

TEMA 7. LA ALFABETIZACIÓN DIGITAL PARA EDUCAR ANTE LAS FAKE NEWS

En la actualidad, el mundo en el que vivimos está en constante evolución. La **era digital** origina una nueva concepción de la realidad en la que vivimos, afectando a la vida cotidiana familiar, a los trabajos, a la enseñanza, etcétera. Por este motivo, uno de los términos más empleados para ayudar a que las personas se familiaricen con las nuevas tecnologías es el de **alfabetización digital**. Para ello, estas herramientas y su aplicación en la sociedad servirán para que el usuario o usuaria esté conectado en la sociedad, impulsando la **igualdad** y la **inclusión** de dichas personas en el mundo actual.

De este modo, es un nuevo método de aprendizaje para el ser humano, más allá de saber **leer y escribir**. Cuánto mayor conocimiento y mayor aprendizaje tengamos de la alfabetización digital y de su aplicación, mayores oportunidades de empleo y mejor soltura en la sociedad tendrá dicho usuario. Por ello, es importante entender la evolución de este concepto, que va más allá de que el usuario sepa utilizar un ordenador.

En este sentido, para muchos expertos en materia educativa creen que es necesario que haya alfabetización mediática y audiovisual en las clases de toda **Europa** y que ésta pueda aparecer en los **informes PISA**. Por ello, también apuestan por la mejora de la formación a los profesores para que se especialicen en esta materia y alfabetizar de manera digital a la población. Sólo así, podemos combatir la ola de desinformación y de creación de 'Fake News', ayudando a una mejor y correcta navegación por **Internet** y en los medios digitales.

7.1. Introducción a la alfabetización digital y su evolución para la sociedad

Es necesario definir para la sociedad y para la educación qué se entiende por alfabetización digital. La **Real Academia de la Lengua Española** define la alfabetización como "la enseñanza a un colectivo o usuario a leer y escribir de manera adecuada". Por ello, la **alfabetización digital** se entiende como la "*habilidad de localizar, analizar, organizar y evaluar información utilizando las nuevas tecnologías, comprendiendo cuál es su funcionamiento para usarla en su beneficio*". Este aprendizaje de la alfabetización digital va dirigido a los más **pequeños** (que ya unen el aprendizaje de la lectura y escritura con el de las nuevas tecnologías) y el de los más **mayores** (que ya alfabetizados, adquieren destrezas con los nuevos dispositivos digitales y las nuevas formas de comunicación online para fomentar su inclusión en la sociedad).

Desde inicios del **siglo XXI**, el mundo ha experimentado un cambio, donde las nuevas tecnologías llegaron para quedarse en la sociedad. Hay que destacar que el alfabetismo digital no es sólo el uso de **Internet**, sino que es también la utilización de los nuevos **soportes electrónicos**, como los ordenadores portátiles, las tablets o los smartphones o aparatos 'inteligentes'. Dicha persona aplica esa utilización de los soportes tecnológicos y la conexión Internet a su vida diaria, no sólo en el ámbito profesional sino también personal. En este apartado especial, las redes sociales

juegan un papel fundamental, en la socialización de las personas con el objetivo de crear nuevos espacios de interacción. Por este motivo, hay varios criterios por los que debe de estar fundamentada la alfabetización digital:

- Habilidades instrumentales con las TIC.
- Habilidad para buscar, seleccionar, organizar, utilizar, aplicar y evaluar la información.
- Colaboración, cooperación, comunicación efectiva y capacidad para compartir.
- Creación y publicación de contenidos.
- Pensamiento crítico, creatividad, innovación y solución de problemas.
- Comprensión social y cultural, ciudadanía digital.
- Seguridad e identidad.

La enseñanza de la **alfabetización digital** es diferente en cada una de las etapas de nuestra vida. No es lo mismo enseñar a **niños** (cuyos contenidos se basan más en el juego, el aprendizaje de contenidos y en el disfrute) que en **adultos** (cuyos objetivos están más enfocados al terreno profesional, y al perfeccionamiento y conocimiento de los usos que se le debe de dar al contenido digital).

También se hace especial hincapié a la educación y enseñanza de la alfabetización digital en relación a las '**Fake News**' para los más pequeños. Los **menores** deben de ser un colectivo protegido, debido a los malos usos de los portales web, donde hay contenido no recomendado para su edad. Por este motivo, es necesario poner una **protección y seguridad interactivas** a aquellas webs que puedan ofrecer noticias falsas, incorporando anuncios publicitarios dedicados al ocio o a un contenido para un público más adulto.

7.2. La brecha digital

Es evidente que el ser humano, a día de hoy, tiene en sus hogares un dispositivo electrónico y acceso a **Internet** (esta última afirmación, se produce en casi toda la población, sólo en pocas zonas rurales no hay conexión Internet). Pero la **alfabetización digital** también tiene un problema para aquellas personas que todavía no se encuentran tecnológicamente metidos en la nueva dinámica de la sociedad. De este modo, nace el término de **brecha digital**, que se entiende como aquellas dificultades de las personas que no pueden acceder de manera económica o técnica a las **nuevas tecnologías**. También, la brecha digital se produce cuando hay diferencias entre una comunidad tecnológica, y otra que no tiene conocimientos básicos sobre cómo manejar las mismas en su vida cotidiana.

Por ello, en muchos países ya se están desarrollando programas, políticas e iniciativas para que el acceso a **Internet** y a las nuevas tecnologías sea **universal**. De este modo, cualquier comunidad podrá integrarse en la nueva dinámica de la sociedad, independientemente de la persona que sea, grupo de edad, raza, sexo, religión, etcétera. Un ámbito donde se pone de manifiesto el acceso a

Internet es la **educación**, donde conseguiremos que los alumnos y las alumnas puedan educarse y alfabetizar de manera digital, aprendiendo conceptos, programas y otros contenidos en red.

Según muchos expertos en materia de **Comunicación**, inciden en que el problema de la **brecha digital** se pondrá solución si en cada hogar, o en cada rincón hay un dispositivo digital para que la persona pueda acceder a dicho **contenido interactivo**. Una diferencia donde también se puede aprovechar la educación tecnológica de las personas con la educación acerca de las 'Fake News'.

7.3. La seguridad en Internet, un aspecto fundamental

Un aspecto fundamental a la hora de entender la alfabetización digital y su aplicación (directa o indirectamente) a las '**Fake News**' es la **seguridad** en la navegación por **Internet**. Desde que nos conectamos por Internet, ya sea desde conexión por cable, por wifi o por conexión de datos a través de teléfonos móviles o smartphones, siempre ocurre que nos aparecen peligros, virus u otros mensajes dañinos para el funcionamiento regular de nuestro acceso.

Uno de los puntos clave para un acceso a Internet seguro entre sus webs es la actualización del navegador. Por ello, se evitará sufrir virus en enlaces rotos o dañados, y volver a caer en malas prácticas cibernéticas como el '**phishing**' (*explicado ya en el Tema 3, dedicado a los 'Medios y redes sociales'*). En cuanto al resto de virus, existen diferentes tipos de virus que afectan a la navegación segura por Internet, como el **criptolocker** (que descarga un programa en tu equipo a través del correo electrónico) o el **keylogger** (programas que captan la información de una persona).

Por este motivo, hay diferentes soluciones para conseguir una **navegación** segura, donde también pueden incidir las '**Fake News**'. Las noticias falsas o bulos siempre circulan por estos ámbitos, donde los enlaces web en los que aparecen suelen contener mensajes ofensivos, publicidad engañosa, o programas que contienen un virus que daña nuestra navegación y, por ende, el dispositivo o equipo desde el que navegamos. En este sentido, estas son algunas de las claves para navegar de manera segura por Internet:

- **Concienciación:** Cuando accedemos a Internet, tenemos que ser conscientes de los riesgos que tomamos. Por eso es fundamental ser cuidadoso y precavido con las páginas que visitamos y los archivos que descargamos.
- **Un buen antivirus:** Aunque no lo sea todo, contar con un buen software de seguridad, que esté siempre actualizado, es una de las principales medidas que se pueden tomar para evitar ser víctimas de un ciberataque.
- **Actualizar el sistema operativo:** Tener correctamente actualizado el sistema operativo es una de las principales garantías para no dejar abiertas las puertas de entrada a tu equipo que los ciberdelincuentes puedan explotar.

- **Evitar descargas no conocidas:** Una de las mayores brechas de seguridad viene de la descarga de archivos. Por eso, si no estás totalmente seguro del origen de lo que estás descargando, mejor evítalo o verifícalo antes de la descarga.
- **Cuidado con los correos:** Es fundamental una lectura detallada de los emails que te parezcan raros o sospechosos, aunque provengan de conocidos. Muchas veces, los ciber delincuentes hacen simulaciones idénticas al original.
- **Los temas importantes, en casa:** Si queremos realizar trámites importantes como realizar compras o acceder a la banca online, lo mejor es hacerlo desde equipos que controlemos. Por eso, usar el equipo de casa o tú móvil siempre será más seguro que hacerlo en el de un tercero.
- **Certificado de seguridad:** Las transacciones se deben hacer con certificado de seguridad (HTTPS) válido y reconocido por entidad certificadora de confianza.
- **Redes WiFi ajenas:** Uno de los mayores problemas con los equipos portátiles viene de buscar WiFi allá donde vamos. El peligro es que no podemos saber si estamos ante una red de confianza o de un tercero que podría examinar nuestros datos.
- **Riesgos de la geolocalización:** Esta característica puede ser positiva, pero debemos tener cuidado con registrar nuestra posición cuando vayamos a estar lejos de casa, porque esa información puede abrirle las puertas de nuestro hogar a los delincuentes.
- **Rastros de las imágenes:** Esto no supone inseguridad en sí, pero lo cierto es que las imágenes que subimos a la Red dejan un rastro digital histórico, por lo que hay que tener cuidado con subir algo de lo que nos podamos arrepentir.
- **Siempre cerrar sesión:** Un grave problema que me encuentro a menudo como perito informático es que los usuarios acceden a sus correos y no cierran la sesión en sitios no seguros. Deben tener cuidado de cerrarlo. Además, siempre recomiendo activar la doble verificación.
- **Protegerse en la nube:** Otro tema a tener en cuenta es la sincronización en la nube en ordenadores y, especialmente, en teléfonos móviles. Por ejemplo, la mayoría de los terminales Android sincroniza los datos de nuestro correo dejando copia en servidores de Google de todo nuestro histórico, posicionamiento o imágenes. Por ello, debemos tener cuidado ya que todos los lugares por los que navegamos quedarán almacenados.

BIBLIOGRAFÍA Y RECURSOS ONLINE

- Alfabetización mediática:
 1. <https://gaptain.com/blog/alfabetizacion-mediatica-que-es-y-porque-introducirla-en-el-aula/#:~:text=La%20alfabetizaci%C3%B3n%20medi%C3%A1tica%20es%20la,%20reconocer%20la%20publicidad%20nativa.>
 2. <https://www.startgoconnection.es/importancia-de-la-alfabetizacion-digital-en-la-sociedad-actual/>
 3. https://www.es.wikipedia.org/wiki/Alfabetismo_digital#La_brecha_digital

4. <https://ticnegocios.camaravalencia.com/servicios/tendencias/por-que-la-alfabetizacion-digital-es-tan-importante/>
5. <https://www.unir.net/educacion/revista/alfabetizacion-digital/>
6. <https://www.startgoconnection.es/importancia-de-la-alfabetizacion-digital-en-la-sociedad-actual/>
7. <https://www.feandalucia.ccoo.es/docu/p5sd8726.pdf>