

Patricia de-Casas-Moreno
Macarena Parejo-Cuéllar
María del Mar Ávila Vegas

Ciberseguridad y competencias mediáticas en la era digital

Protección, privacidad y ciudadanía digital

Horizontes Universidad

Octaedro

Ciberseguridad y competencias mediáticas en la era digital

Protección, privacidad y ciudadanía digital

Apoyos y agradecimientos:

Esta iniciativa se realiza en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation) - Instituto Nacional de Ciberseguridad (INCIBE) en el proyecto C109/23 «Proyecto estratégico UEx (Escuela Politécnica de Cáceres)-INCIBE». Asimismo, se desarrolla en el marco de Alfamed (Red Interuniversitaria Euroamericana de Investigación en Competencias Mediáticas para la Ciudadanía), con el apoyo del Proyecto I+D «Investigación, diseño e implementación de una propuesta curricular de formación de profesorado en alfabetización mediática en el ámbito euroamericano» de la Convocatoria Proyectos de Generación de Conocimiento 2023 (código PID2023-146288NB-I00), financiado por MICIU (AEI) 10.13039/501100011033 y por FEDER (UE).



Patricia de-Casas-Moreno,
Macarena Parejo-Cuéllar
y María del Mar Ávila Vegas

Ciberseguridad y competencias mediáticas en la era digital

Protección, privacidad y ciudadanía digital

Octaedro

Colección Horizontes Universidad

Título: *Ciberseguridad y competencias mediáticas en la era digital. Protección, privacidad y ciudadanía digital*

Primera edición (papel): febrero de 2026

Primera edición (PDF): noviembre de 2026

© Patricia de-Casas-Moreno, Macarena Parejo-Cuéllar y María del Mar Ávila Vegas

© De esta edición:
Ediciones OCTAEDRO, S.L.
C/ Bailén, 5 – 08010 Barcelona
Tel.: 93 246 40 02
octaedro@octaedro.com
www.octaedro.com



Esta publicación está sujeta a la Licencia Internacional Pública de Atribución/Reconocimiento-NoComercial 4.0 de Creative Commons. Puede consultar las condiciones de esta licencia si accede a:
https://creativecommons.org/licenses/by-nc/4.0/

ISBN (papel): 978-84-1079-230-
ISBN (PDF): 978-84-1079-231-9

Maquetación: Fotocomposición gama, sl
Diseño y producción: Octaedro Editorial

Publicación en acceso abierto - *Open Access*

Sumario

Prólogo 9
Dr. Ángel Hernando Gómez

1. Competencia mediática y digital en la sociedad hiperconectada 13

2. Ciberseguridad y protección en el entorno digital 25

3. Fraudes en la red y seguridad digital a través de la alfabetización mediática 37

4. Ciudadanía digital: Responsabilidades, derechos y alfabetización crítica 49

5. Competencia mediática y ciberseguridad en el futuro de internet 63

6. Conclusiones y recomendaciones 77

7. Referencias bibliográficas 83

Prólogo

Dr. Ángel Hernando Gómez
Catedrático de Psicología
Universidad de Huelva

El mundo de hoy en día se caracteriza por la velocidad y la interconexión. Sin duda, la irrupción de internet, así como las redes sociales y las tecnologías digitales, ha conseguido transformar los diferentes contextos, pero, sobre todo, en el ámbito de la comunicación y las relaciones. Este cambio de paradigma ha dado lugar a una sociedad hiperconectada, donde el flujo informativo toma un rol importante debido a la actualización constante de información y por la integración en gran parte de la tecnología en nuestra vida cotidiana.

En este escenario, que hemos argumentado, la ciberseguridad ya no es solo un tema técnico, sino que se convierte en un desafío social. Por ejemplo, la protección de los datos, la privacidad de los usuarios y la actitud crítica de la ciudadanía (ahora digital) se han alzado como dimensiones esenciales para garantizar una sociedad democrática, el ejercicio responsable de la comunicación y la defensa de los derechos fundamentales de cualquier ciudadano. En este sentido, la presente obra nace para dar respuestas a estas inquietudes. Su finalidad, además de describir los retos de la era digital, es ofrecer las claves y estrategias para abordar este contexto mediado por las tecnologías con ayuda de las competencias mediáticas y digitales. A lo largo de las siguientes páginas, las autoras pretenden dar un enfoque innovador, apostando por que los ciudadanos sean capaces de convertirse

en usuarios activos y se puedan desenvolver de manera segura y ética.

Entre los aportes más llamativos hay que destacar la relación estrecha que establecen tres términos, que serán los ejes vertebrales de toda la obra: la ciberseguridad y las competencias mediáticas y digitales. El primero de los conceptos ha sido analizado desde un punto de vista informático, mientras que los otros dos conceptos se han desarrollado desde una mirada educomunicativa, donde la educación y la comunicación colaboran de forma estrecha para brindar lo mejor de ambas áreas académicas. La validez de este binomio está atestiguada por una sociedad que sea capaz de analizar la información, detectar noticias falsas o bulos (desinformación) y comprender las implicaciones éticas de la distribución de sus propios mensajes.

El libro tiene un total de cinco capítulos, a través de los cuales se realiza un extenso recorrido para tener una visión amplia sobre la materia de estudio seleccionada. De este modo, el primer capítulo asienta las bases teóricas de la competencia mediática y digital, analizando cómo el empleo de internet ha cambiado los hábitos de consumo, los valores y las relaciones. El segundo capítulo recoge los retos del entorno digital, tratando temas como la desinformación y la privacidad. El tercer capítulo aborda los fraudes en la red, poniendo hincapié en la necesidad de desarrollar una adecuada alfabetización mediática para evitar manipulación y fraudes a través de estrategias educativas, que fortalezcan la educación y la seguridad digital. El cuarto capítulo se centra en la ciudadanía digital y en sus derechos y responsabilidades desde la ética. Por último, el quinto capítulo proyecta una mirada más allá del presente, explorando los desafíos emergentes propiciados por las tecnologías. La inteligencia artificial (IA), el *big data* o la automatización de los procesos obligan a establecer estrategias sólidas de ciberseguridad.

Por otro lado, la obra finaliza con un apartado de conclusiones y recomendaciones. Este punto no solo se limita a exhibir un listado de buenas prácticas, sino que, a partir de un decálogo diseñado de forma minuciosa, se plantean las líneas de acción para la educación en este ámbito. El planteamiento de las auto-

ras queda confirmado en las conclusiones, destacando que la ciberseguridad debe comprenderse con ayuda de la competencia mediática y digital, ya que son pilares fundamentales para conseguir una sociedad que apueste por la inclusión y la defensa de los derechos digitales.

Más que una estructura temática, esta obra constituye un proyecto que aboga por la reflexión y la acción. El lector de estas páginas podrá deleitarse con la combinación del rigor académico y, además, un enfoque práctico. Cada capítulo está diseñado con una lógica secuencial para que sea útil para investigadores, especialistas, docentes, estudiantes, entre otro público objetivo de interés. Asimismo, esta obra se identifica por su visión integradora e interdisciplinar, ofreciendo una hoja de ruta para comprender los retos y oportunidades de los hábitos digitales.

Para concluir, es importante señalar que la seguridad en internet es una condición necesaria para garantizar el derecho a la información, la privacidad y la participación ciudadana. Por lo tanto, la lectura de este libro, sin duda, no solo va a ampliar el conocimiento de los lectores, sino que deja un mensaje evidente: la ciberseguridad es, en última instancia, un ejercicio de la ciudadanía. Y la ciudadanía, para ser óptima, debe ser mediática, crítica y digital.

1

Competencia mediática y digital en la sociedad hiperconectada

En un mundo identificado por la revolución digital, la sociedad actual se caracteriza por estar hiperconectada, y transforma continuamente las formas de comunicación, información, trabajo y relaciones. Esta nueva realidad insta al desarrollo de competencias mediáticas y digitales como instrumentos necesarios para conseguir que la ciudadanía sea activa, crítica y responsable en un entorno digitalizado. La digitalización, además de ofrecer oportunidades únicas para acceder a una información más detallada y actualizada, permite hacer partícipe a la ciudadanía en este ecosistema protagonizado por las tecnologías. No obstante, también ofrece desafíos éticos, informativos y educativos, los cuales deben ser revisados desde una perspectiva crítica y multidisciplinar (Area y Pessoa, 2012).

En palabras de Ferrés y Piscitelli (2012), las competencias mediáticas y digitales no solo están vinculadas con el uso técnico de las tecnologías. Más bien, se centran en desarrollar la capacidad para comprender, analizar críticamente y producir contenidos mediáticos en múltiples formatos y plataformas. En este punto, la alfabetización mediática e informacional (AMI) desempeña un papel fundamental para que la ciudadanía sea capaz de ejercer su pleno derecho en la era digital. Por su parte, Aparici y García-Marín (2018) manifiestan que la competencia mediática supone una alfabetización que va más allá de saber usar dis-

positivos, ya que, además, se trata de comprender los lenguajes mediáticos, identificar aquellas intenciones persuasivas y promover la autonomía informativa del ciudadano.

En relación con estas ideas, Ruiz (2023) indica que la competencia mediática se encuentra muy vinculada con la seguridad digital, ya que la exposición constante a plataformas digitales conlleva riesgos para la privacidad, la protección de datos y la integridad digital del usuario. Por tanto, la competencia mediática actual debe integrar habilidades para identificar amenazas digitales, gestionar la privacidad y ejercer un consumo responsable y seguro de la información.

Con la llegada de la revolución 4.0, caracterizada por la digitalización, las transformaciones han afectado a múltiples dimensiones, tanto en el ámbito físico como, por ejemplo, en la robótica, el internet de las cosas (IoT), etc., así como en el ámbito digital con la inteligencia artificial (IA), la cadena de bloques (*blockchain*) o la realidad virtual y aumentada. Además, se han reconfigurado los espacios de comunicación y entretenimiento mediante plataformas digitales (Schwab, 2024). Sin duda, este desarrollo tecnológico ha supuesto importantes desafíos para la privacidad. La recolección masiva de los datos personales por parte de las empresas y los proveedores de servicios ha puesto en jaque la protección de la información personal, manifestando la necesidad de reforzar las medidas de seguridad y transparencia en el manejo de los datos (Isaak y Hanna, 2018). De este modo, la alfabetización digital se convierte en una necesidad debido a que esta debe contemplar la privacidad como una competencia básica. Sin ella, la ciudadanía está expuesta a manipulaciones y vulneraciones de derecho (Parcerisa et al., 2024).

El presente capítulo aborda el desarrollo conceptual y práctico de la competencia mediática y digital, y analiza su evolución teórica, su relación con conceptos claves como la ciberseguridad y ciudadanía digital, así como sus implicaciones en los usos de internet. Además, a lo largo de las siguientes páginas se abordarán temas como las brechas digitales, los impactos de las redes sociales en sus diferentes ámbitos, así como la necesidad de polí-

ticas inclusivas y educativas, que garanticen el acceso equitativo y seguro al entorno digital.

1.1. Fundamentos teóricos para la adaptación al entorno digital

El concepto de competencia, dentro del ámbito educativo y comunicativo, ha sido desarrollado en las últimas décadas. La Unesco (2011a), por ejemplo, señala que esta se entiende como una combinación de conocimientos, habilidades, actitudes y valores que permiten a los individuos desenvolverse de forma eficaz en contextos diferentes. En el caso de las competencias mediáticas y digitales, este conjunto de características está orientado a la comprensión crítica de los medios de comunicación y al empleo ético de las tecnologías de la información y la comunicación (TIC).

Investigadores como Buckingham (2019) han destacado que estas competencias deben incluir, además, el reconocimiento de las tecnologías y medios emergentes, identificados por las dinámicas algorítmicas, así como el papel de la inteligencia artificial (IA) en la selección y desarrollo de contenidos. Por su parte, Pérez-Tornero (2013) sostiene que esta competencia debe entenderse como una herramienta de empoderamiento democrático, la cual contribuye a la participación activa y consciente del ciudadano en la esfera pública. La competencia mediática debe contemplar como eje transversal la seguridad digital, incorporando la protección frente a posibles riesgos en línea, la gestión de la privacidad y, además, una actitud ética para fortalecer la resiliencia frente a la manipulación y los ataques informáticos (García-Ruiz, 2023).

Según el Marco Europeo para la Competencia Digital de los Ciudadanos (DigComp) mostrado en la figura 1, la competencia digital abarca un total de cinco áreas centradas en la información y la alfabetización informacional, la comunicación y la colaboración, la creación de contenidos digitales, la seguridad y la resolución de problemas (Carretero et al., 2017). Hay que señalar

que estas áreas de acción no solo dan respuesta a necesidades técnicas, sino también a retos culturales y sociales con la integración en la sociedad digital. Frente a lo expuesto, es importante señalar que una parte esencial del tema tratado es su vinculación con la ciberseguridad. Este concepto es entendido como la capacidad para proteger los dispositivos, los datos personales y la identidad digital frente a los riesgos de internet.

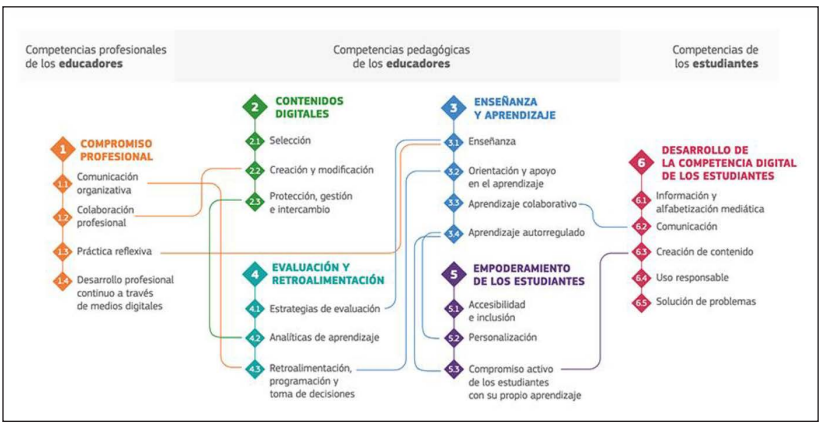

Figura 1. Marco DigComp.

La ciberseguridad está ligada al concepto de ciudadanía digital. Por lo tanto, esto implica ejercer los derechos y deberes ciudadanos en entornos digitales, promoviendo valores como el respeto, la responsabilidad, la privacidad y la participación activa. En este sentido, la ciudadanía digital se alza como un nuevo paradigma que articula las competencias digitales con una visión ética y crítica del entorno tecnológico. Esta afirmación manifiesta que no es suficiente con saber emplear de forma adecuada las tecnologías, sino que también es importante comprender su funcionamiento, sus implicaciones y sus posibles impactos en la sociedad. Desde esta perspectiva, es prescriptivo reforzar una educación mediática y digital, que fomente la reflexión, el pensamiento crítico y la responsabilidad social para y por los medios de comunicación (Ribble, 2012).

Esta innovación basada en las TIC desempeña un papel notorio al facilitar la creación, la modificación, el almacenamiento, la

gestión, la guarda y custodia, y la recuperación de la información mediante el empleo de dispositivos digitales (Chacho-Guambaña et al., 2025). Según González (2024) hay cinco etapas históricas para comprender este tema que nos ocupa en relación con la seguridad digital e informática. Los primeros pasos de la informática se caracterizaban por componerse de sistemas simples debido a la falta de conectividad. Debido al aumento de la digitalización y, por ende, la conectividad, se crean los primeros estándares y protocolos de seguridad, lo que conlleva la preocupación por salvaguardar los datos personales. Con la consolidación de estos avances y la aparición de las primeras amenazas emergentes (*firewalls* y antivirus), surge la necesidad de crear conciencia al respecto. Es entonces cuando se inicia la era de la ciberseguridad, en la que los ataques se vuelven cada vez más sofisticados y se implementan sistemas avanzados de protección. Por último, llega el momento de las tecnologías emergentes y, con ellas, el empleo de la IA, la biometría, entre otras herramientas, para reforzar la protección de datos en un ecosistema cada vez más hiperconectado.

Según Hobbs (2010) y Secker y Morrison (2022), la alfabetización mediática es el proceso de acceso, análisis, evaluación, creación y participación de la ciudadanía con la información desde una mirada tradicional hasta la comprensión crítica de los medios en el contexto digital. Por su parte, autores como Jenkins et al. (2009) han manifestado la importancia de las nuevas alfabetizaciones participativas en la cultura digital, donde las habilidades colaborativas, la apropiación de contenidos y la capacidad de generar conocimiento colectivo son tan importantes como la alfabetización tradicional. Gracias a ello, se evidencia que la función de los usuarios pasivos ha quedado relegada a un segundo plano, dejando paso a los conocidos prosumidores. Estos perfiles se caracterizan por ser usuarios activos en el consumo de información, pero, a la misma vez, crean, generan y propagan contenido en el marco de la cultura participativa e inteligencia colectiva.

En materia pedagógica, Siemens (2004), basándose en las teorías de aprendizaje conectivista, señala la importancia de una

educación digital centrada, además de en los contenidos, en las conexiones, las redes y los flujos de información en los que los individuos están inmersos. Esta perspectiva destaca que el conocimiento tradicional, conocido por su flujo unidireccional, ha cambiado debido a la evolución de los medios de comunicación y, por ende, a la revolución tecnológica propiciada por los avances de la sociedad. Ahora, los flujos comunicativos son bidireccionales y se construyen colectivamente en entornos digitales interconectados, donde el acceso, la evaluación crítica y la curación de información son habilidades esenciales.

Tras todo lo expuesto, se ofrecen una serie de recomendaciones (figura 2) para potenciar la competencia mediática con un enfoque en seguridad digital. Aunque en capítulos posteriores estas líneas argumentales se van a tratar con más rigor y de manera más detallada, es necesario establecer las primeras directrices (Gandini et al., 2025):

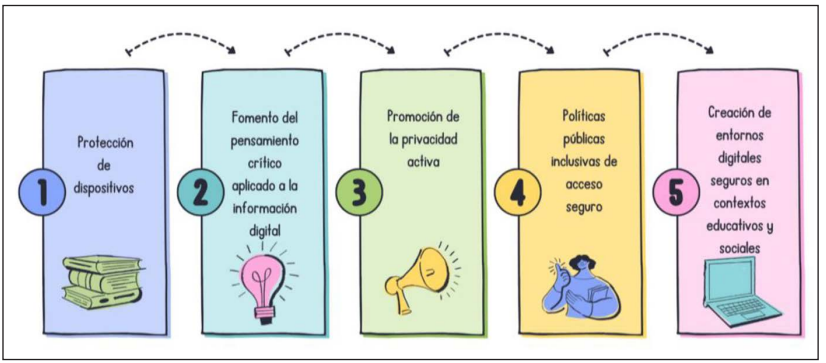

Figura 2. Recomendaciones para potenciar la competencia mediática.

- Educación integral en seguridad digital. Es fundamental incluir en todos los programas educativos módulos específicos sobre este tema. Este aprendizaje debe ser continuo y adaptado a todas las edades y grados de competencia del usuario.
- Fomento del pensamiento crítico aplicado a la información digital. Es urgente desarrollar habilidades para analizar la veracidad y la fiabilidad de las fuentes. Esto incluye comprensión y análisis crítico.

- Promoción de la privacidad activa. Enseñar a los usuarios a manejar herramientas de control sobre sus datos, empoderando a los usuarios para controlar su privacidad.
- Políticas públicas inclusivas de acceso seguro. Es importante garantizar la conectividad y el acceso equitativo, en especial en aquellas poblaciones más vulnerables. Las políticas deben estar orientadas a reducir brechas digitales y a promover el uso crítico y seguro de la tecnología.
- Creación de entornos digitales seguros en contextos educativos y sociales. Hay que incorporar protocolos de actuación frente a incidentes digitales, talleres de sensibilización e implicación directa de los diferentes grupos de interés.

1.2. Usos de internet en la sociedad y sus implicaciones

Con la llegada de la web 2.0, término acuñado por Tim O'Reilly, el papel de internet en los diferentes contextos cotidianos (economía, política, comunicación y educación) de los usuarios ha alcanzado una relevancia sin precedentes (van-Dijk et al., 2018). Esta transformación digital no solo ha traído consigo ventajas relevantes, sino que también ha generado múltiples desafíos para la sociedad, como por ejemplo la aparición de brechas digitales, lo que ha provocado desigualdades sociales (Galperín, 2017). Como indican Fonts-Fernández et al. (2024), estas brechas no solo son de acceso, sino también de uso y competencia, lo que refuerza la necesidad de una correcta alfabetización mediática para reducirlas. Este acceso desigual a las tecnologías y a las competencias digitales se traduce en la dificultad de manejar de manera segura y crítica la información (OECD, 2022). Además, esta brecha se refleja en el desconocimiento o vulnerabilidad frente a los riesgos asociados con la seguridad digital.

Las nuevas generaciones se identifican por ser nativos digitales. Este tipo de personas operan sin fronteras entre lo físico y lo digital (Elizalde, 2020). Asimismo, este paradigma plantea un reto importante para las organizaciones, ya que las amenazas ci-

bernéticas son cada vez mayores y más sofisticadas. Por lo tanto, es urgente crear soluciones de seguridad que protejan los datos sensibles y personales, sin sacrificar la experiencia del usuario o la eficiencia operacional (Madariaga, 2025). En este punto, con el aumento de demanda de información y la necesidad de interactuar, emergen los llamados «ciudadanos digitales» o «ciberciudadanos», que son aquellas personas que emplean las herramientas digitales para ejercer su participación social y política, fortaleciendo sus derechos individuales y colectivos a través de diferentes formas de interacción *online* (Castells, 2015). Este tipo de perfil, además, emerge como una extensión de la ciudadanía tradicional, trasladando al espacio virtual los principios, los derechos y las responsabilidades para que la ciudadanía actúe con ética y seguridad en este tipo de espacios (Ribble, 2012). Hay que destacar que la ciudadanía digital implica no solo la capacidad de participar, sino también la de proteger, de manera individual y colectiva, las prácticas dentro del ecosistema digital, promoviendo prácticas responsables. Debido a ello, se podrá conseguir una participación auténtica y crítica en una sociedad hiperconectada (Deursen y van-Dijk, 2019).

En este orden, hay que hacer especial alusión al uso de internet que hacen los más jóvenes de la sociedad. Para ellos, la red de redes ofrece grandes oportunidades, pero a la misma vez presenta riesgos importantes como la exposición a contenidos inapropiados (ciberacoso, sextorsión, desinformación o contacto con desconocidos). Este tipo de amenazas influye en una población vulnerable que no posee una adecuada alfabetización mediática y digital, y, por ende, el desarrollo de las habilidades necesarias para navegar de manera segura. Unicef (2025) señala la importancia de que los progenitores establezcan una serie de normativas claras y, además, fomenten el diálogo, supervisando, incluso, el uso digital de este colectivo. Es importante fortalecer una educación digital integral que sea capaz de combinar competencias técnicas, pensamiento crítico y valores éticos, empoderando a los menores como ciudadanos críticos responsables. Además, la organización celebra, cada segundo martes de febrero, el Día de Internet Segura para sensibilizar y actuar ante estos

desafíos. Al mismo tiempo, bajo esta premisa impulsa la creación de entornos digitales seguros.

Por otro lado, con el auge de las plataformas y la aparición de las redes sociales, las formas de comunicación han cambiado de forma exponencial, desde el acceso hasta la producción de contenidos. En un principio, las aplicaciones digitales se diseñaron con propósitos claros centrados en facilitar la comunicación interpersonal, fomentar la interacción social o posibilitar la creación y difusión de contenido audiovisual. No obstante, el empleo de los usuarios de estas plataformas y redes ha cambiado, ya que, además de ser espacios de entretenimiento, se han convertido en espacios de aprendizaje donde se desarrollan competencias informales, lo que sustituye la formación tradicional (Jenkins, 2006).

Las múltiples plataformas existentes, como por ejemplo X, Facebook, TikTok, entre otras, han logrado una comunicación global instantánea, pero, a la misma vez, han generado fenómenos como la infoxicación, la viralización de contenidos falsos y la fragmentación del discurso público (McChesney, 2013). Esta realidad obliga a la ciudadanía a desarrollar una mirada crítica sobre los medios, las fuentes de información y los algoritmos. Este último concepto, tal y como señala Gillespie (2014), no se determina como un código matemático neutral únicamente, sino que se comprende como una construcción sociotécnica para priorizar diferentes contenidos en función de los intereses comerciales o ideológicos. La lógica algorítmica, que podemos observar en el ecosistema informativo digital actual, plantea retos importantes relacionados con la diversidad de opiniones, el pluralismo informativo y la formación de las conocidas burbujas de filtro. Estas burbujas son consideradas un estado de aislamiento intelectual producido por los algoritmos (Pariser, 2017).

En el campo político, internet ha facilitado formas de activismo digital, campañas electorales en línea y nuevos canales de participación ciudadana. Sin embargo, en este contexto, se han observado prácticas ilícitas como la manipulación informativa, la desinformación y la polarización de los agentes implicados

(Howard et al., 2018). Por su parte, en el contexto educativo, las TIC han conseguido esbozar un amplio abanico de oportunidades para el aprendizaje personalizado, el acceso a recursos educativos abiertos y el desarrollo de competencias transversales. Sin embargo, debido al auge de las tecnologías en la aplicación pedagógica, se han vislumbrado desigualdades de acceso y uso (van-Dijk, 2006). Sin duda, solo una ciudadanía con alta competencia mediática podrá afrontar la desinformación y fortalecer la democracia (Chalezquer y Salaverría, 2023).

La evolución de los dispositivos tecnológicos ha provocado un aumento en la demanda de conectividad inmediata por parte de la sociedad. Esta popularización de estar conectados constantemente ha generado cambios sociales en lo que respecta a los comportamientos, y se han desarrollado adicciones de índole emocional, cultural e ideológica por el uso incesante de estos dispositivos (Valle-Peris, 2022). A pesar de todas las implicaciones y retos que representa internet, nadie deja de usarlo. En este sentido, el ciudadano digital debe ser conocedor de sus derechos y deberes, sobre todo, en lo que respecta a los tiempos de conexión, usos y empleo de sus datos personales. Sin duda, en un mundo donde la tecnología desempeña un papel hegemónico, el usuario debe aprender a convivir con los medios electrónicos y digitales. En este punto, hay que prestar especial atención a las comunidades virtuales, nichos digitales donde la ciudadanía interactúa sin ningún tipo de formación específica, compartiendo contenido sin establecer regulaciones adecuadas (Bata-Islas et al., 2022).

Esta realidad pone de relieve la necesidad urgente de integrar la seguridad digital como parte intrínseca de la educación digital y mediática con el fin de que los usuarios no solo accedan y produzcan contenidos, sino que también puedan identificar riesgos y proteger sus derechos digitales, contribuyendo a un ecosistema más seguro y confiable (Livingstone et al., 2021b). A continuación, en la figura 3, se indican una serie de recomendaciones de seguridad digital para mejorar la educación y el conocimiento sobre este tema:

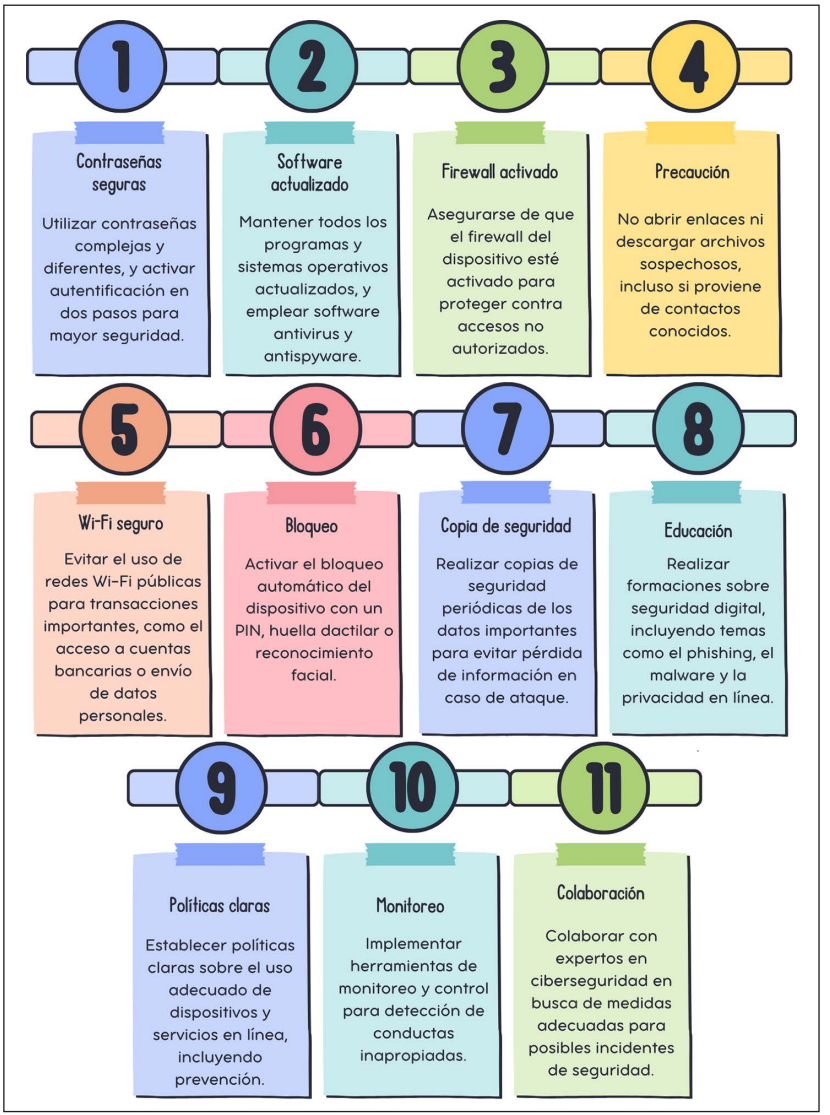

Figura 3. Seguridad digital. Recomendaciones.

Frente a lo expuesto, además, es evidente la importancia de reforzar las políticas públicas y educativas para garantizar la conectividad, así como la promoción del uso crítico, reflexivo y seguro de las tecnologías, lo que fomenta una inclusión digital integral (OECD, 2022).

2

Ciberseguridad y protección en el entorno digital

La ciberseguridad se ha convertido en un pilar imprescindible para conseguir que la ciudadanía se vuelva críticamente responsable, así como capaz de desenvolverse con correcta autonomía en los actuales ecosistemas mediáticos hiperconectados. A pesar de que este ámbito trasciende desde una perspectiva técnica, debido a la convergencia mediática, se ha convertido en un tema social, cultural y político debido a la creciente dependencia de las sociedades contemporáneas de infraestructuras digitales y la multiplicación de interacciones en línea (Bada & Sasse, 2019). En este sentido, es importante comprender las dimensiones de la protección en los entornos digitales con el fin de conocer los riesgos emergentes, la vulnerabilidad de los usuarios, pero, sobre todo, la necesidad urgente de desarrollar competencias mediáticas, que ofrezcan un empleo informado, ético y seguro de las tecnologías de la información y la comunicación (TIC) (Livingstone et al., 2021b).

Según García-Salvador (2022), nuestra presencia en el escenario digital es cada vez más amplia y esto provoca que se genere una ingente cantidad de información, lo que conforma nuestra identidad digital. Esto implica que nuestros datos personales estén expuestos a usos inadecuados, manipulaciones o incluso suplantaciones. De este modo, es imprescindible reforzar la seguridad en línea y establecer mecanismos claros de rendición de cuentas para proteger a los usuarios, garantizando el respeto a

los derechos y libertades fundamentales. Este desafío ha propiciado un intenso conocimiento sobre cómo desarrollar correctos sistemas de identidad digital y por ello existe una propuesta para crear un Marco Europeo de Identidad Digital con la finalidad de impulsar herramientas tecnológicas seguras.

Hay que destacar que la digitalización masiva de los contenidos ha traído consigo un crecimiento desmesurado de la información existente en la red. Además, esto ha provocado un aumento de los riesgos relacionados con la manipulación algorítmica, la desinformación y las violaciones de la privacidad (Tufekci, 2015). En este punto, la ciberseguridad debe comprenderse como una práctica transversal, la cual no solo abarca la protección de datos y sistemas, sino también la promoción de la alfabetización mediática para reconocer y afrontar amenazas múltiples, como por ejemplo aquellas que afectan a la seguridad individual de la sociedad o a la salud democrática de la ciudadanía (McDougall et al., 2018).

En esta línea de estudio, múltiples autores han conceptualizado el término *ciberseguridad* como un conjunto de prácticas socioeducativas y un derecho digital fundamental vinculado a la garantía de un entorno seguro con el uso de las tecnologías, tanto en el ámbito de la protección de datos como en relación con la perseveración de la integridad física y emocional de las personas en línea. También se configura como una dimensión clave de la ciudadanía digital, exigiendo a los usuarios el desarrollo de competencias críticas y de autoprotección para interactuar en entornos hiperconectados (Fuentes, 2024; Delgado et al., 2025).

Es importante remarcar que la transformación digital ha reconfigurado la manera en la que se produce, comparte, circula y consume la información. Debido a ello, el ecosistema mediático actual se caracteriza por ser un escenario en el que la interactividad, la inmediatez y la personalización de los contenidos se han convertido en una ventaja (Couldry y Mejias, 2019). El auge de la demanda por parte de la población también exhibe núcleos de manipulación y control social, y para evitarlo los ciudadanos deben desarrollar habilidades de pensamiento crítico, competencias mediáticas y conciencia sobre términos relacionados

como la huella digital, los derechos digitales y la privacidad en línea (Floridi, 2021a).

Sin duda, es importante reflexionar en materia de ciberseguridad desde dos ámbitos, la comunicación y la educación, con el objetivo de reducir riesgos y a la vez empoderar a la audiencia en un ecosistema primado por la opacidad de los algoritmos y las asimetrías de poder de las grandes corporaciones tecnológicas (Zuboff, 2019). Si somos capaces de conseguir todo lo argumentado, se contribuye a crear una ciudadanía capaz de participar activamente en sociedades digitales, protegiendo su integridad y privacidad, mientras ejercen sus derechos de acceso a la información, libertad de expresión y protección de datos personales (European Commission, 2023a). De este modo, el presente capítulo propone ofrecer una reflexión crítica sobre los riesgos y retos de internet, así como de la necesidad de reforzar la competencia mediática como vía de autoprotección. A su vez, se articulará el análisis de estos riesgos con estrategias de intervención que resulten útiles para la ciudadanía digital.

2.1. Riesgos de internet: Desafíos para una sociedad digital (des)informada

La preocupación por la privacidad en línea ha ganado relevancia en la literatura académica reciente. Algunos estudios señalan que el escaso nivel de alfabetización en privacidad digital entre los usuarios de redes sociales debilita su seguridad informativa y limita su capacidad para tomar decisiones autónomas sobre sus propios datos (Bartsch y Dienlin, 2016; Masur, 2020). Ante esta realidad, se proponen modelos de alfabetización que no solo busquen proteger la privacidad individual, sino también empoderar a las personas para participar activamente en los procesos de transformación social a través de la autodeterminación informacional. Según Martínez et al. (2025), este enfoque permite comprender que la privacidad digital no es solo una cuestión individual, sino un problema de raíz estructural. Además, señala que la vigilancia masiva, la explotación sistemática de datos y el

desequilibrio de poder entre los usuarios y las grandes plataformas tecnológicas configuran un escenario en el que la falta de alfabetización en privacidad agrava las desigualdades existentes en el ecosistema digital.

En este orden, la convergencia mediática y, por ende, digital ha intensificado los desafíos vinculados a la circulación de noticias falsas, la desinformación y la manipulación de los algoritmos. Esto provoca que se convierta en una amenaza latente para la estabilidad democrática y la confianza pública en los medios de comunicación. Debido a este crecimiento, Cantero-de-Julián (2021) afirma que existen los siguientes objetivos tomados en cuenta por las políticas nacionales en materia de ciberseguridad:

- Promover la seguridad y libertad de la ciudadanía en el ciberespacio.
- Reforzar la prevención, la detección, la reacción, el análisis, la recuperación y la respuesta frente a los desafíos de internet.
- Promover campañas de sensibilización para la ciudadanía sobre los riesgos derivados de internet.
- Transformar la ciberseguridad en cultura y conseguir que la ciudadanía comprenda que es un problema de todos.
- Impulsar la seguridad de los sistemas de información y comunicación.
- Proporcionar recursos para combatir los desafíos y fomentar la alfabetización mediática para conseguir una ciudadanía digital.
- Proteger la privacidad e identidad digital de virus, fraudes y bulos.

Frente a lo expuesto, conviene realizar un esbozo sobre los principales riesgos a los que la ciudadanía se enfrenta en el actual ecosistema, caracterizado por la revolución 4.0. En primer lugar, según Tandoc et al. (2018), las noticias falsas o también conocidas como *fake news*, se han convertido en uno de los principales riesgos en ciberseguridad. Estas se pueden definir como información manipulada con el único fin de engañar, captar la atención y obtener beneficios económicos o políticos. La propagación de este tipo de contenidos en las redes sociales y las plataformas digi-

tales se ha visto potenciada en los últimos tiempos debido a que los algoritmos priorizan la viralidad sobre la veracidad del contenido, generando cámaras de eco y burbujas informativas, que, a su vez, refuerzan sesgos y dificultan el discernimiento crítico (Pariser, 2011).

Un estudio realizado por Vosoughi et al. (2018) muestra que este tipo de noticias falsas se difunden rápido y tienen un alcance mucho más alto a través de las redes sociales. Esto es debido a que estas informaciones apelan a las emociones para captar la atención de los usuarios. Este tipo de acciones plantea retos sustanciales para la competencia mediática, ya que requiere el desarrollo de habilidades para analizar y verificar las fuentes, reconocer los sesgos mediáticos e informativos y comprender las lógicas de los algoritmos, condicionantes del consumo informativo (McDougall et al., 2018). Asimismo, las plataformas tecnológicas han sido señaladas por su rol en la amplificación de la desinformación, lo que ha generado tensiones entre la libertad de expresión y la necesidad de garantizar entornos informativos saludables (Gillespie, 2018).

Múltiples son los riesgos, algunos de los cuales se muestran en la figura 4, a los que nos enfrentamos en la actualidad, como la desinformación, el ciberacoso, la suplantación de identidad, los discursos de odio, la manipulación algorítmica, el acceso a contenidos inapropiados, la publicidad encubierta y los riesgos asociados al comportamiento digital. Todos ellos representan riesgos significativos en los entornos digitales. La desinformación se manifiesta en la difusión de noticias falsas y contenidos manipulados que buscan engañar a la ciudadanía, afectando la opinión pública y debilitando la confianza en los medios digitales (Wardle y Derakhshan, 2017). Según Smith et al. (2008), el ciberacoso se define como cualquier forma de acoso o intimidación producido a través de dispositivos digitales, que genera daños psicológicos en las personas que interactúan en los entornos digitales. Por su parte, la suplantación de identidad implica apropiarse de datos personales con el fin de engañar, extorsionar o manipular a las víctimas (Marwick & boyd, 2011).

En otro orden, en relación con los discursos de odio, hay que señalar que este tipo de prácticas cada vez es más frecuente en

los entornos digitales. La falta de regulación efectiva y el anonimato de los usuarios que realizan este tipo de prácticas ilícitas ha conseguido convertirlo en un fenómeno global, lo que ha reforzado la violencia y erosionado la cohesión social (Matamoros-Fernández, 2017). Informes recientes de la Unión Europea (UE) destacan el incremento de contenidos de odio y subrayan la importancia de instaurar políticas de moderación y alfabetización digital para paliarlo (European Commission, 2023a).

Cuando hablamos de la manipulación algorítmica, hay que trasladarse a las redes sociales. Los algoritmos se desarrollan en plataformas como Facebook, TikTok, YouTube, entre otros, y ejercen una función de recomendación, priorizando contenido diseñado para maximizar el tiempo de visualización sin tener en cuenta los impactos de la calidad informativa (Bakshy et al., 2015). Noble (2018) señala que estos algoritmos son capaces de reproducir sesgos raciales y de género, lo que afecta al acceso a información veraz, de calidad y equitativa. Este escenario refuerza la importancia del desarrollo de una correcta alfabetización y selección de contenidos adecuados (Livingstone et al., 2021b).

Por otro lado, hay que destacar que la multiplicidad de contenidos y formas de interacción digital también conllevan otro tipo de riesgos asociados con el contenido y el comportamiento. En cuanto al contenido, el acceso a materiales inapropiados (pornografía, conductas dañinas relacionadas con el suicidio, anorexia, entre otros) supone un peligro, en especial para los más jóvenes (Livingstone et al., 2011). Además, a ello se le suma que la publicidad encubierta o el emplazamiento del producto en entornos digitales influyen de forma persuasiva en los usuarios más vulnerables. Por su parte, los riesgos relacionados con el comportamiento están vinculados, sobre todo, con los jóvenes, ya que pueden ser objeto de prácticas abusivas (ciberacoso, *grooming*, *sexting*, entre otros). Además, este tipo de prácticas merman la salud mental y el bienestar psicológico, social y académico de los usuarios debido al empleo incesante de internet (Kowalski et al., 2014; Nixon, 2014).

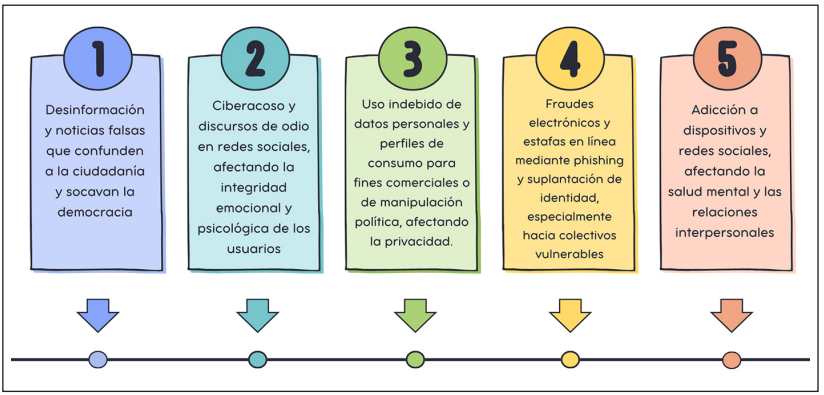

Figura 4. Principales riesgos.

A pesar de que de todos estos riesgos hablaremos con detalle en los próximos capítulos, hay que mencionar que la gestión de los riesgos digitales debe ir acompañada de metodologías y recursos educativos que permitan implicar de forma activa a la ciudadanía, aplicables tanto en espacios formales como informales de aprendizaje.

2.2. Privacidad digital y competencia mediática, estrategias para una navegación segura

La privacidad digital constituye un derecho fundamental para las sociedades hiperconectadas, ya que están muy vinculadas con la protección de la dignidad humana, la autonomía personal y la seguridad (Solove, 2021). No obstante, la complejidad de los entornos digitales y la falta de regularización y transparencia de las plataformas dificultan la gestión de la privacidad por parte de los usuarios, debido a la falta de información sobre cómo se recopilan, procesan y comercializan sus datos (Zuboff, 2019).

En este contexto, conviene revisar el concepto de *big data* en el tema que nos ocupa. Este término se refiere al conjunto de procesos y tecnologías que permiten gestionar y analizar grandes volúmenes de datos (Laney, 2001). Esta capacidad para manejar datos masivos se potencia cuando se combina con técnicas de

inteligencia artificial (IA) y el aprendizaje automático, habilitando predicciones y análisis complejos que pueden transformar múltiples sectores (Mayer-Schönberger y Cukier, 2013).

La huella digital tiene un cometido importante en la vida de los usuarios. Se define como el rastro de datos que un usuario es capaz de dejar al interactuar en línea. Esta huella incluye datos explícitos proporcionados en las redes sociales, así como información pasiva recolectada mediante *cookies* y otras tecnologías de rastreo (Mayer-Schönberger y Cukier, 2013). La gestión de esta huella implica llevar a cabo estrategias de autoprotección como el uso de contraseñas seguras, la revisión de configuraciones de privacidad, el uso de redes VPN y la adopción de buenas prácticas de higiene digital (Bada y Sasse, 2019).

Desde la visión consolidada de las competencias mediáticas, es crucial capacitar a la ciudadanía para comprender los riesgos asociados a la exposición de los datos personales, así como las implicaciones derivadas en términos de vigilancia, discriminación algorítmica y la manipulación (Floridi, 2021a). La protección de la privacidad no puede ser únicamente responsabilidad de los individuos, sino que las instituciones gubernamentales deben reforzar las políticas de regulación para evitar la vulneración de los derechos digitales. Según Ferrés y Piscitelli (2012), las competencias mediáticas deben atender a las siguientes dimensiones, tal como se muestra en la figura 5.

La protección de datos personales hace referencia a un conjunto de derechos y obligaciones destinados a proteger y salvaguardar la información personal de las personas frente a prácticas ilícitas, garantizando que los datos sean tratados de manera correcta, leal y transparente a través de reglamentos adecuados, como por ejemplo el Reglamento General de Protección de Datos, UE 2016/679. Este reglamento establece que el ciudadano tiene derecho a conocer, acceder, rectificar y suprimir sus datos personales, así como a limitar su tratamiento. En este punto entra en juego el derecho al olvido digital, entendido como el derecho que permite a las personas solicitar la supresión de sus datos personales en internet cuando resulten inadecuados, irrelevantes o ya no sean necesarios (Cobeñas, 2022).

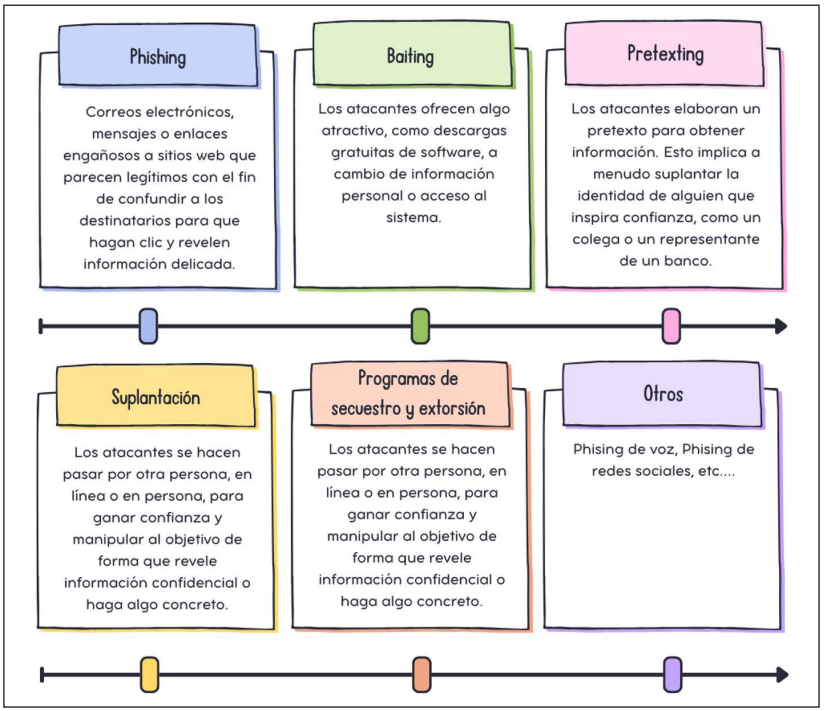

Figura 5. Recomendaciones sobre competencias mediáticas.

En el actual panorama surgen retos éticos, legales y sociales. Según Mosco (2017), es importante establecer normas y regulaciones internacionales que protejan la privacidad, eviten la vigilancia abusiva, promuevan la equidad y orienten el uso ético de las tecnologías digitales. La UE ha impulsado una robusta y sólida política de ciberseguridad para hacer frente a las actividades ilegales en internet, protegiendo a usuarios y plataformas de información. Entre sus principales iniciativas conocidas se encuentran el programa *Safer Internet Plus* (2005-2008), centrado en proteger a los usuarios frente a contenidos nocivos, y su continuación *Safer Internet* (2009-2013), con foco en la seguridad infantil en línea. De forma paralela, se creó la Agencia Europea de Ciberseguridad (ENISA) en 2004, con el objetivo de reforzar la ciberseguridad en Europa a través de certificaciones, análisis de riesgos y cooperación entre Estados. Por su parte, España también ha avanzado en este ámbito. En el año 2013 presentó su primera Estrate-

gia Nacional de Ciberseguridad. Asimismo, creó el Consejo Nacional de Ciberseguridad en 2014, responsable de coordinar las acciones a escala estatal. Desde entonces, el marco normativo ha evolucionado con la reforma del Esquema Nacional de Seguridad (2015) y el Real Decreto-ley 12/2018, que refuerza la protección de sectores estratégicos. La Estrategia de Seguridad Nacional de 2017 y la Estrategia Nacional de Ciberseguridad de 2019 consolidan la importancia de la ciberseguridad como eje fundamental de la seguridad del país (García-Salvador, 2022).

Por otro lado, el Reglamento General de Protección de Datos (GDPR) establece en el ámbito europeo un marco robusto para la protección de los datos personales, ofreciendo a los ciudadanos derechos como el acceso, la rectificación, la supresión, la portabilidad de sus datos y la posibilidad de oponerse a ciertos tratamientos. Este marco tiene la finalidad de equilibrar la innovación tecnológica con la protección de la privacidad, promoviendo la transparencia y la rendición de cuentas en las organizaciones que manejan los datos personales de los usuarios (European Union, 2016). Por su parte, a escala nacional, España contempla múltiples legislaciones que se han alineado con el GDPR, incorporando marcos específicos encargados de regular la protección de datos y la privacidad en los entornos digitales, como por ejemplo la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, que refuerza los derechos de los usuarios y establece obligaciones para las plataformas y proveedores de servicios digitales (BOE, 2018).

La vertiginosa y veloz transformación tecnológica no solo afecta a la ciudadanía, sino también a las instituciones y organismos reguladores. Estos se enfrentan a una brecha digital relacionada con el tiempo necesario para comprender estas nuevas realidades con el fin de adaptar sus marcos normativos (Vera-Baceta et al., 2022). En este sentido, Naciones Unidas (2019) señala que muchas de las leyes ya dictadas pertenecen a una era predigital, lo que dificulta su aplicación en el contexto actual, en el que el entorno digital se ha visto expuesto a modificaciones. Estos cambios generan conflictos, lo que exige la reinterpretación jurídica y la actualización de las leyes existentes. Ante este desafío, el

Gobierno de España (2021) presentó en julio de 2021 la Carta de Derechos Digitales (https://bit.ly/4o93LTb), un documento pionero que, aunque sin valor normativo, establece principios clave para orientar futuras legislaciones. Su objetivo es garantizar derechos individuales y colectivos en el entorno digital, incluyendo la libertad, la igualdad, la participación ciudadana y los derechos laborales. No plantea nuevos derechos fundamentales, sino la reinterpretación de los existentes en contextos digitales.

Atendiendo a lo narrado, es indispensable que la educación en privacidad digital se integre de manera transversal junto con programas de alfabetización mediática, dotando a los usuarios de herramientas críticas y prácticas para gestionar su identidad digital, proteger sus datos personales y ejercer sus derechos en línea (Livingstone et al., 2021b). Además, se requiere una aproximación sistémica que combine legislación, competencias mediáticas y responsabilidad de las plataformas para crear estrategias de navegación segura.

La identidad digital es entendida como el conjunto de datos que identifican a un individuo en el entorno en línea. La protección de esta identidad implica la implementación de tecnologías robustas (contraseñas seguras, cifrado, etc.), así como la responsabilidad individual en la gestión de la información personal. La seguridad informática es una disciplina dinámica que busca garantizar que las organizaciones y usuarios alcancen sus objetivos minimizando los riesgos asociados con las TIC (Areitio, 2008).

En definitiva, la ciberseguridad se convierte en un elemento indispensable para la protección de los derechos humanos en la era digital, reforzando la autonomía de los individuos y fortaleciendo las democracias contemporáneas. La interconexión de las tecnologías digitales con la vida cotidiana tiene una doble cara: por un lado, ofrece nuevas posibilidades de aprendizaje, participación y desarrollo; y, por otro lado, demanda una comprensión crítica, medidas de protección y un compromiso ético para salvaguardar los derechos y el bienestar de los usuarios en el mundo digital.

3

Fraudes en la red y seguridad digital a través de la alfabetización mediática

El constante y fácil acceso a la red de redes nos ha conducido a nuevas formas de comunicación, llenas de posibilidades tales como comprar por internet, vender ropa de segunda mano, revisar nuestras cuentas bancarias o acceder y firmar documentos oficiales y un largo etcétera (Ramasundaram et al., 2023). Sin embargo, estas opciones que nos brinda el nuevo contexto digital no están exentas de peligros. Internet también plantea una serie de retos y amenazas, entre los cuales los fraudes ocupan un lugar destacado. Desde timos en línea hasta el robo de información personal, los fraudes digitales se han vuelto cada vez más sofisticados. Por eso, Vílchez-Vera et al. (2025, p. 188) resaltan la importancia de la alfabetización digital y mediática «como un proceso necesario para el acceso universal a la información y el conocimiento, así como para la construcción de un mundo interconectado».

Estos enfoques son los que ayudarán a los usuarios a comprender, analizar, y evaluar de forma crítica los contenidos digitales, identificar posibles riesgos en línea y actuar de manera segura y ética en entornos digitales. Precisamente, estos autores (Vílchez-Vera et al., 2025) se han preocupado por testar y probar distintos prototipos, que, si bien están destinados a personas vulnerables como pueden ser los mayores, resultan de enorme utilidad, ya que incluyen su aplicación práctica por etapas, la organización educativa para personas sin experiencia digital y la

evaluación continua del aprendizaje. A continuación, en la figura 6, se realiza un resumen de los ocho modelos propuestos por estos investigadores con enfoques distintos y que van desde el pensamiento crítico al *storytelling*, la autenticidad, el gobierno electrónico, la lucha contra las *fake news*, la didáctica educativa, el desarrollo evolutivo, hasta una visión integral.

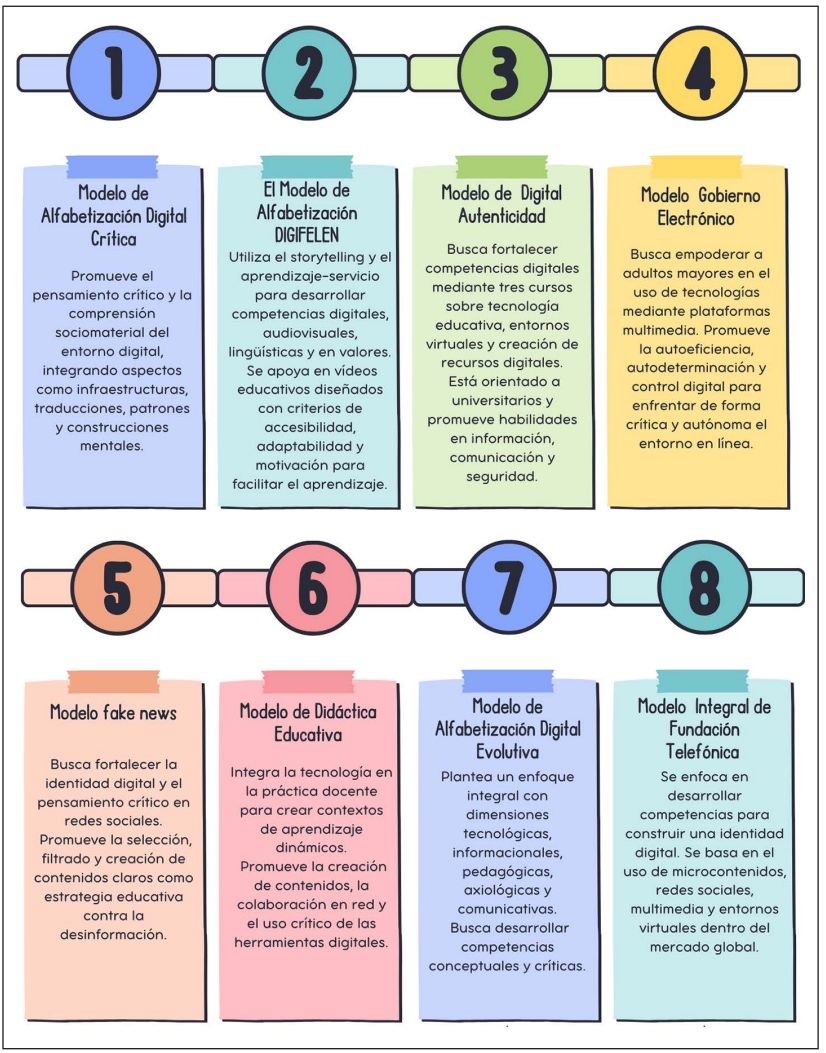

Figura 6. Modelos de Vílchez-Vera et al. (2025).

Con independencia del modelo educativo adoptado, resulta evidente que en la era digital la ciudadanía está expuesta a una cantidad abrumadora de información. Esto conlleva riesgos significativos, ya que, como afirman Ruiz et al. (2025, p. 5), «los usuarios se ven expuestos a información falsa o engañosa», frente a la cual deben actuar con pensamiento crítico y capacidad para identificar posibles manipulaciones informativas.

A lo largo del año 2024, el Instituto Nacional de Ciberseguridad (INCIBE, 2025) gestionó cerca de diez mil incidentes de ciberseguridad. Esta cifra representa un aumento del 16,6 % con respecto al año 2023. De estos, el 67,6 % (65 808 incidentes) afectaron a la ciudadanía y el 32,4 % (31 540 incidentes) a empresas, incluyendo pymes, micropymes y autónomos. Además, este problema no puede abordarse desde una perspectiva edadista ni centrarse solo en determinados grupos etarios. Diversos estudios demuestran que las víctimas de ciberataques y delitos informáticos pertenecen a distintas franjas de edad. Por ejemplo, el *Informe sobre Cibercriminalidad en España*, elaborado por el Ministerio del Interior (2023), señala que el fraude informático es la modalidad delictiva con mayor incidencia en todos los grupos de edad, siendo especialmente elevada en personas mayores de 65 años, que registran los porcentajes más altos.

Otras fuentes muestran una realidad diferente. Según la encuesta sobre *Inseguridad en la red* del Centro de Investigaciones Sociológicas (CIS) (2024), el grupo más afectado por estafas o intentos de estafa en línea corresponde a personas entre 25 y 34 años, con un 61,3 %. En contraste, los mayores de 65 años son quienes menos afirman haber sufrido este tipo de delitos, con solo un 23,8 %. Un reportaje de Maldita.es (2025) señala que esto en parte se puede deber al temor que sienten a ser estafados y que los lleva a ser más cautos en la red de redes.

Además de la formación, algunos autores como Mendoza-Michilot et al. (2025) hablan de la importancia que para propiciar lo que denominan «la ciberhigiene» tienen los medios de comunicación, a los que no es posible dejar a un lado en toda esta contextualización. Del mismo modo, abogan por diseñar «una estrategia informativa mínima que la prensa podría consi-

derar en su quehacer cotidiano para orientar a las personas sobre cómo prevenir, denunciar y hallar una solución a los fraudes informáticos». Esto, sin obviar que son plataformas de denuncia que pueden dar voz a la vez que concienciar con la exposición de casos reales de fraude a otras personas.

Con este contexto ya descrito, el presente capítulo abordará cuestiones como los engaños en la red y las posibilidades y técnicas para detenerlos. Desde una óptica crítica y responsable, abogando por la formación tecnológica, pero también de alfabetización digital, se reflexiona sobre los juegos psicológicos y cómo evitar caer en las redes de estos delincuentes.

3.1. Fraudes en internet y estrategias de detección

A la hora de hablar de fraudes en internet cobra una especial relevancia el término *ingeniería social*. Y es que, hoy en día, «los ciberdelincuentes han dejado de enfocarse en ataques masivos y genéricos, y ahora priorizan estrategias más dirigidas y personalizadas» (González-Hugo y Quevedo-Sacoto, 2025, p. 16). El Consejo de la Unión Europea (2025) define esta práctica como una estrategia utilizada por individuos o grupos de ellos para manipular y engañar a las personas con la intención de que revelen información delicada o lleven a cabo acciones que pongan en riesgo su seguridad. Se basa en la psicología y el comportamiento humano más que en conocimientos técnicos.

Estos ataques han evolucionado de una manera tan significativa que, en ocasiones, cuesta mitigar y, lo que es más importante, detectar. La inteligencia artificial (IA), el *big data* y el aprendizaje automático han contribuido a ello, y, lo que es más preocupante, algunos autores consideran que, con el paso del tiempo, se intensificarán (Pochmara y Świetlicka, 2024).

Para algunos expertos la ingeniería social es el arte del engaño y adquiere varias formas para lograr de la ciudadanía caiga en sus perversas intenciones. Según información publicada por el Instituto Nacional de Ciberseguridad (INCIBE, 2019), las técnicas de ingeniería social más empleadas para manipular a sus víctimas y

lograr que estas revelen información confidencial o realicen acciones perjudiciales son las que se mencionan en la figura 7. Aunque existen múltiples variantes, la mayoría de estos ataques se fundamentan en una serie de principios psicológicos básicos:

- Respeto a la autoridad. Las personas, tanto en el entorno laboral como en su vida cotidiana, tienden a obedecer a figuras de autoridad. Los atacantes se aprovechan de esta predisposición suplantando a superiores jerárquicos o incluso a representantes de las Fuerzas y Cuerpos de Seguridad del Estado.
- Voluntad de ayudar. En ambientes profesionales, es común que los empleados estén dispuestos a colaborar y ayudar a sus compañeros. Los ciberdelincuentes explotan esta actitud haciéndose pasar por empleados de la empresa o técnicos informáticos que necesitan acceso para instalar herramientas, que en realidad son sistemas de control remoto no autorizados.
- Miedo a perder un servicio. Esta técnica es frecuente en campañas de *phishing*. Se basa en alarmar al usuario con mensajes que advierten de accesos sospechosos, cambios de política o amenazas de suspensión del servicio, con el fin de inducirle a ingresar en páginas fraudulentas y entregar sus credenciales.
- Presión social o miedo al rechazo. Algunos ataques se apoyan en el temor de los usuarios a perder su reputación o no ser aceptados por la sociedad. Un ejemplo son los correos de sextorsión, donde se amenaza con divulgar supuestos vídeos íntimos que, en realidad, no existen.
- Ofertas gratuitas. Este tipo de engaño se basa en ofrecer productos o servicios «gratis» a cambio de información personal. Suelen difundirse a través de ventanas emergentes en webs poco fiables, o mediante mensajes en redes sociales y aplicaciones de mensajería.

Un ciberataque de esta categoría puede venir disfrazado de diferentes formas. Desde un correo electrónico que parece proceder de una persona de confianza solicitando información sensible hasta un mensaje de texto supuestamente de nuestra entidad bancaria en el que nos advierte que han intentado cambiar las claves y nos ofrece un enlace sospechoso. El objetivo no es otro que ob-

tener contraseñas, acceso a cuentas bancarias, números de la Seguridad Social... En este sentido, las técnicas utilizadas pueden ser muchas. Una de las más habituales es el *phishing*. Pueden ser de voz, textos masivos, personalizados o a través de redes sociales, por ejemplo, pero el *modus operandi* es el mismo: confundir pareciendo legítimos para obtener datos personales que después son utilizados en su propio beneficio (Mayo-del-Amo, 2022).

En este sentido, una de las amenazas más peligrosas es el *ransomware*. Se trata de un tipo de *malware* que retiene como rehenes los datos confidenciales o el dispositivo de una víctima, amenazando con mantenerlos bloqueados, o algo peor, a menos que la víctima pague un rescate al atacante (Kosinski,2024). Hernández-Morales y González-Brito (2023, p. 525) hablan de que en relación con esta técnica ha aumentado la doble y triple extorsión en ataques de *ransomware*, donde además de cifrar datos se amenaza con filtrar información o realizar nuevos ataques. También se ha expandido el modelo de *ransomware* como servicio, facilitando su uso incluso a delincuentes con poca experiencia técnica. Junto a esta modalidad, encontramos otras fórmulas como los programas de secuestro y extorsión, en los que podemos recibir una amenaza de revelar información delicada sobre la víctima, que puede ceder por miedo, o una llamada de alguien que suplanta su identidad (Unión Europea, 2025).

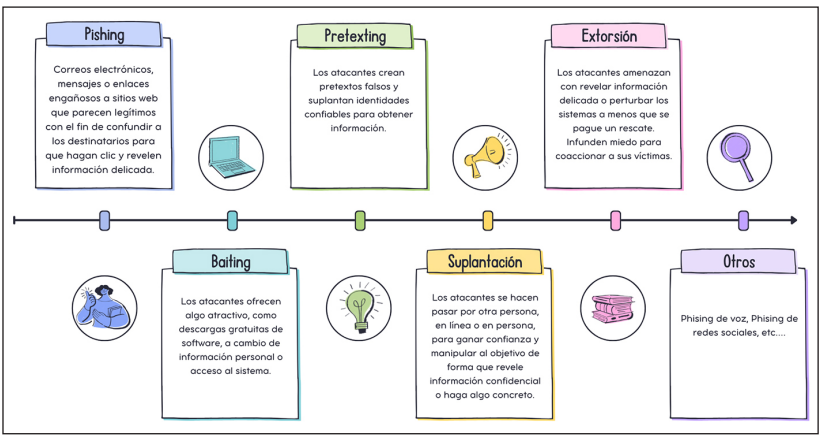

Figura 7. Técnicas de ingeniería social. Consejo de la Unión Europea (2025).

Además, no podemos obviar otra serie de delitos como el *doxing*, que es la técnica de desvelar información personal sin consentimiento y que viola la intimidad (Puican-Ordoñez, 2024) y el *sexting*. Esta última ha sido estudiada a fondo (Chacón-López et al., 2019; Aránguez-Sánchez y Olariu, 2021; Giménez-Gualdo, 2022; Hervás-Paredes, 2023; Yagos-Estrada, 2024; etc.), sobre todo, porque en muchas ocasiones implica a menores. Un estudio de la Universidad de Granada (Chacón-López et al., 2019) revela que uno de cada tres estudiantes admite practicar *sexting*, a pesar de los riesgos personales y profesionales que implica. En muchos casos lo hacen para explorar o consolidar vínculos de amistad, aunque no siempre son conscientes de que, al perder el control de las imágenes, pueden exponerse a situaciones de extorsión o a la difusión no consentida de sus fotografías. Esto puede acarrear graves consecuencias emocionales, psicológicas y legales, e incluso provocar situaciones extremas, ya que la divulgación de imágenes íntimas sin consentimiento expone a las personas a humillaciones y vejámenes (Pérez-Alarcón, 2023, p. 1).

Para aprender a detectar este tipo de fraudes hay múltiples guías y herramientas. En concreto, el INCIBE (2019), en un artículo de su blog titulado *Busca otro al que engañar, yo no voy a picar,* advierte que, en líneas generales, los atacantes suelen enviar mensajes que aparentan provenir de entidades legítimas, como bancos o empresas conocidas, con el objetivo de engañar al destinatario y obtener información confidencial, como contraseñas o datos bancarios. Sin embargo, este tipo de mensajes suelen tener señales claras de alerta, como direcciones de correo sospechosas, saludos genéricos y un tono urgente que busca provocar una reacción rápida. También es común que incluyan enlaces fraudulentos o archivos adjuntos maliciosos.

La detección y prevención del fraude en línea requiere una combinación de estrategias tecnológicas, individuales e institucionales. Según López-Sánchez (2019), es fundamental implementar sistemas proactivos como filtros de correos electrónicos capaces de identificar mensajes sospechosos mediante el análisis de enlaces, remitentes y patrones de contenido; herramientas de

aprendizaje automático para reconocer comportamientos anómalos de usuarios y sitios web; autenticación de dominios, y protocolos de seguridad que validen la legitimidad de las recepciones. También, navegadores con alertas tempranas que adviertan sobre sitios potencialmente peligrosos. Ello sin olvidar la importancia de que la educación y concienciación de los usuarios permite reconocer señales típicas de fraude, como errores gramaticales, solicitudes urgentes de información personal o URL alteradas. De forma complementaria, Morales-Ramírez (2025) enfatiza que la prevención del fraude también implica acciones individuales como proteger la información financiera con tarjetas exclusivas para compras en línea, activar alertas bancarias, navegar en sitios HTTPS, mantener dispositivos actualizados con antivirus y habilitar autenticación en dos pasos, así como verificar la autenticidad de páginas y ofertas y limitar la entrega de datos personales. En lo institucional, recomienda implementar sistemas de vigilancia y análisis de comportamiento, utilizar inteligencia artificial para detectar fraudes en tiempo real, fomentar la colaboración entre gobiernos, empresas y usuarios, y desarrollar campañas de concienciación que fortalezcan la cultura de ciberseguridad. En línea con esto, INCIBE (2025) recomienda ser especialmente cauteloso con correos inesperados, evitar hacer clic en enlaces dudosos, no descargar archivos adjuntos de origen desconocido y no responder a mensajes sospechosos. En caso de caer en una trampa, es crucial cambiar contraseñas, activar la autenticación en dos pasos y, si se descargó un archivo, realizar un análisis con un antivirus y desconectar el equipo de la red para prevenir mayores daños. Por último, el organismo resalta la importancia de la concienciación y la formación continua de los usuarios, sobre todo en entornos corporativos, como medida preventiva ante este tipo de amenazas. En conjunto, estas recomendaciones ofrecen un enfoque práctico y multidimensional para detectar y prevenir fraudes en internet.

3.2. Herramientas y estrategias para una ciudadanía crítica y segura

Una de las principales herramientas para fortalecer la ciberseguridad ciudadana es la alfabetización digital, entendida como la capacidad de utilizar de forma segura y efectiva las tecnologías de la información. Sin embargo, esta formación debe ir acompañada del sentido común y pensamiento crítico. Esta combinación será la que logrará promover el desarrollo de competencias digitales sólidas que no solo incluyan el manejo técnico de herramientas, sino también la capacidad de reflexionar de forma crítica sobre el uso de la tecnología, evaluar la veracidad de la información y reconocer situaciones de riesgo en línea (Cruz y Chicaiza, 2025).

Ya no basta con instalar un antivirus o evitar sitios web sospechosos. La protección en línea debe ir acompañada de competencias clave como el pensamiento crítico, la verificación de la información, la alfabetización en seguridad digital, el cuidado de los dispositivos y un uso responsable de las redes sociales (Organización de los Estados Americanos y Twitter, 2021). En un entorno donde los ciberdelincuentes utilizan técnicas cada vez más sofisticadas para engañar a los usuarios, como correos electrónicos falsos, mensajes alarmantes o anuncios manipulados, saber detenerse a pensar antes de hacer clic se convierte en un primer acto de defensa. Una ciudadanía que piensa de forma crítica es menos vulnerable a fraudes, estafas y manipulaciones emocionales, así como más capaz de tomar decisiones seguras.

A pesar de la relevancia de los programas educativos en ciberseguridad, como la guía *La ciberseguridad al alcance de todos* (INCIBE, 2022), que ofrece instrucciones claras para proteger dispositivos, crear contraseñas seguras, activar la verificación en dos pasos y navegar de forma segura, así como consejos prácticos para detectar fraudes, noticias falsas y proteger la privacidad en línea, estudios como el de Beltrán-Muñoz (2024) muestran que una parte significativa de la población aún carece de la formación necesaria. Otros autores destacan la necesidad de diseñar e implementar programas que involucren a toda la comunidad

educativa y aborden problemas como el consumo de pornografía y la seguridad en línea (Aznar-Martínez et al., 2024). En este sentido, Pacheco et al. (2024) proponen la gamificación, a través de simulaciones, desafíos y competencias que permiten a los estudiantes practicar habilidades en entornos controlados, como una estrategia efectiva para enseñar alfabetización en ciberseguridad de manera práctica y atractiva.

Algunas soluciones prácticas pasan por los consejos que ofrecen la Agencia Española de Protección de Datos (AEPD) y el Instituto Nacional de Ciberseguridad (INCIBE) (s. f). Uno de los principales mensajes que ofrecen estas entidades parece obvio pero es preciso recordar: existe la necesidad de proteger de forma adecuada nuestros dispositivos electrónicos, ya que en ellos almacenamos gran cantidad de información sensible: desde contactos y fotos hasta documentos, credenciales de acceso y datos bancarios. Para ello, advierten de la importancia del uso de contraseñas, cifrado de datos, instalación de antivirus y precaución al conectarse a redes wifi públicas.

Es cierto que la gestión de contraseñas es un tema complejo, pero resulta fundamental no reutilizarlas en distintos servicios y crearlas con un alto nivel de seguridad, combinando letras, números y símbolos. Asimismo, se recomienda el uso de gestores de contraseñas para quienes tienen dificultades para recordarlas, así como la activación de la verificación en dos pasos siempre que sea posible, ya que constituye una capa adicional de protección frente a accesos no autorizados.

Otro punto esencial que apuntan AEPD e INCIBE es la realización periódica de copias de seguridad, lo cual puede ser la única forma de recuperar datos valiosos en caso de pérdida, robo del dispositivo, error humano o *malware*. Estas copias pueden almacenarse tanto en soportes físicos como en servicios en la nube.

En lo que respecta a la navegación web, la guía enseña a identificar sitios seguros, aquellos que utilizan HTTPS y muestran el icono del candado, y recuerda la importancia de evitar transacciones o el envío de información sensible cuando se navega desde redes no seguras. También se recomienda cerrar siempre la

sesión al finalizar cualquier trámite en línea, sobre todo cuando se ha utilizado un dispositivo compartido. En relación con la protección de los datos personales, se anima a los usuarios a reflexionar antes de proporcionar información, en especial cuando no queda claro quién la solicita, con qué finalidad o cómo será tratada. Se recuerda que los ciudadanos tienen derecho a acceder, rectificar y eliminar sus datos, así como a ejercer el derecho al olvido si cierta información aparece en buscadores sin su consentimiento.

Las redes sociales y los servicios de mensajería instantánea también ocupan un espacio importante. Se aconseja limitar la cantidad de información personal que se publica y tener especial cuidado con quién puede acceder a ella, configurando de forma correcta los niveles de privacidad. Además, se alerta de la proliferación de engaños y estafas en estos canales, instando a no reenviar cadenas de mensajes ni hacer clic en enlaces dudosos. Uno de los fraudes más comunes abordados es el *phishing*, mediante el cual los ciberdelincuentes suplantan la identidad de entidades conocidas para engañar al usuario y robarle información. La guía enseña cómo reconocer estos intentos fraudulentos y cómo actuar en caso de sospecha.

En el entorno doméstico, también se dedica atención a la seguridad de la red wifi, y se explica cómo proteger el rúter y evitar intrusos que puedan no solo consumir el ancho de banda, sino también acceder a los dispositivos conectados. El correo electrónico y el uso de la nube también son analizados, y se aconseja el uso de cifrado para enviar documentos sensibles y la verificación en dos pasos para las cuentas de correo. En cuanto al almacenamiento en la nube, se recuerda que, aunque es una herramienta útil, también puede representar un riesgo si no se protege de forma adecuada el acceso a la cuenta.

Por último, se ofrece orientación sobre el uso responsable del intercambio de archivos a través de aplicaciones P2P (*P2P* significa '*peer-to-peer*', es decir, de igual a igual). Las aplicaciones P2P son programas que permiten compartir archivos directamente entre usuarios, sin necesidad de un servidor central, y se destacan los riesgos de compartir de forma accidental carpetas con in-

formación confidencial. Asimismo, se subraya la necesidad de que los padres y madres ejerzan una mediación activa en el uso que hacen los menores de internet, fomentando el diálogo y la educación digital. De forma resumida, la figura 8 muestra los principales puntos que deben seguirse:

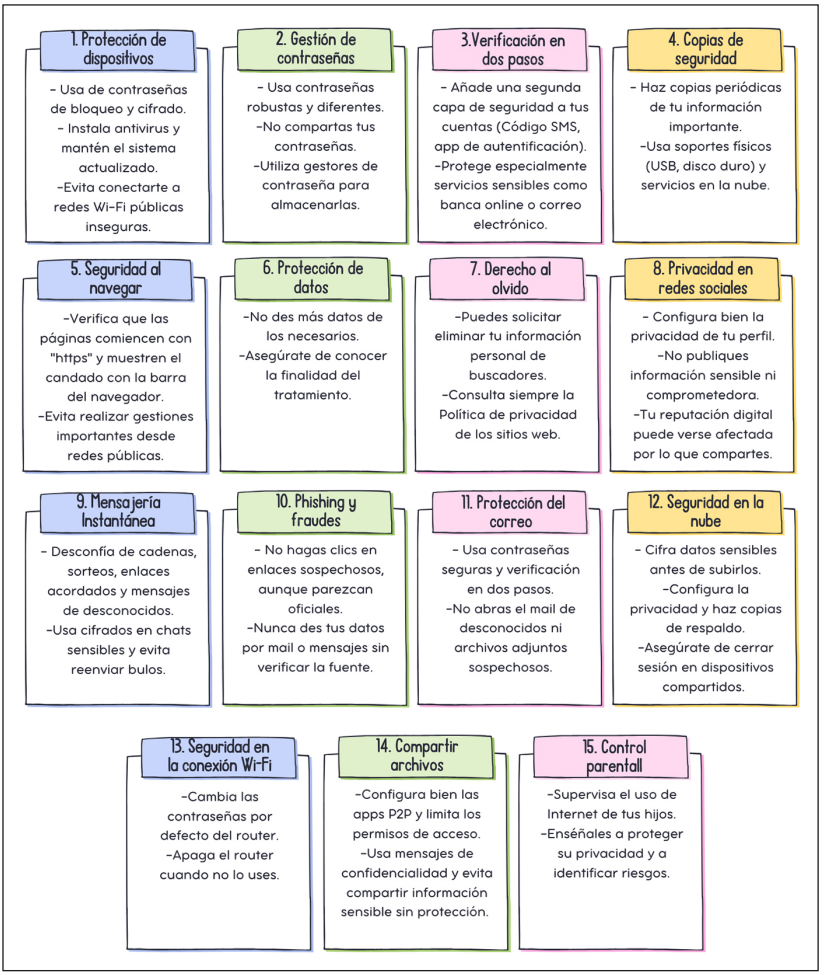

Figura 8. Recomendaciones de seguridad. Agencia Española de Protección de Datos e Instituto Nacional de Ciberseguridad (INCIBE)

4

Ciudadanía digital: Responsabilidades, derechos y alfabetización crítica

El concepto de ciudadanía digital está asociado al de los derechos humanos. Bustamante-Donas (2010) señala que la revolución de las redes digitales ha dado lugar a la cuarta generación de estos. La incorporación de lo digital como un componente clave de la sociedad actual ha ocasionado el surgimiento de nuevos valores, derechos y formas de organización social que, para el investigador, todavía se están gestando. Aparecen nuevos modos de relación humana potenciados por la tecnología, donde emergen comunidades virtuales cuya identidad no se basa en el territorio ni en una lengua común, sino en una visión compartida del mundo. En este contexto, la comunicación a distancia se convierte en el principal vínculo entre las personas, redefiniendo el sentido de pertenencia y el modo en que se construyen las relaciones sociales. Esto plantea la necesidad de repensar los derechos humanos desde una perspectiva renovada, que mantenga una reflexión continua acerca de cómo los avances tecnológicos se relacionan e inciden en el entorno humano.

Por su parte, Santana et al. (2022) hablan de que la noción de ciudadanía digital es todavía un término debatido y tiene distintos enfoques con ciertas contradicciones o criterios no unificados: como desarrollo de competencias digitales, como normas de conducta en línea o como base para la participación social plena en entornos digitales. Para estos autores, el concepto de

ciudadanía digital se ha abordado desde perspectivas institucionales, de poder y de comunidad global. No obstante, critican que muchas definiciones pasan por alto los contextos sociotécnicos y territoriales, y que el enfoque en derechos suele limitarse a la capacitación, sin considerar las desigualdades estructurales del entorno digital. En este punto coinciden investigadores como Escofet-Roig et al. (2025), quienes destacan que la ciudadanía digital es un concepto multidimensional que integra factores como el conocimiento, la actitud y el comportamiento, y se vincula con definiciones representativas como la de Ribble y Bailey (2004). Según estos últimos, su base debe asentarse en la educación desde edades tempranas, con el fin de reducir estas desigualdades y fomentar la conciencia, la sensibilidad y la capacitación digital.

Más allá de distintas definiciones o análisis (Ribble et al., 2004; Bustamante, 2010; Santana y Serra, 2022) lo que está claro es que no puede obviarse que los ciudadanos afrontan grandes desafíos en los entornos digitales, como la manipulación de la información mediante algoritmos e inteligencia artificial (IA), las noticias falsas, el ciberacoso, la pérdida de privacidad y la adicción a las tecnologías. Estos fenómenos configuran lo que Harari (2025) denomina «dictaduras digitales» y representan una amenaza directa a la libertad y a la integridad de las personas. Por ello, se hace indispensable una alfabetización digital profunda que no solo enseñe a usar las tecnologías, sino que forme ciudadanos críticos, capaces de reconocer estas amenazas y de actuar de manera ética y consciente frente a ellas. Máxime cuando en un mundo hiperconectado ser ciudadano digital no es opcional, es casi un mandato; por eso, no basta con saber usar la tecnología, se requiere formación en pensamiento crítico, ética digital y conciencia social. En ese sentido, los derechos y deberes de la sociedad pasan por la alfabetización, pero también por el empoderamiento (Bustamante, 2010).

Trujillo-Flórez (2022) señala que la formación en ciudadanía digital debe basarse en el respeto a la información. Esto supone buscar, seleccionar, referenciar e interpretar datos de forma responsable. También es fundamental emplear la netiqueta, que establece normas de comportamiento en línea. La construcción de redes y comunidades digitales promueve la colaboración más

allá de las fronteras físicas, fomentando el trabajo cooperativo para superar el individualismo y alcanzar la innovación. La digiculturalidad impulsa la convivencia intercultural en entornos digitales. Además, la alfabetización digital va más allá del manejo de herramientas, buscando el empoderamiento personal y social mediante un cambio educativo que promueva la autoformación, la adaptación constante a nuevas tecnologías y el desarrollo del pensamiento lógico y algorítmico.

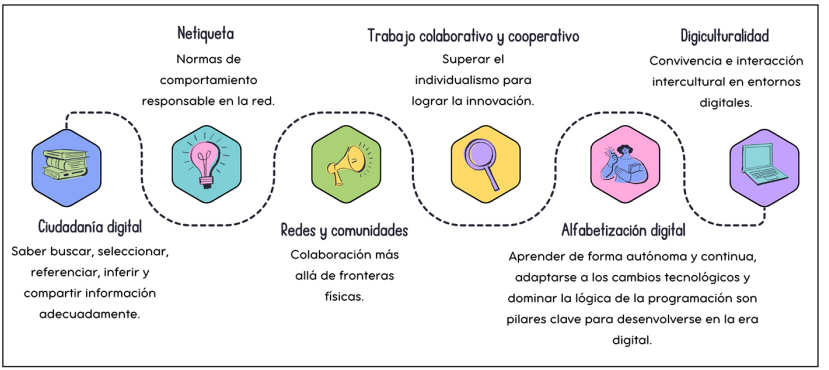

Figura 9. Elementos clave para la formación y el empoderamiento (Trujillo, 2022).

Como muestra la figura 9, la formación en competencias digitales y mediáticas a la vez que el empoderamiento resultan requisitos *sine qua non* para formar una ciudadanía digital activa, crítica, informada y participativa, que no solo consume tecnología, sino que la utiliza para transformar su entorno de manera positiva.

En síntesis, el concepto de ciudadanía digital se entrelaza profundamente con la evolución de los derechos humanos en la era digital, donde surgen nuevos valores y formas de interacción que trascienden las fronteras tradicionales (Pacto Mundial de la ONU, 2022). Ahora bien, a pesar de la riqueza conceptual, la ciudadanía digital sigue siendo un término en construcción y debate, con múltiples enfoques que a menudo no consideran las desigualdades estructurales ni los contextos sociotécnicos específicos. Los desafíos que afrontan los ciudadanos en línea, incluyendo la manipulación informativa, la pérdida de privacidad y las dictaduras digitales, requieren una alfabetización digital críti-

ca que trascienda la mera habilidad técnica para formar sujetos éticos y conscientes. En este sentido, la educación en ciudadanía digital debe promover no solo competencias digitales y mediáticas, sino también el respeto a la información, la netiqueta y la cooperación intercultural. Precisamente por eso, a través de un proceso educativo integral y un empoderamiento continuo será posible construir una ciudadanía digital activa, crítica y capaz de transformar positivamente su entorno.

La educación digital orientada a una ciudadanía responsable requiere combinar conocimientos técnicos, habilidades críticas y actitudes éticas frente a la tecnología. Estrategias de alfabetización mediática y digital permiten a los individuos evaluar la información, identificar noticias falsas y reconocer patrones de manipulación en medios y redes sociales (Gobierno de Canarias, 2014). Además, iniciativas nacionales como el desarrollo de competencias digitales de la ciudadanía, promovido por España Digital, buscan reducir las brechas digitales fomentando la inclusión, el acceso seguro a las TIC y la participación activa en la sociedad digital (España Digital, s.f.). En términos prácticos, estas estrategias se pueden implementar mediante talleres educativos que enseñen a configurar la privacidad en redes sociales, crear contraseñas seguras, identificar correos fraudulentos y aplicar criterios de verificación de información antes de compartirla. También se recomienda el uso de ejercicios interactivos, debates y simulaciones de situaciones reales para que los ciudadanos adopten comportamientos responsables y críticos en entornos digitales. De esta manera, la combinación de formación práctica y alfabetización digital contribuye a desarrollar usuarios informados, conscientes y capaces de participar activamente en la sociedad digital (Morais et al., 2022). Precisamente, en abordar este conjunto se centra el presente capítulo.

4.1. Ética y responsabilidad en la comunicación digital

El contexto digital ha transformado y transmutado las interacciones sociales. Los espacios físicos se han desdibujado y con

ellos las reglas de intercambio de información. Sin embargo, esto también lleva implícito un cambio en la forma de ejercer la libre expresión, generando, con ello, nuevos desafíos éticos vinculados a la responsabilidad y la regulación del discurso.

Es verdad que la libertad de expresión es un derecho fundamental en diversos tratados internacionales como la Declaración Universal de Derechos Humanos (ONU, 1948). En su artículo 19 se menciona expresamente que «todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión».

La propia Constitución española, en su artículo 20, reconoce el derecho a expresar y difundir libremente pensamientos, ideas y opiniones, tanto de forma oral como escrita o por cualquier otro medio. Sin embargo, este derecho no es absoluto. En la esfera de la red de redes, esa libertad de expresar nuestras opiniones debe encontrar el equilibro con otras garantías y derechos fundamentales como pueden ser el honor, la intimidad o la propia imagen, entre otros, así como la privacidad y la protección frente a contenidos perjudiciales. Estos temas colisionan en parte con lo abordado en el capítulo anterior si no se hace un uso correcto y concienzudo de la red de redes.

Internet se ha convertido en un espacio híbrido, donde unas y otras garantías pueden colisionar. La regulación en este ámbito no solo puede provenir de la administración pública, sino también de actores privados que gestionan plataformas digitales, como redes sociales tipo X, Facebook o Instagram, a los que se les exige implementar normas internas y sistemas algorítmicos que determinen qué contenidos se amplifican o se censuran (Crespo-Carchi y Villalva, 2024).

En esta línea, se vuelve especialmente relevante el control *online* ante fenómenos como la proliferación de discursos de odio, la desinformación y la polarización social. Esto se debe, para Bustos-Martínez et al. (2019, p. 38), a que el hecho de comunicarse en un entorno no físico, como las redes sociales, puede generar una sensación de irrealidad, lo que aumenta la impuni-

dad al realizar ciertos comentarios. La distancia emocional causada por la separación física entre quien emite el mensaje y los destinatarios disminuye la percepción de riesgo y crea un contexto en el que dichos comentarios parecen no acarrear consecuencias. Incluso, en ocasiones, esta combinación de garantías se disfraza bajo mensajes de humor (Aranda-Serna, 2024), una estrategia utilizada en especial en ámbitos como la política, que puede fomentar la polarización y, de manera casi imperceptible, amplificar mensajes falsos y ataques coordinados, lo que afecta a los procesos democráticos y aumenta las tensiones sociales.

En relación con las garantías al honor y a la propia imagen, algunos autores como Reneses-Botija et al. (2024) centran su atención sobre todo en los adolescentes. Aunque ellos consideran que los medios de comunicación convencionales son más creíbles, reconocen que, en la práctica, obtienen la mayor parte de su información a través de las redes sociales. Esto se debe, entre otras razones, a que en estas plataformas pueden construir su propia opinión a partir de distintas perspectivas. Sin embargo, en ocasiones terminan siendo, casi sin darse cuenta, víctimas de sesgos cognitivos derivados de consumir contenido compartido por quienes siguen, el cual puede tener un fuerte componente ideológico (Reneses-Botija et al., 2024). Para ello, es necesario diseñar una serie de medidas o programas de prevención (mostrados en la figura 10) que pasan por:

- Conciencia sobre las consecuencias. El estudio evidencia que los jóvenes no desconocen los riesgos asociados al hecho de compartir y consumir contenido falso o dañino, sino que muestran una despreocupación frente a sus efectos. Por ello, los programas de prevención deben enfatizar las posibles consecuencias sociales, legales y personales de la difusión de este tipo de información.
- Intervenciones efectivas. Para captar la atención de los jóvenes, las intervenciones deben incorporar contenidos emocionales, atractivos y conectados con sus intereses. Ejemplos prácticos pueden incluir materiales multimedia, casos cerca-

nos o simulaciones que ilustren las consecuencias reales de compartir noticias falsas.

- Criterios poco fiables de veracidad. Se identifican tres criterios que suelen considerarse erróneamente como indicadores de fiabilidad: la confianza en quien comparte el contenido (por ejemplo, un amigo cercano), la apariencia profesional o sofisticada del material (diseño cuidado, sin erratas y apariencia científica) y la validación mediante comentarios de otros usuarios. Los programas educativos deben enseñar a cuestionar estos criterios y aplicar métodos críticos de verificación.
- Educación integral. La alfabetización mediática no debe limitarse a la detección de noticias falsas, sino que también debe abordar la crítica al discurso de odio y la banalización de mensajes discriminatorios, incluso cuando se presentan mediante humor. De esta manera, se fomenta una ciudadanía digital crítica, responsable y consciente de las implicaciones éticas de sus interacciones en línea.

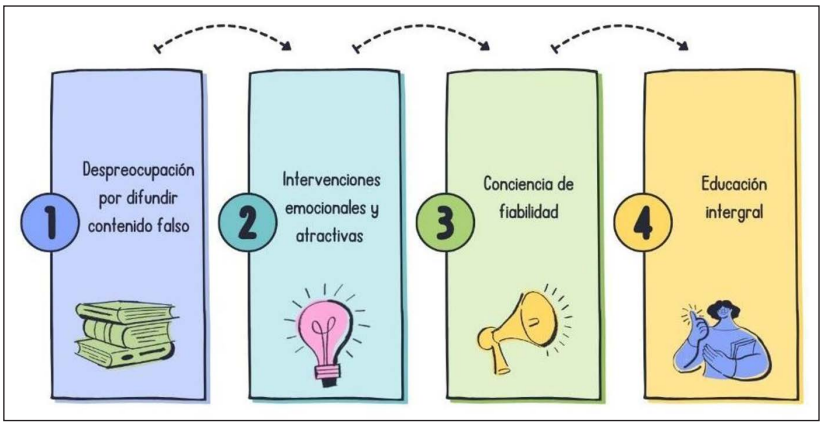

Figura 10. Razones y elementos para la prevención (Reneses et al., 2024).

Estos desafíos plantean la necesidad de políticas de moderación que no solo eliminen contenidos nocivos, sino que también promuevan la diversidad y la inclusión, sin socavar la libertad de expresión legítima. Y en ello también desempeña un papel importante la normativa legal europea. Expertos como García-García (2025), explican que, en los últimos años, se ha

intensificado el control sobre los discursos de odio, tanto desde el marco legal europeo como desde las legislaciones nacionales. Esta evolución ha supuesto, por un lado, la inclusión de un mayor número de expresiones dentro del ámbito penal, ampliando lo que se considera punible. Por otro lado, se han incorporado ciertas medidas legales complementarias, aunque de manera limitada y centradas en aspectos muy concretos, como la evaluación del papel que desempeñan las principales plataformas digitales en la contención de este tipo de contenidos.

A pesar del aumento en la presión normativa, no siempre se ha logrado una mejora sustancial en la eficacia de las políticas de protección en línea. Esto resalta la necesidad de revisar y fortalecer los mecanismos de aplicación. El gran reto radica en continuar alfabetizando y concienciando a la ciudadanía, sin desvincular la ética en la comunicación digital de la cultura de la privacidad, un derecho esencial que se ve constantemente amenazado en la era de la vigilancia masiva y la explotación comercial de datos personales. Para lograrlo, es necesario educar en el buen uso de la tecnología. En este contexto, la Unesco (2023) destaca que la inteligencia artificial (IA) ofrece grandes oportunidades para mejorar y ampliar el aprendizaje. Sin embargo, su despliegue rápido, sin marcos normativos adecuados, representa riesgos, ya que se suelen utilizar sin los controles necesarios que protejan a educandos y docentes. Por ello, es fundamental orientar la IA de manera que aumente la autonomía de los estudiantes y amplíe las opciones pedagógicas, adaptándose a sus necesidades de aprendizaje. En este sentido, la educación debe seguir siendo un esfuerzo colectivo y social, y los centros educativos son el lugar donde los niños socializan y aprenden a convivir.

El desafío de integrar la alfabetización digital y la ética en el uso de la tecnología, promoviendo una educación que prepare a la ciudadanía para navegar de manera crítica y responsable en un entorno digital cada vez más complejo, evidencian que tanto el conocimiento de los marcos legales como la formación en derechos digitales son factores clave para fomentar un uso más seguro y responsable de la tecnología. Cuando las personas comprenden los riesgos y las normativas que regulan el entorno digital,

adoptan comportamientos más autónomos, éticos y conscientes en ámbitos tan diversos como la educación, la salud, las bibliotecas, el comercio en línea o las redes sociales (Zaldívar-Martínez et al., 2025). Esto demuestra que la alfabetización digital no solo informa, sino que también empodera, permitiendo a los usuarios protegerse mejor frente a abusos y reducir la vulneración de sus derechos en entornos digitales. La regulación y la educación, por tanto, deben entenderse como pilares complementarios en la construcción de una ciudadanía digital crítica y protegida.

En conclusión, la ética y la responsabilidad en la comunicación digital requieren abordar de forma simultánea la protección de la libertad de expresión, la promoción de una cultura crítica de la privacidad y la incorporación del autocuidado como práctica social y educativa. Este enfoque integral es necesario para construir un ecosistema digital que fomente la democracia, el respeto a los derechos humanos y el bienestar individual y colectivo.

4.2. Ciberactivismo, participación y seguridad digital

El activismo digital ha emergido como una forma contemporánea de participación social y política, impulsada por el uso estratégico de las tecnologías de la información y la comunicación. Esta modalidad de activismo aprovecha la rapidez, alcance y capacidad de organización que ofrecen los entornos digitales para difundir mensajes, articular demandas y movilizar a la ciudadanía. Según García-Estévez (2018, p. 145-146):

> El ciberactivismo, también conocido como activismo en internet, activismo web o activismo *online*, entre otros, se basa en el uso de las tecnologías de la comunicación y la información con fines activistas, gracias a su rápida y eficaz comunicación, capacidad de difusión de información concreta a audiencias grandes y específicas, así como la coordinación [...]. De hecho, uno de los principales objetivos del ciberactivismo es conseguir el cambio en la agenda pública.

Su evolución está íntimamente ligada al auge de la web 2.0, en especial al impacto de las redes sociales, que han dejado de ser simples plataformas de interacción para convertirse en espacios de expresión colectiva y transformación social. A través de ellas, los usuarios no solo comparten contenidos, sino que también generan debates, cuestionan narrativas dominantes y reclaman un papel activo en la esfera pública.

En este nuevo ecosistema digital, la libertad de expresión encuentra un terreno fértil para expandirse, descentralizando la producción y circulación de información, y permitiendo que surjan voces que antes quedaban al margen del discurso oficial. De este modo, el ciberactivismo representa una forma de resistencia y participación alternativa, que desafía las estructuras tradicionales de poder y abre nuevas posibilidades para el ejercicio de la ciudadanía. Precisamente, esta misma autora (García-Estévez, 2018) habla de diferentes formas o herramientas de activismo digital como instrumentos para lograr objetivos políticos y sociales, adaptándose continuamente a nuevas formas de comunicación. Entre las herramientas más destacadas se encuentran:

- SMS y correo electrónico. Fueron los primeros medios masivos de convocatoria y coordinación, como ocurrió en las protestas del 13 de marzo de 2004 en España y en campañas internacionales como «No a la Guerra» de Irak.
- Redes sociales. Plataformas como Facebook y X permiten difundir información, coordinar acciones, presionar a los poderes y recaudar fondos, y el *hashtag* es un recurso central.
- Plataformas de firmas *online*. Sitios como Change.org, Oiga.me o Avaaz.org facilitan la movilización ciudadana; un ejemplo destacado fue la recogida de más de un millón de firmas para suprimir las reválidas educativas en España.
- Aplicaciones de sondeos masivos. Herramientas como *Appgree* permiten a grupos enviar propuestas y votarlas, lo que potencia la participación colectiva.
- Vídeos y pódcast. Se usan para generar impacto, viralización y concienciación sobre causas sociales.

- Memes e imágenes sarcásticas. Nacen alrededor del año 2000 y son efectivos por su capacidad de difusión y crítica social directa.
- Blogs, canales IRC, foros y chats. Espacios de información, debate y movilización; algunos están vinculados al *hacktivismo* y a comunidades de activismo digital más especializadas.

En conjunto, estas herramientas permiten a los ciudadanos informarse, organizarse, sensibilizar a otros y ejercer presión social, mostrando la flexibilidad y evolución constante del ciberactivismo frente a los cambios tecnológicos y sociales.

Desde la perspectiva de los estudios sobre movimientos sociales, la tecnopolítica (Candón-Mena y Montero-Sánchez, 2021) distingue cómo los movimientos sociales contemporáneos han migrado desde el ciberactivismo reactivo hacia prácticas tecnopolíticas estratégicas. Es decir, no se trata solo de usar redes digitales, sino de diseñar estrategias de acción política integradas con instrumentos digitales como nodos tácticos para la acción colectiva. Sola-Morales y Sabariego (2021) refuerzan esta mirada al introducir la categoría epistemológica de «nuevos movimientos sociales globales», definidos por su naturaleza generacional, digital y global, donde la tecnopolítica es fundamental para comprender su identidad. Todo ello conlleva una auténtica transformación teórica pero también práctica del concepto de movimiento social (Olivo y Rueda-Estrada, 2025). De hecho, la aparición de términos como *ciberprotesta* y *hacktivismo* evidencian esta expansión.

El *hacktivismo*, entendido como la convergencia entre activismo social y herramientas informáticas, ha protagonizado algunos de los hitos más significativos en la historia reciente de la ciberseguridad y la política internacional. Según el artículo de González-Valenzuela (2023), diversos casos emblemáticos muestran cómo este fenómeno ha evolucionado, pasando de acciones simbólicas a operaciones con repercusiones geopolíti*cas*. Uno de los episodios más conocidos es la operación Chanology de Anonymous contra la Iglesia de la cienciología, en la que se combinaron ataques de denegación de servicio, filtraciones do-

cumentales y campañas mediáticas. Este caso consolidó a Anonymous como un actor global del *hacktivismo* y abrió un debate sobre la legitimidad de las acciones digitales como forma de protesta. En un plano distinto, pero igualmente influyente, WikiLeaks y su fundador, Julian Assange, protagonizaron en 2010 el llamado *Cablegate*, una filtración masiva de documentos diplomáticos que puso en cuestión la transparencia de las instituciones gubernamentales y generó un impacto profundo en la política internacional.

En 2013, Edward Snowden filtró documentos clasificados de la Agencia Nacional de Seguridad de Estados Unidos que revelaban la existencia de programas de vigilancia masiva. Estas filtraciones tuvieron un impacto global y transformaron de manera duradera la percepción ciudadana sobre la privacidad y los derechos digitales. Otro hito destacado es *Stuxnet*, un *malware* extremadamente sofisticado dirigido contra el programa nuclear iraní. Atribuido de forma extraoficial a Estados Unidos e Israel, este caso evidenció que el *hacktivismo* podía ir más allá de la protesta, convirtiéndose en un instrumento de ciberguerra capaz de afectar infraestructuras críticas estatales. Por último, Aaron Swartz representa una vertiente diferente del *hacktivismo*: la lucha por el acceso libre al conocimiento. Swartz impulsó iniciativas como *Demand Progress* y promovió la liberación de publicaciones académicas restringidas, por lo que se convirtió en un símbolo de la defensa de la ciencia abierta y de la democratización de la información.

En conjunto, estos casos muestran que el *hacktivismo* no es un fenómeno homogéneo, sino una práctica multifacética que oscila entre la protesta digital, la filtración de secretos de Estado y la ciberguerra. Más allá de las diferencias en motivaciones y consecuencias, todos ellos han contribuido a redefinir el debate contemporáneo sobre ética, seguridad, transparencia y libertad en el entorno digital.

En cuanto a la ciberprotesta, el activismo digital ha demostrado repetidamente que los espacios virtuales pueden convertirse en movimientos reales con consecuencias políticas concretas. Algunos ejemplos destacan esta evolución: el colectivo #YoSoy132

en México, que tras las elecciones presidenciales dio continuidad a iniciativas como #Verificado19S, destinadas a verificar información tras el sismo que afectó al país; la tragedia de Ayotzinapa, que gracias a la presión digital se transformó en un símbolo de la lucha contra la impunidad tras la desaparición de estudiantes; y la Primavera Árabe, cuyos acontecimientos fueron inicialmente difundidos a través de redes sociales, impulsando una ola de movilizaciones contra regímenes autoritarios en el Norte de África y Oriente Medio.

También resulta significativo el movimiento 15M en España, conocido como los «indignados», que se apoyó en el uso comunitario de las redes para coordinar protestas masivas contra el bipartidismo y las políticas de austeridad. Este movimiento, que dio lugar al surgimiento del partido político Podemos, ejemplifica cómo la interacción digital puede generar nuevos espacios políticos. Por último, el artículo resalta la #WomensMarch, una protesta organizada a través de redes sociales que reunió a cientos de miles de mujeres en Washington D.C. y otras ciudades, apenas un día después de la investidura presidencial de Donald Trump, para expresar su rechazo al sexismo.

Estos episodios ayudan a entender que la utilización de *hashtags* puede trascender el entorno en línea y generar acciones colectivas de impacto real, lo que subraya el potencial estratégico de las redes como herramientas de movilización sociopolítica. La convergencia entre interacción digital y acción pública redefine así el alcance del activismo en el siglo XXI (Nacion321, 2017).

En todo este entramado, el periodismo también encuentra su desafío. La investigación de Kruzkaya-Ordóñez et al. (2024) subraya que el periodismo contemporáneo afronta crecientes desafíos vinculados a la ciberseguridad, tanto en la recolección de información como en la protección de las fuentes. La digitalización de los procesos informativos ha ampliado las posibilidades de vigilancia, espionaje y manipulación de datos, lo que sitúa al periodista en una posición de vulnerabilidad frente a actores estatales, corporativos o incluso criminales. En este contexto, se hace evidente la necesidad de desarrollar competencias específicas en seguridad digital, que incluyan el uso de comunicaciones

cifradas, el resguardo de dispositivos y la gestión segura de archivos sensibles. Asimismo, el documento destaca que el periodismo de investigación es particularmente susceptible a ciberataques, ya que suele abordar temáticas de interés estratégico para el poder político y económico.

La ciberseguridad, por tanto, no debe considerarse solo como un asunto técnico, sino como un componente esencial de la libertad de prensa y la democracia, dado que, sin garantías de seguridad digital, los periodistas no pueden ejercer su labor con independencia ni proteger a sus informantes.

5

Competencia mediática y ciberseguridad en el futuro de internet

Hablar del futuro de internet es hablar del futuro de nuestra vida en sociedad. Las tecnologías digitales son ahora esenciales, pues son la base de nuestras relaciones personales, la economía, la política, la cultura y la educación. En apenas dos décadas hemos pasado de conectarnos de forma ocasional a estar siempre hiperconectados, siendo habitual que los dispositivos nos acompañen en cada momento del día. Este cambio ha traído beneficios como el acceso rápido a la información, nuevas formas de comunicación y colaboración y oportunidades para la innovación científica y cultural. Pero también implica riesgos que afectan a la privacidad, la seguridad y la confianza en el mundo digital (Floridi, 2021b).

En este contexto, la competencia mediática (capacidad de analizar de forma crítica los mensajes y la información que recibimos) y la competencia digital (habilidad para usar de forma práctica y segura las herramientas tecnológicas) son claves para entender y desenvolverse en el entorno digital. No basta con usar la tecnología, se necesitan habilidades críticas y éticas para reconocer riesgos, cuestionar mensajes, proteger la información personal y actuar de manera responsable (Ferrés y Piscitelli, 2012). El ciudadano del siglo XXI ya no puede limitarse a ser consumidor pasivo de contenidos digitales: debe convertirse en un sujeto crítico capaz de navegar con criterio en un entorno marcado por

la desinformación, los algoritmos de recomendación y las nuevas formas de manipulación (Livingstone et al., 2021a).

Los capítulos anteriores de este libro han mostrado cómo internet ha transformado la comunicación, los riesgos que plantea en términos de seguridad y la importancia de la alfabetización crítica para enfrentarse a fenómenos como las noticias falsas, el ciberacoso o los fraudes en línea. Este capítulo pretende dar un paso más: analizar el futuro de internet y de la ciberseguridad con el fin de identificar los escenarios que marcarán los próximos años y preguntarnos qué competencias necesitaremos los ciudadanos para desenvolvernos en ellos.

Este capítulo analiza las nuevas tecnologías y riesgos en ciberseguridad, como la inteligencia artificial generativa (IAG), los *deepfakes*, el internet de las cosas (IoT), el metaverso, la computación cuántica y la biometría. También reflexiona sobre cómo formar ciudadanos digitales críticos y resilientes, con la educación y la formación como ejes centrales. El objetivo es plantear cómo queremos que evolucione nuestra relación con la tecnología y avanzar hacia una sociedad más justa, segura y consciente de los retos futuros.

5.1. Nuevas tecnologías y desafíos emergentes en ciberseguridad

El panorama digital actual cambia con mucha rapidez. Las nuevas tecnologías modifican la forma en que nos comunicamos, trabajamos y accedemos a la información. Esta transformación trae consigo oportunidades de desarrollo económico y social, aunque también nuevos retos en materia de seguridad y privacidad (Brundage et al., 2018). La ciberseguridad, entendida en un principio como un asunto técnico limitado a la protección de infraestructuras, redes y servicios de comunicación, se ha convertido en un problema general que afecta a todos los ámbitos de la vida digital. Como señala van-Dijk (2020), «la verdadera desigualdad en las sociedades digitales no está simplemente en el acceso a dispositivos o conexiones, sino en las habilidades y ca-

pacidades que las personas tienen para utilizarlos de manera efectiva».

Este cambio se debe a factores como la expansión de la IAG, la proliferación de los *deepfakes* y otros métodos de manipulación audiovisual, el crecimiento del IoT, el desarrollo de entornos como el metaverso y el uso cada vez más habitual de la biometría como método de autenticación. A ello se suman los riesgos que, en un futuro próximo, planteará la computación cuántica; su rápido avance «podría volver vulnerables los métodos de cifrado actuales y casi todas las comunicaciones cifradas» (Cyber Defense Magazine, 2025).

Son protagonistas del cambio porque no solo representan innovaciones técnicas, sino que alteran de forma directa la manera en que nos informamos, nos comunicamos y protegemos nuestra identidad en línea. También afectan de forma simultánea a la economía, la política y la vida cotidiana, generando oportunidades de desarrollo, pero también nuevas vulnerabilidades que ponen a prueba la seguridad y la confianza en el entorno digital. Cada una de estas tecnologías tiene sus puntos fuertes y débiles que deben analizarse con cuidado (figura 11).

En este sentido, conviene subrayar que la falta de alfabetización mediática y digital incrementa la vulnerabilidad frente a estos desafíos. No basta con desarrollar soluciones técnicas si los ciudadanos no están preparados para comprender los riesgos y actuar en consecuencia.

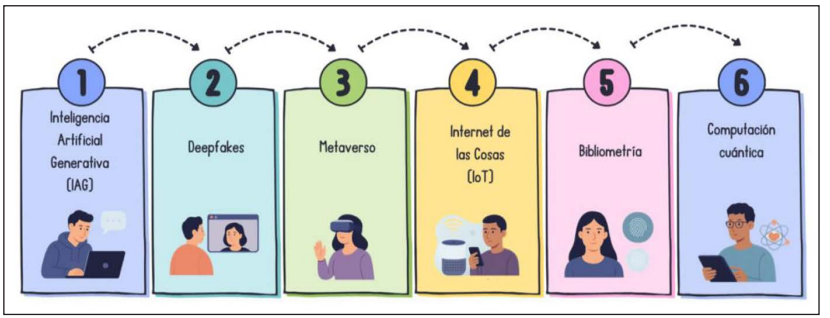

Figura 11. Tecnologías emergentes en ciberseguridad.

La IAG se ha consolidado como una de las innovaciones más importantes de los últimos años. Herramientas como ChatGPT, DALL·E o MidJourney han demostrado su capacidad para producir textos, imágenes, vídeos y música de forma muy realista. Estas aplicaciones tienen un potencial enorme en ámbitos como la educación, donde pueden ayudar a personalizar el aprendizaje; la comunicación, con la creación de materiales accesibles y adaptados a distintos contextos, y en la investigación científica, mediante la generación de simulaciones y modelos predictivos (Ramanpreet et al., 2023). Sin embargo, también tienen un lado negativo. La IAG ya se utiliza para automatizar campañas de *phishing*, con mensajes que imitan el estilo y el idioma del destinatario, lo que incrementa las posibilidades de engaño (Kreps et al., 2020). También se han registrado casos de uso para programar código malicioso o para crear campañas de desinformación a gran escala. Esta capacidad de producir mensajes persuasivos a bajo coste supone una amenaza con respecto a la confianza en los medios de comunicación y en la información que circula por la red (Bada et al., 2019).

Frente a este panorama, las instituciones han empezado a reaccionar. La Comisión Europea, por ejemplo, ha propuesto la Ley de Inteligencia Artificial (European Commission, 2023b), que establece obligaciones de transparencia y responsabilidad en el desarrollo de estos sistemas. Sin embargo, la regulación siempre llega con cierto retraso respecto a la innovación tecnológica, y esa diferencia se convierte en un desafío emergente para la ciberseguridad, porque deja espacio a malos usos como la desinformación, el *phishing* o la creación de contenidos falsos a gran escala. Ante ello, la competencia mediática y digital resultan esenciales. No se trata de rechazar estas herramientas, sino de aprender a contextualizarlas, comprender cómo funcionan y reconocer cuándo se están usando con fines engañosos o fraudulentos.

En continuidad con lo anterior, los *deepfakes* se han convertido en uno de los fenómenos más preocupantes del panorama digital reciente. Gracias a técnicas de aprendizaje profundo es posible generar vídeos, audios o imágenes en los que una persona aparece diciendo o haciendo algo que en realidad nunca ocurrió. Aunque estas tecnologías se han popularizado en el ámbito del

entretenimiento y la creatividad digital, sus aplicaciones maliciosas generan un serio desafío en términos de seguridad y confianza (Chesney y Citron, 2019). Uno de los principales riesgos de los *deepfakes* es que pueden hacer que la gente dude de lo que es verdad. Durante procesos electorales ya se han detectado vídeos manipulados que buscan desprestigiar a candidatos o sembrar dudas sobre instituciones democráticas (Vaccari y Chadwick, 2020). En un mundo donde la velocidad de propagación de la información supera con creces la capacidad de verificación, la difusión de estos contenidos puede influir en la opinión pública antes de que exista tiempo para desmentirlos (Paris y Donovan, 2019). Investigadores y empresas están creando sistemas para detectar manipulaciones, pero los *deepfakes* son cada vez más difíciles de reconocer. Por eso, es clave que los ciudadanos aprendan a revisar y verificar la información antes de compartirla.

Además del impacto político, los *deepfakes* se han convertido en instrumentos de acoso y violencia digital. La creación de vídeos pornográficos falsos sin consentimiento afecta en especial a mujeres y menores, lo que genera daños psicológicos y reputacionales de gran alcance. Este tipo de agresiones plantea dilemas legales complejos sobre los derechos de imagen y la protección de la identidad en entornos digitales (Barba, 2024). Un ejemplo cercano de estas prácticas se vivió en Almendralejo (Badajoz) en 2023, cuando varias adolescentes fueron víctimas de *deepfakes* de carácter sexual creados y difundidos sin su consentimiento. El proceso judicial responsabilizó a quince menores de delitos de pornografía infantil y contra la integridad moral. Este caso evidencia que los riesgos descritos no son una amenaza futura o lejana, sino una realidad presente que nos afecta directamente. Asimismo, subraya la necesidad de reforzar tanto la alfabetización mediática como la educación en valores y la protección legal de los menores (*El País*, 2023). A escala global, también se han producido casos muy mediáticos, como la difusión en 2024 de imágenes falsas de carácter sexual de la cantante Taylor Swift, que se viralizaron en redes sociales y generaron un debate internacional sobre la necesidad de nuevas leyes contra este tipo de violencia digital (*The Guardian*, 2024).

Del mismo modo, el IoT se ha convertido en una realidad cotidiana. Relojes inteligentes que monitorizan nuestra salud, altavoces que responden a nuestras órdenes, cámaras de seguridad conectadas a la nube o sistemas que controlan la temperatura de nuestra casa forman parte de la vida diaria de muchas personas. Se estima que en 2030 habrá casi 30 000 millones de dispositivos conectados en todo el mundo (Statista, 2023).

La incorporación de dispositivos en el entorno digital incrementa el riesgo de ciberataques. Muchos de estos dispositivos se comercializan con contraseñas predeterminadas fáciles de adivinar, con sistemas de actualización poco frecuentes o sin medidas de seguridad robustas. El ataque de la botnet Mirai en 2016 es un buen ejemplo: miles de cámaras y rúters mal configurados o con contraseñas débiles fueron usados para lanzar un ataque masivo de denegación de servicio (DDoS) que afectó a plataformas como Twitter (ahora X), Spotify o Netflix (Kolias et al., 2017).

Más allá de las infraestructuras, el IoT plantea interrogantes sobre la privacidad. Los dispositivos recopilan información extremadamente sensible: hábitos de consumo, datos de localización, rutinas de sueño o constantes vitales. Cuando estos datos se almacenan sin garantías o se comercializan sin consentimiento, el usuario se expone a riesgos que van desde el robo de identidad hasta la vigilancia masiva (Zuboff, 2019). Por todo ello, el IoT requiere que los ciudadanos conozcan prácticas básicas de seguridad: cambiar contraseñas predeterminadas, mantener actualizados los dispositivos y limitar los permisos de acceso. A la vez, los gobiernos y las empresas deben trabajar en la creación de estándares comunes que refuercen la seguridad de estos sistemas hiperconectados.

En una línea similar de transformación tecnológica, el término *metaverso* ha pasado de ser un concepto propio de la ciencia ficción a convertirse en un espacio de desarrollo tecnológico en el que grandes corporaciones han invertido mucho dinero. Se trata de entornos virtuales que combinan realidad aumentada, realidad virtual y redes sociales, en los que los usuarios interactúan mediante avatares digitales (Dwivedi et al., 2022). El metaverso promete nuevas formas de aprendizaje, experiencias cultu-

rales interactivas y posibilidades de trabajo colaborativo a distancia. Sin embargo, este entorno emergente también abre la puerta a ciertos riesgos. El primero de ellos es la suplantación de identidad: los avatares, que son representaciones digitales de los usuarios, pueden ser robados o manipulados, causando fraudes o acoso. El segundo riesgo está vinculado a las transacciones económicas, que a menudo se realizan mediante criptomonedas o activos digitales no regulados, lo que incrementa las probabilidades de estafas y pérdidas financieras (Zhuk, 2024).

Un aspecto sensible del metaverso es la recopilación de datos biométricos. Dispositivos como las gafas de realidad virtual registran movimientos corporales, expresiones faciales y reacciones fisiológicas. Estos datos, altamente personales, podrían usarse para vigilancia comercial o política, lo que plantea dilemas éticos sobre el consentimiento y la privacidad (Dwivedi et al., 2022). Ante estas amenazas, es importante extender la competencia mediática y digital a los entornos del metaverso. No basta con dominar la parte técnica; es necesario promover una cultura digital basada en el respeto, la privacidad y la protección de la identidad.

Más allá de estas transformaciones, existen también amenazas emergentes que podrían cambiar el concepto de ciberseguridad. Una de ellas es la computación cuántica, que promete resolver operaciones matemáticas de forma exponencialmente más rápida que los ordenadores actuales. Esta capacidad pone en riesgo los algoritmos de cifrado que hoy garantizan la seguridad de las comunicaciones bancarias, los correos electrónicos o las transacciones en línea (Mosca, 2018). Ante este desafío, instituciones como el National Institute of Standards and Technology (NIST) ya trabajan en el desarrollo de sistemas de criptografía poscuántica (NIST, 2025) con el objetivo de asegurar que la protección de los datos y la privacidad de los usuarios sigan garantizadas a pesar de estos avances tecnológicos.

La biometría es otra de las áreas que despiertan preocupación. Métodos como el reconocimiento facial, las huellas dactilares o el escaneo de iris se han popularizado como mecanismos de autenticación por su comodidad y rapidez. Sin embargo, los datos

biométricos tienen un problema: a diferencia de las contraseñas, no pueden cambiarse en caso de filtración. Una base de datos comprometida con millones de registros faciales supondría un riesgo de por vida para la identidad digital de los usuarios (Ratha et al., 2001). No debemos olvidar que nuestros datos son valiosos, pero los biométricos lo son todavía más, porque forman parte de nuestra identidad y no se pueden reemplazar. Un caso reciente que refleja ese peligro fue el proyecto Worldcoin, que ofrecía criptomonedas a cambio de escanear iris con dispositivos llamados Orbs. Miles de personas accedieron motivadas por ese incentivo económico, muchas sin ser conscientes del riesgo real. La polémica llevó a que la Agencia Española de Protección de Datos (AEPD) ordenara en marzo de 2024 la suspensión cautelar de esta actividad en España (*El País*, 2024). Por último, a finales de 2024, la Oficina Estatal de Supervisión de la Protección de Datos de Baviera (BayLDA), junto con el respaldo de la AEPD, ordenó eliminar todos los registros de iris recopilados, tras considerar que las prácticas incumplían el Reglamento General de Protección de Datos (RGPD).

Por último, el auge del cibercrimen como servicio (CaaS) ha convertido el delito informático en un negocio global. Plataformas clandestinas ofrecen *kits de malware*, alquiler de *botnets* o campañas de *phishing* listas para usar, lo que facilita que cualquiera pueda cometer delitos en internet (Europol, 2022). Hoy los atacantes ya no necesitan diseñar desde cero sus herramientas: pueden obtenerlas listas para usar en mercados ilícitos de la *dark web*. Esto significa que actividades que antes exigían amplios conocimientos técnicos ahora están al alcance de cualquiera que esté dispuesto a pagar, lo que multiplica el número de potenciales delincuentes y amplifica el impacto de sus ataques.

Un ejemplo cercano se produjo en junio de 2025 en Almendralejo (Badajoz) (Ayuntamiento de Almendralejo, 2025), donde el Ayuntamiento denunció una campaña de *phishing* mediante correos electrónicos falsificados que usaban su logo e identidad corporativa para engañar a proveedores y ciudadanos con pagos fraudulentos. A escala nacional, un caso muy mediático fue el ataque de *ransomware* al SEPE (Servicio Público de Empleo

Estatal) en 2021 (*Revista Ciberseguridad*, 2021), que paralizó durante semanas sus sistemas y afectó a miles de trámites en toda España. Y en el plano internacional destaca el ciberataque de WannaCry en 2017 (Cloudflare, 2017; Kaspersky, 2017), que se extendió a más de 150 países y comprometió hospitales, empresas y organismos públicos.

Estos ejemplos muestran cómo el cibercrimen afecta tanto a administraciones locales como a grandes instituciones nacionales e internacionales, y cómo este fenómeno multiplica la exposición de empresas, instituciones y ciudadanos a ataques digitales. El denominador común de estas amenazas es que combinan avances tecnológicos con vulnerabilidades sociales y educativas. Por ello, la respuesta no puede limitarse a la innovación técnica; se requiere también una ciudadanía capaz de entender, cuestionar y anticiparse a los riesgos.

5.2. Construcción de una ciudadanía digital crítica y resiliente

Si el apartado anterior mostraba los retos tecnológicos de la ciberseguridad, en este resulta imprescindible poner el foco en las personas. Las amenazas digitales no se combaten solo con cortafuegos, algoritmos o leyes. Lo que marca la diferencia es que sepamos entender el entorno digital en el que nos movemos y actuar en consecuencia. En este sentido, la resiliencia (preparación) digital se define como la capacidad de anticipar, resistir y recuperarse frente a incidentes cibernéticos. Se trata de un concepto que no solo abarca la dimensión técnica, sino también la emocional, ética y social (OECD, 2023). Una ciudadanía preparada es aquella que protege sus datos y dispositivos, desarrolla un pensamiento crítico, cuestiona la información que recibe y entiende que cada acción en internet tiene consecuencias.

La educación es clave para construir esta ciudadanía digital. A lo largo de los últimos años, informes de organismos internacionales como la Unesco (Unesco, 2011b) o la Comisión Europea (European Commission, 2023b) han insistido en que la alfabeti-

zación mediática y digital debe concebirse de manera amplia, incorporando no solo habilidades técnicas, sino también competencias críticas, éticas y de seguridad. Algunas estrategias fundamentales se detallan a continuación y se resumen en la figura 12.

5.2.1. Integración en el plan de estudios

La ciberseguridad no puede quedar relegada a una asignatura opcional, debe formar parte de la educación desde primaria hasta la universidad. En países como Estonia se ha demostrado que introducir contenidos de seguridad digital en áreas como lengua, ciencias sociales o matemáticas contribuye a normalizar prácticas responsables desde edades tempranas (Ferrés y Piscitelli, 2012).

5.2.2. Formación de profesores

Ningún programa educativo puede tener éxito si el profesorado no cuenta con los conocimientos y herramientas necesarias. Sin embargo, muchos estudios evidencian que los docentes aún presentan carencias en materia de alfabetización digital y ciberseguridad (Buckingham, 2019). La formación continua, la provisión de recursos didácticos actualizados y la creación de redes de apoyo son esenciales para que los educadores puedan guiar a sus alumnos en este terreno.

5.2.3. Programas de sensibilización

La educación en ciberseguridad no es solo cosa de los colegios. La familia, asociaciones, medios de comunicación y empresas también deben implicarse en campañas que promuevan prácticas seguras y fomenten el respeto y cooperación en internet. Iniciativas como el *Safer Internet Day* en la Unión Europea o los programas de INCIBE en España son ejemplos de cómo las políticas públicas pueden extender el aprendizaje más allá del aula (INCIBE, 2022).

5.2.4. Desarrollo del pensamiento crítico y la verificación informativa

La desinformación es un gran problema, impulsada por algoritmos de recomendación y técnicas como los *deepfakes*. La educación debe enseñar a los estudiantes a identificar fuentes fiables, contrastar datos y comprender cómo los algoritmos influyen en lo que ven. Esta alfabetización crítica previene la manipulación y refuerza la autonomía intelectual (Pariser, 2011; Tandoc et al., 2018).

5.2.5. Inclusión e igualdad

La ciudadanía digital no puede excluir a los sectores más vulnerables. Las diferencias en el acceso a dispositivos, conectividad y formación generan desigualdades que aumentan el riesgo digital. Es imprescindible garantizar que las políticas educativas contemplen medidas de igualdad, proporcionando recursos a los colectivos más desfavorecidos. En esta línea, iniciativas como el programa Conéctate35, que ofrece internet satelital subvencionado en zonas rurales a un precio asequible, son un paso importante para reducir la brecha digital (Conéctate35, 2023).

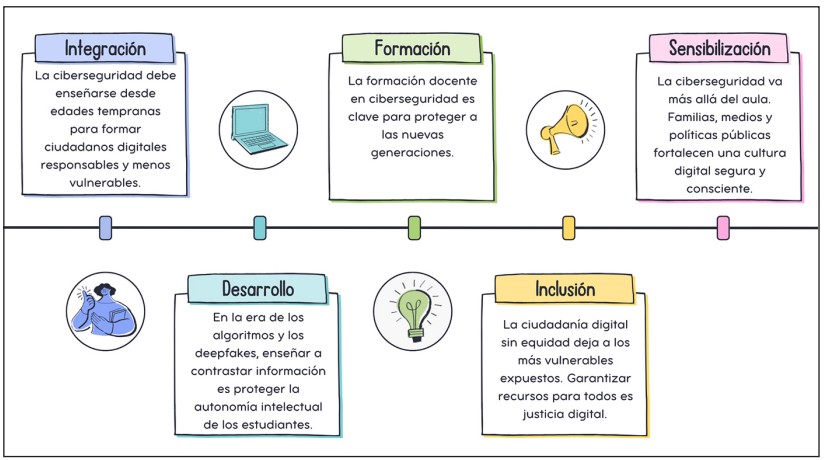

Figura 12. Estrategias fundamentales.

Además de las estrategias generales, es necesario concretar modelos pedagógicos que hagan posible la integración de la ciberseguridad en la alfabetización mediática y digital (figura 13). Entre los más relevantes se encuentran:

- Conectivismo y aprendizaje en red. Este modelo propuesto por Siemens (2004) plantea que el conocimiento digital se construye en red. Aplicado a la ciberseguridad, promueve comunidades de aprendizaje colaborativas en las que los ciudadanos comparten experiencias, recursos y estrategias de protección.
- Aprendizaje basado en problemas (ABP). Propone trabajar con situaciones reales que obligan a los estudiantes a investigar, analizar y proponer soluciones. En el ámbito de la ciberseguridad, los escenarios pueden incluir ataques de *phishing*, filtraciones de datos o campañas de desinformación. Este enfoque fomenta la capacidad de respuesta crítica y prepara a los ciudadanos para enfrentarse a retos concretos (Morales-Bueno, 2018).
- Gamificación y simulación. La gamificación se ha consolidado como un recurso eficaz para la enseñanza de competencias digitales. Simulaciones que reproducen ciberataques en entornos controlados permiten a los usuarios experimentar consecuencias de sus decisiones sin riesgo real, aumentando su motivación y conciencia (Marciano et al., 2024). Este modelo se utiliza tanto en la educación formal como en la formación corporativa.
- Formación continua. La ciberseguridad es un campo en constante evolución. Por ello, la educación digital debe concebirse como un proceso continuo a lo largo de la vida. Programas para adultos, talleres comunitarios y recursos en línea de acceso abierto permiten que los ciudadanos mantengan sus competencias siempre actualizadas (Carretero et al., 2017).
- Ética y valores. Enseñar ciberseguridad consiste en transmitir conocimientos técnicos y cultivar valores como el respeto, la responsabilidad y la conciencia de que las acciones en línea tienen un impacto colectivo. La ética digital se convierte así en un componente inseparable de la competencia mediática (Ribble, 2012).

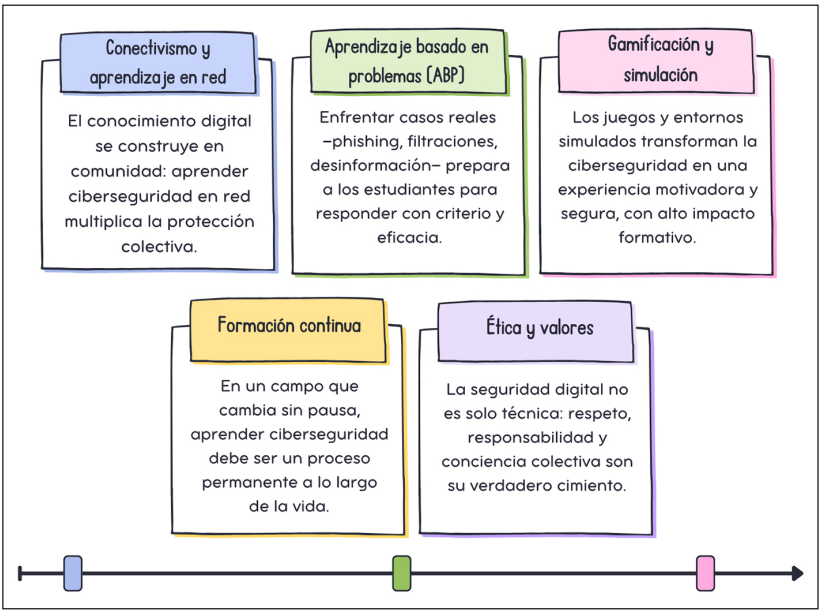

Figura 13. Modelos pedagógicos para integrar la ciberseguridad en la alfabetización digital.

La educación en materia en ciberseguridad, únicamente, no puede centrase en técnicas o momentos aislados de formación. Es necesario instar modelos pedagógicos innovadores, aprendizaje colaborativo y compartido, actualización permanente sobre la materia de estudio y un fuerte componente ético. De este modo, será posible que la sociedad sea capaz de desarrollar una actitud crítica, consciente y capaz de desenvolverse en un contexto digital complejo.

6

Conclusiones y recomendaciones

Internet forma parte de nuestra vida cotidiana. Nos levantamos y lo usamos para mirar las noticias, para hablar con la familia, para consultar el tiempo o para organizar el día. Durante la jornada lo empleamos en el trabajo, en el colegio o en nuestras actividades personales, y al final del día lo seguimos utilizando para entretenernos. Lo hacemos casi sin darnos cuenta, como si siempre hubiera estado ahí. Sin embargo, lo que muchas veces olvidamos es que este espacio en el que pasamos tantas horas no está libre de riesgos. Igual que cuando salimos a la calle sabemos que debemos mirar antes de cruzar o que tenemos que cerrar la puerta de casa al salir, también necesitamos aprender qué precauciones tomar en la vida digital.

La seguridad en internet no se logra solo con programas informáticos ni con leyes que sancionen los delitos. Claro que esas medidas son importantes, pero lo que de verdad marca la diferencia son las prácticas cotidianas de cada persona. La competencia mediática y digital, entendida como la capacidad para comprender cómo funcionan los medios (analógicos y digitales) y la red para actuar con sentido crítico, es el verdadero escudo que nos protege. No se trata de ser expertos en informática, sino de contar con hábitos sencillos que nos permitan reconocer riesgos y actuar con responsabilidad.

Uno de los retos más frecuentes es la desinformación. Todos hemos recibido en alguna ocasión un mensaje alarmante en el grupo de WhatsApp, un vídeo sospechoso en redes sociales o una no-

ticia con un titular demasiado llamativo como para ser cierto. Muchas veces la primera reacción es compartirlo sin pensarlo mucho, sobre todo si proviene de alguien cercano. Pero en realidad esa cadena de reenvíos es lo que da fuerza a las noticias falsas. Basta con detenerse un momento y preguntarnos si la fuente es fiable, si aparece en un medio de comunicación reconocido o si tiene algún dato que se pueda comprobar. Durante la pandemia provocada por el covid-19, por ejemplo, circularon mensajes que ofrecían remedios caseros milagrosos o que sembraban dudas sobre las vacunas. Esos bulos se propagaron tan rápido porque la gente los compartía sin verificar. Una competencia mediática básica, como la de contrastar la información antes de difundirla, puede marcar la diferencia entre la confusión generalizada y la protección colectiva.

La privacidad es otro aspecto clave. Cada acción en la red deja un rastro, aunque no siempre seamos conscientes de ello. Una búsqueda en un navegador, una fotografía compartida, un comentario en una red social o una aplicación instalada se convierten en piezas que, juntas, puedan ayudar a dibujar un perfil muy detallado sobre nosotros. Ese perfil puede ser utilizado para ofrecernos anuncios adaptados. Pero también puede terminar en manos equivocadas. Muchas aplicaciones que parecen gratuitas obtienen beneficios recopilando y vendiendo datos de los usuarios. Algo tan sencillo como revisar los permisos de una aplicación, ajustar las opciones de privacidad de nuestras redes sociales o eliminar de forma periódica las aplicaciones que ya no usamos puede reducir mucho nuestra exposición. Incluso el gesto de pensar dos veces antes de publicar una foto personal o una información que pueda resultar sensible tiene un impacto enorme en la protección de nuestra identidad digital.

La privacidad de los menores merece una mención especial. Muchas familias comparten imágenes de sus hijos en internet sin pensar que esas fotos permanecerán disponibles durante años y pueden ser usadas por terceros sin control. Educar en privacidad también implica reflexionar sobre lo que publicamos de los demás, en especial de los más vulnerables.

No todas las personas, sin embargo, tienen las mismas oportunidades para protegerse. La brecha digital sigue siendo una

realidad. Hay quienes tienen dispositivos de última generación, buena conexión a internet y formación para moverse con seguridad. Y hay quienes apenas cuentan con un teléfono básico, una conexión inestable o escaso conocimiento sobre cómo funciona la red. Esta desigualdad hace que los más vulnerables estén más expuestos a fraudes, engaños o ataques. Los mensajes falsos que imitan a los bancos, por ejemplo, suelen afectar en especial a personas mayores, que confían en lo que reciben por *SMS* o correo electrónico. Pensar en la seguridad digital como un derecho implica asumir que todas las personas deben tener la oportunidad de aprender a desenvolverse con seguridad, sin importar su edad, nivel educativo o lugar de residencia. Iniciativas como el programa Conéctate35, que lleva internet asequible a zonas rurales, son un buen ejemplo de cómo reducir esta brecha y garantizar la igualdad de oportunidades en el acceso digital.

La educación es la herramienta más poderosa para lograrlo. Igual que enseñamos a los niños a leer o a sumar, debemos enseñarles a navegar en internet de manera segura. Desde edades tempranas es posible inculcar hábitos muy básicos pero eficaces: no hablar con desconocidos en línea, no compartir contraseñas, pedir ayuda a un adulto si reciben un mensaje que les incomoda... Durante la adolescencia conviene profundizar en la capacidad crítica: comprender cómo los algoritmos deciden qué aparece en sus pantallas, identificar noticias falsas, reflexionar sobre la imagen que construyen al publicar contenido en redes sociales. En la vida adulta, el aprendizaje no debe detenerse, porque la tecnología cambia rápido y los riesgos evolucionan. Programas de formación continua, talleres comunitarios y recursos accesibles en línea pueden ayudar a que las personas se mantengan actualizadas.

Para que esta educación funcione, el profesorado necesita apoyo. No es necesario que los docentes se conviertan en expertos en ciberseguridad, pero sí que tengan la formación y los recursos para transmitir conocimientos básicos y fomentar actitudes responsables. Un profesor de Historia puede enseñar a analizar de forma crítica una fuente digital, un profesor de Lengua puede trabajar con sus alumnos la verificación de noticias, y un profesor de Ciencias de la Salud puede explicar qué riesgos supone compartir datos de

salud en aplicaciones sin garantías. Además, las familias también tienen un papel central, ya que muchos niños aprenden a usar la tecnología en casa antes que en la escuela. Establecer normas claras, hablar abiertamente de los riesgos y acompañar a los hijos en el uso de las redes sociales son formas efectivas de prevención.

La educación no puede quedarse limitada al aula. La sociedad en su conjunto tiene que implicarse. Las campañas en medios de comunicación, los programas organizados por asociaciones locales o las iniciativas promovidas por organismos públicos son herramientas valiosas para llegar a un público más amplio. Iniciativas como el *Safer Internet Day* o los talleres impulsados por entidades como INCIBE (Instituto Nacional de Ciberseguridad) en España demuestran que es posible trasladar la cultura de la seguridad digital más allá del entorno escolar. Cuando los mensajes llegan a la familia, a la comunidad y al lugar de trabajo, su impacto se multiplica.

La regulación también es otra pieza clave. Las leyes deben adaptarse al ritmo de la innovación. El Reglamento General de Protección de Datos en Europa fue un avance decisivo en la protección de la privacidad, pero la aparición de nuevas tecnologías, como la inteligencia artificial generativa o el uso de datos biométricos, plantea retos que exigen respuestas rápidas. La regulación no debe verse como un obstáculo para la innovación, sino como una forma de garantizar que la tecnología se desarrolla de manera justa y segura, protegiendo siempre los derechos de las personas.

Las empresas tecnológicas, por su parte, no pueden desentenderse. Su responsabilidad no termina cuando ofrecen un producto atractivo o rentable. Tienen el deber de diseñar plataformas seguras, reaccionar con rapidez ante los abusos y ofrecer a los usuarios herramientas claras y accesibles para protegerse. No se puede dejar que la seguridad dependa solo del criterio individual de los usuarios. El bienestar de las personas debe estar por encima de los beneficios económicos.

La seguridad digital tampoco conoce fronteras. Un ciberataque, una campaña de desinformación o un fraude en línea puede pasar de un país a otro en cuestión de horas. Por eso, la cooperación internacional es indispensable. Los Estados deben compartir información, coordinarse en organismos multilatera-

les y establecer estándares comunes que permitan actuar con rapidez y eficacia. La globalización de la tecnología requiere también una globalización de las soluciones. En este contexto, el fenómeno del cibercrimen como servicio (CaaS) demuestra cómo el delito informático se ha convertido en un mercado global, lo que multiplica la necesidad de esa cooperación internacional.

Frente a todo esto, la resiliencia digital se convierte en un objetivo fundamental. Ser resiliente no significa estar a salvo de todos los riesgos, porque eso es imposible. Significa estar preparado para anticiparse, actuar con prudencia y recuperarse cuando algo ocurre. Tener copias de seguridad de los archivos más importantes, usar contraseñas robustas, mantener los dispositivos actualizados y contar con redes de apoyo son ejemplos de cómo se puede reforzar esa resiliencia. También implica un componente emocional y social: saber pedir ayuda, mantener la calma y apoyarse en la comunidad cuando ocurre un problema. Tampoco podemos olvidar los riesgos emergentes: el desarrollo de la computación cuántica amenaza los sistemas de cifrado actuales, lo que hace imprescindible avanzar hacia la criptografía poscuántica para garantizar la seguridad de los datos en el futuro.

La ética completa este panorama. No es suficiente con saber usar la tecnología, hay que usarla bien. Respetar la privacidad ajena, no difundir mensajes de odio, no participar en el acoso digital y pensar en las consecuencias de lo que publicamos son prácticas que hacen del entorno digital un lugar más seguro para todos. La competencia mediática no es solo un conjunto de habilidades técnicas, es también un compromiso con valores como el respeto, la empatía y la responsabilidad.

Todo esto nos lleva a una conclusión clara. La seguridad digital no puede sostenerse solo en programas informáticos más sofisticados ni en leyes más duras. Se necesitan personas formadas y conscientes, instituciones que protejan de verdad, empresas que actúen con responsabilidad y comunidades que fomenten la solidaridad y el cuidado mutuo. La competencia mediática es el elemento que une todos estos aspectos. Apostar por su desarrollo es apostar por un futuro en el que la vida digital sea más segura, más justa y humana, y en el que cada persona, sin importar

su edad o su experiencia, pueda disfrutar de los beneficios de internet sin quedar desprotegida frente a sus riesgos.

La seguridad digital comienza con gestos sencillos. La figura 14 muestra un decálogo con diez recomendaciones prácticas para mejorar la seguridad en el uso cotidiano de la tecnología.

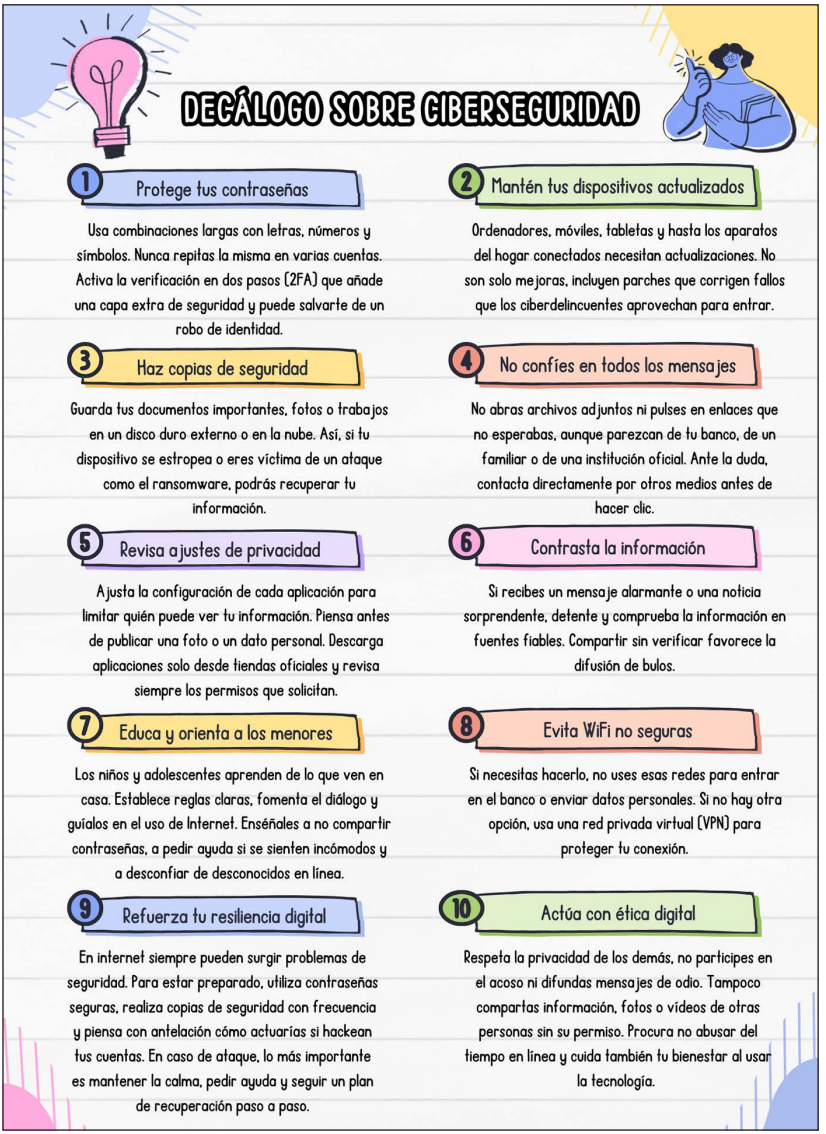

Figura 14. Decálogo de recomendaciones sobre ciberseguridad.

7

Referencias bibliográficas

Agencia Española de Protección de Datos e Instituto Nacional de Ciberseguridad (INCIBE) (s. f.). *Guía de privacidad y seguridad en internet*. https://l1nq.com/G61Z5

Aparici, R., y García-Marín, D. (2018). *Comunicar y educar en el mundo que viene*. Gedisa.

Aranda-Serna, F. J. (2024). Memes as symbols of hate speech: The influence of graphic humour on freedom of expression and politics. *VISUAL REVIEW. International Visual Culture Review Revista Internacional de Cultura Visual*, *16*(2), 241-253. https://doi.org/10.62161/revvisual.v16.5222

Aránguez-Sánchez, T., y Olariu, O. (2021). *Feminismo digital: Violencia contra las mujeres y brecha sexista en internet.* Dykinson.

Area, M., y Pessoa, T. (2012). De lo sólido a lo líquido: Las nuevas alfabetizaciones ante los cambios culturales de la Web 2.0. *Comunicar*, *20*(38), 13-20. https://doi.org/10.3916/C38-2012-02-01

Areitio, I. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Paraninfo.

Ayuntamiento de Almendralejo (2025). *Alerta de suplantación de identidad: Fraude por correo electrónico en nombre del Ayuntamiento de Almendralejo*. Almendralejo. https://bit.ly/3VyNDgo

Aznar-Martínez, B., Casarramona-Basany, A., Grané-Morcillo, J., Lorente-De-Sanz, J., Prats-Fernández, M. À., y Ballester-Brage, L. (2024). Uso responsable de internet y seguridad digital: Revisión sistemática de

programas educativos. *Estudios sobre Educación*, *47*, 125-152. https://doi.org/10.15581/004.47.006

Bada, M., y Sasse, M. A. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. https://arxiv.org/abs/1901.02672

Bakshy, E., Messing, S., y Adamic, L. A. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science*, *348*(6239), 1130-1132. https://doi.org/10.1126/science.aaa1160

Barba, C. (2024). *Deepfakes sexuales: impacto, prevención y perspectivas de género en el entorno digital*. Revista MH&CJ. https://doi.org/10.21134/zt4eht31

Bartsch, M., y Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147-154. https://doi.org/10.1016/j.chb.2015.11.022

Bata-Islas, M. A., Portillo-Vázquez, M., Jiménez-Solares, C. M., y Esparza-Hernández, L. G. (2022). Estrategias pedagógicas para la sociedad del conocimiento, información y cultura del internet. *Revista Arbitrada Interdisciplinaria Koinonía*, *7*(14), 81-101. https://doi.org/10.35381/r.k.v7i14.1876

Beltrán-Muñoz, A. (2024). Educar y proteger: Análisis de la educación en ciberseguridad para combatir la ciberdelincuencia. *Revista de Educación y Derecho*, *30*. https://doi.org/10.1344/REYD2024.30.44082

Boletín Oficial del Estado (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*. https://bit.ly/4lPb8NP

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ..., y Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint*. https://doi.org/10.48550/arXiv.1802.07228

Buckingham, D. (2019). *The media education manifesto*. John Wiley & Sons.

Bustamante-Donas, J. (2010). La cuarta generación de derechos humanos en las redes digitales. *TELOS: Cuadernos de Comunicación e Innovación*, *85*, 80-89. Fundación Telefónica. https://bit.ly/41xUZEA

Bustos-Martínez, L., De-Santiago-Ortega, P. P., Martínez-Miró, M. Á., y Rengifo-Hidalgo, M. S. (2019). Discursos de odio: Una epidemia

que se propaga en la red. Estado de la cuestión sobre el racismo y la xenofobia en las redes sociales. *Mediaciones sociales*, *18*, 25-42. http://dx.doi.org/10.5209/MESO.64527

Candón-Mena, J., y Montero-Sánchez, A. (2021). *Del ciberactivismo a la tecnopolítica: Las nuevas formas de acción colectiva*. Comunicación Social.

Cantero-de Julián, J. I. (2021). *Ciberseguridad y comunicación: guía para una comunicación segura* (Vol. 6). Ediciones de la Universidad de Castilla La Mancha. https://bit.ly/4mnkCju

Carretero, S., Vuorikari, R., y Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. Publications Office of the European Union. https://doi.org/10.2760/38842

Castells, M. (2015). *Networks of outrage and hope: Social movements in the internet age*. Polity Press.

Centro de Investigaciones Sociológicas (2024). *Inseguridad en la red* (Estudio nº 3443, febrero de 2024). https://l1nq.com/iqygw

Chacón-López, H., Caurcel, M. J., y Romero-Barriga, J. F. (2019). Sexting en universitarios: Relación con edad, sexo y autoestima. *Revista Suma Psicológica*, *26*(1), 1-8. https://doi.org/10.14349/sumapsi.2019.v26.n1.1

Chacho-Guambaña, J. M., Granizo, G. P. C., Ruilova, G. A. S., Acurio, J. V. L., y Cuadro, E. I. D. (2025). Tendencias emergentes en ciberseguridad: Retos actuales y futuros en entornos TIC. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *9*(57), 339-349. https://doi.org/10.29018/issn.2588-1000vol9iss57.2025pp339-349

Chalezquer, C. S., y Salaverría, R. (2023). Combatir la desinformación con alfabetización mediática: análisis de las tendencias en la Unión Europea. *Revista latina de comunicación social*, *81*, 1. https://doi.org/10.4185/RLCS-2023-1552

Cloudflare (2017). *¿Qué fue el ataque del ransomware WannaCry?* https://bit.ly/46gubKA

Chesney, R., y Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*(6), 1753-1820. https://dx.doi.org/10.2139/ssrn.3213954

Cobeñas, M. D. P. G. (2022). La pirámide informacional y el derecho al olvido digital. *Revista UNIANDES Episteme*, *9*(2), 244-263.

Conéctate35.es (2023). *Conoce el servicio 'Conectate35.es': Banda ancha vía satélite en zonas rurales poco pobladas*. https://bit.ly/47jFXWF

Consejo de la Unión Europea (2025, 11 de febrero). Cybersecurity: Social engineering. *Consilium*. https://sl1nk.com/nY1TU

Couldry, N., y Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

Crespo-Carchi, G., y Villalva, D. (2024). Libertad de expresión frente a la regulación en la difusión de contenidos en internet. *Digital Publisher CEIT*, *9*(5), 339-352.

Cruz, I. L., y Chicaiza, R. P. M. (2025). Enseñanza de la educación ciudadana en el desarrollo del pensamiento crítico en la era digital. *Digital Publisher CEIT*, *10*(3), 1285-1297.

Cyber Defense Magazine (2025). *The impact of quantum decryption*. Cyber Defense Magazine. https://www.cyberdefensemagazine.com/the-impact-of-quantum-decryption/

Delgado, J. C. V., Muñoz, G. F. R., Padilla, B. A. M., y Quiñónez, V. H. L. (2025). Ciberseguridad y protección de datos personales: desafíos y perspectivas. *GADE: Revista Científica*, *5*(1), 675-688. https://doi.org/10.63549/rg.v5i1.642

Deursen, A. J. A. M., y van-Dijk, J. A. G. M. (2019). The first-level digital divide shifts from inequalities in physical access to inequalities in material access. *New Media & Society*, *21*(2), 354-375. https://doi.org/10.1177/1461444818797082

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ..., y Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

El País (2023). *Identificados 10 menores como autores de los desnudos con inteligencia artificial de Almendralejo*. https://bit.ly/4g6vSi3

El País (2024). *La Agencia de Protección de Datos prohíbe seguir recogiendo datos de iris a Worldcoin, que daba criptomonedas a cambio.* https://bit.ly/45Ux1pz

Elizalde, I. (2020, enero 29). Principales retos para las TIC en educación. *Director TIC*. https://bit.ly/3UBJNmh

Escofet-Roig, A., Rubio-Hurtado, M. J., y Vilà-Baños, R. (2025). *Digital citizenship: Digital participation profiles of women participating in digital literacy programmes*. *Digital Education Review*, *47*, 181-194. https://doi.org/10.1344/der.2025.47.181-194

España Digital (s.f.). *Desarrollo de competencias digitales de la ciudadanía y lucha contra las brechas digitales*. https://bit.ly/45THMsf

European Commission. (2023a). *Digital Services Act: Ensuring a safe and accountable online environment*. https://bit.ly/478qCYJ

European Commission (2023b). *Joint Communication on the EU Policy on Cybersecurity*. European Union.

European Union (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. *Official Journal of the European Union*. https://bit.ly/41fO3vv

Europol (2022). internet Organised Crime Threat Assessment (IOCTA 2022). *Europol*. https://bit.ly/47kuwOv

Ferrés, J., y Piscitelli, A. (2012). La competencia mediática: Propuesta articulada de dimensiones e indicadores. *Comunicar*, *20*(38), 75-82. https://doi.org/10.3916/C38-2012-02-08

Floridi, L. (2021a). *The ethics of artificial intelligence: Principles, challenges, and opportunities*. Oxford University Press.

Floridi, L. (2021b). *The logic of information: A theory of philosophy as conceptual design*. Oxford University Press.

Fonts-Fernández, C. L., y Stable-Rodriguez, Y. (2024). Modelo de Competencias Digitales, Informacionales y Mediáticas para la Transformación Digital. *Revista gestión de las personas y tecnología*, *17*(49), 31-52. http://dx.doi.org/10.35588/tjtd5y16

Fuentes, R. A. S. (2024). Ciberética y derechos humanos: una reflexión respecto de los desafíos digitales en la búsqueda de una sociedad más pacífica y tolerante. *Revista de Derecho y Ciencias Sociales*, *31*, 83-90.

Gandini, A., Keeling, S., y Reviglio, U. (2025). Conceptualising the 'algorithmic public opinion': Public opinion formation in the digital age. *Dialogues on Digital Society*, 29768640251323147. https://doi.org/10.1177/29768640251323147

Galperín, H. (2017). *Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe*. Ministerio Educación Perú.

García-Estévez, N. (2018). Origen, evolución y estado actual del activismo digital y su compromiso social. Ciberactivismo, hacktivismo

y slacktivismo. En *Actas del II Congreso Internacional Move. net sobre Movimientos Sociales y TIC* (pp. 139-159). Compolíticas.

García-García, J. (2025). Respuestas normativas para enfrentar el discurso del odio desde la experiencia europea. *European Public & Social Innovation Review*, *10*, 112. https://doi.org/10.31637/epsir-2025-1904

García-Ruiz, R. (2023). *La alfabetización mediática y digital en el currículum: propuestas didácticas transformadoras*. Dykinson.

García-Salvador, L. (2022). *Ciberseguridad y protección de datos en el entorno digital* [Trabajo final de grado, Universidad de Valladolid]. UVaDOC. https://bit.ly/3H83UWd

Gillespie, T. (2014). The relevance of algorithms. En T. Gillespie, P. J. Boczkowski y K. A. Foot (Eds.), *Media technologies: Essays on communication, materiality, and society* (pp. 167-194). MIT Press.

Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

Giménez-Gualdo, A. M., Sánchez-Romero, E. I., y Torregrosa Díez, M. (2022). El lado oscuro de internet: ¿Predice el cyberbullying la participación en sexting? *Revista Latinoamericana de Psicología*, *54*, 112-119. https://doi.org/10.14349/rlp.2022.v54.13

Gobierno de Canarias (2014). *Estrategias formativas de ciudadanía digital*. https://bit.ly/4gdxw1r

Gobierno de España (2021). *Carta de derechos digitales. Plan de Recuperación, Transformación y Resiliencia*. https://bit.ly/4o93LTb

González, H. (2024, junio 4). Historia de la seguridad informática: Línea del tiempo. *Blog HerschelGonzalez*. https://bit.ly/3GMo0Fu

González-Hugo, M. P., y Quevedo-Sacoto, A. S. (2025). Tendencias actuales en ataques de ingeniería social: Revisión de literatura. *MQRInvestigar*, *9*(1), e203. https://doi.org/10.56048/MQR20225.9.1.2025.e203

González-Valenzuela, C. (2023, 25 de noviembre). *Casos de hacktivismo que han marcado la historia: Desde Anonymous hasta Edward Snowden*. *Computer Hoy*. https://bit.ly/3I1WbJF

Harari, Y. N. (2025, 3 de julio). *La inteligencia artificial puede abrir la puerta a las primeras dictaduras digitales de la historia; la información es la base del poder político*. *La Vanguardia*. https://bit.ly/3I2BwoO

Hernández-Morales, J. A., y González-Brito, H. R. (2023). *Análisis de los desafíos actuales en la prevención de los ciberataques por ransomware*

[Documento PDF]. Universidad de las Ciencias Informáticas; idUS – Depósito de Investigación de la Universidad de Sevilla. https://l1nq.com/sXFl8

Hervás-Paredes, L. M. (2023). *Intimidad, sexting e impunidad: Un análisis crítico jurídico en la legislación ecuatoriana* [Trabajo de grado, Universidad Nacional de Chimborazo].

Hobbs, R. (2010). *Copyright clarity: How fair use supports digital learning*. Corwin Press.

Howard, P. N., Woolley, S. C., y Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics, 15*(2), 81-93. https://doi.org/10.1080/19331681.2018.1448735

INCIBE (2018, 14 de junio). *Busca otro al que engañar, yo no voy a picar*. https://bit.ly/3V3AOe2

INCIBE (2019). *Ingeniería social: Técnicas utilizadas por los ciberdelincuentes y cómo protegerse*. Oficina de Seguridad del Internauta, Instituto Nacional de Ciberseguridad. https://sl1nk.com/1gwj4

INCIBE (2022). *La ciberseguridad al alcance de todos*. Instituto Nacional de Ciberseguridad de España.

INCIBE (2025). *Infografía: Balance de ciberseguridad de INCIBE 2024* [Infografía]. Ministerio para la Transformación Digital y la Función Pública. https://l1nq.com/nvs31

Isaak, J., y Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56-59. https://doi.org/10.1109/MC.2018.3191268

Jenkins, H. (2006). *Convergence culture: Where old and new media collide*. NYU Press.

Jenkins, H., Purushotma, R., Clinton, K., Weigel, M., y Robison, A. J. (2009). *Confronting the challenges of participatory culture: Media education for the 21st century*. MIT Press.

Kaspersky (2017). *What is WannaCry ransomware?* https://bit.ly/47tEn4B

Kolias, C., Kambourakis, G., Stavrou, A., y Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80-84. https://doi.org/10.1109/MC.2017.201

Kosinski, M. (4 de junio de 2024). *¿Qué es el ransomware?* IBM Think. https://bit.ly/4p8AbNX

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., y Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073-1137. https://doi.org/10.1037/a0035618

Kreps, S. E., McCain, R., y Brundage, M. (2020). All the news that's fit to fabricate: AI-generated text as a tool of media misinformation. *Journal of Experimental Political Science, 9*(2), 104-117.

Kruzkaya-Ordóñez, A., Suing, A., Punín, M. I., y Carpio, L. (2024). Ciberseguridad y periodismo: Estrategias para garantizar la seguridad de la información. *RISTI: Revista Ibérica de Sistemas e Tecnologías de Información* (Número Extra 72), 382-392.

Laney, D. (2001). 3D data management: Controlling data volume, velocity and variety. *META Group*.

Livingstone, S., Haddon, L., Görzig, A., y Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children*. EU Kids Online.

Livingstone, S., Mascheroni, G., y Staksrud, E. (2021a). European research on children's internet use: Assessing the past and anticipating the future. *New Media & Society, 23*(3), 483-500. https://doi.org/10.1177/1461444816685930

Livingstone, S., Stoilova, M., y Nandagiri, R. (2021b). *Children's data and privacy online: Growing up in a digital age*. Policy Press.

López-Sánchez, J. (2019). *Métodos y técnicas de detección temprana de casos de phishing*. https://bit.ly/4gbcNeG

Madariaga, B. (2025, mayo 29). SEIDOR y Cisco revolucionan la ciberseguridad con IA, SSE y SASE. *Director TIC*. https://bit.ly/45a13E1

Maldita.es (2025, 18 de junio). Mayores y timos: Por qué la alfabetización digital, el acompañamiento y los entornos accesibles son la clave para una vida digital segura. *Maldita Timo*. https://l1nq.com/nackk

Marciano, V., Du Toit, J., y Maluleka R. (2024). *Gamification in Cibersecurity training: High-level properties of cibersecurity games*. Human Aspects of Information Security and Assurance.

Matamoros-Fernández, A. (2017). Platformed racism: The mediation and circulation of an Australian race-based controversy on Twitter, Facebook and YouTube. *Information, Communication & Society, 20*(6), 930-946. https://doi.org/10.1080/1369118X.2017.1293130

Marwick, A. E., y Boyd, D. (2011, September). The drama! Teen conflict, gossip, and bullying in networked publics. In *Teen Conflict, Gossip, and Bullying in Networked Publics (September 12, 2011). A Decade in internet Time: Symposium on the Dynamics of the internet and Society*. https://bit.ly/3IPHCcp

Martínez, J. J. Z., Moreno, J. A. R., y Ponzo, L. C. H. (2025). Alfabetización digital y derechos de privacidad en la era de las TIC: Análisis documental desde la perspectiva legal y ética del manejo de información. *Revista de Investigación en Tecnologías de la Información*, *13*(29), 71-81. https://doi.org/10.36825/RITI.13.29.007

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258-269. https://doi.org/10.17645/mac.v8i2.2855

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Mayo-del-Amo, C. (2022). *Análisis y técnicas de prevención, detección y ataques de phishing* (Trabajo de fin de máster). Universidad Nacional de Educación a Distancia.

McChesney, R. W. (2013). *Digital disconnect: How capitalism is turning the internet against democracy*. New Press.

McDougall, J., Zezulkova, M., van Driel, B., y Sternadel, D. (2018). *Teaching media literacy in Europe: Evidence of effective school practices in primary and secondary education (NESET II report)*. Publications Office of the European Union. https://bit.ly/3J8K0Lb

Mendoza-Michilot, M., Dejo-Vásquez, M., y Najar-Ortega, R. (2025). El papel de los medios frente al fraude informático: Difusión, prevención y alfabetización. *Contratexto*, *43*, 221-288. https://doi.org/10.26439/contratexto2025.n43.7160

Ministerio del Interior (2023). *Informe sobre la cibercriminalidad en España, 2023* (NIPO 126 20 021 2). Gobierno de España. https://l1nq.com/3NVAc

Morais, J., Simões, J., Lourenço, J., y Sargo Lopes, S. (2022). Perceptions on gamification towards cybersecurity literacy: Social sustainability of educative projects. *Revista EDaPECI*, *22*(3), 63-77. http://dx.doi.org/10.29276/redapeci.2022.22.3182471.63-77

Morales-Bueno, P. (2018). Aprendizaje basado en problemas (ABP) y habilidades de pensamiento crítico ¿una relación vinculante? *Revista Electrónica Interuniversitaria de Formación del Profesorado*, *21*(2), 91-108. https://doi.org/10.6018/reifop.21.2.323371

Morales-Ramírez, O. (2025). Ciberfraude: principales métodos de ataque y estrategias para su prevención. *Revista Científica Multidisciplinaria*, *9*(3), 490-4916. https://doi.org/10.37811/cl_rcm.v9i3.18122

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38-41.

Mosco, V. (2017). *To the cloud: Big data in a turbulent world*. Paradigm Publishers.

Nación321 (2017, 25 de octubre; actualización 2024, 16 de febrero). *5 ocasiones en que las redes sociales movilizaron al mundo*. Nación321. https://bit.ly/4p4f2V0

Naciones Unidas (2019). *The age of digital interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation*. https://bit.ly/4fc2Zk2

NIST (2025). *Post-Quantum Cryptography Standardization*. National Institute of Standards and Technology.

Nixon, C. L. (2014). Current perspectives: The impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics*, *5*, 143-158. https://doi.org/10.2147/AHMT.S36456

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

OECD (2022). *Bridging the digital divide: Policies to improve digital inclusion*. OECD Publishing. https://doi.org/10.1787/31cfd8c7-en

OECD (2023). *Digital education outlook 2023: Toeards and Effective Digital Education Ecosystem*. OECD Publishing.

Olivo, D. C., y Rueda-Estrada, V. (2025). Acción colectiva digital: reinterpretación de conceptos en movimientos sociales. *SAPIENTIAE Revista de Ciências Sociais, Humanas e Enghenerias*, *11*(1), 63-78.

ONU (1948). *Declaración Universal de los Derechos Humanos*. https://bit.ly/3JYXARM

Organización de los Estados Americanos y Twitter (2021). *Alfabetización y seguridad digital: La importancia de mantenerse seguro e informado*. https://bit.ly/465gijD

Pacheco, F., Staino, D., y Sliafertas, M. (2024). Educación en ciberseguridad mediante estrategias de gamificación. *CONAIISI 2024*. https://doi.org/10.13140/RG.2.2.32723.59681

Pacto Mundial de la ONU (2022, 3 de mayo). *¿Qué son los derechos digitales y cuál es su relación con los ODS?* https://bit.ly/42nSViH

Parcerisa, L., Massó, B., y Lindín, C. (2024). Gobernanza digital de la educación: Tensiones y retos en el derecho a la privacidad y la protección de datos. En P. Rivera-Vargas y J. Jacovkis (Coords.), *Plataformas digitales y corporaciones tecnológicas en la escuela: Una mirada desde los derechos de la infancia.* Octaedro.

Paris, B., y Donovan, J. (2019). *Deepfakes and cheap fakes. The manipulation of audio and visual evidence.* Data & Society Research Institute Report.

Pariser, E. (2011). *The filter bubble: What the internet is hiding from you*. Penguin.

Pariser, E. (2017). *El filtro burbuja: Cómo la web decide lo que leemos y lo que pensamo*s. Taurus.

Pérez-Alarcón, S. C. (2023). *El sexting: Características y alcance de la práctica del sexting como delito informático*. https://bit.ly/47URjAv

Pérez-Tornero, J. M. P., Gómez, J. I. A., Liaño, S. G., Giménez, M. D. M. P., Cabalin, C., Malavé, N. M., ..., y Aledo, B. B. (2013). Educación y medios de comunicación. *Sphera Pública, 12*, 5-17.

Pochmara, J., y Świetlicka, A. (2024). Cybersecurity of industrial systems–A 2023 report. *Electronics, 13*(7), 1191. https://doi.org/10.3390/electronics13071191

Puican-Ordoñez, A. L. (2024). *El doxing y su necesaria incorporación en los delitos informáticos* [Tesis de licenciatura, Universidad Señor de Sipán]. Repositorio Institucional USS. https://bit.ly/3JILLz9

Ramanpreet K., Dušan G., y Tomaž, K. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Ramasundaram, A., Pandey, N., Shukla, Y., Alavi, S., y Wirtz, J. (2023). Fluidity and the customer experience in digital platform ecosystems. *International Journal of Information Management, 69*. https://doi.org/10.1016/j.ijinfomgt.2022.102599

Ratha, N. K., Connell, J. H., y Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal, 40*(3), 614-634. https://doi.org/10.1147/sj.403.0614

Reneses-Botija, M., Riberas-Gutiérrez, M., y Bueno-Guerra, N. (2024). ¿Quién comparte fake news? Consumo y distribución de información entre adolescentes y su relación con el discurso de odio. *Revista de Educación*, *1*(406). https://doi.org/10.4438/1988-592X-RE-2024-406-645

Revista Ciberseguridad (2021). *El ataque de ransomware colapsa el SEPE*. https://bit.ly/47Agx7g

Ribble, M., y Bailey, G. (2004). Digital Citizenship: Focus Questions for Implementation. *Learning & Leading with Technology, 32*(2), 12-15.

Ribble, M. (2012). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). ISTE.

Ruiz, F. C. (2023). Herramientas digitales para fomentar la alfabetización mediática en la era digital. *Revista Ingenio Global*, *2*(1), 35-45. https://doi.org/10.62943/rig.v2n1.2023.60

Ruiz, B. H. Y., López, M. F. M., Marín, J. Z. C., Cárdenas, M. C. R., Veloz, M. G. V., y Jiménez, E. L. J. (2025). Innovaciones en la alfabetización mediática: Formando ciudadanos críticos en la era de la información. *South Florida Journal of Development, 6*(1), e4905. https://doi.org/10.46932/sfjdv6n1-010

Santana, L. E., y Serra, I. (2022). *El enfoque de derechos humanos y ciudadanía digital en la ciudad*. CEPAL.

Secker, J., y Morrison, C. (2022). Copyright Education and Information Literacy. In: *Navigating Copyright for Libraries: Purpose and Scope*. (pp. 285-318). Walter de Gruyter. https://doi.org/10.1515/9783110732009

Schwab, K. (2024). The Fourth Industrial Revolution: what it means, how to respond1. En *Handbook of research on strategic leadership in the Fourth Industrial Revolution* (pp. 29-34). Edward Elgar Publishing.

Siemens, G. (2004). Elearnspace. Connectivism: A learning theory for the digital age. *Elearnspace. org*, 14-16.

Smith, P. K., Mahdavi, J., Carvalho, M., y Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49*(4), 376-385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Sola-Morales, C., y Sabariego, J. (2021). Tecnopolítica y movilización digital: Una aproximación al estudio de los movimientos sociales

globales. *Teknocultura*, *18*(1), 121-145. https://doi.org/10.5209/tekn.66241

Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.

Statista. (2023). Number of IoT connected devices worldwide from 2019 to 2030 by communicatins technology. *Statista Research Department*. https://bit.ly/4gdqs56

Tandoc, E. C., Lim, Z. W., & Ling, R. (2018). Defining "fake news". *Digital Journalism*, *6*(2), 137-153. https://doi.org/10.1080/21670811.2017.1360143

The Guardian. (2024). Calls for action after AI-generated sexual images of Taylor Swift spread online. *The Guardian*. https://bit.ly/3VBL0dU

Trujillo-Flórez, L. M. (2022). Competencias digitales para el siglo XXI: Una visión desde la ciudadanía digital. *Panorama*, *16*(31), 360-385.

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal*, *13*, 203-218.

Unesco (2011a). *Media and information literacy curriculum for teachers*. Unesco Publishing. https://bit.ly/3UZhkHr

Unesco (2011b). *Digital literacy in education: Policy brief*. https://bit.ly/3Ha2eeM

Unesco (2023). *El uso de la IA en la educación: Decidir el futuro que queremos*. https://bit.ly/4nkGlJ4

Unicef. (2025). *Día de Internet Segura*. https://bit.ly/46tM9Lj

Valle-Peris, M. (2022). Evolución y consecuencias de la hiperconectividad. *Proyecta 56, an Industrial Design Journal*, *2*, 58-75. https://doi.org/10.25267/P56-IDJ.2022.i2.05

Vaccari, C., y Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society*, *6*(1), 1-13. https://doi.org/10.1177/2056305120903408

van-Dijk, J. (2006). Digital divide research, achievements and shortcomings. *Poetics*, *34*(4-5), 221-235. https://doi.org/10.1016/j.poetic.2006.05.004

van-Dijk, J., Poell, T., y De-Wall, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.

van-Dijk, J. (2020). *The Digital Divide*. Cambridge: Polity Press.

Vera-Baceta, M.-Á., Navarro, G., y Gómez-Hernández, J.-A. (2022). Riesgos de la aceleración digital: Una mirada desde el Marco DIGCOMP2.2 y los derechos digitales de la ciudadanía. *Anuario ThinkEPI*, *16*, e16a19. https://doi.org/10.3145/thinkepi.2022.e16a19

Vílchez-Vera, A., Paredes-León, F., Martínez, R., Moreno, L., y Huaches, S. (2025). Prevención contra las estafas electrónicas en adultos mayores: Aproximación a un modelo educativo de alfabetización digital. En *Tecnologías inclusivas: Construyendo un futuro educativo accesible* (p. 187). Conaic.

Vosoughi, S., Roy, D., y Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146-1151. https://doi.org/10.1126/science.aap9559

Yagos-Estrada, G. C. (2024). *El ciberdelito del sexting y las dificultades probatorias* [Trabajo de grado, Universidad Nacional de Chimborazo, Riobamba, Ecuador].

Wardle, C., y Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for research and policy making*. Strasbourg, Council of Europe.

Zaldívar-Martínez, J. J., Rodelo-Moreno, J. A., y Hernández-Ponzo, L. C. (2025). Alfabetización digital y derechos de privacidad en la era de las TIC: Análisis documental desde la perspectiva legal y ética del manejo de información. *Revista de Investigación en Tecnologías de la Información*, *13*(29), 71-81. https://doi.org/10.36825/RITI.13.29.007

Zhuk, A. (2024). *Ethical implications of AI in the metaverse*. AI and Ethics. https://doi.org/10.1007/s43681-024-00450-5

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Índice

Prólogo 9

1. Competencia mediática y digital en la sociedad hiperconectada 13
   1.1. Fundamentos teóricos para la adaptación al entorno digital 15
   1.2. Usos de internet en la sociedad y sus implicaciones 19

2. Ciberseguridad y protección en el entorno digital 25
   2.1. Riesgos de internet: Desafíos para una sociedad digital (des)informada 27
   2.2. Privacidad digital y competencia mediática, estrategias para una navegación segura 31

3. Fraudes en la red y seguridad digital a través de la alfabetización mediática 37
   3.1. Fraudes en internet y estrategias de detección 40
   3.2. Herramientas y estrategias para una ciudadanía crítica y segura 45

4. Ciudadanía digital: Responsabilidades, derechos y alfabetización crítica 49
   4.1. Ética y responsabilidad en la comunicación digital 52
   4.2. Ciberactivismo, participación y seguridad digital 57

5. Competencia mediática y ciberseguridad en el futuro de internet 63
5.1. Nuevas tecnologías y desafíos emergentes en ciberseguridad 64
5.2. Construcción de una ciudadanía digital crítica y resiliente 71
5.2.1. Integración en el plan de estudios 72
5.2.2. Formación de profesores 72
5.2.3. Programas de sensibilización 72
5.2.4. Desarrollo del pensamiento crítico y la verificación informativa 73
5.2.5. Inclusión e igualdad 73
6. Conclusiones y recomendaciones 77
7. Referencias bibliográficas 83

Ciberseguridad y competencias mediáticas en la era digital

Protección, privacidad y ciudadanía digital

Esta es una obra académica que aborda los retos y oportunidades del ecosistema digital desde un enfoque transversal basado en la competencia mediática y digital. El libro parte de la premisa de que, en un mundo hiperconectado, no es posible entender la ciberseguridad únicamente desde una dimensión técnica, sino que debe integrarse con habilidades críticas, éticas y comunicativas que fortalezcan una ciudadanía digital informada y responsable.

La obra está estructurada en cinco bloques temáticos que recorren los usos de Internet en la sociedad, los riesgos más frecuentes en entornos digitales (como el fraude, la desinformación o el robo de identidad), y las responsabilidades individuales y colectivas en el entorno digital. Una de sus principales fortalezas es que cada capítulo no solo presenta información actualizada y bien fundamentada, sino que está orientado a promover la reflexión crítica a través de la alfabetización mediática. Así, la competencia mediática no es un tema aislado, sino el hilo conductor de todo el libro.

Otra de sus aportaciones destacadas es el equilibrio entre teoría y práctica. A lo largo del texto se presentan herramientas de análisis, modelos educativos, estrategias de protección digital y propuestas pedagógicas, que permiten aplicar los conocimientos tanto en contextos educativos como profesionales. Además, el enfoque ético y social del libro permite comprender la ciberseguridad no solo como una defensa tecnológica, sino como un derecho y un deber ciudadano.

Esta obra se dirige especialmente a investigadores, docentes, profesionales de la comunicación y educadores interesados en formar a ciudadanos críticos y seguros en entornos digitales. Su valor reside en ofrecer una visión amplia, actual y comprometida con los valores democráticos, proponiendo una educación digital que empodere a las personas frente a los desafíos contemporáneos.

En definitiva, este libro constituye una aportación relevante y original en el campo de la ciberseguridad desde la perspectiva de la competencia mediática, ofreciendo conocimientos rigurosos, reflexiones profundas y estrategias prácticas para vivir Internet con seguridad, ética y sentido crítico.

