterior?

5. ¿Por qué no debemos, como personas adultas, alarmarnos y sobre-reaccionar a lo que nos cuenten menores sobre su uso de Internet?

6. ¿Por qué no debemos compartir imágenes de menores de 14 años públicamente?

7. ¿Por qué es importante que, como personas adultas, no compartamos contenidos poco contrastados como imágenes con un titular sin ningún otro desarrollo o fuente a través de redes sociales y mensajería *online*?

8. ¿Por qué es fundamental aprender a distinguir noticias falsas o capciosas y no compartir nada que no sea información de calidad?

REDES SOCIALES, FOROS Y REPOSITORIOS DE VÍDEOS

Revolución social

4

OBJETIVOS FORMATIVOS



Aprender a escuchar y asistir a los y las menores en el uso de redes sociales

- I Entender cuál es el papel de sus mayores.
- I Reflexionar sobre cómo asistirlos.
- I Descubrir pautas para educar en el uso responsable.

CONTENIDOS FORMATIVOS



- I Las redes sociales, la definición de la identidad y el refuerzo social.
- I Gestión emocional e Internet.
- I Pautas básicas en el uso de las redes sociales.

APUNTES

Las redes sociales han supuesto una profunda revolución en nuestra forma de **socializar, relacionarnos y autopercebirnos**. Millones de personas las utilizan cada día en todo el mundo y las generaciones jóvenes, más que ninguna otra, encuentran ampliamente satisfecho en ellas el refuerzo social, tan importante a estas edades.

Para casi cualquier adolescente hoy en día en España, las redes sociales son un espacio clave a muchos niveles.

Este tipo de plataformas suponen un medio de expresión de la identidad muy poderoso. Las generaciones anteriores a las conocidas como “nativas digitales”, expresaban su identidad en la adolescencia sobre todo a partir del grupo: la subcultura, las tribus urbanas, la moda y la ropa, la música... En función de sus influencias sociales, culturales, económicas, geográficas, etc., se decantaban por uno u otro y, gracias al grupo, se facilitaba la difícil tarea de definir su identidad propia.

La globalización posibilitó entonces la sofisticación de la subcultura y las tribus urbanas. Llegó un punto en el que empezó a ser perfectamente posible que sintieras más identificación con una persona japonesa de tu edad que escuchaba la misma música, veía las mismas series o leía los mismos libros, que con los vecinos y vecinas con quienes creciste. Los sistemas culturales de las tribus urbanas se diversificaron y se volvieron más específicos: había más donde elegir y reivindicarse porque llegaban más expresiones de las subculturas de distintos puntos del globo. Era más probable que encontraras “tu lugar en el mundo”.

Las redes sociales suponen, por ahora, la máxima potencia de este proceso. Entonces, se empezó a tener más acceso a contenidos de las diferentes subculturas alrededor del mundo; **hoy el acceso es pleno**. De repente, ni siquiera es necesario pertenecer a un grupo para construir y expresar tu identidad, porque simplemente en función de tus intereses y tus gustos puedes encontrar **miles de pares en todo el mundo** con

inquietudes prácticamente iguales a las tuyas que así lo expresan en sus publicaciones.

En las redes sociales y servicios similares como los repositorios de vídeos o los foros, la mayoría de los y las adolescentes expresan su identidad y se definen más que en ningún otro espacio. También en ellas conocen y se relacionan con las amistades, interactúan con la sociedad y reinventan códigos, escuchan música, se entretienen, definen gustos y eligen ídolos. Por eso no podemos, como personas adultas, comparar el uso que hacemos de estas plataformas con el suyo ni pretender que su apego sea el mismo.

› ¿ENTONCES?

Entonces, tratemos de acompañar a estas generaciones en su descubrir.

Como comentábamos en el primer capítulo, si queremos acercarnos a nuestro alumnado, hijos, hijas o menores a cargo para que hagan un uso seguro de Internet, lo primero que tenemos que hacer es escuchar. La familia es primordial a la hora de establecer valores y prioridades, por eso es importante que nos pongamos en el lugar de los y las menores, nos formemos en el mundo digital y aprendamos a identificar factores de riesgo, comprendiendo y sabiendo situar las problemáticas en este medio para ayudarles a crear esquemas de comportamiento.

Ya sabemos que Internet y las redes sociales son un medio poco definido y muy dinámico que entraña riesgos. Sin embargo, muchas veces el mal uso o el uso excesivo de la tecnología responde a problemas emocionales y del comportamiento que no tienen necesariamente que ver con la presencia en Internet: ansiedad, falta de atención, crisis de autoestima, aislamiento, etc.

Como en cualquier otro ámbito de la vida, lo fundamental a la hora de educar en el uso seguro de Internet es fomentar la **educación en valores, atender a las necesidades propias y el equilibrio**.

› ¿SON NEGATIVAS LAS REDES SOCIALES?

La realidad es que, aunque suponen oportunidades importantes para la socialización y la autopercepción de las personas, las plataformas de las redes sociales están pensadas para generar una participación muy simplificada y basada en el refuerzo superficial e inmediato. Sean Parker, primer presidente de una de las grandes redes sociales y quien consiguió popularizar estas plataformas en un inicio, reconoció que explotaron “una vulnerabilidad de la psicología humana” y añadió que trabajaron de forma consciente para que todas las interacciones tuvieran un efecto similar a la dopamina, el neurotransmisor relacionado con la sensación de placer y recompensa del cerebro del que hablábamos en el segundo capítulo. “Teníamos que dar un poquito de dopamina cada rato. O bien porque alguien había dado a ‘me gusta’ o porque habían comentado tu foto”².

› ¿A QUÉ EDAD PUEDEN TENER PRESENCIA EN REDES SOCIALES?

No siendo igual en todos los países, en el Estado español el acceso a redes sociales está regulado por la Ley Orgánica 15/1999, del 13 de diciembre, que establece que “podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de **14 años se requerirá el consentimiento de los padres o tutores**”. Es decir, que a partir de los 14 años no necesitarán del consentimiento de los padres o tutores; antes sí.

Además, algunas plataformas pertenecientes a compañías extranjeras reducen el mínimo de edad para registrar un perfil en su página a los 13 años, a pesar de que ello no concuerde con la normativa. Esto ocurre porque al estar localizadas fuera de España, no han de

² Luna, José Antonio (20 de febrero de 2018). “Renegados de Silicon Valley que pasaron a luchar contra la tecnología”. Artículo de eldiario.es.

regirse por la ordenación española. Asimismo, otras muchas no recomiendan el registro ni siquiera con consentimiento de los padres, madres o tutores.

En cualquier caso, para un o una menor es considerablemente sencillo crear una cuenta falsa registrando una edad superior a la suya o modificando sus datos.

En el caso de los repositorios de vídeos, la edad mínima suele ser también de 13 años en su registro, aunque algunas cuentan con una marca propia para menores de 13 años.

En general, no conviene dar consentimiento a menores de 14 años para un perfil personal en redes sociales.

➤ **¿CÓMO ENSEÑO A HACER UN USO RESPONSABLE DE LAS REDES SOCIALES?**

Si tu hijo o hija es mayor de 14 años y se ha creado un perfil individual, es hora de plantearnos cómo afrontar esta etapa para ayudar a que haga un uso positivo y seguro de las redes sociales.

En primer lugar has de tener en cuenta que pueden acceder a Internet y a las redes sociales de múltiples maneras y en infinidad de dispositivos, aun cuando no estén en casa. Por eso, no conviene ser excesivamente taxativos: cuanto más restrictivos seamos más van a entender Internet como un medio en el que rebelarse.

Lo principal es crear un **espacio de diálogo** cuanto antes y aprovecharlo para establecer pautas básicas:

- a) **Tiempo de conexión máximo a redes sociales:** cada familia debe adecuarlo a su consideración, pero, en general, tanto los menores como cualquier otra persona debería limitar el uso de redes sociales a 30-40 minutos diarios.

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

Algunas redes sociales permiten establecer máximos de tiempo de uso, igual que también lo permiten los dispositivos móviles. Investígalo y **negociad el tiempo máximo**.

Es muy importante que hasta que el o la menor esté preparado, seamos las personas adultas quienes mantengamos el control sobre el uso de los dispositivos y las redes sociales. Si nos hemos comprometido a utilizarlo menos de media hora al día y no se cumple nuestro acuerdo, es importante que haya consecuencias.

- b) **Coherencia:** también es fundamental que seamos **coherentes** con lo que acordamos con nuestros hijos e hijas, también con el alumnado. Si les pedimos cumplir un máximo diario pero luego, por nuestra parte, nos pasamos las tardes chateando por mensajería instantánea, no servirá de nada.



- c) **Espacios y pertenencia de dispositivos:** los espacios son muy importantes, sobre todo en los primeros años de presencia en redes sociales. Debemos negociar qué espacios deberán permanecer libres del uso de los dispositivos electrónicos, incluidos teléfonos inteligentes —si es que tiene uno—, y qué espacio estará reservado a la tecnología. Suelen establecerse como espacios libres de móviles y tabletas aquellos como la cama o el cuarto propio, la mesa a la hora de desayunar, comer o cenar en familia, en general, momentos compartidos, las visitas al abuelo o la abuela, el coche (teniendo en cuenta que muchos accidentes ocurren por distracciones mirando el *smartphone*, no es mala idea inculcar desde la adolescencia temprana la idea de que el coche no es un lugar para el teléfono).

En el caso del ordenador, en general, es más recomendable colocarlo en una **zona común** para el uso de toda la familia que hacerlo en el cuarto de un o una menor, y especificar además que solo se use cuando haya personas adultas en casa —al menos hasta que tenga suficiente madurez y conocimiento de los riesgos digitales—. De esa manera estaremos cerca con frecuencia y podremos ofrecer mayor apoyo en las tareas, comentar cuestiones de seguridad y uso positivo de Internet y asegurarnos de que no hay comportamientos problemáticos.

En el caso de los dispositivos electrónicos como tabletas y móviles, las familias españolas cada vez los regalan antes a sus hijos e hijas. Especialistas como la Fundación ANAR establecen que la edad recomendada para que los y las menores tengan un teléfono inteligente propio es de 15 años, cuando el niño o niña tiene mayor capacidad crítica a la hora de ponerse en riesgo frente a situaciones posibles en la red. Por supuesto, esta edad depende de las circunstancias y la madurez de la persona. Si, por ejemplo, tiene que volver sin acompañamiento a casa en autobús, especialistas recomiendan tener un teléfono común para uso esporádico de la familia (por ejemplo, si se tienen más hijos o hijas) en lugar de uno que use en exclusivo y considere propio.

- d) **Neuronas espejo y tono:** en 1996 Giacomo Rizzolatti hizo uno de los más importantes descubrimientos en el campo de la neurociencia de las últimas décadas, identificó las **neuronas espejo**.

Estas neuronas, también llamadas neuronas cubelli, hacen que al ver los movimientos y expresiones de otra persona, podamos sentir sensaciones y emociones similares a las que ella está sintiendo. Es un mecanismo reflejo y está muy ligado a la empatía. Sucede, por ejemplo, cuando estamos hablando con una persona y vemos en su expresión facial que algo de lo que hemos dicho le ha sentado mal; de pronto, nosotros también nos sentimos mal por un momento y, normalmente, tratamos de corregir nuestro descuido. En Internet, cuando interactuamos con otras personas, la mayoría de las veces no nos vemos. Por eso, aunque tengamos la sensación de que compartimos espacio con cientos de personas, lo cierto es que navegamos en soledad y somos conscientes de ello.

Como ocurre con algunas personas cuando conducen y se sienten protegidos por la seguridad del coche, a veces en las redes sociales, repositorios y foros nos permitimos tratar al resto con desprecio, e incluso odio si la cosa se tensa un poco. Es vital que evitemos este tipo de comportamiento.

Los y las menores no solo sufren la misma desafección de las emociones de los demás cuando están en Internet, sino que aprenden a socializar en un entorno en el que resulta absolutamente normal insultar y vejar a personas desconocidas.

Por mucho que pensemos que nos ampara el anonimato, en Internet esto es un mito. Y no solo ello, sino que infligimos daño. **Lo que se dice en Internet no es menos real, ni duele menos.** Si estamos tratando con una persona desconocida, nunca sabremos si está pasando por un momento terrible, si tiene depresión o si es vulnerable. También a nosotros y nosotras nos afecta: la escalada de tensión que supone luchar verbalmente con alguien desconocido nos acompaña y nos afecta psicológicamente, no se queda en la pantalla. Debemos educarnos y educar a nuestros hijos e hijas, o al alumnado como docentes, para que deje de ser habitual el tono beligerante entre desconocidos en las redes sociales. Gracias a ello, de hecho, sería mucho más sencillo identificar a personas con un comportamiento alarmante en estas plataformas y denunciar sus intervenciones.

- e) **Conocer los riesgos:** a la hora de que tu hijo o hija empiece a utilizar las redes sociales, es importante **familiarizarse con los riesgos** que entrañan y dárselos a conocer. En el capítulo 6 veremos en profundidad riesgos y ciberseguridad de Internet en general, dado que ninguno es exclusivo de las redes sociales.

Pautas que defender con menores en el uso de redes sociales

- a) **Mi uso:** a la hora de hacer uso de las redes sociales, lo hago con **responsabilidad y atendiendo a mis necesidades:** siempre con un **objetivo concreto** (no viendo un post detrás de otro como un hámster en una rueda), atendiendo a cómo me hacen sentir los contenidos, participando de forma positiva y aportando cosas, respetando los tiempos máximos de conexión que he fijado con mis mayores, profundizando en mis intereses, respetando a las demás personas y poniéndome en el lugar del resto de internautas.
- b) **Mis datos:** tengo mucho cuidado de **no publicar ningún dato sensible:** la dirección de casa, mi fecha o año de nacimiento, mi nombre completo, mis contraseñas, detalles de mi intimidad. Es una tontería decirle a personas desconocidas dónde estoy y dónde voy a estar y puede ponerme en verdadero peligro.
- Me informo sobre las **normas y medidas de seguridad** de la red social y mantengo mis **ajustes de privacidad** de manera que mi perfil sea privado y solo mis conocidos puedan ver lo que publico.
- c) **Mis comentarios:** en Internet, como en el resto de lugares, **respeto a los demás y cuido mis reacciones y comentarios.** El que algunos usuarios y usuarias vuelquen sus frustraciones en la red no es excusa para que lo haga yo también. Aprendo a ponerme en el lugar de los demás y a reaccionar de manera calmada y reflexiva ante provocaciones de personas desconocidas. No pago mis frustraciones en Internet bajo ningún concepto.
- d) **Solicitudes:** no tengo porqué aceptar las solicitudes de personas que no conozco. ¿Para qué iba a hacerlo? ¿Entablaría conversación con alguien desconocido en la calle a quien no puedo ver la cara?

Reflexiono antes de abrirle la puerta a mi mundo virtual a personas que no conozco.

- e) **Los datos de mis amigos y amigas:** las fotografías son uno de los datos personales más sensibles porque permiten que se nos reconozca. No puedo compartir fotos ni datos de mis conocidos sin su consentimiento. Tampoco etiquetarles a mala idea, menos aún si el que lo haga les hace sentir humillación. Recuerda que toda información privada de una persona que no te haya dado su permiso para publicarla no se puede difundir. Incluso puedes llegar a vulnerar sus derechos e incumplir la ley.
- f) **Datos e imágenes de terceros:** ocurre lo mismo con la información personal de personas que no conozco. Aunque me la hayan enviado a mí primero, no debo compartirla bajo ningún concepto sin permiso. Debemos aprender a dar el valor a las imágenes y datos de las personas que realmente tienen y no contribuir a vulnerar los derechos.
- g) **Información sin contrastar:** no debo compartir información superficial que sea susceptible de ser falsa, y menos cuando fomenta el odio y la discriminación en las redes.
- h) **Si no me siento bien por la interacción con otro internauta,** por algún contenido sensible que he recibido, porque me siento en peligro por alguna razón: paro inmediatamente. No borro nada, mantengo la calma y voy directamente a hablar con mi padre, madre o tutor legal para que me ayuden a valorar la situación y tomar la mejor decisión posible.
Las redes sociales pueden ponerme en un peligro real, así que siempre priorizo mi seguridad sin preocuparme de lo que puedan pensar mis mayores, porque ellos siempre preferirán que esté a salvo por muy horrible que parezca el lío en el que me he metido.
- i) **No gasto dinero online:** los gastos en Internet son solo para personas adultas dado que existen peligros reales como los timos, el robo de datos bancarios, etc. Si necesito comprar algo *online*, lo hablo con mis mayores.
- j) **Denuncio:** aprendo a utilizar las herramientas de denuncia de las redes sociales para solo utilizarlas en caso de que alguien esté incumpliendo las normas de las mismas.

Cuestionario para la reflexión

PRÁCTICA PARA PADRES, MADRES Y TUTORES LEGALES

Sigamos aprendiendo de nuestros hijos e hijas sobre el uso que hacen de las redes sociales (en caso de que lo hagan).

1. ¿Qué redes sociales te gustan? ¿Por qué esas más que otras? ¿Qué tienen de particular? ¿Me las recomendarías? _____

2. ¿A qué dedicas el tiempo en redes sociales? _____

3. ¿Tienes perfiles públicos o privados? _____
4. ¿Quiénes son tus contactos o seguidores? ¿Te siguen personas desconocidas? ¿Cómo decides a quién seguir o qué solicitudes de amistad aceptar? _____

5. ¿En redes sociales navegas con objetivos concretos o deambulas por los contenidos? ¿Participas activamente? _____
6. ¿Qué sientes cuando recibes 'me gustas' o alguien comenta tus publicaciones? _____

7. Cuando interactúas con personas desconocidas en foros o comentando publicaciones públicas, ¿lo haces respetuosamente? _____

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

8. ¿Has tenido alguna mala experiencia en redes sociales que quieras compartir conmigo? _____
9. ¿Conoces los peligros que supone publicar información privada o chatear con personas desconocidas en las redes sociales? _____
10. Sabes que puedes contar conmigo si te sientes en peligro, ¿verdad? _____



APLICACIONES Y VIDEOJUEGOS

Mucho más que un juego

OBJETIVOS FORMATIVOS

Conocer el mundo de las aplicaciones y los videojuegos para educar en un uso comedido y responsable:

- I Adoptar pautas de seguridad en las descargas.
- I Prestar atención a los códigos de edad.



CONTENIDOS FORMATIVOS

- I Introducción a los videojuegos y aplicaciones.
- I Pautas para la descarga, códigos de edad, consejos de uso.



APUNTES

La industria del videojuego y las aplicaciones para móviles ha revolucionado la forma en que nos entretenemos. Sus descargas se cuentan por millones y su uso se multiplica año tras año en toda la población.

Algunas aplicaciones resultan muy positivas y se han convertido en herramientas que nos facilitan el día a día e incluso nos ayudan a potenciar nuestras capacidades y ahorrar tiempo a la hora de hacer tareas poco provechosas.

Pero de la misma manera, muchas de ellas tienen interfaces muy estimulantes, con dinámicas repetitivas que las convierten en juegos o **plataformas preocupantemente adictivas que no nos proporcionan recompensa real alguna más allá del entretenimiento.**

Es innegable que algunos videojuegos y aplicaciones fomentan el desarrollo cognitivo y el aprendizaje de los y las menores, pero un uso excesivo o la continuada exposición a plataformas y contenidos para los que no están preparados emocionalmente puede derivar en hábitos y conductas negativos.

Por ello, como adultos comprometidos con inculcar el uso responsable y seguro de la tecnología, tenemos que tener muy en cuenta los hábitos de los y las menores en el uso de *apps* y videojuegos, así como la actualidad de esta industria que no siempre es tan transparente e inocua como debiera.

Los videojuegos: hoy en día el acceso a los videojuegos se ha diversificado enormemente. Se puede jugar desde la consola en la televisión, la consola portátil, el móvil, la tableta, la televisión inteligente y el ordenador. Multitud de plataformas ofertan juegos *online*, entre ellas, algunas redes sociales. Además, existen videojuegos para todos los gustos, cada vez más enfocados a un tipo de público concreto, con diseño e interfaces muy atractivas, hechos en tres dimensiones, realistas o muy simples, con múltiples colores, efectos de sonido y recompensas constantes.

› PAUTAS PARA LA DESCARGA Y USO DE APLICACIONES Y VIDEOJUEGOS

I Descargas: tengamos en cuenta que sobre todo el teléfono móvil, aunque también el ordenador o la tableta, es el objeto donde, tanto padres y madres como menores, guardamos más **información personal**. En general, no prestamos toda la atención y el cuidado que deberíamos a la hora de hacer descargas, sobre todo teniendo en cuenta la frecuencia con que se desarrollan *apps* fraudulentas que pueden hacer uso o directamente robar o eliminar este tipo de información privada. Algunas, incluso, están diseñadas para conseguir nuestros datos y así suplantar nuestra identidad. Por eso conviene tener en cuenta una serie de aspectos antes de descargar una *app* o un juego:

1. **Tiendas oficiales:** descargar en las **tiendas oficiales** hace que los riesgos sean considerablemente menores que en las que no lo son. En ellas existen más herramientas de denuncia y actualización. En las no oficiales, la exposición al peligro está prácticamente garantizado.
Pero esto no implica que en las plataformas de descargas oficiales de Android e iOS no existan las aplicaciones fraudulentas y el riesgo a la exposición y robo de datos personales. Por eso es muy recomendable seguir las demás pautas que proponemos.
2. **Opiniones, valoración y descargas de otras personas usuarias:** fíjate en las **opiniones que han dejado otros usuarios y usuarias** y sospecha si hay un desajuste en la relación entre las opiniones, descargas, fecha en que se creó, etc. Revisa las opiniones de otras personas en busca de comportamientos extraños o denuncias.
3. **Comprobación de desarrollador, fecha, descripción, política de privacidad, etc.:** en general, aplicaciones que hacen uso fraudulento de los datos, lo hacen desde desarrolladores nuevos, la fecha en que ha salido no concuerda con el enorme

número de descargas, la descripción no está redactada si no que aparece únicamente un listado de características, contiene erratas, etc.

Es fundamental dedicar unos minutos a leer la política de privacidad, dado que en ella pueden estar diciéndonos que venderán nuestros datos a terceros o que accederán a nuestras fotografías.

Teniendo en cuenta la cantidad de información (datos bancarios, fotografías, conversaciones privadas, contactos, historial, etc.) y procesos sensibles (compartir tu ubicación, encender el micrófono o la cámara del dispositivo, etc.) que existen en nuestros dispositivos, deberíamos actuar con mucho más recelo del que solemos. Parece que **en el mundo virtual somos menos conscientes de nuestra exposición al peligro**. Descargar aplicaciones sin tener en cuenta el riesgo es al mundo virtual lo que al real sería dejar la puerta de casa abierta para que entre todo el mundo aunque ni siquiera estemos presentes.

4. **El mito de la gratuidad:** nadie ofrece un servicio gratuito sin esperar nada a cambio. **Las aplicaciones gratuitas no existen**. En Internet, si no pagas, normalmente es que te estás vendiendo tú, tu privacidad, tus datos.

Las aplicaciones cuya estrategia es la venta de nuestros datos privados consumen además muchos recursos del dispositivo al estar constantemente enviando la información a las plataformas *online* que gestionan o compran esos datos. No solo estamos vendiendo nuestra privacidad, sino también la memoria, el procesador, la batería y los datos móviles (WiFi, 3G, 4G, etc.) de nuestros dispositivos.

En el caso de los **videojuegos freemium o gratuitos**, muy de moda últimamente, su estrategia es ofrecer el juego de forma gratuita para poco a poco derivar en una estructura que trata de embaucar a quien lo usa para que gaste dinero. Por su dinámica de juego, se basan en la estimulación constante y requieren que estés pendiente permanentemente para lograr jugar de forma

gratuita o sin gastar una fortuna. En general, son poco adecuados para menores porque estas dinámicas son muy adictivas y sus contenidos no suelen ofrecer ningún beneficio más allá de la distensión.

5. **Antivirus y verificadores de seguridad:** los **antivirus y verificadores** nos permiten saber si se está desarrollando un uso externo anómalo de nuestros dispositivos y, en el caso de los antivirus, protegernos de algunas amenazas.

También podemos averiguar qué permisos tienen nuestras aplicaciones chequeando los ajustes del dispositivo.

6. **Si descargas habitualmente:** conviene que sigas con detenimiento y mayor frecuencia las pautas del siguiente capítulo sobre ciberseguridad: cambiar las contraseñas de cuando en cuando, mantener los dispositivos actualizados, instalar herramientas de seguridad, etc.

I Contenidos: hoy en día la oferta de aplicaciones y videojuegos es muy amplia, así como los contenidos que ofrecen. Por eso es muy importante que estos se **adecúen a la edad y grado de madurez** de nuestros hijos e hijas o alumnado.

1. **Que no sean adictivos:** en general, los colores, las dinámicas repetitivas, la sobrestimulación y la falta de profundización de los contenidos esconden aplicaciones cuya dinámica de juego es en sí misma adictiva. Es muy negativo que niños, niñas y adolescentes se habitúen al uso de juegos con diseños muy simples y estimulantes. Al final, estarán desarrollando hábitos negativos de los que les resultará muy difícil desprenderse.
2. **Clasificación por edades:** existen varios tipos de códigos para clasificar los videojuegos por edades. En Europa se ha desarrollado el **código PEGI**, en América está regulado por la **Entertainment Software Rating Board (ESRB)** y en Japón, uno de los países más relevantes del mundo en la industria del videojuego, el **sistema CERO**.

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

- a) **PEGI: clasifica los contenidos por edades** refiriéndose a la adecuación de sus contenidos, no a la dificultad: para mayores de 3, 7, 12 o 16. También cuenta con etiquetas que revelan si contiene lenguaje soez, discriminación, drogas, produce miedo, muestra sexo o violencia, y si incluye juego en línea (mediante el cual se interactúa con otros jugadores y jugadoras muchas veces desconocidos). La **etiqueta PEGI OK** se utiliza para juegos denominados “casuales” que son de descarga rápida en móviles, tabletas, redes sociales, etc. Significa que ha sido aprobada para todos los públicos.

PEGI 3



PEGI 7



PEGI 12



PEGI 16



Lenguaje Soez



Discriminación



Drogas



Miedo



Sexo



Violencia



En línea



PEGI OK



- b) **ESRB:** aunque es más común encontrar el sistema de clasificación PEGI en Europa, es posible encontrar el americano ESRB. Este **se distribuye en 7 etiquetas:** primera infancia (E-C, Early-Childhood), todos los públicos (E, Everyone), a partir de 10 años (E10+, Everyone +10), adolescentes a partir de 13 años (T, Teen), adultos o mayores de 17 años (M, Mature),

solo adultos (A, Adults only +18) y pendientes de clasificar (RT, Rating pending).



- c) **CERO:** como ocurre con el ESRB, es menos común de encontrar en Europa, ya que normalmente se accederá a juegos comercializados en el continente. Sin embargo, como en Internet se puede acceder directamente a los desarrolladores, es importante saber que esta clasificación existe y que **está basada en la ESRB** (aunque en algunos casos es cuestionable ya que, por ejemplo, la etiqueta para la primera infancia puede incluir contenidos ofensivos).

3. **Ojo:** aunque existan las clasificaciones por edades estas **no garantizan** que el uso o contenidos de un videojuego sean 100% adecuados para el grado de madurez de los menores. Por eso prestar atención a cómo son y se desarrollan las aplicaciones que utilizan es más que recomendable.

- I Implicate: juega con tus hijos e hijas e interésate por sus gustos.** Si en lugar de pariente eres docente, implícate también. No dejes que los videojuegos se conviertan en un refugio en el que como persona adulta no tienes cabida. Recuerda que es mejor que el lugar de juego (donde se encuentra la consola o la tableta, etc.) esté en un lugar común, en lugar de en un cuarto privado. Hablad sobre ello y no te orilles en contra de lo que les gusta, sino hazlo desde la comprensión y la cercanía. Intercambiad información sobre apps, últimas tendencias, normaliza su uso, pero transmitiendo siempre una actitud lúcida y reflexiva en lo que se refiere a la privacidad, tiempo de uso, etc.

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC



- I Tiempo de uso:** negociad un **máximo y enseña a valorar el tiempo de ocio, el equilibrio y el aire libre.** Aunque se ha generalizado el que los y las adolescentes tengan un tiempo libre cada vez más enfocado a las tecnologías, debemos hacer lo que esté en nuestra mano por fomentar su uso equilibrado. Enséñales a valorar las actividades al aire libre y trata de practicarlas conjuntamente.

No es recomendable cortar de raíz el tiempo de juego, sino avisar con tiempo y sin alarma o dejar que sean ellos y ellas quienes se encarguen de poner fin dentro de lo pautado.

- I **No dejes que se convierta en un premio por el buen comportamiento o los logros:** solo fomentará el valor del tiempo de juego y que los y las menores idealicen el tipo de estimulación que estos les proporcionan.

Es **mejor negociar un tiempo de uso** y que ellos y ellas lo administren como consideren; siempre asegurándonos de que el acuerdo se cumple.

- I **Tampoco lo conviertas en una forma de tenerles entretenidos:** cada vez es más común ver a menores, sobre todo niños y niñas pequeñas, enchufadas a la tableta o la consola portátil durante horas para no molestar a sus mayores. Esto no es inofensivo: **creará un hábito que no resultará fácil corregir.**

La liberación continuada de dopamina y cortisol que proporcionan la gran mayoría de videojuegos son comparables a las que liberamos al consumir comida basura, y su impacto neurológico y el poco aporte puede equipararse a la forma en que afecta a nuestra nutrición su consumo. Por ello es importante **prestar atención a estos hábitos y no normalizar los atracones de videojuegos.**

- I **Problemas físicos:** la postura y la cercanía de los dispositivos a los ojos pueden generar problemas físicos. En el capítulo 7 estudiaremos pautas para evitarlos.
- I **Controles parentales:** la mayoría de consolas y dispositivos electrónicos cuentan con controles parentales para proteger a los y las menores mediante limitaciones en la clasificación por edades, la conexión a Internet, etc. Conviene familiarizarnos con ellos para valorar su instalación, informando antes a nuestro hijo o hija, siempre en consonancia con la edad y grado de madurez.

Cuestionario para la reflexión

PRÁCTICA PARA PADRES, MADRES Y TUTORES LEGALES

1. ¿Cuánto tiempo diario puede utilizar para jugar en la consola, el móvil, el ordenador o la tableta? _____ h

2. ¿Puede mi hijo o hija descargar aplicaciones, juegos o música sin permiso o en mi ausencia?

☐ Sí ☐ No

3. ¿Puede descargar aplicaciones o videojuegos que no se ajusten a su edad?

☐ Sí ☐ No

4. ¿Vamos a instalar controles parentales para las tiendas de aplicaciones?

☐ Sí ☐ No

5. ¿Has instalado algún antivirus?

☐ Sí ☐ No

6. ¿Debería decírmelo si juega a algún videojuego fuera de casa cuya clasificación por edades sea superior a la suya o que incluya violencia, sexo, lenguaje soez, etc.?

☐ Sí ☐ No

7. ¿Qué tipo de videojuegos le gustan? _____

8. ¿Cuál es su videojuego favorito? _____

9. ¿Juega *online*?

☐ Sí ☐ No

10. ¿Interactúa o se comunica con otras personas en línea?

☐ Sí ☐ No

CIBERSEGURIDAD

Dando valor a nuestros datos

OBJETIVOS FORMATIVOS



Comprender la importancia de la seguridad en Internet y los dispositivos móviles:

- I Aprender a apreciar y transmitir el valor de nuestra intimidad y datos personales.
- I Conocer pautas básicas de ciberseguridad.

CONTENIDOS FORMATIVOS



- I Huella digital.
- I Amenazas más comunes que afectan a menores en Internet.
- I Medidas de ciberseguridad básicas.

APUNTES

La vasta mayoría de la población en el Estado español tiene teléfono inteligente. Para el 91,9% de la sociedad³ es el dispositivo preferido y que más se utiliza. Esto, además de un cambio sin precedentes en la forma en que nos comunicamos, relacionamos e informamos, supone también, junto con los otros muchos usos que damos a Internet, una revolución en la manera en que almacenamos, transportamos y exponemos nuestros datos personales.

En Internet nuestra identidad está conformada por nuestra **huella digital**. La huella digital es el rastro que vamos dejando en nuestras interacciones con Internet:

1. **Cuando compartimos información personal** o intervenimos en Internet: al participar en las redes sociales, rellenar formularios, hacer compras, compartir nuestra ubicación, etc.
2. **Cuando otras personas comparten nuestra información:** al subir una foto o un vídeo en el que aparecemos, etiquetarnos en alguna publicación, escribir nuestro nombre, etc.
3. **Y, en general, cuando navegamos:** ya que los navegadores guardan nuestro identificador o nombre de usuario o usuaria y las preferencias de navegación a través de las denominadas *cookies*.

La huella digital siempre permanece, no se puede borrar.

Considerando la nueva realidad social que nos plantea Internet y el modelo de vida que nos atribuye, la identidad y la huella digitales representan buena parte de lo más valioso que a día de hoy poseemos. Son todos los datos que perfilan quiénes somos, tanto digital como personalmente, y aquellos que salvaguardan nuestra seguridad identitaria, económica e incluso física y anímica. Nuestros datos en Internet

³ Informe de la sociedad digital en España 2018, de Telefónica.

pueden incluir fotografías con las que cualquiera puede identificarnos, ubicaciones, direcciones, cuentas bancarias, hábitos, contactos, detalles íntimos, pretextos para la extorsión, etc.

En el caso de las personas adultas, hemos aprendido a ser parte de Internet habiendo socializado primero de forma analógica y presencial. Sin embargo, una parte significativa de los y las menores han crecido existiendo ya Internet y no establecen una diferencia conceptual tan significativa entre el mundo real y el virtual.

Es vital que aprendamos a **dar el valor que tienen nuestra intimidad y nuestros datos personales en Internet**. Y es fundamental que ahondemos en cómo transmitir este valor a las generaciones jóvenes para que puedan hacer un uso seguro de Internet y la tecnología digital.



➤ ALGUNOS DE LAS AMENAZAS MÁS COMUNES

En este capítulo vamos a repasar algunas de las amenazas más comunes entre los y las menores, y cómo proteger nuestros dispositivos mediante recursos y herramientas de ciberseguridad.

- a) **Extravío o robo de dispositivos:** al hacer mucho más uso de ellos y teniendo en cuenta su portabilidad, no es raro que perdamos o suframos el robo del *smartphone*, la tableta o incluso el ordenador portátil. Tengamos siempre en cuenta que esto puede ocurrir y que, más que la pérdida material, **lo que importan son los datos personales** que contienen algunos dispositivos.
- b) **Phishing:** se trata de una comunicación, a través de *e-mails*, mensajes SMS, MMS, mensajería instantánea o a través de una red social, incluso una llamada, fraudulenta en la que nos intentan **robar datos personales y/o bancarios**. Los ciberdelincuentes tratan de embaucarte bajo excusas como una oferta publicitaria, de amistad o trabajo, o se hacen pasar por una entidad conocida como una empresa de telefonía. Para evitar caer en este tipo de fraude, es importante analizar con calma y de manera rigurosa toda comunicación que provenga de una empresa o un particular a quien no conocemos. En ambos casos son comunes las erratas, la urgencia (una promoción que acaba pronto, un problema técnico que tiene que resolverse inmediatamente, etc.), los enlaces externos.
- En el caso de que sea una empresa la que se pone en contacto contigo pidiendo alguna acción sospechosa por tu parte, lo mejor es no interactuar. Si tenemos dudas, siempre es recomendable llamar o escribir al contacto oficial de la empresa para asegurarnos de que no es un fraude y contrastar la comunicación en Internet para ver si hay personas afectadas por un timo similar.
- c) **Ciberacoso, acoso virtual o cyberbullying:** tiene lugar cuando se produce un **acoso a través de las tecnologías de la información** (redes sociales, mensajería instantánea, *e-mail*, *blogs*, etc.). Suele involucrar la publicación de información falsa o confidencial, ataques y amenazas. Causa mucho sufrimiento y ansiedad y, en ningún caso, está justificado. De hecho, puede suponer un delito penal.
- d) **Sexting:** ocurre al **compartir o recibir fotografías o vídeos en actitud sensual, provocativa o explícitamente sexuales** de uno o una misma o de otra persona. Es una forma de exhibicionismo que fácilmente puede tener terribles consecuencias y complicarnos mucho la vida.

El *sexting* entre adolescentes es **una de las principales fuentes de la pornografía infantil**. Los y las menores con frecuencia creen que las fotos o vídeos enviados solo serán vistos por la persona a la que se lo envían, pero pueden acabar siendo vistos por miles de personas.

- e) **Grooming:** cuando hablamos de *grooming* hablamos del **acoso sexual por parte de una persona adulta a alguien menor de 18 años** a través de Internet. Los delincuentes suelen hacerse pasar por personas de su edad y estrechar lazos a través de las redes sociales, chats, foros, servicios de mensajería instantánea, etc. Preguntan sobre sus intereses, sus gustos y tratan de ganar su confianza para que les envíen fotos, activen la *webcam* o incluso para quedar. Con frecuencia una vez que, como víctimas, empiezan a sospechar o a ver que el acosador no es quien dice ser o se niegan a hacer lo que pide, **utilizan la información que ya tiene para extorsionarles**. Son frecuentes las amenazas del tipo de: “si no lo haces, le contaré a tus padres lo que has estado haciendo”.
- f) **Sextorsión:** tiene lugar cuando una persona sufre **extorsión o chantaje sexual a través de la amenaza de publicar contenidos íntimos o comprometidos suyos**. Esos contenidos pueden estar en poder de quien chantajea por un *hackeo*, su envío o por *sexting* o *grooming*. Normalmente el chantajista amenaza con difundir los contenidos si no recibe algo a cambio: dinero, más fotos, vídeos o encuentros sexuales.
- g) **Ciberviolencia de género:** Internet es únicamente un medio más en el que la cultura y las estructuras sociales se reproducen. Como tal, el machismo y la violencia contra las mujeres se perpetúan. Por ello, las **niñas, adolescentes y mujeres adultas sufren mayor grado de acoso, son más vulnerables y están más expuestas en Internet**.

➤ APRENDIENDO A PROTEGER LOS DISPOSITIVOS ELECTRÓNICOS PARA MI CIBERSEGURIDAD Y LA DE MIS MENORES A CARGO

- a) **Acceso a los dispositivos:** tenemos que **bloquear la entrada a nuestros dispositivos electrónicos**, sobre todo la de aquellos en los que guardemos información sensible como fotos, o conversaciones

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

privadas, y/o acceso a otros datos personales como los bancarios. Podemos hacerlo a través de una **contraseña, patrón, reconocimiento facial o dactilar**, etc. En el caso de los y las menores, es recomendable que hasta que no tengan la madurez y confianza suficientes, y no comprendan los riesgos que implica Internet, lo hagamos conjuntamente para que entiendan que no es un acceso privado suyo, sino compartido con sus mayores.

b) **Contraseñas, consejos:**

- Elige contraseñas de ocho caracteres o más (son más difíciles de rastrear).
- Es mejor utilizar palabras inventadas que solo tú conoces (puedes usar reglas nemotécnicas para recordarlas).
- Utiliza letras, números y símbolos entremezclados.
- Trata de cambiarlas, al menos, cada seis meses.
- Inventar una contraseña distinta para cada plataforma.
- Evita apodos, número de teléfono o direcciones.
- Guárdala para ti sin compartirla con nadie.
- Que sea única pero que la puedas recordar.
- Si se te da mal retenerlas, puedes utilizar un gestor de contraseñas o llavero.



- Evita que el dispositivo recuerde nuestras contraseñas si no es mediante una herramienta específica de seguridad y asegúrate de salir de la sesión si es un dispositivo extraño.
 - Ejemplo de contraseña poco segura: lnes2006.
 - Ejemplo de contraseña segura: 1cHama9%.
- c) **Verificación en dos pasos:** algunas plataformas ofrecen este sistema que proporciona una segunda capa de seguridad además de la contraseña. Normalmente funcionan a través del envío de un código mediante mensaje SMS. Son muy recomendables ya que disminuyen considerablemente las probabilidades de un ataque. Están disponibles sobre todo en el caso de los servicios de correo electrónico, de alojamiento de archivos, etc., que puedan contener gran cantidad de información personal.
- d) **Biometría y patrones:** en general la **biometría** (reconocimiento de la huella dactilar o facial) es un sistema muy recomendable para accesos a dispositivos como el teléfono o aplicaciones en las que se puede acceder a tus datos bancarios. Los **patrones** también son, en general, más difíciles de *hackear* digitalmente que las contraseñas, aunque hay que tener en cuenta que pueden ser observados mientras los introduces.
- e) **Antivirus:** instala siempre un **antivirus** que te avise cuando esté teniendo lugar un proceso sospechoso en el dispositivo que pueda indicar que tienes virus.
- f) **Antimalware:** es similar al antivirus pero más específico para **evitar** *malware*, es decir, programas o aplicaciones que sean perniciosos o estén haciendo procesos fraudulentos en el dispositivo.
- g) **Cortafuegos o firewall:** vigilan que nadie pueda acceder a tu dispositivo desde fuera sin tu permiso. Te permite **bloquear lo que entra y lo que sale** desde dispositivos como tu ordenador a la red. Instálalo en los dispositivos que lo permitan. La combinación del antivirus, el *anti-malware* y el cortafuegos es perfecta para proteger tus dispositivos.
- h) **Actualizaciones:** mantén la **actualización de los dispositivos al día**, de lo contrario nuestra exposición al robo de datos será mayor.
- i) **Copias de seguridad:** para evitar perder los contenidos del dispositivo es recomendable hacer copias de seguridad.

- j) **Herramientas de seguridad en caso de pérdida o extravío:** existen herramientas que te permiten **localizar y bloquear** el dispositivo e incluso borrar sus contenidos en caso de extravío o robo.
- k) **Conexión a Internet:** si nos conectamos a **redes wifi públicas**, es fundamental no enviar información privada o comprometida ni realizar compras o conectarnos a servicios que contengan nuestros datos bancarios.
- l) **Herramientas de control parental:** todos o casi todos los dispositivos electrónicos ofrecen **herramientas de seguridad, bienestar y control parental** y cada vez más frecuentemente lo hacen también las aplicaciones, juegos y plataformas dirigidas a menores. Resultan de mucha utilidad para evitar que los y las menores accedan a contenidos no recomendables para su edad, grado de madurez y comprensión del riesgo. Sin embargo, **no pueden en ningún caso sustituir el acompañamiento y la mediación parental** e incluso, si se utilizan mal, pueden suponer una pérdida de confianza por parte del menor que, como hemos ido viendo, es lo más importante a la hora de trabajar con ellos y ellas el uso seguro de Internet y la tecnología. Estas herramientas son útiles a la hora de limitar el acceso a ciertas plataformas o aplicaciones, pero una vez dentro no regulan los contenidos publicados por los y las usuarias. Para esto, existen opciones en las propias plataformas para establecer los ajustes de privacidad, comentarios ofensivos, tiempos de uso y seguridad. Como es lógico, debemos ser razonables con la aplicación de estas herramientas. Si nuestros hijos o hijas tienen un grado de madurez suficiente, no tiene sentido utilizar controles parentales. En general, para mayores de 14 años, es más recomendable orientar y hablar sobre qué tipo de contenidos reciben, comparten y consumen que establecer controles parentales muy estrictos.
- m) **Herramientas de monitorización online:** también existen herramientas para la vigilancia de lo que los y las menores hacen *online*. Si no existen razones de peso, no son recomendables. Resulta mucho más útil establecer un clima de confianza y tratar de que el acceso a Internet se haga desde zonas comunes y en presencia de personas adultas.

Cuestionario para la reflexión

PRÁCTICA PARA PADRES, MADRES Y TUTORES LEGALES

1. ¿Tienen los dispositivos a los que tienen acceso mis menores a cargo bloqueo de pantalla mediante contraseña, biometría o patrón?

☐ Sí ☐ No

2. ¿Conocemos el desbloqueo para acceder a ellos o es privado?

☐ Lo conocemos ☐ Es de su uso personal

3. ¿Utilizan contraseñas seguras para acceder a las plataformas y aplicaciones que contienen información y datos personales (fotografías, conversaciones, vídeos, datos bancarios, direcciones, ubicación, etc.)?

☐ Sí, la misma para todas ellas
☐ Sí, una para cada plataforma o aplicación
☐ No

4. ¿Renováis las contraseñas al menos cada 6 meses?

☐ Sí ☐ No

5. ¿Hay instalado un antivirus en todos los dispositivos a los que tienen acceso?

☐ Sí ☐ No

Cuaderno 2

USO SEGURO DE INTERNET Y LAS TIC

6. ¿Hay instalado un *antimalware* en todos los dispositivos a los que tienen acceso?

☐ Sí ☐ No

7. ¿Hay instalado un cortafuegos en todos los dispositivos a los que tienen acceso?

☐ Sí ☐ No

8. ¿Qué opinas sobre el uso de controles parentales y de herramientas de monitorización *online*? ¿Los utilizas?

DECÁLOGO PARA EDUCAR EN EL USO SEGURO DE INTERNET

Kit de herramientas

OBJETIVOS FORMATIVOS



Disponer de las pautas principales para educar en el uso seguro de Internet:

- I Asegurar su puesta en práctica.

CONTENIDOS FORMATIVOS



- I Relación de pautas para educar en el uso seguro de Internet.

APUNTES

1. **Genera diálogo y escucha:** como hemos ido viendo a lo largo de esta guía, lo más importante es crear un **clima de confianza** mutua en el que nuestro hijo, hija o alumnado pueda hablar de su vida en Internet y podamos preguntar sobre sus gustos y preferencias. Según nuestra personalidad, disposición y tiempo libre, nos será más o menos sencillo, pero por muy complicado que sea, si queremos educar en el uso positivo y seguro de Internet, tendremos que preguntar de vez en cuando, preocuparnos por saber, compartir y, sobre todo, escuchar.
2. **Enseña a valorar:**
 - a) El tiempo: estableciendo un **tiempo máximo** frente a las pantallas, promoviendo el equilibrio entre el mundo real y el digital, y evitando la navegación compulsiva.



b) El cuerpo: es importante seguir una serie de pautas para **evitar el malestar físico** derivado del uso de las pantallas:

- Mantener una distancia de al menos 70 cm de la pantalla del ordenador, 30-40 cm de la del móvil y la tableta.
- Acostumbrarse a descansar la mirada dirigiéndola a un punto lejano cada 20-30 minutos.
- Iluminar bien la zona, pero evitando reflejos en la pantalla.
- Mantener las pantallas limpias.
- Tener una buena graduación de gafas y lentes, si las necesitamos.
- Mantener una postura cómoda, prestando especial atención al cuello.
- Si se ha de pasar mucho tiempo delante de la pantalla (por trabajo o estudio), levantarse de 5 a 10 minutos cada hora.
- Parpadear para hidratar el ojo.

c) Las capacidades:

- La inteligencia: **si buscamos respuestas inmediatas en el buscador no utilizamos la cabeza**. Es importante no detener lo que se está haciendo para resolver una duda en Internet. O utilizamos nuestro cerebro o lo apuntamos para buscarlo después.
- El pensamiento crítico: aprender a discernir y **tener opinión propia** es lo que nos permite gestionar la información y que no nos engañen.
- La creatividad: hacer cosas sin la ayuda permanente de Internet **nos ayuda a sentirnos mejor** porque nos demostramos lo que somos capaces de lograr.
- El potencial: dedicar demasiadas horas a los contenidos digitales **impide que practiquemos otras muchas cosas**.

d) La autoestima: a la hora de utilizar la tecnología es fundamental que tengamos en cuenta nuestros objetivos vitales. De lo

contrario, en Internet es muy fácil dejarse llevar. **Preguntémos siempre por qué estamos haciendo lo que estamos haciendo, y si no hay respuesta, abandonémoslo.**

También lo es que busquemos refuerzo positivo real y duradero. Los “me gusta” y otros reconocimientos en Internet nos producen sensación de placer, pero no tienen mayor recorrido.

- e) La seguridad: **manteniendo siempre el control**, informándonos de las medidas de seguridad y respetando los derechos de los y las demás.
- f) La privacidad: **guardando la información que alguien desconocido no tiene por qué conocer**: nombre, apellidos, dirección, contraseñas, fotos, intereses, miedos, etc. Y en el caso de menores, la edad o año de nacimiento.

3. **Transmite la importancia de la huella digital**: ya hemos visto que toda acción que llevamos a cabo en Internet queda registrada, al igual que el uso que otras personas hagan de nuestros datos personales. Por eso es tan importante **enseñar a reflexionar antes de publicar** o llevar a cabo acciones en Internet de las que podamos arrepentirnos.

4. **Aprende a identificar y evitar los malos hábitos en Internet y los medios digitales⁴**:

- a) Navegación en bucle: cuando pasamos de un contenido a otro sin objetivo concreto: vídeos, demasiados capítulos de una serie o *scroll* interminable en alguna red social. Tras ello nos sentimos como anestesiados y anestesiadas. Son formatos con mucha carga dopaminérgica, **que nos hacen malgastar gran cantidad de tiempo** y, a menudo, **sentirnos culpables**.
- b) Evasión: sea porque estamos tristes, sentimos soledad, estrés, es muy común recurrir a Internet, a las redes sociales,

⁴ Información basada en el manifiesto y las reflexiones de Nosurf.

a las series, a los juegos, para no pensar en la razón de nuestro sufrimiento. El problema es que esto no solo **no nos ayuda a reflexionar y remendar nuestros problemas**, sino que nos hace sentir cada vez más soledad, tristeza, etc.

- c) Aplazamiento: cuanto más tarea tenemos pendiente, más nos metemos en Internet sin ton ni son para retrasar el momento de ponernos a trabajar. Al igual que con la navegación en bucle, nos decimos “cinco minutos más”, como si nos costase separarnos del móvil o el ordenador. Al igual que el resto de hábitos negativos que podemos tener en Internet, **el aplazamiento solo nos perjudica**, no nos aporta nada.
- d) Búsquedas a discreción: da igual que estemos en un momento de plena concentración e inspiración a punto de resolver un enigma nunca antes resuelto, de pronto nos surge una duda y la tenemos que buscar en Internet inmediatamente. Normalmente son dudas irrelevantes o cuestiones que recordaríamos si pensásemos treinta segundos —¿cómo se llamaba la actriz de la serie esta?— pero, cada vez con más frecuencia, sacamos el móvil y lo miramos ávidamente. Aunque nos parezca un hábito inofensivo, **nos hace perder la concentración y acostumbra a romper continuamente nuestro flujo de pensamiento**.

Si estamos haciendo tareas complejas como estudiar o escribir una canción, nos las hace más difíciles y nos impide aprovechar todo nuestro potencial.

- e) Indagación interminable: a veces dedicamos más tiempo a recabar información para hacer algo que a practicar eso que queremos hacer. Nos ocurre, por ejemplo, cuando nos ponemos un objetivo tipo: “quiero aprender francés” y dedicamos mucho tiempo a buscar las mejores academias, los pros y los contras de hacerlo *online*, las herramientas más eficaces. Muchas veces incluso **abandonamos el objetivo porque perdemos el interés** antes de llevarlo a cabo.
- f) Otros: también podemos identificar otros como la irritabilidad, la falta de sueño, los cambios de humor, pero solo

podremos vincularlos a las conductas en Internet si hemos trabajado ese espacio de diálogo para hablar y discutir lo que hacemos en la red.

5. Concreta y negocia límites:

a) Lugares de uso: **negociad en qué sitios están permitidas las pantallas.** Tal como hemos ido viendo, la mayoría de especialistas recomiendan, sobre todo hasta los 14-15 años, que los dispositivos se utilicen en **zonas comunes** mientras sus mayores estén en casa. De este modo, vamos trabajando la responsabilidad propia, pero estando cerca y, de vez en cuando, vigilantes.

b) Tiempo de uso: ya sabemos que depende de la madurez de cada menor. Negociemos conjuntamente qué nos parece apropiado, aunque **no debería sobrepasar la 1 o 2 horas como mucho de ocio digital** (mayores de 12 años).

Si el grado de madurez lo permite, lo más recomendable es que una vez se ha negociado el tiempo máximo diario, dejemos que los y las menores sean **responsables de cumplirlo** con nuestra supervisión. Sin embargo, existen funciones para limitar el tiempo de uso que podemos valorar utilizar conjuntamente. Las encontramos en las opciones de configuración de casi todos los dispositivos y aplicaciones.

c) Controles parentales: es recomendable crear perfiles de usuario y usuaria limitados de acuerdo con la edad. Gracias a ellos podremos restringir el acceso a ciertas aplicaciones, aplicar controles parentales y valorar usar las alertas sobre un uso indebido. Es muy sencillo configurarlos, pero **lo razonable es hacerlo de manera informada y conjunta.** Solo hay que acceder a los ajustes del dispositivo y dirigirse al apartado de usuarios o cuentas. Ahí podremos seguir los pasos fácilmente.

d) No olvidar: las consolas y televisiones inteligentes también pueden configurarse de acuerdo con su edad y necesidades.

- e) No sobredimensionar: es mejor **no premiar ni castigar** con el uso de la tecnología.
- f) Edad: como hemos visto en capítulos anteriores, las edades adecuadas para utilizar cada aplicación están tipificadas en la mayoría de aplicaciones, juegos, redes sociales, etc.

6. Sé coherente:

- a) Respetando los límites que habéis marcado.
- b) Trabajando los buenos hábitos.
- c) No enviando *fake news*, bulos o información poco contrastada: en la actualidad esto supone contribuir a la desinformación y genera un clima preocupante.
- d) Evitando las páginas web cuyo compromiso con la legalidad y la ética sean cuestionables: piensa que todos y todas conformamos Internet y que, al interactuar y consumir contenidos sórdidos o ilegales, estamos impulsando el que Internet se inunde de ellos y potenciando su creación.
- e) No publicando nunca tus datos personales (contraseñas, ubicación, edad, año de nacimiento, direcciones, información bancaria, etc.).
- f) No respondiendo a personas desconocidas.
- g) No interactuando con *banners* ni mensajes sospechosos.

7. Mantente al día:

- a) Conoce las tendencias de Internet, aplicaciones, juegos, redes sociales y la evolución tecnológica.
- b) Conoce los **riesgos y cómo actuar en cada caso:**

■ ¿Qué hacer si mi hijo, hija o alguien de mi alumnado responde a patrones de adicción a la tecnología? Habla con él o ella y, si eres docente, con la familia. En este caso, conviene que la familia contacte con un perfil profesional que pueda ayudar a entender y trabajar las causas.

- ¿Qué hacer si mi hijo, hija o alguien de mi alumnado es víctima de acoso en Internet? Habla con él o ella y, si eres docente, con la familia. Ofrece tu apoyo sin juzgar, recaba pruebas (por eso es importante no borrar nada), y denuncia gratuitamente en el teléfono 900 116 117 (de 9:00 a 21:00 horas todos los días del año) o, si lo prefieres, rellena el formulario *online*: <https://www.is4k.es/ayuda>
 - ¿Qué hago si mi hijo, hija o alguien de mi alumnado es testigo de acoso en Internet? Hablar con él o ella y ofreced vuestro apoyo, si es necesario. Valorad conjuntamente si es mejor denunciar.
 - ¿Qué hacer si mi hijo, hija o alguien de mi alumnado está acosando a alguien en Internet? Habla con él o ella y, si eres docente, con la familia; y en función de la magnitud del acoso y el conflicto, se habrá de valorar contactar con especialistas de la psicología o, si fuera necesario, la policía.
- c) Conoce vuestros derechos en Internet.
- d) Incorpora herramientas y usos tecnológicos en el resto de la educación de los y las menores.

8. Conviértete en gurú de la ciberseguridad:

- a) Cambia contraseñas de manera periódica.
- b) Contrasta y elige un navegador que respete tu privacidad.
- c) Acostúmbrate a borrar las *cookies*.
- d) Sospecha de cualquier comunicación que pida tu acción inmediata o alguna acción de pago.
- e) Mantén los dispositivos actualizados.
- f) Instala un buen antivirus, *antimalware* o un cortafuegos (con VPN).
- g) Descarga aplicaciones solo de plataformas oficiales.
- h) Asegúrate de que las aplicaciones que descargas no activan permisos como la ubicación o la cámara sin que seas consciente.



- i) Evitando acceder a información sensible desde redes wifi públicas y protegiendo las redes de casa.
- j) Comprueba con cuidado y precaución que la pasarela de pago es fiable antes de realizar ninguna compra.

9. **Transmite los valores para socializar en redes sociales:**

- a) **Enseñando a no depender de la tecnología:** valorando la desconexión, acabando con las notificaciones de las aplicaciones de mensajería y redes sociales, desactivando avisos de lectura de mensajes de los servicios de mensajería: como el “leído” y respetando el tiempo máximo de las pantallas.

b) Enseñando a diferenciar entre contacto virtual y amistad:

- I Transmitiendo que no podemos saber con seguridad si al otro lado de la pantalla la otra persona es quien dice ser.
- I Haciendo contactos digitales con inteligencia y precaución.
- I Conservando siempre el control y no cediendo nunca al chantaje.
- I No pidiendo amistad en las redes a personas que no conozco.
- I Solo participando en eventos en los que conozco al menos a la mayoría de participantes.

c) Enseñando a no compartir ni publicar nada de lo que nos podamos arrepentir:

- I Restringiendo el acceso a los perfiles: los perfiles en las redes sociales pueden ser privados o públicos.
- I No enviando nunca fotos ni vídeos de los que nos podamos arrepentir: valorando si merece la pena correr el riesgo que supondría el peor de los escenarios.
- I Cuidando los datos personales: sin publicar nunca información como el nombre y apellidos, dirección, fecha, año de nacimiento o edad, número de teléfono y planes.

d) Enseñando a ponerse en el lugar de los demás:

- I No acosando ni maltratando a nadie en Internet: si se plantea hacerlo, recordémosle que se plantee por qué. Si su grupo de amigos o amigas presiona para hacerlo, que se pregunte por qué. El ciberacoso es ciberacoso aunque empiece por lo que pensábamos que era una broma.
- I No reenviando nunca fotos, vídeos, textos, mensajes comprometidos que puedan hacer daño o ridiculizar a otras personas: da igual que no conozca personalmente a la persona, que sea famosa, que le haya hecho daño, que sea

cómico. Nunca está justificado. Recuérdale que también es vuestra responsabilidad construir un Internet del que todos y todas podamos disfrutar y sentirnos a salvo.

- No etiquetando ni vinculando a alguien sin su permiso en materiales que puedan comprometer, ridiculizar o vejar.
- No consumiendo (viendo, puntuando, clicando, compartiendo, etc.) contenidos que vayan en contra de sus principios o la vida, los derechos, la dignidad, la intimidad o la seguridad de otras personas: cada uno y cada una somos responsables de nuestras acciones y tenemos que evitar que estas contribuyan a dar impulso a plataformas y mensajes que vayan en contra de nuestros principios.
- Cuidando los datos personales de otras personas: si nos han llegado, no los difundimos. De igual modo que tus datos personales son información valiosa para ti, también lo son los suyos para el resto.
- No haciéndonos nunca pasar por alguien existente para tratar de engañar o fastidiar a otras personas, ni para hacer la broma. La suplantación de identidad es ilegal y puede meternos en problemas legales. Como ya hemos dicho, el anonimato en Internet es una ilusión. Nuestros movimientos y acciones quedan registrados y son pruebas que se pueden usar en nuestra contra.

e) Enseñando a buscar ayuda:

- Hablando: explicando que si se encuentra en una situación difícil es mejor hablar con su familia, amigos, amigas o personal del colegio o instituto cuanto antes: a veces tenemos la sensación de que si la gente de nuestro entorno se entera de que nos hemos metido en un lío, todo se volverá mucho peor y se nos juzgará injustamente. No es cierto. A las personas que se preocupan por ti lo que más les importa es que estés a salvo. En Internet nos podemos meter en problemas graves. Mejor explicar cuanto antes

que tenemos una dificultad para evitar que se vuelva más grande.

- Dando apoyo: si conozco a alguien que está sufriendo o está ejerciendo acoso en Internet es mi obligación hablarlo con una persona adulta que pueda denunciarlo y hablar con la víctima.
- Recabando pruebas: si estás sufriendo acoso del tipo que sea, es mejor que no borres ningún dato o comunicaciones para poder utilizarlos como prueba. Sí debes, por si acaso:
1. Retirar la información o material audiovisual que consideres sensible. 2. Limpiar el dispositivo con un antivirus. 3. Cambiar tus claves personales.
- Denunciando: llama de forma gratuita a 900 116 117 (de 9:00 a 21:00 horas todos los días del año) o, si lo prefieres, rellena el formulario *online*: <https://www.is4k.es/ayuda>

10. **Educa en la importancia de la ciudadanía digital:** la ciudadanía digital comprende la noción de nosotros y nosotras mismas como agentes sociales imprescindibles para entender, construir y participar en Internet desde el respeto, la seguridad, la empatía y el empoderamiento. Es fundamental que las generaciones jóvenes que han crecido con y en Internet lideren el desarrollo de la ciudadanía digital para hacer de Internet un universo positivo que trascienda en un mundo más justo; uno que respete y valore los derechos humanos, que luche contra el odio y la discriminación y que aproveche la tecnología para mejorar las cosas, no para empeorarlas, no para adormecerlos.

Cuestionario para la reflexión

PRÁCTICA PARA PADRES, MADRES Y TUTORES LEGALES

1. ¿Qué es lo más importante en la mediación de padres, madres y tutores legales por el uso seguro de Internet con adolescentes?

- ☐ Evitar que utilicen Internet y la tecnología a toda costa
- ☐ Demostrar que yo sé mucho de tecnología y vida digital
- ☐ Establecer un diálogo de confianza donde puedan expresarse sobre sus experiencias y dudas en Internet

2. ¿Qué debo compartir por mensajería instantánea sin dudarlo?

- ☐ Noticias que no puedo saber con seguridad si son verdaderas
- ☐ Fotografías comprometidas de personas que no conozco
- ☐ Reportajes de los que desconozco su origen
- ☐ Vídeos con violencia explícita
- ☐ Nada de lo anterior

3. ¿Qué es más importante?

- ☐ Ser coherente
- ☐ Jugar a videojuegos con mi hijo o hija
- ☐ Conocer a sus contactos en redes sociales

DECÁLOGO PARA CHICAS Y CHICOS DE 12 A 18 AÑOS SOBRE EL **USO SEGURO** DE **INTERNET**

OBJETIVOS FORMATIVOS



Disponer de pautas clave en el uso seguro de Internet desde la perspectiva adolescente:

- I Hacer uso de estos principios básicos como guía para el avance de los y las menores.

CONTENIDOS FORMATIVOS



- I Decálogo de uso seguro en Internet.

APUNTES

1. **VALORO mi tiempo:** no lo dedico todo a Internet. Disfruto del aire libre, de las conversaciones cara a cara, de pasarlo bien sin estar pendiente del móvil o de lo que otras personas piensen de mí en las redes sociales.
Valoro también mi cuerpo y no me dejo los ojos en una pantalla.
2. **REFLEXIONO antes de publicar o enviar nada:** me aseguro de que no hay ninguna posibilidad de que pueda arrepentirme. Imagino el peor de los escenarios, ¿merece la pena?
3. **PROTEJO mis datos personales:** no publico ni comparto con desconocidos, aunque hayamos hablado *online* con anterioridad, información personal como mi edad, contraseñas, dirección, año de nacimiento, fotografías, miedos, dudas, etc. Si alguien me pide este tipo de información, voy a hablar directamente con alguien mayor que pueda aconsejarme.
También aviso a mis amigos y amigas de cómo quiero que traten mi información personal como fotos y vídeos en los que aparezco, configuro la privacidad de mis perfiles en redes sociales de manera inteligente y no descargo ni compro nada sin permiso.
4. **OFREZCO mi mejor versión en Internet:** utilizo Internet y la tecnología en general para cosas productivas para mí o aquello en lo que creo. Me planteo siempre cuál es el objetivo de lo que estoy



haciendo y, si no tengo ninguno, paro y dedico mi tiempo a algo que me haga sentirme mejor a largo plazo.

5. **TRATO a los y las demás con respeto:** no pago mis frustraciones *online* con personas desconocidas o vulnerables. Recuerdo que el anonimato no existe en Internet ni la idea de que no dejo rastro. Todo lo que hago en Internet deja huella: tanto a nivel de rastro, como emocionalmente.

6. **NO ALIMENTO al troll:** cuando me encuentre con personas que insultan, acosan o repiten la misma cosa una y otra vez, no me dejaré llevar por su provocación. No siempre tengo que contestar en Internet y pasar de personas que se comportan de esta manera es demostrar que no nos afectan sus provocaciones. VALORARÉ utilizar las herramientas de bloqueo o denuncia de las redes sociales o los foros, pero siempre asegurándome de que estoy haciendo un buen uso de ellas.

7. **CONFÍO en mi padre, madre y profesorado:** compartiendo las cosas que me preocupan o me hacen sentir mal en Internet; también las cosas buenas.

8. **GUARDO la calma si me meto en un lío:** no me dejaré convencer por nadie que no conozco y seguiré mi instinto: si me están haciendo sentir mal, no borraré ninguna conversación, las guardaré como prueba, hablaré con mis padres o tutores y valoraremos qué hacer a continuación.

A la gente que me quiere lo que más le importa es mi seguridad. Utilizaré la inteligencia para no empeorar las cosas.

9. **RESPETO los límites de edad** y si veo algo muy impactante como un vídeo muy violento o sexualmente explícito, lo hablaré con mis padres o tutores.

Aunque piense que no, hay cosas que pueden herir mi sensibilidad y afectarme más de lo que imagino.

10. **NO COMPARTIRÉ NI CONSUMIRÉ** (haciendo *click*, dando a “me gusta”, visitando una página, etc.) contenido que vaya en contra de mis principios, ni noticias falsas o poco contrastadas. Sé muy bien lo que está bien y lo que está mal, y quiero ser parte de un Internet en el que todo el mundo se sienta bien y a salvo.

PRÁCTICA PARA PADRES, MADRES Y TUTORES LEGALES

- [illegible]

BIBLIOGRAFÍA

- » *Descubriendo los eSports en España, 2019*, de Wink TTD.
Garrido-Lora, M.; Busquet Durán, J.; Munté-Ramos, R. A. (2016).
«De las TIC a las TRIC. Estudio sobre el uso de las TIC y la brecha digital entre adultos y adolescentes en España». *Análisis. Quaderns de Comunicació i Cultura*, 54, pp. 44-57. DOI: <http://dx.doi.org/10.7238/a.v0i54.2953>
Guía de privacidad y seguridad en Internet, AEPG, www.aepd.es, INCIBE, www.incibe.es
Informe sociedad digital en España 2018, de Fundación Telefónica.
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. <https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf>

***Somos más contra el odio y el
radicalismo*** es un proyecto de formación
y sensibilización para adolescentes de
14 a 18 años, en prevención del radicalismo
violento y para combatir los mensajes
de odio en Internet, promoviendo los
derechos humanos y el respeto
a la diversidad.

#Somos más

