

7. Algunos peligros del uso de las tecnologías en el campo de la salud



ROSA ELIZABETH SEVILLA GODÍNEZ*
GEORGINA VEGA FREGOSO**

DOI: <https://doi.org/10.52501/cc.464.07>

Resumen

Este capítulo analiza los riesgos éticos, legales y sociales derivados de la incorporación de tecnologías emergentes en el ámbito de la salud, particularmente la inteligencia artificial, el Big Data y la digitalización de los servicios médicos. Se examina cómo estas herramientas, aunque prometen eficiencia y precisión diagnóstica, plantean dilemas relacionados con la privacidad, la autonomía del paciente y la responsabilidad profesional. El texto subraya que la ciberseguridad y la protección de datos personales son condiciones indispensables para garantizar la confianza en la medicina digital. Asimismo, se advierte sobre el peligro de que los algoritmos reproduzcan sesgos estructurales, pues generan desigualdades en el acceso y calidad de la atención. Desde la perspectiva del bioderecho, se propone que la regulación tecnológica debe estar orientada por principios bioéticos y derechos humanos, para asegurar que la innovación no se convierta en una amenaza para la dignidad humana. El capítulo concluye que el reto contemporáneo consiste en equilibrar el potencial transformador de la tecnología con la obligación ética y jurídica de proteger al paciente como sujeto de derechos.

* Doctora en Ciencias Socio-Médicas. Investigadora en el Centro Universitario de Ciencias de la Salud, de la Universidad de Guadalajara, México. ORCID: <https://orcid.org/0000-0002-6935-5788>; Scopus: 57201449035; correo electrónico: elizabeth.sevilla@academicos.udg.mx

** Doctora en Ciencias Sociales. Profesora-investigadora en el Centro Universitario de Ciencias de la Salud, de la Universidad de Guadalajara, México. ORCID: <https://orcid.org/0000-0001-8943-1699>

Palabras clave: *inteligencia artificial, big data, ciberseguridad, atención médica.*

Introducción

En su libro *La convivencialidad* (1973), Iván Illich aborda un concepto útil para proponer en nuestro pensamiento de profesionales un criterio ético para responder a la pregunta ¿qué significa usar la tecnología en el campo de las ciencias de la salud? Este concepto es *equilibrio multidimensional de la vida humana*. A Illich este concepto amplio le permite, como a nosotras, entrar al problema de fondo en este capítulo: ¿Cómo es la relación que los médicos y cualquier otro profesional de ciencias de la salud establecen con la herramienta? En este caso, la herramienta son las tecnologías.

La palabra *tecnología* no se refiere solo a máquinas o dispositivos digitales, sino a un conjunto organizado de conocimientos, técnicas y procedimientos que permiten intervenir en la realidad para transformarla. La ciencia es un producto social, por ello, atendiendo al contexto mexicano, en menos de una década hemos acelerado la incorporación de las tecnologías debido a que nos proveen rapidez y precisión en el diagnóstico, facilitan la comunicación entre el médico y el paciente, contribuyen a la rápida consulta y al conocimiento de distintos padecimientos, y agilizan la configuración de opciones de tratamiento, entre otras cosas (García, 2022; Monobanda, 2024).

Entre otras ciencias de la salud, es en la práctica de la medicina donde, de manera importante, se refleja el desarrollo de la tecnología: en la atención a distancia, en el acceso a las consultas con la telemedicina y en procesos de atención como las cirugías de control remoto. El campo de la tecnología médica presenta diversos niveles de sofisticación y, con ello, un profuso aumento de datos e informaciones que, en ocasiones, se vuelve difícil manejar; por ello, a pesar de estos avances y beneficios, también existen peligros asociados al uso de las diversas tecnologías (tabla 7.1), por ejemplo, el adecuado resguardo de la información que se maneja en el sector salud, que implica datos sensibles, pues la información sobre el estado de salud de los pacientes requiere un estricto control de seguridad y confidencialidad (Cervera, 2024; Pavón, 2024). En este capítulo se abordan algunos de esos peligros a los que se enfrentan los pacientes, los profesionales y los servicios de salud debido a estos desarrollos tecnológicos.

Tabla 7.1. Peligros en el uso irracional de la tecnología

<i>Peligro</i>	<i>Atenta contra</i>
Datos personales	Uso inadecuado Confidencialidad
Opacidad en las decisiones	Autonomía y proceso decisional
Anonimización	Dignidad de la persona
Trato diferente con un humano Deshumanización del acto médico	Fiabilidad de las decisiones
Reducción del paciente a datos	Integridad corporal simbólica
Ataque a bases de datos hospitalarias	Privacidad y seguridad, uso comercial de datos clínicos
Dependencia tecnológica	Singularidad y relacionalidad

Fuente: elaboración propia.

El desarrollo tecnológico y la tecnología en el ámbito médico

En sentido amplio, el desarrollo tecnológico es un proceso por el cual una sociedad crea o mejora sus tecnologías con el objetivo de resolver problemas o paliar necesidades, generalmente se asocia con conceptos como innovación y un fortalecimiento de la producción inter y transdisciplinar del conocimiento científico. En materia de avances tecnológicos en el área de ciencias de la salud, cada año se reportan novedades; a continuación, en la tabla 7.2 se presentan algunos de los principales desarrollos tecnológicos susceptibles de usarse en alguna de las fases de la atención.

Tabla 7.2. Avances recientes: tecnología y medicina

<i>Inteligencia artificial</i>	Robots quirúrgicos que integran tecnologías de realidad aumentada e inteligencia artificial (IA)	Vacunas con tecnología de ARN mensajero
<i>Wearables para la salud</i>	Gemelos digitales permiten la simulación precisa del comportamiento de órganos y sistemas humanos vía super-computadoras e IA	Órganos en chip y bioimpresión 3D
<i>Nanotecnología en medicina</i>	Medicina regenerativa para la reparación de órganos dañados	Tecnología de edición genética CRISPR

Fuente: Elaboración propia con información de Guio (2024).

Estas contribuciones tecnológicas generan más información en torno a la salud de los pacientes y representan un reto en el resguardo y gestión para los médicos y las instituciones de salud; por ejemplo, una adecuada organización y gestión de los datos impulsa una atención más eficaz y personalizada, pero ¿qué tan seguros están nuestros datos?

Ernesto Trens Flores, en su artículo “El desarrollo tecnológico y las políticas de salud” (2000), plantea que, cuando una institución incorpora un servicio o usa un método nuevo, se opera un cambio tecnológico; también plantea que la tecnología tiene un ciclo de vida, digamos que atraviesa por fases: introducción, aceptación, madurez en el conocimiento, transferencia y declinación. El autor sostiene que la incorporación de tecnologías en el campo de la salud tiene dos vertientes: por un lado, la industria paramédica, responsable del desarrollo de equipo médico; por el otro, la industria farmacéutica, quien se encarga de investigar y desarrollar nuevos medicamentos. Además, existe una tercera vertiente, la de la gestión de datos hospitalarios y de salud, en donde es imprescindible el uso tecnológico para la organización y manejo de un gran cúmulo de datos, es decir, Big Data.

En el artículo “Aplicación del *bid data* en la gestión sanitaria hospitalaria: oportunidades, retos y perspectivas futuras”, Carlos García Ruiz y colaboradores (2025) señalan justamente que “el actual aumento del volumen de datos clínicos, generados por las distintas aplicaciones que componen los entornos hospitalarios, ofrecen posibilidades para mejorar la calidad asistencial e incrementar la eficiencia y productividad mediante el uso de Big Data”; sin embargo, el uso masivo de datos también abre un horizonte donde la vigilancia y estrategias de ciberseguridad son imprescindibles para garantizar que no existan abusos tanto de instancias de gobierno como de corporativos nacionales y transnacionales.

Equidad en el acceso y costos de atención

Como hemos expuesto, la aplicación de la tecnología en el campo de la salud juega un papel muy importante; para ello, se deben destinar los recursos suficientes para reducir la inequidad por el acceso desigual a servicios e innovaciones tecnológicas entre la población mexicana.

El equipo y la tecnología médica, desde la aparición de la cápsula endoscópica hasta los robots Da Vinci, demandan millones de dólares, recursos que no siempre se encuentran disponibles para beneficiar a las mayorías; por ello, la primera estrategia, que no genera costos innecesarios y no excluye a ningún grupo social, es la atención primaria a la salud (APS).

En México, en 2022, según el HospiRank 2022, elaborado por Global Health Intelligence, de los 3 655 hospitales mexicanos registrados, solo 24 contaban en ese año con equipos de cirugía robótica; de esos, solo ocho son hospitales públicos, y siete de ellos se encuentran solamente en Ciudad de México. Sin embargo, es necesario tener en mente que, a pesar de que la tecnología tiene múltiples beneficios y usos en salud, la equidad debe ser una guía en el acceso, sobre todo considerando que México tiene un elevado índice de Gini, un poco más de la mitad de la riqueza del país se concentra en una décima de la población, más de la tercera parte vive en pobreza multidimensional (educación, salud, alimentación, vivienda, seguridad social) y solo el 30% de la población indígena no presenta pobreza (Meneses, 2025).

Esto permite identificar un peligro: la tecnología solo es la herramienta, un medio, en tanto el lugar de nacimiento y residencia actúa como determinante de la salud. De hecho, según la región de origen, la probabilidad de acceder plenamente a una atención médica oportuna y de calidad varía de forma drástica. ¿Es ético excluir a unos y privilegiar a otros?

Otro ejemplo del uso ético de la tecnología es la telemedicina, con ella se acortan distancias, se facilita en un nivel la comunicación, se agilizan los diagnósticos y los tratamientos en las poblaciones más alejadas; esto funciona como una tecnología que permite al Estado garantizar derecho a la salud a los grupos sociales que se encuentran subatendidos (Alegre et al., 2024).

Si se hace una revisión desde la perspectiva de la geografía de la salud, se podrá identificar que nuestro país tiene una diversidad orográfica y sociocultural que hacen complejo que el Estado garantice el pleno acceso a servicios de salud; por tanto, el diseño e implementación de las tecnologías digitales en salud generan equidad. Como profesionales de la salud, debemos cuidar no generar diferencias de atención con el uso de tecnología, de acuerdo al género y a la edad, para no imponer cargas extras a los pacientes, considerando que no en todos los lugares se tiene acceso a internet o que hay un importante grupo de población que aún no está familiarizado con el uso de

tablets, computadores y celulares (Cárdenas, 2025). Para lograr una equidad, cobertura, calidad y acceso universal es necesario disminuir la desigualdad que impera en más de la tercera parte de la población que no cuenta con acceso a internet en México (Jiménez, 2022).

Con esta perspectiva, la Organización Mundial de la Salud, en el documento *Estrategia Mundial sobre Salud Digital 2020-2025* (2021), promueve cuatro estrategias, de las cuales la cuarta busca que las tecnologías digitales se encaminen a generar soluciones con un enfoque en igualdad de género y equidad en salud (Vidal, 2023), lo que disminuiría las diferencias de atención (Cárdenas, 2025). Por otro lado, el Objetivo de Desarrollo Sostenible núm. 9 busca que los países fortalezcan la innovación e infraestructura en salud (Jiménez, 2022), lo que debería reflejarse en un beneficio global.

Existe una diferencia entre considerar la determinación social de la salud y los determinantes sociales de la salud. La determinación social plantea que la salud y la enfermedad están condicionados por procesos históricos estructurales, ligados al modo de producción, las relaciones de poder, la desigualdad y la organización social; por ejemplo, que en el mundo impere un sistema económico capitalista neoextractivista, tiene un costo y un peso específico en las posibilidades de enfermar o mantener la salud de la población empobrecidas; concretamente, imaginemos a la familia de un minero que trabajaba en la mina Pasta de Conchos, ubicada en Nueva Rosita (Coahuila, México), ¿cómo la tecnología puede contribuir a que su salud se mantenga y, en caso de enfermar, no muera?

Como forma complementaria, los determinantes sociales de la salud no miran procesos, sino contextos aislados e individualizados: variables de ingreso, educación, vivienda, trabajo y acceso a servicios; es decir, plantean que la forma en que las personas nacen, se desarrollan, envejecen y viven determina si es capaz de mantenerse sano o enfermar; sin embargo, ¿conoces las condiciones de trabajo de un minero en la actualidad?

Algunos autores señalan la necesidad de ampliar estas ideas y proponen hablar de determinantes digitales en salud, a fin de identificar y reducir las brechas que puedan generar diferencias en la salud de las personas y comunidades (Vidal et al., 2023) por las desigualdades en el acceso y uso de las tecnologías (Díaz de León, 2020), a la par que se promueve la asequibilidad digital desde el Estado y los gobiernos locales (Alarcón, 2025).

Ciberseguridad y uso ético de tecnología en ciencias de la salud

La ciberseguridad es la práctica de proteger personas y datos de los ataques de *hackers* o ciberataques; en este marco y considerando que las brechas digitales en México limitan el acceso y uso exitoso de las herramientas (Hincapie, 2024) y servicios para el cuidado, prevención y control de la salud (Bagolle, 2022) que provee la telemedicina, debemos reparar en la alfabetización digital tanto para médicos y otros profesionales de la salud como para los pacientes. La alfabetización digital y la brecha digital deben incluirse como elementos de desigualdad; podemos hablar de brecha digital en el área rural, brecha digital en personas con discapacidad, brecha digital en personas de mayor edad (Panadés, 2024) y brecha digital en personas socialmente desfavorecidas (Vidal et al., 2023). Entonces, una perspectiva ética plantea que el uso de la tecnología debe ir dirigida a todas las personas sin importar el género, edad, sexo, nivel socioeconómico, territorio o discapacidad, pues de esta manera se puede hablar de inclusión y equidad (Alarcón, 2025; Bagolle, 2022).

La disponibilidad de la tecnología puede provocar que las personas que más requieren de atención médica sean las más desfavorecidas por no contar con el acceso a una red de internet ni conocimiento en el uso de la tecnología, y que no se vean favorecidas con el desarrollo de la digitalización en salud (Panadés, 2024). El Observatorio Nacional de Inequidades en Salud evidenció en un informe que las personas con mayor concentración de pobreza son las más afectadas en diferentes indicadores: razón de mortalidad materna, tasa de mortalidad infantil, mortalidad en menores de cinco años, tasa de mortalidad general, tasa de mortalidad por condiciones crónicas, carencias sociales relacionadas con salud y servicios hospitalarios; aunque no lo señala, no es necesario hacer un gran análisis para intuir que se puede agregar una diferencia de los beneficios derivados por los servicios relacionados con la tecnología en salud (Secretaría de Salud, 2019).

El uso equitativo de la tecnología en salud debe encaminarse como una política pública de acceso universal que priorice la atención primaria y reduzca la falta de cobertura en las regiones que más lo necesitan. Con ello, se puede contribuir a disminuir la inequidad en los servicios de atención en

salud en las poblaciones más desfavorecidas, sin olvidar que el alto costo del uso de la tecnología en el campo de la salud conlleva al mismo tiempo un posible acceso no equitativo para todos (Gutiérrez, 2022).

Por otro lado, es prioritario resguardar la seguridad de los datos de salud. Los datos contenidos en los servidores de los hospitales tienen 10 veces más información que la de las tarjetas de crédito (Cartwright, 2023), ya que archivan recetas, datos de identidad, tratamiento, alergias, datos de contacto, número de identificación social, derechos a seguros, direcciones, etc. (De Luca y López, s.f.; Pavón, 2024). Incluso los datos personales en salud son los más cotizados en los mercados negros (Alzuri, 2021; Cervera, 2024), y son blanco de *hackers* (CAF, 2022).

El sector salud fue el sector que más ciberataques recibió en 2019; el costo promedio llegó a 7,13 millones de dólares, lo doble que en cualquier otro sector (Alzuri, 2021). Este dato se agrava si se considera que se tarda casi un año en detectar un ataque a la institución (Alzuri, 2021).

Desde el año 2020, los costos de la brecha de seguridad digital han incrementado en un 53% (Cervera, 2024). Se ha estimado que el costo promedio de una brecha de seguridad (que implica pérdida de datos, corrección del daño, reputación) para una empresa latinoamericana alcanza 1,16 millones de dólares (Gomero, 2024).

En 2022, hubo un incremento del 84% en los ciberataques en el sector salud (s,a, 2024); en ese mismo año, las empresas latinoamericanas sufrieron al menos un ataque de ciberseguridad, algunas hasta casi cuatro al año. México ocupó el segundo lugar, con un 17% de incidentes de seguridad (Gomero, 2024). En la tabla 7.3 se muestran algunos casos de ciberataques.

Tabla 7.3. *Ejemplos de ataques a la seguridad de los datos digitales en los últimos años*

Lugar	Ataque	Estrago	Costo
Reino Unido	WannaCry	Interrumpió los servicios en un tercio de hospitales y alrededor del 8% de consultas de medicina general (19 000 citas canceladas)	

Nota. Tabla 7.3 continúa en la siguiente página

Tabla 7.3 (Continuación)

<i>Lugar</i>	<i>Ataque</i>	<i>Estrago</i>	<i>Costo</i>
Hollywood Presbyterian Medical Center de los Ángeles (EU)	Ransomware	Sistemas afectados volvieron a estar operativos	Pagó un rescate para liberar sus sistemas informáticos (40 bitcoins con un valor equivalente a 15 000 euros)
Hospital Universitario de Düsseldorf (Alemania)	Sin datos	Se afectaron los servidores y se cerró el servicio de urgencias	Primera muerte derivada de un ataque cibernético
Hospital Clínic de Barcelona (España)	Filtraron historias clínicas e investigaciones	Cancelación de procesos e intervenciones a pacientes	
Canadian Capital Health Communication Center	Ransomware	Afectación total al sistema de ambulancias	Impedimento a los paramédicos para localizar llamadas
Lurie Children's Hospital de Chicago	Ransomware	Inhabilitada la línea de red informática del hospital	Venta de datos robados del hospital
Octapharma	Ransomware	Cerró centros de plasma en 35 estados de EEUU	Se publicaron datos de donantes, de laboratorio, datos de empleados y de la empresa

Fuente: Elaboración propia a partir de Cervera, 2024; CSOA, 2024.

Al mundo los delitos cibernéticos le cuestan alrededor del 0.5% del PIB. En América Latina y el Caribe, cuestan cerca de 90 000 millones de dólares (BID, 2016), mientras que el ciberespionaje y la ciberguerra se encuentran en el lugar 14 de los riesgos a nivel mundial. Se estima que se posicionará en el quinto lugar dentro de los siguientes dos años (WEF, 2025). Por ello, es vital fortalecer la seguridad cibernética. México es parte del Convenio de Budapest sobre delitos cibernéticos, creado en 2001, el cual establece diferentes lineamientos para protección ante estos ataques a través de leyes sustantivas y procesales (BID, 2016). Además, es necesario contar con herramientas que permitan salvaguardar los datos y asegurar su confidencialidad en garantía de los derechos de las personas, para proteger las cuestiones bioéticas (Alegre, 2024). En 2017, México estableció estrategias de ciberseguridad y legislación en ciberseguridad; cuenta además con Equipos de Respuesta ante Incidentes de Seguridad informática (csirt, por sus siglas en inglés) (BID, 2024).

México también cuenta con una normativa en el campo de telesalud desde 2021, y en el Expediente Clínico Electrónico desde 2012 (Alegria, 2024); además, a nivel federal, aplica la Norma Oficial Mexicana NOM-241-SSA1-2025,

Buenas Prácticas de Fabricación de Dispositivos Médicos, en la que se señalan códigos de seguridad para restringir el acceso a los datos y el respaldo de la información que contienen.

Por otro lado, en lo que compete a personal de salud y administrativo para mitigar los riesgos de un ciberataque, es prioritaria la formación continua en prácticas de ciberseguridad y tener un control estricto del uso de datos de los pacientes a solo personal autorizado (Cervera, 2024). Es importante capacitar a los profesionales de la salud en los aspectos éticos derivados del uso de la tecnología en salud (Panadés, 2024). No ventilar información a terceros como si fuera un dato sin repercusiones desastrosas. Lograr todo esto demanda una actitud ética frente a los avances de la difusión y aplicación del uso de los dispositivos tecnológicos para la atención en salud, pues ello conlleva también la amplitud de posibilidades de ingreso a amenazas de ciberseguridad. Pongamos el ejemplo del uso de la Inteligencia Artificial: ¿Cómo garantizamos la autonomía del paciente si, como médicos, delegamos o nos ayudamos de la ia en el proceso de decisión de un diagnóstico?

Cabe señalar que en México existe un marco normativo en el sistema jurídico en relación con la protección de datos personales. No es el objetivo de este capítulo ahondar en ello, solo destacar que en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos se engloban los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), que los pacientes pueden ejercer en relación con el uso de sus datos personales en el campo sanitario; además, existe la Ley Federal de Protección de Datos Personales en Posesión de Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Hincapie, 2024).

Conclusiones

La era actual está inmersa en la Cuarta Revolución, donde la Industria 4.0 tiende a la automatización y el intercambio de datos. Si bien esta industria permea en el sector salud a través de distintos dispositivos con sensores, procesamiento de datos, intercambio de datos con otros sistemas o dispositivos que ayudan al diagnóstico, tratamiento, intervenciones quirúrgicas, entre otras, tiene aún mucho camino por recorrer en torno a la alfabetización,

acceso, cobertura, equidad y el uso ético, para reconocer que el desarrollo y la innovación van ligados a un mayor bienestar de la población en general.

Referencias

- Alarcón, I. *et al.* (2025). Abordaje de los determinantes digitales de salud: principales ventajas y retos de la salud digital en el mundo actual. *Atención Primaria*, 57. <https://doi.org/10.1016/j.aprim.2025.103311>
- Alegre, V. *et al.* (2024). Salud digital en América Latina: legislación actual y aspectos éticos. *Rev Panam Salud Publica*, 48:e40. <https://doi.org/10.26633/RPSP.2024.40>
- Alzuri, P. *et al.* (2021). *Protegiendo la salud digital, una guía de ciberseguridad en el sector salud*. Banco Interamericano de Desarrollo.
- Bagolle, A. *et al.* (2022). *La gran oportunidad de la Salud Digital en América Latina y el Caribe*. Banco Interamericano de Desarrollo.
- Banco de Desarrollo de América Latina (2022). *Inteligencia artificial y telemedicina en el sector salud. Oportunidades y Desafíos*. CAF. Banco Interamericano de Desarrollo
- (2024). *Innovación y tecnología en salud en América Latina y el Caribe*. BID.
- (2016). *Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe?* BID.
- Cárdenas Ramos, M. *et al.* (2025). Empoderamiento del paciente y ética en telemedicina: una mirada desde la atención primaria. *Atención Primaria*, 57(7). <https://doi.org/10.1016/j.aprim.2025.103227>
- Cervera, A. y Goussens, A. (2024). Ciberseguridad y uso de las TIC en el sector salud. *Atención Primaria*, 56, 1-7.
- Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing*, 37(5), 1123-1132. <https://doi.org/10.1007/s10877-023-01013-5>
- Corporación de Salud Ocupacional y Ambiental (2024). *Ciberseguridad para profesionales de la salud: más allá de las barreras físicas*. <https://corporacionsoa.co/Memorias%202024/Inteligencia%20Artificial/Ciberseguridad%20sector%20salud.pdf>
- De Luca, S. y López, P. (s.f.). La ciberseguridad en productos sanitarios, un pilar fundamental para la protección de los pacientes. *Farmabiotec*, 78.
- Díaz de León, C. (2020). Las TIC en el sector público del sistema de salud de México: Avances y oportunidades. *Acta Universitaria*, 30, e2650. <http://doi.org/10.15174.au.2020.2650>
- García, C. (2025). Aplicación del Big Data en la gestión sanitaria hospitalaria: oportunidades, retos y perspectivas futuras. *Ocronos*, 8(8), 1335.
- García, S. *et al.* (2022). La transformación digital para una salud pública más equitativa y sostenible en la era de la interdependencia digital. *Rev Panam Salud Publica*, 46, e1. <https://doi.org/10.26633/RPSP.2022.1>
- Gomero, R. y Sánchez, D. (2024). Ciberseguridad en servicios de apoyo al médico ocu-

- pacional de la ciudad de Lima. Estudio piloto. *Revista Médica Herediana*, 55(1), 38-46. DOI: <https://doi.org/10.20453/rmh.v35i1.5298>
- Guio, L. (31 de diciembre de 2024). *Estos son los avances más importantes en la ciencia y la medicina durante el 2024*. Medicina y Salud Pública. <https://medicinaysaludpublica.com/noticias/salud-publica/estos-son-los-10-avances-mas-importantes-en-la-ciencia-y-la-medicina-durante-el-2024/25703>
- Gutiérrez, C. y López, M. (2022). La salud en la era digital. *Rev. Med. Clin. CONDES*, 33(6), 562-567.
- Hincapie, J. et al. (2024). *Medicina en la era digital: alcances y perspectivas*. Universidad Nacional Autónoma de México.
- Illich, I. (1973). *La convivencialidad*. Barral Editores.
- Inter-American Development Bank (2025). *Cybersecurity Report*. Global Cybersecurity Capacity Centre.
- Jiménez, M. (2022). *Telemedicina y equidad*. OSEKI. <https://oseki.eus/areas/desigualdades-sociales-de-la-salud/>
- Manobanda, M. et al. (2024). Salud y bienestar en la era digital en América Latina durante los últimos diez años. *Reincisol*, 3(6), 5067-5087. [https://doi.org/10.59282/reincisol.V3\(6\)5067-5087](https://doi.org/10.59282/reincisol.V3(6)5067-5087)
- Meneses, S. (2025). México frente a la universalidad en salud: desigualdad, segmentación y reformas contradictorias. *Gaceta Sanitaria*. 10.1016/j.gaceta.2025.102533
- Panadés, R. et al. (2024). Análisis de retos y dilemas que deberá afrontar la bioética del siglo XXI en la era de la salud digital. *Atención Primaria*, 56, 1-8. <https://doi.org/10.1016/j.aprim.2024.102901>
- Pavón, I. et al. (2024). Telesalud y seguridad de la gestión de la información para los entornos médicos actuales. *Revista Cubana de Informática Médica*, 16(1), e616.
- Roveri, C. (2022). Inteligencia artificial para el bienestar y una vida sana en Latinoamérica: Hacia un ecosistema de innovación responsable para la salud digital. *Análisis Carolina*, 21, 1-19. https://doi.org/10.33960/AC_21.2022
- S,A. (2024). Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad. *Hospitalaria*, 144, 4-38.
- Secretaría de Salud (2025). Norma Oficial Mexicana NOM-241-SSA1-2025, Buenas Prácticas de Fabricación de Dispositivos Médicos. *Diario Oficial de la Federación*. <https://www.dof.gob.mx/normasOficiales/9497/salud/salud.html>
- García-Saio, S. et al. (2019). *Primer informe sobre desigualdades en salud en México*. Secretaría de Salud; Organización Panamericana de la Salud.
- Trens, E. (2000). El desarrollo tecnológico y las políticas de salud. *Revista de la Facultad de Medicina*, 43(1), 24-27.
- Vidal, J. et al. (2023). Abordaje de la transformación digital en salud para reducir la brecha digital. *Atención Primaria*, 55. <https://doi.org/10.1016/j.aprim.2023.102626>
- World Economic Forum (2025). *The Global Risks Report 2025 20th Edition*. Geneva Switzerland