REDES SOCIALES VY MENORES

GUÍA PRÁCTICA







3

DE LA A LA Z PARA UNA ALFABETIZACIÓN DIGITAL

EDUCACIÓN DIGITAL: ¿LA ASIGNATURA PENDIENTE?

«Las tecnologías digitales están cambiando a un ritmo creciente el modo en que las personas viven, trabajan, se instruyen y sociabilizan en todas las partes del mundo. Estas tecnologías ofrecen nuevas posibilidades para que las personas mejoren en todos los aspectos de su vida, incluido en el acceso a la información, la gestión de los conocimientos, las redes, los servicios sociales, la producción industrial y las diversas modalidades de trabajo. De la misma manera que el conocimiento, las capacidades y las competencias evolucionan en el contexto de la era digital, también evoluciona el significado de ser alfabetizado». Así de contundente se expresaba la Unesco cuando en 2017 sumó a la tradicional celebración del 8 de septiembre como Día Internacional de la Alfabetización¹ un concepto adicional: la alfabetización digital. Ponía así el foco en la necesidad de aprender a entender y utilizar de forma provechosa la tecnología.

La alfabetización digital incluye no solo «la habilidad para localizar, analizar, organizar, entender y evaluar información utilizando la tecnología» (como la define Wikipedia), sino también el desarrollo de competencias digitales que permitan su uso creativo, crítico y seguro. No es una mera declaración de intenciones: la «competencia digital» está clasificada como una de las ocho competencias clave en el sistema educativo español, marcada como objetivo en educación Primaria, ESO y Bachillerato y elevada a rango de «Orden» por

¹ es.unesco.org/themes/alfabetización-todos/dia-alfabetización.

el Boletín Oficial de Estado² (BOE). «Se trata de desarrollar una actitud activa, crítica y realista hacia las tecnologías y los medios tecnológicos, valorando sus fortalezas y debilidades y respetando principios éticos en su uso, e implica la motivación y la curiosidad por el aprendizaje», dice el BOE. Ahí es nada.

«La alfabetización digital y la adquisición de competencias digitales es un proceso permanente, no es una asignatura que lleve a un aprobado y no se logra en un curso académico», advierte María Zavala, miembro de The Digital Citizenship Institute y autora del blog iWomanish.com. «Implica saber utilizar las máquinas y las herramientas tecnológicas, interpretar lo que se está haciendo con la tecnología y pensar para qué se está usando. Y si no conseguimos incorporar esa capacidad para pensar, seremos usuarios de tecnología, pero no ciudadanos digitales. En este proceso hay que ir ayudando poco a poco a que el niño entienda lo que está haciendo desde el primer momento en que empieza a relacionarse con pantallas, de forma que cuando llegue a la adolescencia tenga ya plena consciencia, sea capaz de tomar decisiones y no se generen situaciones ni de pánico, ni de ingenuidad».

La familia, y no solo la escuela, desempeña en esta labor un papel esencial que, sin embargo, no siempre se cumple. Según el estudio «Actividades, mediación, oportunidades y riesgos online de los menores en la era de la convergencia mediática», de EU Kids Online, tan solo un 18 % de los niños y niñas españoles de nueve a 17 años asegura que sus padres y madres los animan a descubrir y aprender cosas en Internet. No solo eso, tampoco los acompañan: apenas un 23 % de los menores dice que sus progenitores hablan con ellos de lo que hacen en la Red, ni siquiera con los más pequeños, de nueve a 12 años. Y eso, que, como vimos en el capítulo 1, pasan una media de algo más de tres horas al día en este entorno. Cuando se entra a analizar en función del sexo del vástago, además, se comprueba que los padres y madres animan más a los chicos que a las chicas en el proceso de aprendizaje y descubrimiento, lo cual de forma involuntaria empieza a configurar, desde muy temprana edad, un sesgo de género ante el uso y comprensión de la tecnología entre niños y niñas.

¿Cuándo fue la última vez que te sentaste con tu hijo o tu hija a investigar sobre un tema en Internet? Si ya es adolescente, ¿lo hiciste cuando era más pequeño? ¿Cómo es posible que los menores pasen tanto tiempo conectados, sin que nadie les pregunte por qué y para qué?

No se trata solo de aprovechar ese tiempo de conexión para incentivar el aprendizaje, sino de algo tan básico como enseñarles a buscar en la Red, filtrar la información y contrastar las fuentes: en definitiva, explicarles pautas para que sepan cómo desenvolverse en Internet y redes sociales. Parece sencillo, ¿verdad? Sin embargo, el estudio de EU Kids Online revela que a más de la mitad de los chavales, el 57 %, no le resulta fácil elegir la palabra clave

² www.boe.es/diario boe/txt.php?id=BOE-A-2015-738.

para las búsquedas online (no hablemos ya de cómo formular una búsqueda avanzada) y que el 71 % no sabe comprobar si la información que encuentra online es cierta.

Así, ¿cómo pretendemos que interioricen la necesidad de verificar contenidos, contrastar noticias y no dejarse embaucar por falsedades? ¿Cómo se enfrentarán de adultos a la creciente desinformación que impregna la sociedad? De hecho, vista la velocidad a la que se propagan hoy las noticias falsas, habría que preguntar también a los adultos si ellos son capaces de distinguirlas.

A pesar de estas dificultades, solo el 17 % de los menores pide ayuda a su padre o a su madre cuando se encuentra con una situación en Internet que no sabe manejar, y apenas un 14 % habla con ellos sobre cosas que les han molestado en la Red. Este porcentaje se reduce incluso más, como cabe esperar, a medida que avanzan en edad, y se ve acentuado en ocasiones por la actitud de los padres, cuando en lugar de ayudarles, les recriminan por el uso de la tecnología, ya sea porque están convencidos de sus efectos nocivos, ya sea por propio desconocimiento.

Si la primera vez que tu hijo o hija recurre a ti porque le insultan en Instagram, le ordenas que cierre la aplicación, ¿qué piensas que hará a partir de entonces? Si cuando te cuenta que le han dejado un comentario desagradable en TikTok, le contestas que eso le pasa por estar ahí perdiendo el tiempo, ¿crees que volverá a pedirte ayuda? Si le regañas porque al buscar online, le ha saltado un anuncio de citas en la pantalla, ¿qué supones que te dirá cuando le surja un problema realmente grave?

Una posible respuesta es simplemente enseñarle a bloquear a otro usuario en Instagram, eliminar y restringir comentarios en TikTok y cerrar ventanas emergentes. Pero incluso si se trata de una plataforma de la que nunca has oído hablar, recuerda que más allá de aplicaciones y herramientas, hay una cuestión esencial: educarle para que aprenda a gestionar y afrontar una situación conflictiva, sea cual sea el entorno en el que se genere. El digital, al fin y al cabo, solo es uno más.

MANUAL DE COMPETENCIAS DIGITALES PARA LA CIUDADANIA

Pero, ¿qué significa ser competente digital? ¿Qué habilidades hay que adquirir y qué implica? Si tan importantes son, ¿qué criterios se aplican? Si los menores son proclives a trastear a una edad cada vez más temprana con Internet y redes sociales, ¿cómo canalizar ese interés para evitar que se conviertan en analfabetos con móvil?

Para intentar clarificar la cuestión, en 2013 la Comisión Europea desarrolló, en colaboración con el Joint Research Center, el «Marco Europeo de Competencias Digitales para la Ciudadanía»³, que en 2016 se actualizó con nueva terminología... lo cual demuestra lo rápido que evoluciona todo. El documento desglosa 21 competencias clave, agrupadas en cinco áreas: «Información y alfabetización digital», «Comunicación y colaboración online», «Creación de contenidos digitales», «Seguridad» y «Resolución de problemas».

Desde su publicación, este modelo se ha convertido en una referencia para potenciar y evaluar los conocimientos y aptitudes digitales, en los que propone diferentes niveles de complejidad. Entre los ámbitos que contempla, incluye el de las redes sociales, síntoma de que estas plataformas sirven también de campo de experimentación y aprendizaje online.

Siguiendo el modelo y las 21 competencias que describe, te propongo a continuación cómo aplicarlo para educar a nuestros hijos e hijas a desenvolverse en Internet y redes sociales y enseñarles a sacar el mejor partido al entorno digital.

ÁREA «INFORMACIÓN Y ALFABETIZACIÓN DIGITAL»

Competencia 1.

Navegar, buscar y filtrar datos, información y contenidos digitales

Realizar búsquedas online con precisión en diferentes dispositivos, webs v aplicaciones, con las palabras clave, las etiquetas y los comandos adecuados, entendiendo cómo clasifican la información los motores de búsqueda.

Hablar de cómo clasifican la información los motores de búsqueda implica referirse a los algoritmos y su poder para ordenar, priorizar, ocultar o destacar los resultados y, por tanto, los contenidos que consumimos. Algoritmos que programan las compañías tecnológicas en cuyas plataformas realizamos las búsquedas y cuyo criterio no es, por tanto, casual, sino un compendio de la serie de variables con las que inicialmente se han configurado. Algoritmos que aplican inteligencia artificial para interpretar y aprender qué es lo que buscamos habitualmente, en qué contenidos solemos hacer clic, cuáles nos gustan más, qué compartimos con nuestros amigos, en cuáles dejamos comentarios. Algoritmos que determinan lo que consideran más relevante para cada uno de nosotros y en función de eso nos muestran unos resultados u otros, que criban nuestros intereses y a la vez los moldean, porque seleccionan qué debemos encontrar. Y cuyo criterio para ordenar la información no reside en

ec.europa.eu/irc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digitalcompetence-framework-citizens-update-phase-1-conceptual-reference-model.

la calidad o veracidad del contenido, ni tampoco en su importancia, sino en las palabras y comandos que hemos introducido en la búsqueda y en nuestra reacción a lo que otras veces nos han mostrado.

La forma en la que los buscadores de Internet clasifican la información varía de uno a otro (Google no es el único que existe, aunque sea el más utilizado) y los gestores de webs se afanan en comprender y aplicar sus pautas para lograr que sus respectivas páginas ganen relevancia y avancen posiciones en los resultados: es la labor que realizan los especialistas en search engine optimization (SEO), que ha dado lugar a toda una profesión.

Las redes sociales introducen sus propios criterios para decidir qué y cómo sirven lo que buscamos, con el fin último de que pasemos el mayor tiempo posible dentro de la propia red, consumiendo contenidos que nos gustan (priorizan los que obtienen más likes, más respuestas o comentarios, y los que se comparten más) y sin visitar otras webs (cobran preeminencia los vídeos y fotos por encima de los posts de enlaces de texto). Y al mismo tiempo, aprenden qué nos interesa, qué nos atrae, con qué nos identificamos y qué pensamos, para sin nosotros ser conscientes, clasificarnos y elaborar perfiles de cada uno de nosotros. Perfiles que empresas, marcas y partidos políticos emplean en las campañas publicitarias que contratan en cada red social.

Llegados a este punto, ¿cómo mejorar las búsquedas online?

Aunque Google sea el principal buscador en Internet, no está de más conocer que existen también otros como Bing (desarrollado por Microsoft), Yahoo y DuckDuckGo (este último, minoritario, asegura que no guarda el historial de navegación de sus usuarios). Conviene explicar también a los menores que los resultados de búsqueda pueden variar si se realizan desde dispositivo móvil u ordenador y que, puesto que el orden en que se muestran no tienen por qué obedecer a la calidad ni a su importancia, sino al criterio del algoritmo, es recomendable no quedarse con lo primero que encuentran y rastrear con atención. Es más: por lo general, los primeros hallazgos que muestra Google suelen ser publicidad, debidamente identificados con la palabra «Anuncio»... pero en chiquitito: la mayoría de los niños (y muchos adolescentes) no advierten la diferencia y hacen clic sin pensarlo. Por cierto, la Wikipedia no es infalible, aunque suela encabezar los resultados y sea uno de los recursos más habituales entre los chavales para el «copia-pega» en los trabajos de clase.

En Google, lo habitual es introducir directamente el término o la frase en el cajetín del navegador... y empezar a descartar. Pero para acotar y refinar la búsqueda, algunas opciones son:

Para que nos muestre solo las páginas web que contienen la expresión exacta: escribir la frase entre comillas. Por ejemplo: «videojuegos para menores».

- Para encontrar páginas que contengan dos términos de búsqueda: añadir el símbolo + entre las palabras. Por ejemplo: videojuegos + menores.
- Para hallar qué ha publicado una web determinada sobre el tema que nos interesa: utilizar el comando site: seguido del dominio y el término de búsqueda. Por ejemplo: site:guiainfantil.com videojuegos.
- ▶ Para encontrar documentos en un formato concreto, como pdf, power point, etcétera: utilizar el comando filetype:. Por ejemplo: filetype:pdf videojuegos.
- ▶ Para excluir términos de búsqueda: usar el símbolo -. Por ejemplo: videojuegos -adultos.
- ▶ Para combinar búsquedas por idioma, fecha y otros criterios: recurrir a la página de búsquedas avanzadas de Google en: www.google.es/advanced_search.

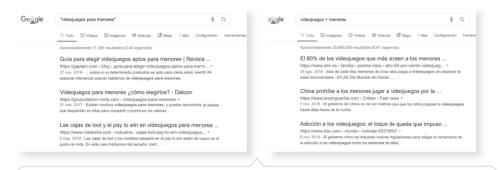


Figura 3.1. Los resultados que muestra Google al realizar una búsqueda dependen de múltiples factores que el algoritmo aplica al ordenador y varían en función de los comandos que se empleen al buscar. Teclear videojuegos para menores arrojará opciones diferentes a videojuegos + menores.

YouTube tiene el segundo buscador más usado del planeta. Aquí, la herramienta de búsqueda filtra los resultados por fecha de subida del vídeo, duración, tipo (canal, vídeo, lista de reproducción), características y relevancia. Otra alternativa es:

- Para buscar vídeos en directo sobre un tema: añadir después del término de búsqueda una coma y la palabra live. Por ejemplo: fortnite, live.
- ▶ Para buscar el canal: escribir channel después de la coma. Por ejemplo: fortnite, channel
- ▶ Para buscar en canales oficiales: teclear partner después de la coma. Por ejemplo: fortnite, partner.

En Instagram, al introducir el término de búsqueda en la aplicación es posible seleccionar por cuentas (las que tienen esa palabra en su nombre de usuario), hashtag (muestra vídeos y fotos que se han etiquetado así en la descripción) y lugares (con los resultados de contenidos cuya geolocalización contiene la palabra clave).

En TikTok el proceso de búsqueda es similar a Instagram, pero el filtrado se realiza por usuarios (con la palabra clave en el nombre), vídeos (etiquetados con esa palabra como hashtag), sonidos (con los audios que incluyen la palabra clave) y hashtag (muestra una relación de hashtags relacionados que contienen el término de búsqueda y el número de veces que se ha visualizado cada hashtag).

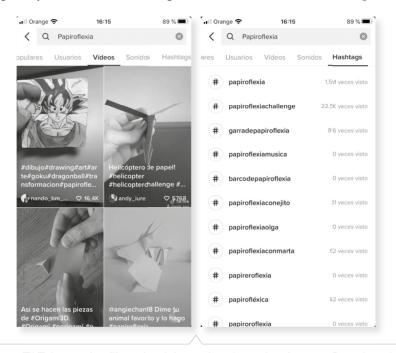


Figura 3.2. TikTok permite filtrar las búsquedas de varias formas. Por ejemplo, para encontrar contenidos sobre papiroflexia que inspiren manualidades, se puede buscar vídeos que contengan esa palabra como hashtag o hashtags relacionados con esa palabra. Descubrimos así que en TikTok hay hasta retos relacionados con papiroflexia: el «papiroflexiachallenge».

En Twitter, en la versión web, con la herramienta de búsqueda avanzada: twitter.com/search-advanced filtras por cuentas, fechas, hashtags, idiomas y mucho más. No está disponible en la aplicación móvil.

Competencia 2. Evaluar datos, información y contenidos digitales

Analizar, evaluar y comparar de forma crítica la fiabilidad y seriedad de datos, informaciones y contenidos online.

Bulos, noticias falsas, informaciones tergiversadas, imágenes trucadas, mensajes que prometen premios o amenazan con catástrofes, vídeos manipulados, memes... circulan impunemente por Internet y redes sociales y han demostrado una alta capacidad para viralizarse y saltar del grupo de WhatsApp a las historias de Instagram, de Twitter a Snapchat, del correo electrónico al WhatsApp y vuelta a empezar.

El tipo de contenidos a los que un menor accede y comparte varía muchísimo, incluso según la edad. En las edades más tempranas, prolifera la circulación de mensajes (falsos) con ofertas y descuentos increíbles que se consiguen con un solo clic, sobre animales en peligro a los que salvar llamando a un número de teléfono o trucos infalibles relacionados con la salud, la medicina o la nutrición (cuyas consecuencias pueden ser nefastas). En la adolescencia, las redes sociales se convierten en su principal fuente de información: los mensajes virales que les envían sus contactos y las cuentas y perfiles a los que siguen representan su canal primario para estar al día de lo que sucede y son más relevantes que los medios de comunicación tradicionales (incluso en sus versiones online).



Figura 3.3. Entre los niños abunda la difusión de mensajes falsos sobre animales en peligro o cuestiones de salud, como estos identificados por Stop Bulos. Cuanto antes aprendan a identificar los mensajes falsos, mejor.

Cuanto antes tenga claro tu hijo o hija que no todo lo que recibe y lee es cierto, mejor. Incúlcale que verosimilitud no es sinónimo de veracidad, que conviene comprobar y contrastar fuentes de información, que las fotos y vídeos se alteran con extrema facilidad, que los pantallazos se pueden falsear, que las cadenas de mensajes suelen tener como objetivo sobrecargar el servidor de la aplicación. Las técnicas de desinformación y falsificación son muchas y muy variadas: vídeos en los que el rostro del protagonista y su voz se sustituyen por el de otra persona en una imagen ultrarrealista para hacernos creer que estamos viendo lo que no es, a través de deepfake (acrónimo de las palabras inglesas fake o falsificación y deep learning o aprendizaje profundo); noticias que omiten datos o se descontextualizan para tergiversar el sentido final de la información y que se apoyan o remiten a fuentes igualmente manipuladas para dar apariencia de verosimilitud; bulos que se difunden en redes sociales a través de «granjas de bots», es decir, servidores dedicados a la creación de cuentas y perfiles falsos que automatizan la emisión de los mensajes para amplificar el impacto y transmitir que «si todos lo dicen, cierto será».

Dicho sea de paso, no solo los menores son susceptibles de dejarse embaucar por noticias falsas: los adultos son también extremadamente propensos a caer en ellas. Si no fuera así, la desinformación no existiría y los bulos se desenmascararían de inmediato. De hecho, el «I Estudio sobre el impacto de las fake news en España», realizado por la Universidad Complutense, revela que solo el 14 % de los españoles es capaz de distinguir una noticia falsa.

En los últimos años, las redes sociales y plataformas online han ido adoptando medidas para intentar identificar y limitar la difusión de falsedades, espoleadas por las críticas de la opinión pública, la pérdida de reputación aparejada a su capacidad para albergar bulos y las obligaciones legales que las autoridades les han impuesto. Ya en octubre de 2018, Facebook, Google, Twitter y YouTube suscribieron ante la Comisión Europea un Código de Buenas Prácticas por el que se comprometían a redoblar sus esfuerzos contra las fake news. Todas ellas han habilitado herramientas para que los usuarios puedan denunciar vídeos, posts e imágenes que consideran falsos. En el caso de Facebook, ha contratado equipos de verificadores de datos que trabajan en varios idiomas para examinar los contenidos etiquetados como potencialmente engañosos tanto en Facebook como en Instagram: sin embargo, no los elimina, simplemente rebaja su visibilidad dentro de la plataforma. Todas ellas (Twitter⁴, Facebook⁵, YouTube⁶ y Google⁷), publican también periódicamente informes de transparencia en los que, entre otras cosas, comunican cuántas denuncias han recibido.

transparency.twitter.com.

⁵ transparency.facebook.com.

transparencyreport.google.com/youtube-policy/flags.

transparencyreport.google.com.

No parece que haya servido de mucho: a YouTube se le ha llegado a llamar el «reino de los hechos alternativos», Facebook confirmó en septiembre de 2019 que su política de noticias falsas no se aplica a los políticos (sus publicaciones no se verificarán ni se restringirá su difusión) y tanto TikTok como Snapchat incluyen filtros face swap para intercambiar el rostro de una persona por el de otra, al más puro estilo deepfake.

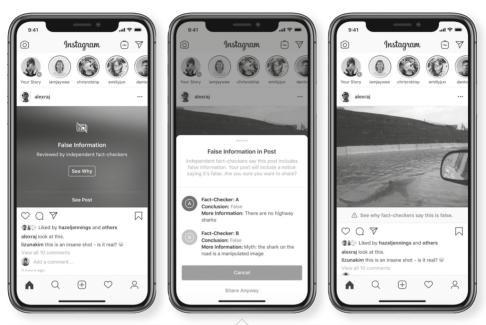


Figura 3.4. Instagram ha comenzado a etiquetar los contenidos que verificadores independientes han comprobado que son falsos o están manipulados, aunque no los suprime.

El escepticismo, el afán por contrastar y la capacidad para analizar datos e informaciones son probablemente las mejores armas personales contra las falsedades online. Es fundamental no escudarse en la velocidad y la instantaneidad para aceptar el consumo rápido y sin digestión de cualquier noticia, querer ampliar información e ir más allá del titular. Comprobar los datos y hacerlo uno mismo, buscando documentación fiable. Desarrollar una actitud crítica (no confundir con criticona ni conspiroparanoica), con el objetivo diferenciar lo que es cierto y lo que es falso en Internet, y saber cómo hacerlo. He aquí algunos consejos:

- Comprobar el autor, la fecha y la fuente de la noticia. Si no está firmada con nombre y apellido, o no consta la fecha de publicación, aumentan las posibilidades de ser falsa. En ocasiones, el enlace de la noticia simula la URL de un medio tradicional con alguna variación.
- Contrastar contenidos con titulares llamativos, alarmistas o **sensacionalistas.** Pueden ser mentira. Conviene realizar una búsqueda adicional en Internet, revisar medios de comunicación y recurrir a fuentes oficiales para comprobar si hacen referencia a esa noticia.
- Sospechar de fotos en las que no está claro el contexto ni cuándo o cômo se tomaron. A veces se reenvían imágenes que pretenden hacerse pasar como actuales, sin serlo. En la herramienta de búsqueda inversa de imágenes de Google: Images.Google.com basta con cargar la foto para identificar cuándo se publicó por primera vez y si ha sido alterada. En Fotoforensics.com se comprueba también si hay alguna manipulación.
- Consultar herramientas y webs especializadas en desmontar **bulos.** Darse un «paseo» por ellas ayuda a descubrir hasta qué punto se tergiversa y retuerce a veces la información. Entre las webs dedicadas a fact-checking (comprobación de hechos) en España destacan Maldito Bulo (maldita.es), que cuenta con especializaciones por temas, y VOST Team (www.vost.es/stopbulos), que se centra en filtrar informaciones falsas en situaciones de emergencia, como incendios forestales. En América Latina, el equipo de periodistas de Factual APF (factual.afp.com) verifica informaciones de agencias de noticias. En el ámbito europeo, el provecto EU versus Desinformation Campaign de la Unión Europea trabaja para identificar y responder a campañas de desinformación, principalmente las promovidas por Rusia, y la organización EU Disinfo Lab (disinfo.eu) persigue campañas de falsedades dirigidas contra los países miembros de la UE y sus valores. Además, The Computational Propaganda Project de Oxford Internet Institute analiza cómo se manipulan las redes sociales e Internet para amplificar o restringir contenidos políticos, desinformaciones y mensajes de odio y manipular la opinión pública, principalmente durante periodos electorales.
- Tener claro que un rumor repetido miles de veces no deja de ser **solo un rumor** si no se comprueba que es verdad. Decir una mentira muchas veces no la hace más cierta.

Como regla general, adviértele a tu hijo e hija que no debe reenviar ni compartir ese tipo de mensajes, para evitar que el bulo se siga difundiendo, y que ha de avisar también a la persona que le envió o compartió dicho contenido, para alertarle de la falsedad. Si la plataforma cuenta con herramientas para ello, la denuncia es una forma de pasar a la acción.

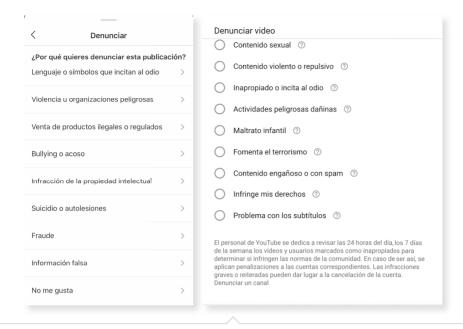


Figura 3.5. Las herramientas de denuncia de Instagram y YouTube ofrecen la posibilidad de marcar informaciones falsas o engañosas.

Competencia 3. Gestión de datos, información y contenidos digitales

Organización, almacenamiento, realización de copias de seguridad y recuperación de datos en entornos digitales.

Niños y adultos guardamos cientos de archivos de fotos, vídeos o documentos en los dispositivos móviles, acumulamos multitud de datos en los perfiles de redes sociales, almacenamos ingente información en el ordenador. ¿Qué pasa si se pierde o te roban el teléfono? ¿Y si se estropea el portátil? ¿Se puede recuperar lo publicado en la red social?

La importancia de realizar copias de seguridad y salvaguardar la información es tal, que tiene hasta un día propio: el 31 de marzo es el «Día Mundial del Back-up». Las opciones para ello son muy variadas.

iCloud es el sistema de almacenamiento en la nube para aparatos con sistema operativo iOs: teléfonos iPhone, tabletas iPad y ordenadores Macintosh. Permite almacenar en la nube fotos, archivos, etcétera, para acceder a ellos desde cualquier lugar.

- Google Drive es el servicio de almacenamiento equivalente de Google, integrado en dispositivos móviles Android. Ofrece 15GB compartidos con correo electrónico Gmail, Google Fotos y el propio Google Drive.
- Dropbox almacena gratis en la nube hasta 2GB de archivos, fotos y documentos.
- OneDrive es el servicio en la nube de Microsoft: además de almacenar, permite compartir y editar archivos (y es muy utilizado para tareas estudiantiles en equipo).

¿Y qué ocurre con lo que se publica en un perfil social? Como criterio general, y aunque parezca obvio, hay que tener claro que cuando se publica una foto, vídeo, comentario, etcétera, en redes sociales, esa información no se guarda en el perfil de cada cual. Se publica en el perfil, pero el contenido se sube y queda almacenado en el servidor de la aplicación o red social, es decir: fuera de tu alcance. Pero cada usuario puede descargar y recuperar su historial.

- WhatsApp ofrece la posibilidad de descargar y almacenar todo el historial en Google Drive (en dispositivos Android) o iCloud (en iOs).
- Instagram envía por correo electrónico todas las fotos publicadas, comentarios e información del perfil, si se solicita en: www.instagram.com/ download/request.
- Facebook incluye en Configuración el apartado Tu información de Facebook, donde generas una copia de todas las publicaciones, fotos, comentarios, reacciones, amigos, historias, mensajes, etcétera de tu perfil.
- Twitter ofrece esta opción en Configuración > Cuenta > Tus datos de Twitter > Descarga tus datos de Twitter.
- TikTok permite descargar los vídeos uno a uno, pero no proporciona un servicio de recuperación de la información.

ÁRFA «COMUNICACIÓN Y COLABORACIÓN ONLINE»

Competencia 4. Interactuar a través de tecnologías digitales

Interactuar a través de diferentes tecnologías digitales y entender cuáles son los medios de comunicación online apropiados para un contexto determinado.

Hay niños y niñas que son auténticos hachas con WhatsApp y, sin embargo, no saben adjuntar un archivo en un correo electrónico. Los hay que superan la adolescencia sin tener claro que el tono de comunicación al escribir un mail no suele ser el mismo que el de un mensaje instantáneo. Y hay otros que publican blogs a través de los que dan rienda suelta a sus inquietudes y desarrollan una afición al tiempo que mejoran la escritura: si tu hijo o hija es de estos últimos, WordPress es el gestor de contenidos más extendido para la creación de blogs.

Cuestión aparte es la discusión sobre si la interacción a través de redes sociales y la mensajería instantánea, y en concreto WhatsApp, está empobreciendo el lenguaje escrito. Faltas de ortografía garrafales, giros gramaticales inauditos, palabras acortadas hasta hacerse casi ininteligibles para los adultos, supresión de vocales, omisión de acentos y signos de puntuación, alteración de consonantes, proliferan en los textos que se envían y reciben por WhatsApp, sobre todo entre los más jóvenes.

Han empeorado las redes sociales la ortografía? Son las culpables de que se escriba peor?

El debate no es nuevo. Ya en 2008, cuando las redes sociales se encontraban aún en fase incipiente, el lingüista David Crystal analizó este tema en su libro Txtng: The Gr8 Db8. Por aquel entonces los mensajes de texto viajaban aún por SMS y cuantos menos caracteres se usaran, mejor. Crystal llegó a la conclusión de que no afectaba a la capacidad lingüística ni literaria de sus usuarios.

Estudios más recientes de la Universidad de Sevilla, como «Escritura ortográfica y mensajes de texto en estudiantes universitarios», ratifican que no existe relación: mandar WhatsApps no provoca más faltas de ortografía, sino que estas se deben al nivel cultural y educativo de quien escribe el mensaje. «El nivel ortográfico en la lengua de escolarización determina las faltas que se cometen en los textos de mensajería instantánea, y no al contrario. Las dificultades ortográficas no dependen de las características del texto, sino de la formación del emisor», concluye el estudio.

Es decir: WhatsApp no tiene la culpa de las faltas de ortografía que puedan cometer los jóvenes (o al menos no es el único culpable). Si tu hijo o hija cae en ellas... probablemente sea porque aún no ha aprendido a escribir bien, ni a través de herramientas digitales, ni sobre el papel.

Competencia 5. Compartir a través de las tecnologías digitales

Compartir datos, información y contenidos digitales con otros a través de las tecnologías adecuadas, hacer de intermediario y saber cómo citar y atribuir la autoría de los recursos.

Todo lo que se publica en Internet tiene un autor y, por tanto, está sujeto a propiedad intelectual. Entender y asimilar esta premisa es esencial cuando se publican y comparten recursos online, por sus implicaciones. Explícale a tus

pdfs.semanticscholar.org/5c41/6de915517775794bfb01f53d975fe01374a8.pdf.

vástagos que a priori no se deben copiar textos de una página web, ni coger imágenes de Google, ni compartir en YouTube películas de cine, ni descargar vídeos o fotos creados por otros y republicarlos como propios, por mucho que estén ahí, al alcance de un clic, y que todo el mundo lo haga.

Ni se debe, ni se puede, porque está regulado por ley. En España, por la Ley 2/2019⁹ de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual. Como detalle adicional, en España el delito de reproducción, copia y distribución está castigado con penas de seis meses a cuatro años de cárcel.

No obstante, sí se puede utilizar parte de un contenido ajeno en un texto que se está elaborando, siempre y cuando se reconozca su autoría y se cite al autor: la forma correcta es entrecomillar el fragmento, nombrar al autor e indicar la fuente, de esta forma no se vulnera la Ley de Propiedad Intelectual. Este procedimiento se aplica también, recuérdaselo, en los trabajos escolares de cualquier nivel: copiar sin citar es plagiar, en los proyectos de carrera y fin de máster universitario, también.

Pero ojo: prohibido copiar íntegramente un artículo completo, aunque se diga dónde se publicó antes, si no se ha solicitado autorización. Si el fragmento se va a incluir en otro contenido digital (un blog, una web), las buenas prácticas incluyen enlazar la página original. En cualquier caso, es recomendable revisar primero el aviso legal que suelen incluir todas las páginas web.

Competencia 6.

Participación ciudadana a través de las tecnologías digitales

Implicarse en la sociedad a través de servicios digitales públicos y privados y buscar oportunidades de autoempoderamiento para una ciudadanía participativa a través de tecnologías digitales apropiadas.

Internet y las redes sociales han abierto nuevas vías para expresar ideas, promover la implicación en acciones sociales, vincularse a comunidades que respondan a los intereses y necesidades de cada cual, facilitar la participación ciudadana, canalizar reivindicaciones, movilizar peticiones... Sin embargo, son una exigua minoría los adolescentes que se implican en estas actividades. Según el informe de EU Kids Online «Actividades, mediación, oportunidades y riesgos online de los menores en la era de la convergencia mediática», apenas un 2 % de los chicos y chicas de entre 13 y 17 años afirma haber participado alguna vez en una campaña o protesta online, o firmar una petición digital. Solo un 5 % asegura discutir online problemas políticos o sociales con otra gente. ¿Por apatía o por desconocimiento de las posibilidades que ofrecen las tecnologías?

www.boe.es/eli/es/l/2019/03/01/2.

En las redes sociales, los hashtags se han convertido en una poderosa herramienta para agrupar conversaciones, dar visibilidad a las temáticas más variadas y conectar a personas con intereses comunes. Prueba de ello son los #FridaysforFuture que una adolescente sueca de 15 años (Greta Thunberg, ¿te suena?) puso en marcha un viernes de agosto de 2018 cuando se sentó frente al Parlamento de Estocolmo para protestar por la inacción ante el cambio climático, y que a través de las redes sociales han unido en la protesta a cientos de miles de estudiantes de todo el mundo.

En las redes sociales cuentan también con perfiles oficiales infinidad de ONG, asociaciones, instituciones, partidos políticos, dirigentes y autoridades, accesibles en teoría con un simple clic: constituyen una fuente de información inagotable. Para iniciar una campaña online, se puede recurrir a Change.org, la mayor plataforma de peticiones del mundo: solo hay que tener más de 16 años para crear o unirse a una petición.

Si adolescentes y jóvenes no se implican, al menos que no sea por no saber cómo hacerlo.



Figura 3.6. La plataforma Change.org recoge más de trescientos millones de peticiones de personas de 196 países. Sus responsables aseguran que casi cada hora, una petición consigue llegar al objetivo de firmas marcado y logra la victoria. Para abrir una campaña online en ella solo es preciso tener más de 16 años.

Competencia 7. Colaboración mediante tecnologías digitales

Utilizar tecnologías y medios online para el trabajo en equipo y la creación y construcción colaborativa de recursos, conocimientos y contenidos.

Solo un 4 % de los alumnos españoles sabe trabajar en equipo, según el informe «Collaborative Problem Solving» 10 de la OCDE. Una lástima, porque tal como señala el World Economic Forum¹¹, «trabajando en grupo, el niño aprende a desarrollar habilidades sociales y a aceptar la forma de ser y de trabajar del resto de compañeros, al igual que le ocurrirá en un futuro en su entorno laboral. Se convierte en una persona activa e involucrada en su propio aprendizaje, desarrolla la empatía, el respeto y la escucha activa. Y de esta manera, se fomenta el pensamiento crítico del niño, es decir, la reflexión autónoma de un tema, la búsqueda de diferentes alternativas, el estudio y análisis de los errores y la defensa final de una idea».

La capacidad para trabajar en equipo no depende de la tecnología empleada, pero utilizar las herramientas digitales idóneas facilitan este objetivo. Aunque en los últimos años los centros educativos han ido incorporando técnicas de trabajo por proyectos entre los alumnos, todavía es frecuente encontrarse con estudiantes universitarios que no saben manejar algo tan sencillo como Google Docs, la herramienta gratuita para elaborar documentos, presentaciones y hojas de cálculo en la nube y de forma compartida para que varias personas trabajen sobre ellos. O que se lían al manejar versiones de un archivo en las que se ha introducido control de cambios.

¿Y las redes sociales ayudan a avanzar en esta dirección? Basta con ver algunos hilos de Twitter, en los que a partir de una exposición inicial de un usuario se agregan comentarios que completan, amplían y profundizan en el tema de discusión. O la amplia variedad de wikis y sitios webs colaborativos en los que cada persona puede borrar, editar o añadir contenido de forma rápida e interactiva: la Wikipedia es el más conocido, pero hay otros muchos, entre ellos Vikidia, una enciclopedia dirigida a chavales entre 8 y 13 años en la que no importa la edad para participar.

¹⁰ www.oecd-ilibrary.org/education/pisa-2015-results-volume-v_9789264285521-en.

¹¹ es.weforum.org/agenda/2019/10/el-aprendizaje-cooperativo-cuando-lo-que-interesa-no-son-loslogros-individuales-sino-el-trabajo-en-equipo.



Figura 3.7. Vikidia es una wiki a modo de enciclopedia realizada por y para niños y niñas entre 8 y 13 años, que editan sus contenidos de forma colaborativa. La versión en español se inició en mayo de 2008 y dispone de alrededor de cinco mil artículos.

Competencia 8. Netiqueta

Conocer las normas de comportamiento cuando se utilizan tecnologías digitales y se interactúa en entornos digitales, adaptar las estrategias de comunicación a una audiencia específica y ser consciente de las diferencias culturales y generacionales en entornos digitales.

En realidad, las normas de netiqueta no son reglas ni leyes, no están escritas en ningún sitio, pero facilitan la convivencia en entornos digitales y sirven de orientación para que fluya la conversación y la interacción. Podría decirse que se resumen en dos ideas principales: «Compórtate online como lo harías de maneras presencial» y «Respeta a los demás y trátales como te gustaría que te trataran a ti».

Conviene insistir a los más jóvenes (y también a los adultos) en las siguientes pautas cuando se relacionan a través de redes sociales, mensajería instantánea y chats:

- No publiques fotos o vídeos en las que salgan otras personas sin **pedirles antes permiso.** Incluso si están en segundo plano, incluso si no son las protagonistas de la fotografía, incluso si también son amigos tuyos. Si vas a compartir la imagen, avísales.
- No etiquetes a nadie en una fotografía o vídeo sin su autoriza**ción.** Aunque todas las redes sociales proporcionan herramientas para que los usuarios controlen y limiten en qué publicaciones se les puede etiquetar, estas restricciones no suelen estar activadas por defecto y la mayoría de las veces no se revisan. El resultado es que en Facebook e Instagram, las imágenes en las que la persona ha sido etiquetada quedan reflejadas en su perfil, en Twitter reciben una notificación cada vez que se les etiqueta (lo que puede ser percibido como spam...).

- No insultes, no humilles, no te burles de los demás y mide tus **críticas.** Un insulto online duele igual o más que el que se grita a viva voz, aunque el silencio parezca ocultarlo. La tecnología no avala la impunidad, ni da ningún derecho extra.
- No digas ni hagas algo que no te atreverías a ejecutar en persona o cara a cara. Sigues siendo tú, aunque sea tras una pantalla.
- **No mientas.** Pero ten en cuenta que te pueden mentir.
- No aceptes en tu círculo de amistad a usuarios cuya identidad real no tengas clara: no tengas problemas en ignorar solicitudes, invitaciones a eventos o grupos, etcétera.
- No permitas que te amenacen, atemoricen, desprecien o avasa**llen** a través de redes sociales y chats. La mejor defensa es avisar cuanto antes a tus padres, profesores, tutores... No te calles.
- No reacciones de manera violenta cuando algo te moleste. Recuerda que las redes sociales permiten denunciar (reportar) a otro usuario, bloquearle o silenciarle.
- Antes de publicar una información o un contenido que te han enviado de manera privada, pregunta si lo puedes hacer.
- No reenvíes ni compartas contenidos que puedan dañar o menoscabar a otras personas, incluso aunque no las conozcas.

Competencia 9. Gestión de la identidad digital

Crear y gestionar una o múltiples identidades digitales, proteger la reputación personal y gestionar los datos generados a través de las diversas cuentas y aplicaciones.

Niños, adolescentes y jóvenes tienen cada vez más integrada su vida online y offline y los sucesivos estudios de EU Kids Online muestran que se reduce paulatinamente el porcentaje de quienes reconocen que les resulta más fácil ser ellos mismos online que cara a cara: se diluyen las fronteras entre lo presencial y lo digital, quizás porque Internet y las redes sociales cobran cada vez más presencia en sus vidas cotidianas.

Sin embargo, esto no significa que sean conscientes de su huella digital y las consecuencias que tendrá en su vida adulta: en ello profundizaremos más adelante.

ÁREA «CREACIÓN DE CONTENIDOS DIGITALES»

Competencia 10. Desarrollo de contenidos digitales

Crear y editar contenido digital en diferentes formatos y expresarse uno mismo a través de medios digitales.

Para ello es preciso tener una idea que desarrollar o expresar, comprender como trasladarla a contenidos digitales a través de texto, foto, vídeo o audio, conocer los programas y aplicaciones con los que crearlos y los canales a través de los que difundirlos: entre ellos, las redes sociales.

Dado que el 83 % de los adolescentes españoles hace un uso intensivo de las plataformas sociales, cabría asumir que este capítulo es asignatura superada. Sin embargo, los estudios y la realidad empírica no corroboran esta suposición: el estudio de EU Kids Online revela que apenas un 10 % de los niños españoles de entre nueve y 12 años y un 12 % de las niñas en esta franja de edad ha creado su propio vídeo o post musical y lo ha subido a las redes para compartir. A medida que crecen, el porcentaje se reduce aún más, y lo hace de forma significativa: solo un 4 % de los chicos y un 7 % de las chicas de entre 13 y 17 años crea y publica contenidos multimedia. Es decir: los niños y adolescentes españoles son grandes consumidores de redes sociales, pero devoran contenidos ideados por otros. Y eso, a pesar de que el 53 % de los menores asegura que sabe cómo crear y publicar vídeos y música online. «Los niños y las niñas españoles aún tienen un importante margen para mejorar en este tipo de habilidades», advierte el informe de EU Kids Online.

Grabar un vídeo con TikTok es muy, muy sencillo, y los múltiples efectos que proporciona esta plataforma añaden amplias opciones de edición. En Instagram, los filtros permiten retocar y mejorar una imagen de múltiples maneras. Pero, además, hay otras muchas herramientas con las que producir contenidos multimedia, desarrollar una idea o guion y decidir, por último, publicarla (o no) en redes sociales.

Algunas, muy simples, como la posibilidad de añadir música a una presentación en power point y guardarla como película. Otros, algo más complejos, como los programas Movie Maker para Windows o iMovie para iOs, con los que editar vídeos con rótulos, efectos y música. Entre medias hay una infinita gama de aplicaciones, como Lumen 5, herramienta online que convierte el contenido de un texto o post en un vídeo breve: traslada el contenido escrito a plantillas de imagen en las que preseleccionar posibles fotos y frases. O las aplicaciones móviles gratuitas InShot y VivaVideo, para editar vídeos y convertir una sucesión de fotos en una película.

En torno a Instagram han surgido también multitud de aplicaciones móviles de retoque fotográfico con las que niños y adolescentes potencian su vertiente más artística y estética, experimentan con efectos y desarrollan narrativas visuales: Adobe PhotoShop Express, PicsArt, Snapseed, VSCO, Prisma, Slow Shutter Cam, ColorPop, PhotoLab, Plotaverse y Photofox son solo algunos ejemplos. Para diseñar historias de Instagram diferentes se puede recurrir a apps como Over, StoryArt y Mojo.

En definitiva, las tecnologías digitales, apps y redes sociales facilitan plasmar y desarrollar la creatividad... pero la capacidad creativa no se improvisa: hay que incentivarla. Antes de agarrar un teclado o una pantalla, el niño debería haber embadurnado sus dedos con pintura de manos, jugado con pinceles, contado historias inventadas... Las nuevas tecnologías son solo un instrumento más.

Competencia 11. Integración y reelaboración de contenido digital

Modificar, refinar, mejorar e integrar información y contenido en otro ya existente para crear nuevo contenido y conocimiento original y relevante.

De nuevo, estar rodeado de tecnología no implica saber utilizarla: solo el 23 % de los españoles entre nueve y 17 años conoce cómo editar o hacer cambios básicos en el contenido online que otros han creado, según el estudio de EU Kids Online. Difícil así no solo ser diestro en esta competencia, sino también crear contenido de forma colaborativa (para avanzar en esta casilla, retrocédase a las anteriores y retome la partida).

Competencia 12. Derechos de autor y licencias

Entender cómo se aplican los derechos de autor y las licencias a la información y a los contenidos digitales.

Toda obra tiene un autor y está sujeta a derechos de propiedad intelectual. Dicho esto, existen diferentes formas de licenciar la propiedad intelectual, procedimiento por el que los autores autorizan a otros a utilizar sus creaciones, de forma legal. Si citar es importante, saber qué recursos se pueden reutilizar y bajo qué condiciones lo es aún más.

Las licencias más extendidas son las Creative Commons¹², con las que los autores dan permiso para que sus obras se puedan copiar, distribuir, editar, remezclar y desarrollar, sin que suponga una violación de la propiedad intelectual. Hay varios tipos de licencias, en función del uso autorizado y las restricciones impuestas: conviene revisar qué criterios se aplican en cada caso. Para encontrar fotos con este tipo de permisos, basta con acudir al buscador

¹² creativecommons.org/licenses.

de Creative Commons¹³: rastrea entre más de trescientas imágenes licenciadas. Hay también decenas de webs de bancos de imágenes gratis, como Freepik y FreeDigitalPhoto, donde se pueden descargar y usar de forma legal. Se acabó, por tanto, bajar imágenes de Google.



Figura 3.8. Ejemplos de tipos de licencias Creative Commons.

Mención aparte merecen las licencias *copyleft*, que se aplican principalmente a software y permiten que otros utilicen, modifiquen y redistribuyan un programa informático o sus derivados, siempre que se mantengan estas mismas condiciones de utilización y difusión: de ahí que a los programas con este tipo de licencias se le denomine software libre.

Y hablando de redes sociales: ¿qué ocurre con la propiedad intelectual de los vídeos, fotos y demás que los chavales publican en una plataforma? Si los derechos de autor son inherentes a toda obra, ¿adónde van los derechos de tu hijo o hija?

¹³ search.creativecommons.org.

Todas las plataformas sociales tienen unos «términos de uso» que las personas deben aceptar al abrir un perfil... y que casi nadie lee nunca antes de consentir someterse a ellas. En este apartado se específica, entre otras cuestiones, qué permisos conceden las personas al crear su cuenta y qué derechos se reserva la plataforma. Y hay una cláusula recurrente en todos ellos que obliga al usuario a ceder una «licencia mundial, no exclusiva, transferible, sublicenciable y exenta de pagos por derechos de autor para alojar, distribuir, modificar, mantener, reproducir, mostrar o comunicar públicamente y traducir tu contenido, así como para crear contenido derivado». En este caso, la frase es de Instagram¹⁴, pero tanto TikTok como Facebook, Twitter, Snapchat y todas las demás incluyen una similar.

La profusión de adjetivos que incluye la frase no es casual.

Significa que cuando tu hijo o hija sube un selfi a una red social, una animación o una imagen, está cediendo sus derechos de autor a la plataforma y autorizándola a que distribuya, modifique, reproduzca, etcétera, su foto. En teoría, se trata de una mera fórmula para que la red social pueda prestar el servicio sin infringir ninguna ley de propiedad intelectual. En la práctica... al abrir un perfil en una red social, automáticamente se ceden los derechos sobre todo lo que se publica y comparte en ella.

Competencia 13. Programación

Desarrollar secuencias de instrucciones aplicables a programas informáticos para solucionar un problema o desarrollar una tarea.

Decía el fundador de Apple, Steve Jobs, que todo el mundo debería aprender a programar, porque programar ayuda a pensar. Su sucesor al frente de la compañía, Tim Cook, llegó a afirmar que programar es más importante que aprender inglés (quizás, tal vez, porque el inglés lo daba por supuesto).

Lo cierto es que el «Marco Europeo de Competencias Digitales para la Ciudadanía» establece que la programación es una de la competencias necesarias, entendiendo como tal la capacidad para comprender sus principios, saber realizar modificaciones en aplicaciones, configuraciones y software informático y codificar dispositivos digitales. Todos los ciudadanos europeos deberían adquirir estas nociones, según la Comisión Europea. ¿Un objetivo demasiado ambicioso?

De una u otra manera, los centros educativos españoles han ido introduciendo asignaturas, actividades o contenidos relacionados con programación y robótica, aunque aún no de forma homogénea. Falta, en ocasiones, una adecuada formación del propio personal docente.

¿Cómo reforzar este aprendizaje desde el hogar?

¹⁴ www.facebook.com/help/instagram/478745558852511.

Una de las herramientas educativas más utilizadas en la mayoría de colegios e institutos es Scratch¹⁵, un lenguaje visual desarrollado por el Massachusetts Institute of Technology (MIT) basado en bloques que se unen a modo de puzle. Es una aplicación gratuita, accesible a través de navegador web y desarrollada específicamente para chicos y chicas de entre ocho y 16 años. La única condición para empezar a trabajar con ella es que un profesor, padre o tutor (es decir, un adulto) valide la cuenta. Para los más pequeños existe también una versión adaptada. Scratch Junior, ideada para niños y niñas entre cinco y siete años. Además, Scratch no es solo un lenguaje de programación: es también una comunidad online en la que los chavales pueden compartir sus animaciones, juegos online e historias interactivas con gente de todo el mundo.

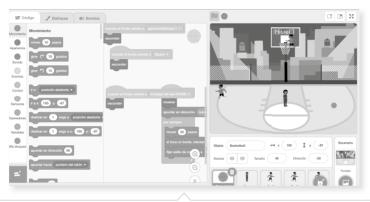


Figura 3.9. Scratch es un lenguaje de programación visual desarrollado por el Massachusetts Institute of Technology (MIT) orientado a facilitar su aprendizaje de forma intuitiva mediante bloques: en lugar de escribir código, se encajan piezas a modo de puzle para desarrollar las órdenes que configuran el proyecto. Está específicamente pensado para chicos y chicas entre ocho y 16 años.

Otra alternativa es Code.org, una organización sin fines de lucro lanzada en 2013 que ofrece cursos y tutoriales online de programación gratuitos, clasificados por edades entre cuatro y 18 años. Menos conocida que Scratch, algunos de sus recursos están disponible solo en inglés.

¿A tu hijo o hija le gustan los videojuegos? ¿Y si fuera capaz de diseñarlos desde cero? Con RPG Maker¹⁶ puede crear videojuegos de rol y construir mundos de fantasía al tiempo que se inicia en la programación. Este software cuenta con una versión de descarga gratuita con un mes de prueba, para instalar en PC. Incluye editores de mapas con los que generar

¹⁵ scratch.mit.edu.

¹⁶ www.rpgmakerweb.com.

entornos con varias estéticas diferentes (supramundo, exterior o mazmorra, entre otros) para configurar los niveles del juego, la posibilidad de personalizar los protagonistas, asignar enemigos de los que huir, lanzar combates contra orcos, murciélagos y otras criaturas, crear diálogos entre los personajes, marcas trampas, túneles o puentes de acceso y ambientarlo todo con música, entre otras muchas opciones.

Un consejo: la clave para diseñar un juego online con Scratch o un videojuego con RPG Maker no es tanto aprender cómo usar sus herramientas (que también), sino decidir qué historia contar: en qué va a consistir la dinámica del videojuego, cuál será el objetivo, qué pruebas tendrá que superar... y cómo se plasmarán en pantalla. Y para eso, más que programar, lo que se necesita es imaginar.

¿Y cómo canalizar la afición a las redes sociales para mejorar las competencias en programación? Algo tan mundano como los filtros y las máscaras faciales son también una buena excusa para ello: tanto Instagram como Snapchat cuentan con aplicaciones oficiales con las que desarrollar este tipo de filtros.

En el caso de Instagram, Facebook abrió en 2019 a todo el mundo su aplicación Spark AR Studio¹⁷, con la que crear máscaras personalizadas y ponerlas a disposición del resto de usuarios de la red social. No es una herramienta tan sencilla como las anteriores y se requiere un poco de paciencia, pero su ventaja es que no precisa ningún requisito técnico concreto, excepto disponer de perfil en Facebook.

En Snapchat, la herramienta equivalente se llama Lens Studio¹⁸, una app con la que diseñar filtros en 2D y 3D, crear animaciones y añadir texturas.

En ambos casos, se trata de pasar de consumidor a creador... y poner a prueba las destrezas personales.

ÁREA «SEGURIDAD»

Competencia 14. Protección de dispositivos

Proteger los dispositivos y contenidos digitales, entender los riesgos y amenazas y conocer las medidas de seguridad, así como adoptar las iniciativas necesarias para asegurar la fiabilidad y la privacidad.

¹⁷ sparkar.facebook.com/ar-studio.

¹⁸ lensstudio.snapchat.com.

Proteger los dispositivos tecnológicos se convierte año tras año en una tarea más compleja, por la diversidad y la proliferación de riesgos, ataques y amenazas. Para contextualizar esta afirmación, basta con citar los datos que proporciona el CCN-CERT, la entidad española dependiente del Centro Criptológico Nacional y adscrita al Centro Nacional de Inteligencia (CNI), responsable de mejorar la ciberseguridad española y ayudar a responder a los ciberataques y ciberamenazas: la cifra anual de incidentes de ciberseguridad que gestiona ha pasado de 4003 en el año 2012 a nada menos que 38 029 en 2018, y la cantidad sigue subiendo. Pero aunque voluminosa, la cifra se refiere solo a los ciberataques que afectan a organismos o empresas públicas, que son los que gestiona el CCN-CERT: es decir, solo la punta del grandísimo iceberg de los riesgos cibernéticos.

«Los seres humanos siguen siendo el eslabón débil en todos los sistemas de seguridad, por lo que, a medida que aumente la eficacia de las protecciones, los agentes de las amenazas modificarán su objetivo, atacando a las personas», advierte el CCN-CERT en su informe «Ciberamenazas y tendencias. Edición 2019»¹⁹. «Es de esperar que los próximos años sean testigo de muchos más correos electrónicos de suplantación de identidad (*phishing*) y sitios web falsos diseñados para engañar al usuario y facilitar el acceso a datos confidenciales, tales como contraseñas o números de tarjetas de crédito. Los dispositivos conectados a Internet vía WiFi ofrecen nuevas formas para que los agentes de las amenazas penetren en las redes internas, atacando a los dispositivos conectados, incluyendo los ordenadores, generalmente, al objeto de sustraer datos o información personal».

El horizonte está pintado de nubarrones.

Porque todo ello se realiza a través de programas maliciosos diseñados en especial para colarse en el ordenador, *smartphone* o tableta. Su peligro aumenta si tenemos en cuenta que los teléfonos móviles que utilizan la mayoría de los niños y adolescentes son en realidad, más que teléfonos, pequeños ordenadores con una capacidad significativa de procesado y almacenamiento de información. A ello se suma que los ataques a dispositivos móviles están creciendo en torno al 85 % anual, sobre todo a través de SMS, mensajería instantánea (WhatsApp y Facebook Messenger) y aplicaciones de redes sociales como Instagram, según datos del CCN-CERT: en definitiva, las apps que más usan los chavales (y también los no tan jóvenes).

Hay muchos y diversos tipos de *malware* (como se denominan en terminología anglosajona): unos diseñados para robar datos personales, otros para provocar que el dispositivo deje de funcionar correctamente, aquellos para tomar el control del aparato y continuar infectando otros equipos. Entre los más habituales están:

¹⁹ www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html.

- **Troyanos**. Se llaman así porque no son lo que aparentan. Suelen llegar como archivos adjuntos en correos electrónicos o a través de programas que parecen inofensivos. Su objetivo es dar el control del aparato a los emisores del troyano... a quienes cada vez les gustan más los dispositivos móviles.
- **Gusanos**. Se multiplican y propagan para saturar y colapsar equipos y redes, son muy hábiles replicándose y extendiéndose. Para ello, crean copias de sí mismos que redifunden como archivos adjuntos en correos electrónicos o mensajes instantáneos que envían de forma automática (y sin que el emisor sea consciente) a los contactos del dispositivo afectado. Para camuflar el «gusano», la temática del mensaje suele estar relacionada con sexo, famosos, temas de actualidad o software pirata.
- **Spyware** o programas espía. Tienen como misión recopilar información del afectado y enviársela a su creador. Se esconden habitualmente en programas gratuitos que el usuario se descarga, en sitios de intercambio de archivos (por ejemplo, de descarga de música o películas gratis) o en adjuntos de mensajes. La mayoría de la gente no sabe ni siguiera que lo tiene instalado: se identifica a veces porque aparecen iconos nuevos o surgen mensajes de error al realizar acciones que antes se ejecutaban sin problemas.
- **Rogueware.** Simulan ser un antivirus (falso) que detecta una infección e intentan sacar dinero vendiendo soluciones o suscripciones a servicios de desinfección. A veces simulan que están escaneando el equipo y son capaces de infectar de verdad si no se abona el dinero. Aparecen al realizar descargas o acceder a páginas de dudosa reputación, por ejemplo.
- **Ransomware**. Bloquean el ordenador o dispositivo móvil, cifrando los archivos, y no lo liberan hasta que se paga el dinero que exigen (últimamente, en bitcoins u otro tipo de criptomoneda).
- **Keylogger**. Capturan la información sobre todo lo que se teclea, sin que te enteres, con la intención de obtener contraseñas, datos bancarios, números de tarjetas de crédito, correos electrónicos, información de redes sociales... Suelen venir con los troyanos.

Los programas maliciosos se camuflan y esconden con eficacia, se propagan con facilidad y causan daños ilimitados. Y las previsiones sobre su evolución futura no son nada halagüeñas. «Durante los próximos años veremos nuevas variantes de malware más difíciles de detectar, y que podrían residir en los sistemas infectados durante un período de tiempo muy largo. Debido a que los atacantes pueden usar los ordenadores comprometidos para una multiplicidad de actividades (minería de criptomonedas, robo de información, etcétera), necesitan acceder a las máquinas varias veces. Para permanecer sin ser detectado, el malware tendrá que ocultarse mejor», alertan desde el CCN-CERT.

Para evitar que los dispositivos se conviertan en víctimas de estos ataques, he aquí algunas prácticas que no solo los niños, también los adultos, deberíamos seguir:

- ▶ **Instalar un antivirus y un cortafuegos.** Su diferencia radica en su misión: el antivirus previene la infección por *malware* y actúa contra él en caso de ser infectado; el cortafuegos bloquea los accesos no autorizados al equipo. En la web de la Oficina de Seguridad del Internauta²⁰ encontrarás antivirus gratuitos tanto para ordenador como para móvil con sistema operativo iOS y Android.
- ▶ **Desconfiar de redes WiFi públicas.** Suelen ofrecerse en aeropuertos, cafeterías, bibliotecas... Pero no son seguras porque no cifran, no protegen, la información que circula por ellas: cualquier usuario podría hacerse con los datos que transmitamos mientras estemos conectados. Son también una vía de entrada para elementos no deseados.
- ▶ **Descargar solo aplicaciones seguras.** Como primera precaución, hay que recurrir siempre a las tiendas de apps oficiales: Google Play y AppStore cuentan con medidas de seguridad para evitar aplicaciones fraudulentas. Además, conviene revisar quién es el desarrollador, los comentarios que han dejado otras personas y el número de descargas (si es una app famosa pero con pocas descargas, quizás se trate de una copia poco fiable).
- ▶ No hacer nunca clic en archivos de dudosa procedencia o con temáticas llamativas.
- ▶ **Actualizar los sistemas.** Mantener el móvil o el ordenador al día con las últimas versiones de las aplicaciones y de los sistemas operativos ayudará a bloquear las ventanas por las que se cuelan los ciberdelincuentes.
- ▶ Desconfiar por sistema de mensajes que propongan hacer clic en una dirección web para ganar un premio, activar un descuento, recibir un cupón y beneficios por el estilo. Especialmente si la URL no va encabezada con https://, si utiliza un acortador que impide saber adónde conduce, si el dominio tiene una terminación extraña o la marca a la que hace referencia está escrita de forma diferente a la habitual. Con la herramienta Google Safe Browsing²¹ se comprueba si un sitio web es o no seguro.

²⁰ www.osi.es/es/herramientas.

²¹ transparencyreport.google.com/safe-browsing/search.



Figura 3.10. Con Google Safe Browsing se puede comprobar si es peligroso visitar determinada web, con solo introducir su URL.

Competencia 15. Protección de datos personales y privacidad

Proteger la privacidad y los datos personales en entornos digitales. Entender cómo usar y compartir información personal o sensible sin exponer a riesgos ni a uno mismo ni a otras personas. Entender que los servicios digitales se rigen por una «política de privacidad» que informa sobre el tratamiento de los datos personales.

El mero hecho de conectarse a Internet, abrir un perfil en una red social, crear una cuenta en una aplicación móvil o configurar un avatar en un juego online implica revelar al menos una parte de la identidad de cada uno, incluso si esta actividad se realiza con un nombre ficticio. Tan solo con esa acción tan común. se está proporcionando algún dato personal: la dirección de correo electrónico a la que se vincula la cuenta o perfil, la dirección de protocolo de Internet (IP) del dispositivo desde el que se efectúa la conexión a la web o red social (que es única e irrepetible para cada aparato y está formada por números), el identificador de cookie que la web o red social que se está visitando instala en el navegador del ordenador o el teléfono móvil para guardar las preferencias de navegación, la localización del teléfono móvil...

Y a ellos se suma, por supuesto, la información sobre uno mismo que cada cual publica, comparte y difunde a través de redes sociales y otros canales online, de forma proactiva o involuntaria.

La preocupación en torno a la necesidad de proteger los datos personales ha crecido de forma paulatina en los últimos años, tanto por la entrada en vigor de diferentes legislaciones que inciden especialmente en este punto y han impulsado la concienciación (entre ellos, el Reglamento General de Protección de Datos de la Unión Europea y la Ley de Protección de Datos Personales y Garantía de Derechos Digitales española) como por los escándalos sobre la utilización sin permiso de datos personales para orquestar campañas políticas destinadas a influir en el voto en procesos electorales (entre ellos, el protagonizado por la consultora Cambridge Analytica y Facebook durante la campaña que llevó a Donald Trump a la presidencia de Estados Unidos).

Pero una cosa es ser consciente y otra saber cómo gestionarlo, sobre todo cuando los protagonistas son los niños y adolescentes, empezando incluso por lo más básico, como la configuración de perfiles en redes sociales o la protección de contraseñas.

El informe «Actividades, mediación, oportunidades y riesgos online de los menores en la era de la convergencia mediática» revela que el 59 % de los niños y el 64 % de las niñas entre nueve y 12 años no sabe cómo cambiar la configuración de privacidad de sus perfiles, a pesar de tenerlos (y no solo uno, sino varios). Incluso en los chavales de más edad, el desconocimiento persiste: el 20 % de los chicos y el 18 % de las chicas entre 13 y 17 años sigue sin tener ni idea de cómo hacerlo.

Como contrapartida, aumenta con la edad el riesgo de uso fraudulento de las contraseñas: cuando se les pregunta si alguien ha utilizado en alguna ocasión sus claves para acceder a su información o fingir ser ellos, solo el 7 % de los niños y el 6 % de las niñas de nueve a 12 años afirma haber tenido ese problema... pero el porcentaje se eleva al 10 % de los chicos y el 12 % de las chicas cuando cumplen entre 13 y 17 años. En solo unos años los incidentes se multiplican en lugar de disminuir, especialmente y de forma relevante en el caso de las chicas.

Conviene recordarles, por tanto, lo siguiente:

- ▶ Los perfiles en redes sociales de los menores de edad han de configurarse como privados por una simple cuestión de precaución y protección, para que sean ellos quienes elijan y seleccionen quién les puede seguir y acceder a su información, y no al revés. Y sí, sí importa quién ve lo que publican. Y no, no deben aceptar a todos los que solicitan unirse a ellos como seguidor, contacto o amigo, han de cerrar la puerta si no los conocen y no saben quiénes son en realidad, o si no están seguros de ello. Y no, no importa el número de seguidores que consigan, porque eso no los hace más importantes ni mejores personas ni más queridos ni más admirados: no deben preocuparse por cuántos followers ganan, pierden o acumulan. En el capítulo 2 vimos dónde y cómo cambiar la configuración de privacidad en las redes sociales que más utilizan los menores.
- ▶ **Las contraseñas son importantes.** Al menos, todavía. Hay quien vaticina el fin próximo de las contraseñas tradicionales de letras y números y preconiza que en breve serán sustituidas totalmente por certificados efímeros (*One Time Password*, en inglés) y tecnologías biométricas, más seguras por su carácter único, personal e intransferible, como la huella dactilar o el reconocimiento facial que teléfonos móviles y ordenadores portátiles incluyen ya. Puede ser, pero también es cierto que, de momento, la inviolabilidad de la biometría no

es tal: en 2014, cuando la actual presidenta de la Comisión Europea, Ursula von der Leyer, era ministra de Defensa, el hacker e investigador de la Techniste Universität Berlin Jan Krissler fue capaz de reproducir su huella dactilar, tomando como referencia fotografías publicadas en medios de comunicación.

Mientras llega la solución definitiva, habrá que seguir echando mano, por tanto, de las contraseñas. Eso sí, recuérdale a tu hijo o hija que no debe utilizar la misma en todos los perfiles ni servicios online en los que se registre. Lo ideal es que tenga una longitud mínima de ocho caracteres y que combine letras mayúsculas, minúsculas, número y algún símbolo, para que sea robusta y difícil de adivinar.

Para no olvidarlas, hay varias opciones. Lo más aconsejable cuando tienen menos edad es que sean los propios padres quienes las «custodien»: ojo, el objetivo no es de esa forma controlar lo que tu hijo publica y los mensajes que recibe y envía, sino salvaguardar las contraseñas y ayudarle si en algún momento necesita recuperarlas. Asume que a medida que crezcan, es probable que ellos mismos las cambien sin contártelo: conviene entonces que conozcan los gestores de contraseñas, herramientas para almacenar de forma segura esta información, como Password Boss, Keeweb y Dashlane.

- Las contraseñas no se comparten. Ni siquiera a tu mejor amigo o amiga, ni a tu novio o novia. Ni se comparten con nadie, ni se piden tampoco a otra persona como prueba de amistad, amor o confianza. Si de verdad quieres a alguien, no le pidas sus contraseñas del móvil ni de sus redes sociales. Si se fían de ti, no toleres que te las reclamen. Son mensajes que deben interiorizar cuanto antes.
- Cuidado al utilizar dispositivos de otras personas. Por ejemplo, el ordenador del colegio, la tableta o el móvil de un amigo o en un cibercafé. La mayoría de los servicios online y redes sociales ofrecen la posibilidad de guardar la contraseña cuando accedes a tus perfiles y cuentas a través de un nuevo dispositivo: hay que rechazar siempre esta opción. Y cerrar la sesión antes de abandonar la aplicación o web, para evitar que se quede abierta y un tercero pueda entrar en ella.

Ahora bien, por mucho que proteja sus perfiles y cuentas con contraseñas robustas, fiables e inquebrantables, aunque no revele a nadie sus claves, pese a que cuide la seguridad de sus equipos y cierre sesión cuando utilice un dispositivo ajeno, hay alguien que siempre y en todo momento tendrá acceso a sus datos y a su información personal, alguien que sabrá constantemente qué hace y deja de hacer en Internet y redes sociales, y que utilizará esa información en beneficio propio y con un fin económico y comercial.

¿Quién? La red social, plataforma online, aplicación móvil o servicio de Internet que tu hijo o hija está usando.

¿Qué tipo de información almacena y cómo la gestiona? Depende de cada caso.

Hasta la actividad más cotidiana, navegar por una página web, conlleva un tratamiento de datos: al visitar ese sitio online, el servidor en el que está alojado envía un archivo de información que se almacena en el navegador del terminal del internauta. Son las famosas *cookies*, que almacenan cantidades de datos que van desde unos pocos kilobytes a varios megas. Estas *cookies* son las que permiten, por ejemplo, recordar las preferencias de cada persona al acceder a un sitio web, realizar un seguimiento y análisis de cómo se comporta y qué visita dentro de la web y recopilar los datos necesarios para mostrar publicidad dirigida específicamente a él o ella. No son dañinas ni infectan el dispositivo y su objetivo es facilitar la navegación... pero en ocasiones se hacen con demasiada información adicional.

¿Cuántas veces te ha ocurrido que visitando una web, de repente te ha aparecido un anuncio sobre algo que estuviste consultando hace días en otra página diferente? Es por obra y gracia de las *cookies*, y eso mismo le sucede a tu retoño: es importante que entienda cómo funcionan y que sea consciente de que sus idas y venidas en Internet quedan registradas, entre otras cuestiones, para intentar venderle algo o convencerle de la bondad de un producto. Que no es casualidad que le aparezcan propuestas publicitarias precisamente sobre temas que le gustan, y que esta publicidad puede adoptar múltiples formatos, desde el clásico *banner* hasta una imagen que surge de repente al intentar entrar en un sitio web o un vídeo que se reproduce antes de visualizar el juego en el que tenía interés.

En esta recopilación de datos, las redes sociales son insaciables. Almacenan y clasifican no solo la dirección de correo electrónico, la fecha de nacimiento, el sexo y el número de teléfono móvil que se proporciona al abrir la cuenta y crear y perfil, no solo los comentarios, fotos y vídeos que en ellas publica cada persona o los mensajes que envía y recibe, sino también ingente información sobre la actividad que dentro de la plataforma realiza cada uno. El objetivo, de nuevo, es contar con información personal detallada para mostrar publicidad adaptada a cada cual.

Instagram, por ejemplo, registra con detalle las personas, marcas y cuentas que sigue; el tipo de vídeo, fotos y comentarios que le gustan; los hashtags que utiliza o que incluyen los contenidos con los que interactúa; las personas con las que más se comunica por mensaje directo; las llamadas de teléfono que efectúa o las direcciones de correo electrónico que tiene en la agenda del móvil, si lo sincronizó con la aplicación; la frecuencia con la que se conecta; los temas que le interesan; el contenido que ve; cómo usa los filtros y las funciones de la cámara de Instagram; qué compra y con qué número de tarjeta de crédito lo paga; qué móvil o tableta emplea (desde el sistema operativo, hasta el espacio de almacenamiento disponible, la ubicación GPS y el operador de telefonía que tiene contratado).

¿Es ilegal que los sitios web y las redes sociales actúen así? En realidad no, aunque con condiciones.

En la Unión Europea, el Reglamento General de Protección de Datos que entró en vigor en mayo de 2016 y comenzó a aplicarse en mayo de 2018, fue pionero en establecer una normativa que deben cumplir todas las empresas, servicios y

plataformas que recopilen y traten datos personales de ciudadanos europeos, aunque la sede de dichas compañías no esté en la Unión Europea. Eso incluye absolutamente todos los sitios web y todas las redes sociales.

Entre las exigencias que impone el Reglamento, figura el que se informe con transparencia a los ciudadanos sobre qué datos se van a almacenar, para qué v durante cuánto tiempo; que se recoja exclusivamente la información necesaria para los fines descritos; que se asegure su protección; que la recopilación se realice con el consentimiento expreso de cada persona y que esta pueda, a su vez, obtener copia de los datos que la empresa ha guardado, rectificarlos, oponerse a que se conserven v solicitar que se eliminen.

De ahí que todas las webs y plataformas de redes sociales (y cualquier otra compañía) estén obligadas a poner a disposición del público su «Política de privacidad», un documento en el que explicar con detalle todo lo anterior y que el internauta o miembro de la red social debe consentir expresamente, antes de que empiecen a recopilarse sus datos personales. Por eso, al visitar una página web por primera vez nos surge un mensaje en el que se nos pregunta si estamos de acuerdo en aceptar las cookies. Por lo mismo, al abrir una cuenta en una red social siempre hay una casilla que hay que marcar antes de crear el perfil.

Esa casilla que (ya lo hemos dicho) casi siempre se acepta sin mirar.

Y entonces, ¿qué hacer?

- No es obligatorio aceptar las cookies de una web. Se pueden deshabilitar, eliminar, bloquear y administrar. Todos los navegadores permiten gestionarlas: en los respectivos centros de asistencia de Google Chrome²², Mozilla Firefox²³ y Safari²⁴ se explica el procedimiento.
- El modo de navegación privada evita el rastreo. Es especialmente útil si se comparte un ordenador (por ejemplo, el del colegio) o la conexión se realiza desde un ordenador público (el de una biblioteca o un cibercafé). Activando el modo de navegación privada se evita que el navegador guarde información sobre las páginas web que se visitan, las búsquedas que se realizan o las contraseñas que se introducen para entrar en una red social. Aunque no nos confundamos: esto no equivale a ser invisible ni anónimo en Internet. Se activa abriendo nueva ventana de incógnito en Google Chrome²⁵, o nueva ventana privada en Mozilla Firefox²⁶ y en Safari²⁷.

²² support.google.com/chrome/answer/95647?hl=es.

²³ support.mozilla.org/es/products/firefox/protect-your-privacy/cookies.

²⁴ support.apple.com/es-es/guide/safari/sfri11471/mac.

²⁵ support.google.com/chrome/answer/95464.

²⁶ support.mozilla.org/es/kb/navegacion-privada-Firefox-no-guardar-historial-navegacion.

²⁷ support.apple.com/es-es/guide/safari/ibrw1069/mac.

Hay que leer la «Política de privacidad» antes de firmar. Excepto TikTok, cuyos contenidos se pueden visualizar sin necesidad de configurar una cuenta, todas las plataformas sociales exigen validar su política de privacidad para entrar en la red (TikTok también al crear el perfil). Pero que no sea posible participar, publicar y comentar en una red social sin realizar previamente esa concesión no significa que no se deba conocer el alcance y sus implicaciones. Aunque solo sea para saber adónde va a parar la información sobre uno mismo y qué ocurrirá con ella. Aunque solo sea para aprender a reclamar los datos personales y borrarlos. Aunque solo sea para tener claro que si participar en una red social es gratis, es porque los ingresos proceden de la publicidad que se contrata en base a la información que cada persona proporciona, lo que convierte a cada miembro de la plataforma en producto de venta. Incluidos nuestros hijos. De eso, y de cómo gestionarlo, hablaremos en profundidad más adelante.

Competencia 16. Protección de la salud y del bienestar

Evitar riesgos para la salud física y psicológica en el uso de la tecnología. Ser capaz de protegerse a uno mismo y otros frente a posibles peligros en entornos digitales y ser consciente de la importancia de la tecnología digital para el bienestar y la inclusión social.

«A pesar de la rápida difusión del acceso a las experiencias digitales y online en todo el mundo, aún existen amplias brechas en el acceso de los niños a la tecnología digital y las comunicaciones. El acceso a las TIC y la calidad de ese acceso se ha convertido en un nueva línea divisoria», advierte el informe «Niños en un mundo digital»²⁸ de Unicef, que apuesta por el poder de la conectividad para desarrollar el potencial de la infancia y romper los ciclos intergeneracionales de la pobreza, cambiando así las reglas de juego para algunos de los niños y las niñas más marginados del mundo.

Y es que la tecnología, Internet y las redes sociales abren nuevas oportunidades a los colectivos en riesgo de exclusión social, pero al mismo tiempo pueden erigirse en un factor adicional de marginalización, al aumentar las diferencias entre quienes sí disfrutan y se benefician de la digitalización y a quienes se les niega esa posibilidad. Porque la realidad es que aunque todos los niños están creciendo en un mundo en el que la transformación tecnológica cobra impulso, no todos están participando en este proceso, lo que condiciona tanto su presente como su futuro.

El presente, porque los niños sin conexión pierden acceso a recursos educativos, información global y oportunidades de aprendizaje, además de renunciar a un instrumento que les permitiría ejercer su capacidad de expresión y

²⁸ www.unicef.org/media/48611/file.

creatividad. «Para los niños desfavorecidos, como por ejemplo quienes viven con discapacidades, la conectividad puede significar la diferencia entre la exclusión social y la igualdad de oportunidades», asegura Unicef.

Y el futuro, porque el horizonte laboral y profesional de quienes permanecen ajenos a la transformación tecnológica se reduce drásticamente hasta llegar a construir un muro infranqueable que impide ganarse la vida. «Aquellos con acceso a tecnologías digitales y a las aptitudes necesarias para hacer el mejor uso de ellas disfrutarán de una ventaja sobre quienes no están conectados ni capacitados», alerta Unicef.

No se trata ni mucho menos de ignorar los riesgos que entraña el uso abusivo de Internet y las redes sociales, ni los peligros a los que los menores pueden quedar expuestos, sino de contextualizarlos. «Estos riesgos no son del todo nuevos: por largo tiempo, los niños han acosado y han sido víctimas del acoso, han estado expuestos a materiales violentos y sexuales, o han tratado de conseguirlos, y siempre han estado en peligro de la acción de los delincuentes sexuales», reconoce Unicef. La diferencia es que antes la puerta de casa ejercía de barrera y ahora los límites espaciales y temporales se diluyen en el entorno online. «Todos los niños hacen frente a la posibilidad de sufrir daños como resultado de las tecnologías y de Internet. Pero para la mayoría de los niños, esta posibilidad sigue siendo solo eso, una posibilidad. Comprender por qué el riesgo se traduce en daño real para ciertos niños, y no para otros, es crucial», señala el informe.

A ello se suma la creciente inquietud por el posible vínculo entre el uso excesivo de Internet y las redes sociales y desórdenes como ansiedad, depresión, irascibilidad v privación del sueño, especialmente entre los adolescentes. ¿Es capaz Instagram de causar un trastorno psicológico de envergadura? ¿Son culpables las redes sociales de la depresión juvenil? ¿Fomentan la hiperactividad o el déficit de atención?

Más allá del alarmismo o la condescendencia, las indagaciones empíricas muestran una de cal y otra de arena. En el estudio «Children's mental health support. Social media, gaming and mental health»²⁹, la organización estadounidense sin ánimo de lucro Child Mind Institute analizó diversas investigaciones realizadas entre menores de edad para contrastar en qué medida las redes sociales podrían estar afectándoles negativamente... Y ni aun así los resultados se pueden considerar definitivos.

El informe de Child Mind Institute cita, por ejemplo, un estudio realizado en 2019 entre adolescentes de 12 a 15 años que descubrió que utilizar más de tres horas diarias las redes sociales está vinculado a síntomas depresivos y dormir menos de siete horas diarias. Sin embargo, recoge también otra encuesta de 2018 con adolescentes entre 13 y 19 años en la que el 81 % de los participantes afirmó que las redes sociales les hacen sentirse más conectados con sus amigos, el 25 % aseguró

²⁹ childmind.org/our-impact/childrens-mental-health-report/2019report/.

que son importantes para su creatividad y otro tanto dijo expresamente que les hace sentirse menos solos. Por otra parte, incluye un estudio de la Universidad de Iowa con 3000 niños y adolescentes que durante tres años comprobó que los niños que jugaban con videojuegos eran más impulsivos y tenían más problemas de atención. No obstante, otro trabajo sobre hábitos digitales de más de 120 000 jóvenes reveló que jugar online menos de una hora al día tiene efectos positivos porque incrementa la resiliencia emocional y las habilidades para resolver problemas.

En resumen, el Child Mind Institute llegó a la conclusión de que «estos estudios muestran una correlación, no una causalidad». Por tanto, no se puede deducir científicamente que lo uno esté motivado directamente por lo otro. «La revisión de estas investigaciones sugiere que los problemas online son a menudo prolongaciones de los comportamientos y las características offline», aventura la organización en su informe. Es decir: los niños y jóvenes con tendencia a la ansiedad tendrán más afán por responder de inmediato a un mensaje de WhatsApp (pero no es WhatsApp el origen de esta ansiedad) y aquellos con menos autoestima se sentirán más deprimidos si sus fotos consiguen poco likes en Instragram o las vidas que reflejan las imágenes de los otros son más interesantes, más estimulantes, más maravillosas y estupendas que la propia (pero Instagram no es culpable de que les falle la autoestima). Con los adultos, por cierto, sucede lo mismo.

Mención aparte merecen las especulaciones sobre el nocivo efecto que sobre la salud tienen las redes WiFi y los campos electromagnéticos de radiofrecuencia que emiten los dispositivos móviles. En concreto, sobre la posibilidad de que los móviles produzcan cáncer u otro tipo de enfermedades graves.

Los científicos llevan algo más de dos décadas intentando dilucidar si la exposición a radiofrecuencia aumenta el riesgo de contraer tumores. De momento, lo único que sí está claro es que las radiaciones electromagnéticas de las redes WiFi no provocan cáncer ni son capaces de generar ningún otro efecto biológico excepto, quizás, un calentamiento de los tejidos, que no es significativo a los niveles de exposición habituales.

En cuanto a los móviles, la International Agency for Research on Cancer (IARC)³⁰, un organismo dependiente de la Organización Mundial de la Salud, revisó en 2011 todos los estudios sobre teléfonos móviles y su relación con diversas modalidades de cáncer y decidió clasificarlos como «posible carcinógeno para humanos», aunque reconoció que los resultados no eran en absoluto concluyentes.

A partir de ahí, el rosario de declaraciones ha sido constante. En 2018 la American Cancer Society³¹ señaló que aunque no se había visto riesgo mayor de cáncer, se aconsejaba que quienes estuvieran preocupados, utilizasen un auricular con el móvil. El Centers for Desease Control and Prevention³² asegura que

³⁰ www.iarc.fr/wp-content/uploads/2018/07/pr208_E.pdf.

³¹ www.cancer.org/latest-news/updated-cell-phone-study-findings-still-inconclusive.html.

³² www.cdc.gov/nceh/radiation/cell phones. FAQ.html.

no hay evidencia científica sobre si el uso de móviles causa cáncer y la Federal Communications Commission³³ insiste en que no hay prueba científica entre el uso de aparatos inalámbricos y tumores u otras enfermedades.

A pesar de todo, periódicamente vuelve a plantearse, cual oleada que viene y va, la duda sobre si los teléfonos móviles pueden causar cáncer, especialmente en los niños, dado que sus sistemas nerviosos están aún en formación y por tanto son potencialmente más vulnerables. «Sus cabezas son más pequeñas que las de los adultos y, por consiguiente, tienen una exposición proporcionalmente mayor al campo de radiación de radiofrecuencia emitida por los teléfonos celulares. Y los niños tienen la posibilidad de acumular más años de exposición a los celulares que los adultos», reconoce el National Cancer Institute³⁴ estadounidense, quien sin embargo es tajante al determinar: «Hasta ahora, los datos de estudios en niños con cáncer no apoyan esta teoría».

Competencia 17. Protección del medioambiente

Ser consciente del impacto de la tecnología digital en el medioambiente.

Subir una foto a Instagram, enviar un mensaje a WhatsApp, ver un vídeo de YouTube o escuchar una canción en Spotify tienen un efecto sobre el medioambiente, la emisión de gases de efecto invernadero y el cambio climático.

Bueno, en realidad, efectuar estas acciones solo una vez no es significativo. Lo relevante es que cada minuto se publican en todo el mundo más de 46 200 posts en Instagram, se envían 41,6 millones de mensajes instantáneos, se ven 4,5 millones de vídeos, se toman 2,1 millones de snaps, se mandan 188 millones de mails, se realizan 3,8 millones de búsquedas en Internet...

... Suma, suma y suma, y la ecuación se completa. El Foro Económico Mundial estima que el sector digital es responsable de la emisión del 1,4 % de los efectos de gases invernadero y la organización ecologista Greenpeace calcula que su huella energética equivale al 7 % del consumo mundial. Ello se debe, entre otros factores, a que para que webs, plataformas y servicios de Internet puedan funcionar, se necesitan centros de datos que operen las 24 horas del día los 365 días del año, redes de comunicación y dispositivos que envíen y reciban la información, y tanto su fabricación como su mantenimiento consumen energía.

«Este crecimiento explosivo de nuestro consumo digital está impulsando nuevas y cuantiosas inversiones en infraestructuras digitales, en particular en nuevos centros de datos que consumen mucha energía para servir como fábricas de la economía digital. Estos centros, que albergan miles de servidores que almacenan e intercambian nuestros mensajes, fotos y vídeos con nuestras tablets y teléfonos, varían mucho en tamaño pero la tendencia es que sean cada vez más grandes.

³³ www.fcc.gov/consumers/guides/wireless-devices-and-health-concerns.

³⁴ www.cancer.gov/about-cancer/causes-prevention/risk/radiation/cell-phones-fact-sheet.

Las instalaciones de alojamiento web y de datos en la nube (cloud hosting) más grandes son capaces de consumir tanta energía como una ciudad de tamaño mediano principalmente para refrigerarse», advierte Greenpeace en su informe «Clicking Clean»35.

La tecnología, las redes sociales e Internet se configuran así como actores con elevada capacidad de impacto en el entorno. Por poner un ejemplo, Gartner asegura que la energía que se necesita para enviar un tuit genera 0,02 gramos de CO2: los 500 millones de tuits que cada día se publican como promedio emiten un total de 10 toneladas métricas de CO2 diarias. El simple hecho de usar un teléfono móvil tiene una elevada repercusión. ¿Por qué? Según un estudio de la Universidad de McMaster³⁶ la energía empleada en la fabricación de un terminal representa aproximadamente entre el 85 % y el 95 % de las emisiones totales que arrojará durante su vida útil... sobre todo si tenemos en cuenta el frenético ritmo de renovación de los teléfonos móviles, que provoca que aproximadamente cada dos años el consumidor tienda a cambiarlo. Querer estar a la última en dispositivo móvil también perjudica al medioambiente.

Como contrapartida, la digitalización puede contribuir positivamente a luchar contra el cambio climático. El Foro Económico Mundial asegura que las tecnologías digitales podrían ayudar a reducir las emisiones mundiales de carbono hasta en un 15 % en 2030 gracias al desarrollo de soluciones más eficientes en transporte, gestión del tráfico, edificación, agricultura... Convocar una reunión de trabajo por Skype invierte menos energía y emite menos gases que el viaje en avión que quizás sería preciso realizar para mantener la reunión de forma presencial.

Por otra parte, las grandes empresas tecnológicas están también destinando recursos para priorizar las energías renovables en sus instalaciones. Facebook, Google y Apple fueron las primeras en apostar por ello. «Ahora se les han sumado cerca de otras 20 compañías de Internet, entre las que figuran también empresas globales que gestionan sistemas de almacenamiento en la nube y de colocación en centro de datos que se habían quedado muy atrás», reconoce Greenpeace.

¿Y qué podemos hacer cada uno de nosotros, como ciudadanos e individuos? Cada gesto cuenta, tanto de los niños como de los adultos.

Replantear la frecuencia de renovación de teléfonos móviles, ordenadores, tabletas y demás equipos tecnológicos. Existe, es cierto, la llamada obsolescencia programada: el periodo de tiempo que los fabricantes establecen previamente para la vida útil de un producto, y que una vez superado, provocan que el aparato deje de funcionar correctamente. Y hay también una cierta tendencia a correr por estar a la última o desechar lo estropeado sin intentar siquiera arreglarlo. Para combatir esto último, hace una década

³⁵ archivo-es.greenpeace.org/espana/Global/espana/2016/report/tecnologia/Clicking_Clean_2017.pdf.

³⁶ sciencedirect.com/science/article/pii/S095965261733233X?via%3Dihub.

surgió en Ámsterdam la iniciativa Repair Café³⁷, talleres no profesionales en los que voluntarios reparan electrodomésticos y aparatos electrónicos; hay ya más de 2000 establecimientos de este tipo en una treintena de países, entre ellos, España.

- No redistribuir cadenas de correos, mensajes, retos, etcétera, que multiplican el consumo de datos y sobrecargan servidores.
- No dejar conectados dispositivos (como el teléfono móvil) a la red eléctrica si ya están cargados.
- **Apagar los equipos** cuando se terminan de usar, en vez de mantenerlos en stand-by.
- **Utilizar la opción de optimización** de energía en el *smartphone*.
- Eliminar del móvil las apps que no se usan.
- **Borrar periódicamente** correos electrónicos, mensajes, archivos que aumentan las necesidades de almacenaje.

Esa nota de voz que vas a enviar por WhatsApp, ¿de verdad hace falta?

ÁRFA «RESOLUCIÓN DE PROBLEMAS»

Competencia 18. Resolución de problemas técnicos

Identificar posibles problemas técnicos al usar los dispositivos y resolverlos (desde los más básicos a los complejos).

La batería de posibles fallos que pueden devenir al emplear dispositivos tecnológicos es ingente y muy variada, digna casi de un manual de instrucciones (esos que, por cierto, tampoco solemos leer al adquirir un aparato).

Como criterio general, es útil tener claro que las aplicaciones, servicios online y fabricantes cuentan con equipos de soporte técnico a los que dirigir consultas y comunicar incidencias. También las redes sociales, ya sea a través de su aplicación móvil o en la versión web: en la app de Instagram se accede en Configuración>Informar de un problema, TikTok ofrece la página de Soporte support. tiktok.com/es/, WhatsApp facilita el contacto a través de www.whatsapp.com/ contact/... En caso de no saber a quién o cómo dirigirse, lo más rápido es realizar la típica búsqueda en Google.

³⁷ repaircafe.org/.

Conviene también actualizar las aplicaciones móviles y programas de software en cuanto se lanzan nuevas versiones. En la mayoría de los casos estas actualizaciones se deben a que se han introducido mejoras en los servicios, correcciones de fallos y errores, optimizaciones en el rendimiento... O que se han cubierto los temidos bugs, esos fallos en la programación o diseño del software que provocan que en un momento dado dejen de funcionar correctamente.

La dimensión de estos bugs aumenta a medida que los programas y servicios se hacen más complejos, lo cual ha motivado que en los últimos años muchas empresas tecnológicas hayan puesto en marcha los denominados programas de Bug Bounty, mediante los que incentivan (con recompensas económicas) que personas ajenas a las compañía investiguen, detecten y comuniquen vulnerabilidades y fallos en los sistemas: son los hackers éticos o buenos, también llamados hackers de sombrero blanco (no confundir con los *crackers* o *hackers* de sombrero negro, quienes buscan agujeros en los sistemas para causar el mal).

Plataformas como HackerOne están especializadas en facilitar la relación entre los equipos de seguridad de una empresa y profesionales o principiantes de la informática dedicados a descubrir bugs. No hay límite de edad para participar en este tipo de plataformas. En 2016 el niño finlandés de diez años Jani Finn se convirtió en el receptor más joven del programa de Bug Bounty de Instagram: detectó un error que le permitía alterar el código en los servidores de la red social, de manera que era capaz de obligarla a borrar comentarios... y eso que ni siquiera tenía la edad permitida para abrirse un perfil. Instagram le premió con 10 000 euros.

Competencia 19. Identificación de necesidades y respuestas tecnológicas

Analizar las necesidades e identificar, evaluar, seleccionar y usar la tecnología precisa para solucionarlas (por ejemplo, en cuestiones de accesibilidad).

Detallar la relación de problemas y dificultades a las que se enfrentan las personas con necesidades específicas en Internet y redes sociales escapa en realidad al objetivo de este libro. Baste recordar que el World Wide Web Consortium, principal organización de estándares en Internet, ha implantado las directrices de cómo debe ser el contenido web para resultar accesible, especialmente a personas con discapacidad, pero también a otras con determinadas limitaciones. Estos estándares, denominados Web Content Accessibility Guidelines (WCAG), establecen que la información y los componentes de una web deben ser perceptibles, operables entendibles y robustos.

La accesibilidad de la tecnología es un elemento primordial porque ejerce de palanca para mejorar la calidad de vida, fomentar la comunicación, facilitar las relaciones sociales y ayudar en la búsqueda de empleo a personas con limitaciones. En este sentido, resulta significativo que el dispositivo que las personas con discapacidad usan para acceder a Internet es, de manera predominante, el teléfono móvil (en un 70 % de los casos), a pesar de su reducido tamaño: es el preferido por delante del ordenador y de la tablet, incluso aunque no cuente con adaptaciones específicas.

Y a la hora de recurrir a aplicaciones móviles, las apps de redes sociales son también las que más utilizan las personas con discapacidad, más incluso que las de búsqueda de trabajo, gestión de transportes o entretenimiento: seis de cada diez personas con discapacidad es miembro de alguna red social. «La potencialidad de las redes sociales puede ser utilizada por las personas con discapacidad para mejorar su integración y participación en la comunidad, acceder a grupos de interés, etcétera. Facilitan que mejoren su plena participación en la vida social», señala el monográfico «Las TIC. Una oportunidad para la inclusión» del Observatorio para la Discapacidad Física.

Competencia 20. Uso creativo de la tecnología digital

Utilizar herramientas y tecnologías digitales para crear conocimiento e innovar en procesos y productos.

«La creatividad es simplemente conectar cosas», afirmaba Steve Jobs, el fundador de Apple. Cabría preguntarse si la creatividad es innata o se aprende, si la tecnología fomenta la creatividad al proporcionar instrumentos con los que romper los límites que constriñen su desarrollo o, por el contrario, la mata porque automatiza procesos.

Si entendemos por creatividad la capacidad de generar nuevas ideas y conceptos, se diría más bien que la creatividad se entrena: mirando desde otro punto de vista, aplicando criterios diferentes, jugando con conceptos, mezclando ideas, investigando, probando y fallando también. Y en ello, las herramientas digitales, Internet, las redes sociales y las aplicaciones móviles son un gran aliado: porque ayudan a experimentar, a dar forma a aquello que solo has podido imaginar, a conectar conocimiento, a abrir puertas.

La creatividad se entrena y las tecnologías digitales sirven de gimnasio. Todo depende del uso que queramos darles, del enfoque que adoptemos, de la capacidad para explorar o quedarnos en la primera pantalla.

Competencia 21. Identificar lagunas en las competencias digitales

Ser capaz de identificar dónde debo mejorar o actualizar mis propias competencias digitales y ayudar a otros en el desarrollo de sus competencias. Buscar oportunidades para el autoaprendizaje y mantenerse al día de la evolución del mundo digital.

³⁸ www.observatoridiscapacitat.org/sites/default/files/documents/2016-06_odf_monografic7_cast.pdf.

Es la última y sin embargo, en mi opinión, la más importante de las competencias contempladas en el «Marco Europeo de Competencias Digitales para la Ciudadanía». La rapidez con la que evoluciona el entorno digital obliga a ser consciente de la necesidad del aprendizaje continuo, tanto en niños como en adultos. El desarrollo de competencias digitales no tiene fin. Y como señala el Foro Económico Mundial: «No es necesario esperar. De hecho, no hay tiempo para esperar. Los niños ya están sumergidos en el mundo digital e influyen en la manera en que será el mundo mañana. Depende de nosotros garantizar que tengan las habilidades requeridas y el apoyo para convertirlo en un lugar que puedan aprovechar».

PARA RECORDAR: DIF7 IDEAS CLAVES

- 1. La adquisición de competencias digitales es un proceso permanente. Se trata de desarrollar una actitud activa, crítica y realista hacia las tecnologías, para aprender a valorar sus fortalezas y debilidades y a respetar principios éticos en su uso. Implica motivación y curiosidad por el aprendizaje. La familia, y no solo la escuela, desempeña en esta labor un papel esencial que, sin embargo, no siempre se cumple.
- 2. El mero hecho de conectarse a Internet, abrir un perfil en una red social, crear una cuenta en una aplicación móvil o configurar un avatar en un juego online implica revelar al menos una parte de la identidad de cada uno, incluso si esta actividad se realiza con un nombre ficticio.
- 3. Las fotos, vídeos, comentarios, etcétera, que se publican en redes sociales, no se suben al perfil de cada cual. Se publican en el perfil, pero el contenido queda almacenado en el servidor de la aplicación o red social, es decir: fuera del alcance del usuario. Pero cada uno puede descargar y recuperar su historial.
- 4. Cuando tu hijo o hija sube un selfi a una red social, una animación o una imagen, está cediendo sus derechos de autor a la plataforma y autorizándola a que distribuya, modifique y reproduzca su foto.
- 5. Cuanto antes tenga claro tu hijo o hija que no todo lo que recibe y lee es cierto, mejor. Incúlcale que verosimilitud no es sinónimo de veracidad, que las fotos y vídeos se alteran con extrema facilidad, que los pantallazos se pueden falsear y que las cadenas de mensajes suelen tener como objetivo sobrecargar el servidor de la aplicación. El escepticismo, el afán por contrastar y la capacidad para analizar datos e informaciones son probablemente las mejores armas personales contra las falsedades online.

- 6. Todo lo que se publica en Internet tiene un autor y, por tanto, está sujeto a propiedad intelectual. No se deben copiar textos de una página web, ni coger imágenes de Google, ni compartir en YouTube películas de cine, ni descargar vídeos o fotos creados por otros y republicarlos como propios, por mucho que estén ahí, al alcance de un clic.
- 7. Internet y las redes sociales han abierto nuevas vías para expresar ideas, promover la implicación en acciones sociales, vincularse a comunidades que respondan a los intereses y necesidades de cada cual, facilitar la participación, canalizar reivindicaciones y movilizar peticiones. En definitiva, vías para ejercer la ciudadanía.
- 8. La tecnología, Internet y las redes sociales abren nuevas oportunidades a los colectivos en riesgo de exclusión social. La accesibilidad de la tecnología ejerce de palanca para mejorar la calidad de vida, fomentar la comunicación, facilitar las relaciones sociales y ayudar en la búsqueda de empleo a personas con limitaciones. A la hora de recurrir a aplicaciones móviles, las apps de redes sociales son las que más utilizan las personas con discapacidad, más incluso que las de búsqueda de trabajo, gestión de transportes o entretenimiento.
- 9. No se puede afirmar que las redes sociales provocan ansiedad, depresión o problemas de salud similares: los problemas online no son más que prolongaciones de los comportamientos offline. Tampoco los teléfonos móviles y las WiFi generan cáncer.
- 10. Las tecnologías digitales, apps y redes sociales facilitan plasmar y desarrollar la creatividad... pero la capacidad creativa no se improvisa: hay que incentivarla. Todo depende del uso que queramos darles, del enfoque que adoptemos, de la capacidad para explorar o quedarnos en la primera pantalla.