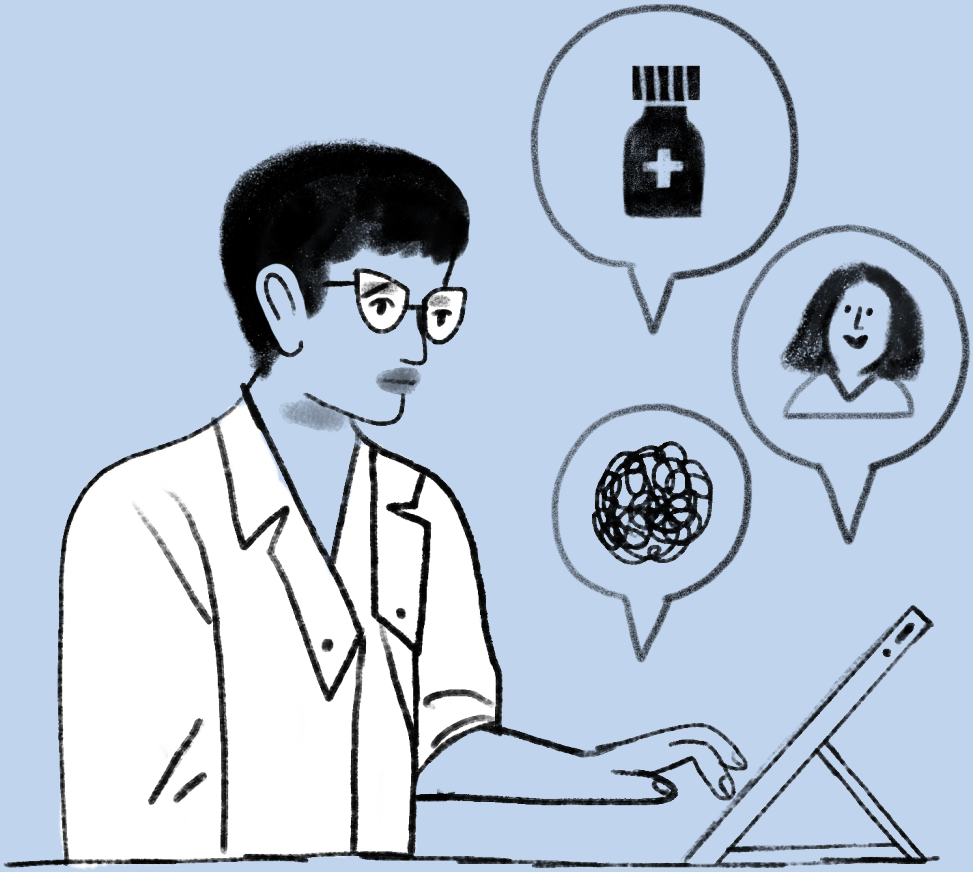

Ciberseguridad y salud pública

Tecnología & Derechos Humanos

TEDIC

MENTE EN LÍNEA

APC

Este material forma parte del proyecto **Mente en Línea**, campaña sobre Salud Mental en Internet para profundizar sobre los distintos factores que impactan en nuestro comportamiento y salud mental a la hora de interactuar con tecnologías.

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

Asunción, Paraguay ~ 2025

Consulta este proyecto en:
www.menteenlinea.org

Elaboración
Dr. Rodrigo Ramalho

Coordinación y edición
Maricarmen Sequera

Asistencia
Maricel Achucarro

Comunicación
Romina Aquino González

Identidad visual e ilustraciones
Adriana Peralta

Diseño y diagramación
Horacio Oteiza

Tabla de contenido

Ciberseguridad y salud pública

Palabras claves: *Ciberseguridad en salud, salud mental digital, protección de datos sanitarios, gobernanza digital*

Introducción

La Estrategia Nacional de Ciberseguridad 2024-2028[1] representa un esfuerzo oportuno del Estado paraguayo por responder a la acelerada digitalización de la vida cotidiana, así como a la creciente digitalización de servicios y operaciones en instituciones públicas y privadas. La estrategia busca fortalecer la resiliencia nacional frente a amenazas cibernéticas, garantizar la protección de datos y sistemas críticos, y promover un entorno digital seguro que ayude a consolidar la confianza ciudadana y empresarial. Para ello, la estrategia aborda diversas áreas críticas mediante objetivos estratégicos bien definidos. Sin embargo, en su conjunto, estas áreas reflejan una perspectiva predominantemente punitiva, cuando lo ideal sería adoptar un enfoque más centrado en las personas y en las comunidades (TEDIC, 2025). Un ejemplo ilustrativo de esta limitación es la aparente escasa participación del Ministerio de Salud Pública y Bienestar Social (MSPBS), que figura como miembro de la Comisión Nacional de Ciberseguridad, en la misma estrategia. Como ejemplo de esto, cabe resaltar que la palabra "salud"[2] aparece solo una vez en todo el documento.

El Paraguay ya ha dado varios pasos hacia la digitalización del sistema de salud. Entre ellos se encuentra la reciente iniciativa para digitalizar las historias clínicas (H. Cámara de Diputados del Paraguay, 2025). También existen varias aplicaciones móviles de salud en el país, así como plataformas digitales conectadas al sistema sanitario, algunas incluso desarrolladas desde el propio sistema público de salud[3]. Este tipo de iniciativas plantean importantes desafíos en materia de seguridad digital. Como fue mencionado arriba, la Estrategia Nacional de Ciberseguridad 2024-2028 reconoce la importancia de proteger infraestructuras críticas y fortalecer la resiliencia ante amenazas cibernéticas. Aun así, la estrategia no contiene una línea estratégica específica para el sector sanitario, lo que representa una oportunidad perdida para fortalecer la ciberseguridad de dicho sector. Esta omisión contrasta con recomendaciones internacionales, como las de la Organización Mundial de la Salud (World Health Organization, 2025), que promueven la intersectorialidad en la gobernanza digital y la necesidad de proteger los sistemas de salud, una recomendación que ya ha sido incorporada en varios países, incluyendo los Estados Unidos[4], el Reino Unido[5], Australia[6] y Nueva Zelanda[7].

---

1 Para conocer el texto completo de la estrategia, ver: CERT-PY (s. f.) Estrategia Nacional de Ciberseguridad del Paraguay 2025-2028. https://www.cert.gov.py/estrategia-nacional-de-ciberseguridad/

2 La palabra "salud" solo aparece en la página 9 de la Estrategia Nacional de Ciberseguridad del Paraguay 2025-2028, y es en alusión a fortalecimientos de la red de banda ancha móvil que ha facilitado el acceso a Internet en instituciones de salud.

3 Desde hace varios años, el Instituto de Previsión Social (IPS) cuenta con una plataforma en línea que ofrece formularios que puedes ser completados, así como con una aplicación móvil que puede ser descargada de manera gratuita llamada IPS te escucha. Ver: Instituto de Previsión Social. (s.f.). IPS te escucha. https://portal.ips.gov.py/sistemas/ipsportal/ips_escucha.php

4 Cybersecurity and Infrastructure Security Agency (s.f.). Healthcare and Public Health Cybersecurity. Recuperado el 27 de Setiembre de 2025, de https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare

5 GOV.UK. (2023). Cyber security strategy for health and social care: 2023 to 2030. https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030

6 Australian Digital Health Agency. (2025). Cyber security. https://www.digitalhealth.gov.au/initiatives-and-programs/cyber-security

7 Health New Zealand (s.f.). Cyber Hub. Recuperado el 27 de Setiembre de 2025, de https://www.tewhatuora.govt.nz/health-services-and-programmes/cyber-hub

El presente documento busca discutir esta relación clave entre salud y ciberseguridad, prestando particular atención a la salud mental. El mismo lo hace desde la perspectiva de "la salud en todas las políticas", impulsada por la Organización Mundial de la Salud (World Health Organization, s.f.a). La iniciativa La salud en todas las políticas (HiAP por sus siglas en inglés), como lo dice su nombre, busca integrar la salud como un objetivo transversal en todas las políticas públicas. Esta perspectiva reconoce que la salud no depende exclusivamente del sector sanitario, sino que está profundamente influenciada por decisiones políticas, sociales y tecnológicas, incluyendo la ciberseguridad. Esta investigación primero discute la seguridad de los datos sanitarios, para luego cubrir áreas importantes como la violencia de género facilitada por la tecnología, otras amenazas digitales a la salud pública, y varios desafíos éticos y de gobernanza. Finalmente, culmina con una discusión de las implicancias de estos puntos para el Paraguay, antes de presentar su conclusión.

La seguridad de los datos sanitarios

El término "datos sanitarios" hace referencia a un tipo particular de datos personales y representa toda información, en cualquier formato, relacionada con el estado de salud física y mental de las personas (Comisión Europea, s.f.). Esta información incluye aquella recolectada en los servicios de atención clínica, como antecedentes médicos, diagnósticos, tratamientos y resultados de laboratorio. Tradicionalmente, estos datos han sido recogidos de manera física y almacenados en fichas clínicas que son resguardadas dentro de las propias instituciones de atención clínica. Sin embargo, en los últimos años, se ha acelerado el proceso de digitalización de esta información, incluyendo iniciativas como la digitalización de las historias clínicas en Paraguay (Ministerio de Salud Pública y Bienestar Social, 2022).

La iniciativa para digitalizar la historia clínica (también llamada registro personal de salud o PHR por sus siglas en inglés) avanza rápidamente en el país (H. Cámara de Diputados del Paraguay, 2025). Estas historias clínicas contienen información altamente personal y sensible, y es imprescindible que el Estado tome las medidas necesarias para protegerla (World Health Organization, 2024a). Aquí, es también importante recalcar que los datos sanitarios no solo se limitan a aquellos contenidos en las historias clínicas, sino que también incluyen la información recogida por aplicaciones móviles y plataformas de salud, y estas, a la vez, deberían ser contempladas en discusiones sobre la ciberseguridad de los datos sanitarios (Salazar-Lazo & Avila-Correa, 2023), ya que aquellas aplicaciones y plataformas registran, almacenan, procesan y usan información igualmente personal y sensible.

La digitalización de los datos sanitarios ofrece importantes ventajas para la atención y el cuidado personal de la salud (Organización Mundial de la Salud, 2021). Por ejemplo, esta digitalización permitiría integrar toda la información clínica relevante a una persona a lo largo del sistema de salud. Como resultado, desde donde sea que esta persona acceda al sistema de salud dentro del país, sus datos podrían estar disponibles para su atención. La digitalización de esta información también trae ventajas para la planificación de políticas públicas de salud y la vigilancia epidemiológica, así como para la investigación y la creación de evidencia y nuevo conocimiento. Sin embargo, el almacenamiento, procesamiento y uso de los datos sanitarios implican importantes aspectos de ciberseguridad que no deberían ser ignorados en la estrategia nacional de ciberseguridad.

El almacenamiento de los datos sanitarios

Almacenar los datos sanitarios de manera segura es una decisión tanto técnica como de salud pública. La seguridad e integridad de los datos sanitarios sostienen la continuidad de la atención clínica a través de todo el sistema sanitario. Pero almacenar los datos sanitarios de manera segura no sólo protege el buen funcionamiento de la salud pública —así como la confianza en el Estado— sino también protege a la propia ciudadanía. El seguro almacenamiento de esta información reduce los riesgos de exposición y de discriminación, por ejemplo, por parte de personas con diagnósticos de salud mental o enfermedades de transmisión sexual. La filtración o el acceso indebido a esta información puede causar daños significativos a estas personas, generando también desconfianza hacia el sistema de salud y socavando iniciativas sanitarias y políticas de salud pública.

Es también indispensable regular la transparente trazabilidad de los datos sanitarios; es decir, la capacidad de rastrear el recorrido completo de los mismos, desde su origen hasta su procesamiento y sus usos finales. Es igualmente importante establecer límites claros a la retención de estos datos, dentro del propio sistema sanitario como fuera del mismo. Esto es particularmente importante en dos áreas. En el área de la investigación, estas regulaciones deben establecer el tiempo máximo de retención de los datos sanitarios por parte de las personas investigadoras y la forma en la que los mismos deben ser eliminados de manera segura. Segundo, en la creciente área de la inteligencia artificial, es igualmente importante establecer límites claros para el tiempo con el cual los algoritmos pueden usar los datos sanitarios para su entrenamiento, estableciendo también protocolos de eliminación segura de estos datos luego de su uso.

La transparente trazabilidad de los datos sanitarios también incluye regular mecanismos bien definidos para el acceso a estos datos. Los mecanismos ayudarían a garantizar que quienes accedan a los mismos lo hagan de manera justificada y con propósitos bien establecidos. Por su parte, esto requiere una delineación clara de las funciones para las que se puede acceder a los datos sanitarios. Asimismo, aseguraría que quienes accedan a estos datos lo puedan hacer de manera proporcional a su rol y en base a las funciones adheridas a ese rol, minimizando la exposición innecesaria de datos sensibles. Estas regulaciones deben también contemplar la responsabilidad ética y legal de quienes almacenan los datos, estableciendo consecuencias claras para posibles daños y vulneraciones de estos, así como para accesos más allá de los límites establecidos. Cabe recalcar que la propia ciudadanía también debería tener derecho a acceder a sus propios datos sanitarios, permitiendo a las personas conocer qué información se ha registrado sobre ellas, cómo ha sido usada y por quién.

De la misma forma, resulta fundamental establecer límites claros de acceso a datos sanitarios por parte de entidades privadas, particularmente en contextos comerciales. En estas situaciones, se corre el riesgo de que los intereses económicos puedan entrar en conflicto con los principios de confidencialidad y autonomía. El Estado, dentro de la estrategia de ciberseguridad, debe establecer un balance claro entre intereses comerciales y de innovación y la prevención de la explotación de información personal, especialmente de datos tan sensibles como los datos sanitarios. Aquí la discusión no se enfoca en la protección técnica frente a accesos no autorizados, sino en garantizar que los derechos de las personas prevalezcan por sobre los intereses comerciales[8]. Sin embargo, es innegable que otro desafío importante en el área de ciberseguridad en salud incluye el prevenir los accesos no autorizados y ataques maliciosos como el ransomware[9]. Es más, en el campo de la salud, este tipo de ataques puede tener consecuencias significativamente graves, que incluyen la exposición de datos altamente personales y sensibles, la interrupción de servicios clínicos y la pérdida de confianza en el sistema de salud.

8 Varias organizaciones internacionales, como la Organización Mundial de la Salud (2021), la Organización para la Cooperación y el Desarrollo Económico (OECD por sus siglas en inglés) (OECD, 2016), y la Comisión Europea (s.f.), reconocen a los datos sanitarios como una categoría especial de datos personales que requiere protecciones adicionales, por lo cual los Estados deben implementar marcos regulatorios claros para proteger estos datos, especialmente frente a sus usos comerciales.

9 El ransomware es un tipo de software malicioso que infecta sistemas digitales y bloquea el acceso de los usuarios a datos y aplicaciones mediante la encriptación de información clave. Para recuperar el acceso, los atacantes generalmente exigen el pago de un rescate (World Health Organization, 2024b).

El uso de los datos sanitarios

Es en el uso de los datos sanitarios donde se concretan sus beneficios clínicos, de gestión de salud pública y de vigilancia epidemiológica, así como sus aportes a la creación de nuevo conocimiento. Los datos sanitarios se pueden usar de diferentes maneras, ya sea para los propósitos directos para los que son recogidos, por ejemplo, ofrecer un diagnóstico o tratamiento luego de haberlos registrado en la historia clínica. Estos datos también se pueden usar de manera secundaria, es decir, con fines distintos a aquellos para los cuales fueron originalmente recolectados, por ejemplo, en proyectos de investigación o para informar decisiones de salud pública[10]. Ya sea para su uso primario o secundario, es necesario que estos datos sean accesibles solo de manera proporcional al rol de aquellos que acceden a los mismos, minimizando la exposición innecesaria de estos datos, y que su uso sea exclusivamente limitado a las funciones designadas a estos roles. El uso de los datos sanitarios por personas o instituciones que no deberían tener acceso a los mismos, fuera del propósito originalmente definido, o sin el consentimiento adecuado vulnera derechos fundamentales de la ciudadanía y puede socavar la confianza en el Estado que debería protegerla.

El consentimiento informado de las personas para el uso de sus datos sanitarios no es simplemente un trámite administrativo, sino la expresión activa de la autonomía sobre la información personal. Teniendo en cuenta que los datos sanitarios pueden ser reutilizados para múltiples fines, es importante que el consentimiento informado contemple estos usos secundarios. Es también importante que las personas puedan modificar o retirar su consentimiento en cualquier momento y el Estado debe proveer estas garantías. Sin dichas garantías, el uso de los datos sanitarios corre el riesgo de convertirse en una práctica extractiva, más orientada a beneficiar a quienes hacen uso de estos que al respeto por los derechos y la autonomía de las personas.

El uso potencialmente dañino de los datos sanitarios puede verse facilitado por la falta de regulación de aplicaciones móviles, dispositivos portátiles o plataformas digitales de salud diseñadas e implementadas por entidades públicas o privadas[11]. Un ejemplo de dicho uso es la venta de datos sanitarios a terceros para la elaboración de perfiles de consumo, que luego son utilizados para dirigir publicidad personalizada (Kaplan, 2016). Esto puede incluir publicidad de productos potencialmente adictivos o perjudiciales para la salud, como alcohol o apuestas en línea, dirigida específicamente a personas con particulares vulnerabilidades a dicha publicidad. El vacío regulatorio en este campo pone en riesgo no solo la privacidad individual, sino también la capacidad de cuidado y protección por parte del Estado.

10 El uso secundario de los datos sanitarios en proyectos de investigación y en la toma de decisiones en salud pública debe realizarse de manera ideal en forma agregada o anonimizada, para así reducir los riesgos de identificación individual y de comprometer el compromiso con la confidencialidad. Esta agregación de datos constituye una práctica clave dentro de los marcos de ciberseguridad orientada a minimizar vulnerabilidades en el manejo de información personal sensible (World Health Organization, 2017, 2021).

11 El consentimiento informado en estos contextos es discutido más abajo, en la sección 5.1. Consentimiento informado y autonomía digital.

Todos estos riesgos se amplifican en entornos digitales, donde la circulación de datos personales puede ser rápida, difícil de rastrear y susceptible a usos secundarios no autorizados. Por ejemplo, laboratorios farmacéuticos podrían utilizar estos datos para segmentar a la población y promover la venta dirigida de ciertos medicamentos. Asimismo, empresas aseguradoras podrían usar esta información para limitar sus coberturas o excluir a ciertas comunidades por ser consideradas 'alto riesgo'. Estas prácticas no solo vulnerarían la privacidad de las personas, sino que también reforzarían desigualdades estructurales en el acceso a la salud, transformando los datos sanitarios en un recurso explotable. No se puede tampoco dejar de recalcar que la exposición de información sensible, como diagnósticos de salud mental, puede derivar en estigmatización y discriminación.

Es indispensable salvaguardar la seguridad de los datos sanitarios, incluyendo su uso debido. En Paraguay, existe actualmente un proyecto de ley de protección de datos personales (SILPY, 2025), que busca establecer un marco legal para la protección de dichos datos. La ley actualmente vigente presenta avances solo en lo que respecta a la protección de datos personales de naturaleza crediticia (TEDIC, 2024). Sin embargo, esta legislación fue concebida en un contexto previo al avance en la digitalización del sistema de salud y no contempla de manera suficiente dicho sistema en el tema de protección de datos. Actualizar en esta dirección tanto la legislación nacional como la estrategia nacional de ciberseguridad es urgente, sobre todo para proteger a las comunidades más vulnerables frente a los varios riesgos digitales descritos en este documento, incluyendo la violencia de género facilitada por la tecnología.

Violencia de género facilitada por la tecnología

La acelerada digitalización de la vida cotidiana, así como la creciente digitalización de servicios y operaciones en instituciones públicas y privadas, trae consigo otras amenazas directas a la seguridad de la ciudadanía. La violencia de género facilitada por la tecnología representa una de estas amenazas. La violencia de género facilitada por la tecnología incluye todo acto cometido, asistido, agravado o amplificado por el uso de tecnologías digitales, que incluyen las redes sociales o plataformas de mensajería, que tenga como resultado el daño físico, psicológico, sexual, económico o simbólico (TEDIC, s.f.a).

Existen numerosos tipos de violencia de género facilitada por la tecnología (TEDIC, s.f.b). Estas violencias afectan de manera desproporcionada a mujeres, niñas y personas con identidades diversas y se manifiestan en múltiples formas, incluyendo la difusión no consentida de imágenes íntimas[12], el acoso sexual en línea y la vigilancia digital[13]. La violencia de género facilitada por la tecnología no puede ser abordada exclusivamente desde el sector sanitario, por ejemplo, brindando atención clínica a las víctimas de estas violencias, ni tampoco solo en compañía del sistema judicial, por ejemplo, aplicando sanciones penales o medidas de protección y reparación de las víctimas. Estas violencias deben ser abordadas como un problema estructural que requiere respuestas intersectoriales, incluyendo la ciberseguridad[14].

La Estrategia Nacional de Ciberseguridad 2024-2028 contempla la promoción de entornos digitales seguros y se compromete a prevenir la violencia de género en línea[15]. Sin embargo, es importante reconocer que la violencia de género facilitada por la tecnología es una expresión digital de violencias históricas y patriarcales que afectan a la sociedad en general y que desde allí se trasladan, reproducen, y refuerzan en el entorno digital. El Programa Nacional de Prevención y Detección Integral de la Violencia[16] reconoce la necesidad de una articulación intersectorial para prevenir la violencia de género en el país. De igual manera, es importante que las políticas de ciberseguridad también incorporen un enfoque intersectorial que incluya al sector salud en su esfuerzo por prevenir, detectar, eliminar y reparar los impactos de estas violencias.

12 Ver: TEDIC. (2021). Difusión de imagen no consentida en Paraguay: Un estudio explorativo. https://www.tedic.org/wp-content/uploads/2021/09/Imagen-no-consentida-Tedic-web.pdf

13 La vigilancia digital incluye, por ejemplo, el uso de spyware -software que se utiliza para espiar y obtener información de dispositivos o para acceder a cuentas sin consentimiento, así como el uso de sistemas de geolocalización para el rastreo de una persona (TEDIC, s.f.b).

14 El Centro Regional de Información de las Naciones Unidas ha reconocido que la violencia de género facilitada por la tecnología representa una amenaza a la seguridad. Ver Naciones Unidas. (2023). Cómo afecta a mujeres y niñas la violencia de género facilitada por la tecnología. Recuperado el 27 de Setiembre de 2025, de https://unric.org/es/violencia-de-genero-facilitada-por-la-tecnologia/

15 Esto es mencionado en varios puntos de la estrategia, incluidos el punto 3.6.5.2.1 en la página 34, y el punto 3.6.7.1.4 en la página 38. Ver: CERT-PY (s. f.) Estrategia Nacional de Ciberseguridad del Paraguay 2025-2028. https://www.cert.gov.py/estrategia-nacional-de-ciberseguridad/

16 Ver: Ministerio de Salud Pública y Bienestar Social. (2017). Articulación intersectorial para frenar violencia contra la mujer. https://www.mspbs.gov.py/portal-12004/articulacion-intersectorial-para-frenar-violencia-contra-la-mujer.html

Otras amenazas digitales a la salud pública

Con la creciente digitalización de la vida cotidiana, incluyendo la forma en la que las personas acceden a información sobre salud, otras innegables amenazas para la salud pública son la circulación de información falsa o engañosa, y la información excesiva que dificulta discernir la veracidad de las fuentes, conocidas respectivamente como desinformación, malinformación e infodemia[17]. La pandemia de COVID-19 fue un claro ejemplo de esto. Durante la pandemia de COVID-19, organizaciones como las Naciones Unidas (s.f.) y la Organización para la Cooperación y el Desarrollo Económicos (OECD por sus siglas en inglés) (OECD, 2022), recomendaban a los gobiernos la toma de medidas, incluidas medidas jurídicas, que contrarresten la desinformación. Es importante aquí recalcar, como lo advierten tanto TEDIC[18] como la OCDE (2022), que estas medidas no deberían comprometer la libertad de expresión y habilitar mecanismos de censura y vigilancia digital, lo que evidencia aún más la necesidad por parte del Estado de dar respuestas equilibradas que protejan tanto la salud pública como los derechos digitales.

Estas amenazas particulares son muchas veces el propio producto de las plataformas digitales que las albergan. Las plataformas comúnmente utilizan algoritmos de recomendación de contenido personalizado en función del comportamiento previo de la persona que las utiliza. En este proceso, los algoritmos priorizan la atención por sobre la veracidad del contenido que promueven, apuntando a maximizar la interacción con la plataforma y a través de ello, la ganancia comercial. Este diseño algorítmico tiende a encerrar a las personas en las llamadas "cámaras de eco", limitando su acceso a fuentes confiables y diversas. Como resultado, y sin intervención del Estado, información desalineada con la seguridad y la salud pública puede fácilmente ser amplificada sin mecanismos efectivos de verificación, moderación o regulación.

Otra amenaza a la salud pública derivada de los mismos algoritmos de personalización es el impacto de estos algoritmos en los patrones de uso digital. Estrategias como el desplazamiento infinito, las notificaciones constantes, los sistemas de recompensas variables y los botones de aprobación social ("me gusta") pueden generar patrones de uso digital dañinos (Montag & Elhai, 2023). El alto consumo de las plataformas digitales que utilizan estos algoritmos puede también traer alteraciones del sueño, de la atención y del estado de ánimo, así como menor actividad física y deterioro de vínculos (Alonzo et al., 2021; Khalaf et al., 2023). Estas consecuencias, aunque no derivadas de ataques cibernéticos tradicionales, deben ser consideradas dentro de una perspectiva de ciberseguridad en salud que promueva entornos digitales seguros y saludables.

17 Para más información con respecto a estos conceptos en relación a la salud, ver: i) Organización Mundial de la Salud. (2024, Febrero 6). Desinformación y salud pública. https://www.who.int/es/news-room/questions-and-answers/item/disinformation-and-public-health; y ii) World Health Organization. (s.f.b). Infodemic. https://www.who.int/health-topics/infodemic

18 Ver: Sequera Buzarquis, M. (2020, 31 de marzo). Preocupante regulación sobre desinformación en tiempos de COVID-19. TEDIC. https://www.tedic.org/preocupante-regulacion-sobre-desinformacion-en-tiempos-de-covid19/

Es también importante volver a recalcar que estas plataformas generalmente exponen a las personas que las utilizan a publicidad de productos nocivos, como alcohol o apuestas en línea, promoviendo su consumo —y muchas veces lo hacen como parte de su propio modelo de negocios (Kaplan, 2016), con los significativos impactos negativos en la salud pública que trae esta exposición (Lyons et al., 2023). Cuando forma parte del propio diseño de las plataformas, esta exposición dirigida representa una forma de explotación digital que vulnera el derecho a la salud, especialmente en comunidades con mayor susceptibilidad a estos productos. En este sentido, y desde una perspectiva de ciberseguridad centrada en las personas y las comunidades que busque promover entornos digitales seguros, es fundamental que las políticas públicas regulen este tipo de daños estructurales al bienestar colectivo y protejan a las poblaciones más vulnerables.

Desafíos éticos y de gobernanza

Aunque suene repetitivo, es relevante contextualizar el hecho de que la acelerada digitalización de la vida cotidiana, así como la creciente digitalización de servicios y operaciones en instituciones públicas y privadas, incluidas las instituciones sanitarias, traen consigo también nuevos dilemas éticos y de gobernanza que requieren una atención apropiada desde una perspectiva de ciberseguridad centrada en las personas. Algunos dilemas son: el consentimiento informado y la autonomía digital, la soberanía de los datos, la justicia digital y equidad algorítmica, e importantes principios de responsabilidad y reparación.

Consentimiento informado y autonomía digital

La mayoría de las personas no está plenamente informada sobre lo que implica la digitalización de sus datos sanitarios, o sobre qué datos comparten a través de aplicaciones móviles, dispositivos portátiles y plataformas digitales de salud, ni sobre cómo estos datos son recolectados, almacenados, procesados y utilizados. Muchas veces, aunque el consentimiento informado suele ser requerido, por ejemplo, mediante la aceptación de términos y condiciones, este proceso rara vez garantiza una comprensión real del alcance del uso de los datos (Kreuter et al., 2020). En este escenario, y dada la magnitud estructural del problema que claramente excede lo individual, responsabilizar exclusivamente a las personas por la protección de sus datos es insuficiente. Al contrario, se requieren políticas públicas[19] que regulen el almacenamiento y uso de estos datos y limiten la explotación de vacíos normativos tanto por parte de instituciones públicas como privadas.

19 En Europa, el Reglamento sobre el Espacio Europeo de Datos de Salud (EEDS) de la Unión Europea -que entró en vigor a partir de marzo del 2025- establece medidas que garantizan por defecto la protección de la privacidad y la seguridad de los datos sanitarios, que reconocen el derecho de las personas a restringir el acceso a partes específicas de su historia clínica, y que regulan el uso secundario de sus datos sanitarios bajo estrictas garantías éticas y de ciberseguridad. Ver: Comisión Europea. (s.f.). Reglamento relativo al Espacio Europeo de Datos de Salud (EEDS). Recuperado el 27 de septiembre de 2025, de https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_es

Soberanía de los datos

Uno de los principales desafíos en materia de ciberseguridad está relacionado con el principio de soberanía de los datos[20], principio que exige garantizar la protección de estos datos en contextos cada vez más interdependientes. En salud, este principio también reconoce los derechos y responsabilidades colectivas con respecto al acceso y uso de los datos sanitarios, y que estos datos, en cierta manera, no pertenecen únicamente a las personas de manera aislada (Hummel et al., 2021). En América Latina, este principio es especialmente relevante por dos razones: primero, el riesgo de que la creciente digitalización de los datos personales, incluyendo los datos sanitarios, reproduzca relaciones históricas de dependencia con centros de poder externos. La buena gobernanza digital debe evitar que la salud digital se convierta en una nueva forma de despojo, donde los beneficios de la innovación tecnológica se concentran en el Norte Global, mientras que los riesgos recaen sobre las comunidades del Sur Global (Milan & Treré, 2019). Segundo, el principio de soberanía de los datos es particularmente importante para prevenir la exclusión sistemática de los pueblos originarios en la toma de decisiones sobre sus datos sanitarios. El principio de la soberanía de los datos exige reconocer y respetar los saberes, derechos y formas de organización propias de los pueblos originarios, quienes históricamente han sido marginados de los procesos de toma de decisiones en salud digital[21]. Adoptar el principio de soberanía de los datos implica integrar justicia social, participación comunitaria y mecanismos que aseguren que el valor generado por los datos, incluidos los datos sanitarios, impacte positivamente en las propias comunidades.

Justicia digital y equidad algorítmica

La creciente interconexión digital entre los sistemas de atención sanitaria, aplicaciones móviles, y plataformas digitales también plantea desafíos adicionales en materia de gobernanza digital y ciberseguridad. Como ya se ha dicho múltiples veces, si estos desafíos no se abordan de manera proactiva, los mismos podrían generar vacíos regulatorios que habiliten la explotación de datos sanitarios, comprometiendo la privacidad y la seguridad de las personas. Un ejemplo claro es la necesidad de la protección de los datos y la privacidad por diseño[22], en contrapartida a la protección de estos por cumplimiento reactivo posterior a una vulneración. En Europa[23], por ejemplo, existen reglamentaciones que obligan a la integración del principio de privacidad por diseño desde la concepción de tecnologías digitales, buscando así proteger a las personas y comunidades del uso inapropiado de sus datos personales, incluyendo los datos sanitarios.

---

20 La soberanía de los datos se refiere al derecho de individuos, comunidades y naciones a controlar, gestionar y decidir sobre el uso de sus datos. Este principio abarca aspectos como la privacidad, el consentimiento, y el almacenamiento, y reconoce que los datos deben estar sujetos a las leyes y valores del territorio y de las comunidades a las que pertenecen. La Organización Mundial de la Salud, en su Estrategia Mundial sobre salud digital 2020-2025, coloca como uno de los primeros principios rectores de la estrategia la necesidad respetar la soberanía de las naciones. Ver: Organización Mundial de la Salud. (2021). Estrategia mundial sobre salud digital 2020–2025. https://iris.who.int/bitstream/handle/10665/344251/9789240027572-spa.pdf

21 Para ver más sobre el concepto de soberanía de datos, sobre todo en lo que respecta a pueblos originarios y comunidades Indígenas, ver: Royal Society Te Apārangi. (2023). Mana Raraunga Data Sovereignty, https://www.royalsociety.org.nz/assets/Mana-Raraunga-Data-Sovereignty-web-V1.pdf

22 Ya en el 2016, TEDIC abogaba por la necesidad de políticas públicas que garanticen la protección de los derechos digitales, incluyendo la privacidad, la transparencia en el uso de datos personales y la rendición de cuentas en entornos tecnológicos. Ver: Sequera Buzarquis, M. (2016, noviembre 23). La importancia de la seguridad en la economía digital #Ciberseguridad https://www.tedic.org/la-importancia-de-la-seguridad-en-la-economia-digital-ciberseguridad/

23 Ver: European Data Protection Board (EDPB). (2020, octubre 20). Directrices 4/2019 relativas al artículo 25: Protección de datos desde el diseño y por defecto (Versión 2.0). https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_es.pdf

Otro principio importante para tener en cuenta es el de la equidad algorítmica. La equidad algorítmica se trata de garantizar que los sistemas automatizados y de inteligencia artificial no reproduzcan o amplifiquen sesgos sociales, económicos o culturales, perpetuando desigualdades estructurales (Panch, Mattie & Atun, 2019). Es importante reconocer que los algoritmos utilizados en el campo de la salud, ya sea para analizar datos en investigaciones científicas o apoyar decisiones clínicas o de salud pública, no son neutrales. El entrenamiento de estos algoritmos muchas veces se realiza con información que refleja inequidades estructurales, por ejemplo, a través de la ausencia relativa de datos procedentes de minorías étnicas. Este entrenamiento, al reflejar desigualdades estructurales, puede entonces derivar en decisiones discriminatorias o inequitativas, una práctica que ha sido ampliamente documentada en varios campos de la salud (Mittermaier, Raza & Kvedar, 2023; Timmons et al., 2023). Por lo tanto, la justicia digital en salud requiere una gobernanza[24] que también asegure que la equidad estructural de la innovación tecnológica no se convierta en un nuevo vector de exclusión.

Responsabilidad y reparación

Es fundamental reconocer que, a pesar de los mejores esfuerzos por garantizar la seguridad del entorno digital, pueden igual ocurrir vulneraciones o daños derivados o facilitados por el uso de tecnologías y de los datos sanitarios. Es por ello que la gobernanza digital debe también incluir mecanismos claros de responsabilidad y reparación. Estos mecanismos deben incluir el desarrollo de protocolos que permitan responder de manera efectiva y justa ante situaciones de violencia, daños o vulneraciones. Aquí, la responsabilidad no debe entenderse únicamente como una herramienta punitiva, sino como un componente esencial de la justicia digital. Por lo tanto, estos mecanismos y protocolos deben también incluir mecanismos concretos de compensación[25], cuidado y reparación para las personas o comunidades afectadas.

24 Como ejemplo, en el 2022, el fiscal general del Distrito de Columbia, Estados Unidos, presentó un proyecto de ley llamado Stop Discrimination by Algorithms Act. Este proyecto de ley buscaba prevenir sesgos algorítmicos que afecten de forma desproporcionada a comunidades vulnerables buscando proteger los derechos civiles digitales de todas las personas. Ver: Office of the Attorney General for the District of Columbia. (2022). AG Racine testimony on Bill 24-558 – Stop Discrimination by Algorithms Act of 2021. https://oag.dc.gov/release/ag-racine-testimony-bill-24-558-stop

25 El Reglamento General de Protección de Datos (GDPR) de la Unión Europea establece medidas para la compensación por daños materiales o inmateriales debidos al uso indebido de sus datos personales, incluyendo los datos sanitarios. Estas medidas incluyen, entre otras cosas, compensaciones económicas y garantías de no repetición. Ver: European Commission. (s.f.). Can my company/my organisation be liable for damages? Recuperado el 27 de Setiembre de 2025, de https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/enforcement-and-sanctions/sanctions/can-my-companymy-organisation-be-liable-damages_en

Implicancias para el Paraguay

La Estrategia Nacional de Ciberseguridad 2024–2028 representa una oportunidad para fortalecer la ciberseguridad y ciberresiliencia del sistema sanitario, así como para la promoción de entornos digitales seguros y saludables. Desde la perspectiva de "La salud en todas las políticas", es indispensable que el sector salud participe activamente en esta estrategia, así como en conversaciones sobre gobernanza digital, y no solo como receptor de medidas, sino como agente activo en su diseño, implementación y evaluación. Dentro de este contexto, y en base a todo lo expuesto anteriormente, se sugieren las siguientes recomendaciones:

Desarrollo de protocolos institucionales y nacionales que consideren el principio de la soberanía de los datos y que regulen el almacenamiento, procesamiento y uso de los datos sanitarios, particularmente de datos sensibles como los relacionados a la salud mental, así como mecanismos de respuesta y reparación ante violencias, daños y vulneraciones.

Coordinación interinstitucional y trabajo intersectorial entre instituciones sanitarias, organismos de salud pública y los demás miembros de la Comisión Nacional de Ciberseguridad de Paraguay, en línea con el enfoque de "La salud en todas las políticas".

Marcos regulatorios para el desarrollo y uso de tecnologías, incluyendo tecnologías de salud, que integren los principios de privacidad, seguridad y equidad por diseño, y que no solo conlleven una mirada legal y punitiva, sino que también tengan en cuenta el impacto de estas tecnologías en la salud individual y colectiva.

Promoción de entornos digitales seguros, que tengan en cuenta la importancia del consentimiento informado y el acceso a la información, que prevengan la violencia de género facilitada por la tecnología y que permitan la integración efectiva de tecnologías emergentes como la inteligencia artificial, sin comprometer la privacidad, la libertad de expresión ni la equidad.

En síntesis, es crucial que la estrategia nacional de ciberseguridad integre la salud como eje transversal. Esta integración no solo fortalecería la resiliencia del sistema de salud y ayudaría a promover entornos digitales seguros, sino que también contribuiría a una gobernanza digital más justa, ética, equitativa y centrada en el bienestar colectivo del país.

Conclusión

La creciente digitalización de la salud en Paraguay representa tanto una oportunidad como un desafío urgente. La misma abre oportunidades para la mejora de la atención sanitaria y el fortalecimiento de la salud pública, pero este mismo proceso de digitalización acelerado también expone a la ciudadanía a riesgos complejos que no pueden ser abordados exclusivamente desde una perspectiva defensiva o punitiva. Proteger la salud en entornos digitales no es solo una cuestión de infraestructura o tecnología; la ciberseguridad en este contexto debería ser entendida más bien como una herramienta para garantizar derechos antes que como una simple barrera contra amenazas externas.

Incorporar la salud como un eje transversal en la estrategia nacional de ciberseguridad permitirá reconocer de manera más inclusiva las necesidades del país en términos de ciberseguridad y entornos digitales seguros. Sin embargo, esta articulación también requiere un compromiso político que priorice el bienestar colectivo por sobre los intereses empresariales, comerciales o tecnológicos. La ausencia de este compromiso podría dejar a la ciudadanía expuesta a prácticas abusivas y debilitar la confianza de la misma en el sistema sanitario.

La inclusión del sector salud en la estrategia nacional de ciberseguridad también favorecería el entendimiento de la ciberseguridad como un proyecto de derechos humanos, donde la privacidad, la equidad y la autonomía de las personas sean los principios rectores. Es solo de esta manera que será posible construir un entorno digital que no reproduzca desigualdades, sino que contribuya activamente al bienestar colectivo de la ciudadanía.

En conclusión, el presente documento busca proponer que la ciberseguridad sea entendida, ante todo, como un acto de cuidado hacia las personas y las comunidades.

Bibliografía

Alonzo, R., Hussain, J., Stranges, S., & Anderson, K. K. (2021). Interplay between social media use, sleep quality, and mental health in youth: A systematic review. Sleep Medicine Reviews, 56, 101414. https://doi.org/10.1016/j.smrv.2020.101414

Australian Digital Health Agency. (2025). Cyber security. https://www.digitalhealth.gov.au/initiatives-and-programs/cyber-security

CERT-PY (s. f.) Estrategia Nacional de Ciberseguridad del Paraguay 2025-2028. https://www.cert.gov.py/estrategia-nacional-de-ciberseguridad/

Comisión Europea. (s.f.). Reglamento relativo al Espacio Europeo de Datos de Salud (EEDS). Recuperado el 27 de septiembre de 2025, de https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_es

Cybersecurity and Infrastructure Security Agency. (s.f.). Healthcare and Public Health Cybersecurity. Recuperado el 27 de septiembre de 2025, de https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare

European Commission. (s.f.). Can my company/my organisation be liable for damages? Recuperado el 27 de Setiembre de 2025, de https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/enforcement-and-sanctions/sanctions/can-my-companymy-organisation-be-liable-damages_en

European Data Protection Board (EDPB). (2020, octubre 20). Directrices 4/2019 relativas al artículo 25: Protección de datos desde el diseño y por defecto (Versión 2.0). https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_es.pdf

GOV.UK. (2023). Cyber security strategy for health and social care: 2023 to 2030. https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030

H. Cámara de Diputados del Paraguay. (2025, 8 de septiembre). Ratifican aprobación a proyecto que establece digitalización de historial clínico. https://www.diputados.gov.py/noticias/noticias/521

Health New Zealand (s.f.). Cyber Hub. Recuperado el 27 de Setiembre de 2025, de https://www.tewhatuora.govt.nz/health-services-and-programmes/cyber-hub

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. Big Data & Society, 8(1), 2053951720982012. https://doi.org/10.1177/2053951720982012

Instituto de Previsión Social. (s.f.). IPS te escucha. https://portal.ips.gov.py/sistemas/ipsportal/ips_escucha.php

Kaplan, B. (2016). How should health data be used? Privacy, secondary use, and big data sales. Cambridge Quarterly of Healthcare Ethics, 25(2), 312–329. https://doi.org/10.1017/S0963180115000612

Khalaf, A. M., Alubied, A. A., Khalaf, A. M., Rifaey, A. A., Alubied, A., & Rifaey, A. (2023). The impact of social media on the mental health of adolescents and young adults: A systematic review. Cureus, 15(8), e42990. https://doi.org/10.7759/cureus.42990

Kreuter, F., Haas, G. C., Keusch, F., Bähr, S., & Trappmann, M. (2020). Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent. Social Science Computer Review, 38(5), 533–549. https://doi.org/10.1177/0894439318816389

Lyons, A. C., Goodwin, I., Carah, N., Young, J., Moewaka Barnes, A., & McCreanor, T. (2023). Limbic platform capitalism: Understanding the contemporary marketing of health-demoting products on social media. Addiction Research & Theory, 31(3), 178–183. https://doi.org/10.1080/16066359.2022.2151866

Milan, S., & Treré, E. (2019). Big data from the South(s): Beyond data universalism. Television & New Media, 20(4), 319–335. https://doi.org/10.1177/1527476419837739

Mittermaier, M., Raza, M. M., & Kvedar, J. C. (2023). Bias in AI-based models for medical applications: challenges and mitigation strategies. NPJ Digital Medicine, 6(1), 113. https://doi.org/10.1038/s41746-023-00858-z

Montag, C., & Elhai, J. D. (2023). On social media design,(online-) time well-spent and addictive behaviors in the age of surveillance capitalism. Current Addiction Reports, 10(3), 610-616. https://doi.org/10.1007/s40429-023-00494-3

Ministerio de Salud Pública y Bienestar Social. (2017). Articulación intersectorial para frenar violencia contra la mujer. https://www.mspbs.gov.py/portal-12004/articulacion-intersectorial-para-frenar-violencia-contra-la-mujer.html

Ministerio de Salud Pública y Bienestar Social (MSPBS). (2022). Del papel a la gestión digital: todos los hospitales generales ya utilizan el HIS. https://www.mspbs.gov.py/portal/25544/del-papel-a-la-gestion-digital-todos-los-hospitales-generales-ya-utilizan-el-his.html

Naciones Unidas. (s.f.) Contrarrestar la desinformación. Recuperado el 27 de Setiembre de 2025, de https://www.un.org/es/countering-disinformation

Naciones Unidas. (2023). Cómo afecta a mujeres y niñas la violencia de género facilitada por la tecnología. Recuperado el 27 de septiembre de 2025, de https://unric.org/es/violencia-de-genero-facilitada-por-la-tecnologia/

OECD. (2016). Recommendation of the Council on Health Data Governance. Organization for Economic Co-operation and Development. https://www.oecd.org/en/publications/health-data-governance-for-the-digital-age_68b60796-en.html

OECD. (2022, 16 de julio). Combatting COVID-19 disinformation on online platforms. OECD Publishing. https://www.oecd.org/en/publications/combatting-covid-19-disinformation-on-online-platforms_d854ec48-en.html

Office of the Attorney General for the District of Columbia. (2022). AG Racine testimony on Bill 24-558 – Stop Discrimination by Algorithms Act of 2021. https://oag.dc.gov/release/ag-racine-testimony-bill-24-558-stop

Organización Mundial de la Salud. (2021). Estrategia mundial sobre salud digital 2020-2025. https://iris.who.int/bitstream/handle/10665/344251/9789240027572-spa.pdf

Organización Mundial de la Salud. (2024, 6 de febrero). Desinformación y salud pública. https://www.who.int/es/news-room/questions-and-answers/item/disinformation-and-public-health

Panch, T., Mattie, H., & Atun, R. (2019). Artificial intelligence and algorithmic bias: implications for health systems. Journal of Global Health, 9(2), 020318. doi: 10.7189/jogh.09.020318

Royal Society Te Apārangi. (2023). Mana Raraunga: Data Sovereignty. https://www.royalsociety.org.nz/assets/Mana-Raraunga-Data-Sovereignty-web-V1.pdf

Salazar-Lazo, C., & Avila-Correa, B. (2023). Estándares de ciberseguridad aplicables a los sistemas informáticos sanitarios para proteger los datos personales. 593 Digital Publisher CEIT, 9(1), 88–102. https://doi.org/10.33386/593dp.2024.1.2156

Sequera Buzarquis, M. (2016, noviembre 23). La importancia de la seguridad en la economía digital #Ciberseguridad. https://www.tedic.org/la-importancia-de-la-seguridad-en-la-economia-digital-ciberseguridad/

Sequera Buzarquis, M. (2020, 31 de marzo). Preocupante regulación sobre desinformación en tiempos de COVID-19. TEDIC. https://www.tedic.org/preocupante-regulacion-sobre-desinformacion-en-tiempos-de-covid19/

Sistema de Información Legislativa del Paraguay. (2025). Protección de datos personales en Paraguay: Presentado por varios diputados nacionales. https://silpy.congreso.gov.py/web/expediente/123459

TEDIC. (s.f.a). La violencia digital es real. ¿Quieres saber más sobre la violencia de género facilitada por la tecnología? Recuperado el 27 de septiembre de 2025, de https://violenciadigital.tedic.org/es/

TEDIC. (s.f.b). Tipos de violencia de género facilitada por la tecnología. En La violencia digital es real. Recuperado el 27 de septiembre de 2025, de https://violenciadigital.tedic.org/es/b/guia/tipos-de-violencia-de-genero-digital/

TEDIC. (2021). Difusión de imagen no consentida en Paraguay: Un estudio explorativo. https://www.tedic.org/wp-content/uploads/2021/09/Imagen-no-consentida-Tedic-web.pdf

TEDIC. (2024). Protección de datos personales en el sector privado en Paraguay. Un estudio exploratorio. https://www.tedic.org/wp-content/uploads/2024/08/Proteccion-datos-personales-WEB.pdf

TEDIC. (2025). Anteproyecto de ley de ciberseguridad: análisis legal y comentarios a la propuesta legislativa. TEDIC. https://www.tedic.org/anteproyecto-de-ley-de-ciberseguridad/

Timmons, A. C., Duong, J. B., Simo Fiallo, N., Lee, T., Vo, H. P. Q., Ahle, M. W., ... & Chaspari, T. (2023). A call to action on assessing and mitigating bias in artificial intelligence applications for mental health. Perspectives on Psychological Science, 18(5), 1062-1096. https://doi.org/10.1177/17456916221134490

World Health Organization (s.f.a). Promoting Health in All Policies and intersectoral action capacities. Recuperado el 27 de Setiembre de 2025, de https://www.who.int/activities/promoting-health-in-all-policies-and-intersectoral-action-capacities

World Health Organization. (s.f.b). Infodemic. https://www.who.int/health-topics/infodemic

World Health Organization. (2021). Global strategy on digital health 2020–2025. World Health Organization. https://iris.who.int/handle/10665/341374

World Health Organization. (2024a). WHO personal data protection policy. World Health Organization. https://www.who.int/publications/m/item/who-personal-data-protection-policy

World Health Organization. (2024b). Cyber-attacks on critical health infrastructure. World Health Organization. https://www.who.int/news-room/questions-and-answers/item/cyber-attacks-on-critical-health-infrastructure

World Health Organization. (2025, marzo 26). WHO/Europe launches guide to strengthen cybersecurity in digital health. https://www.who.int/europe/news/item/26-03-2025-who-europe-launches-guide-to-strengthen-cybersecurity-in-digital-health

World Health Organization. Regional Office for Europe. (2021). The protection of personal data in health information systems: Principles and processes for public health. World Health Organization. https://iris.who.int/handle/10665/341374

www.menteenlinea.org