

Aspectos bioéticos de la telemedicina en Brasil: análisis integral

Juracy Barbosa dos Santos¹, Guilhermina Rego¹, Rui Nunes¹

1. Faculdade de Medicina da Universidade do Porto, Porto, Portugal.

Resumen

La telemedicina ha ganado protagonismo en Brasil, especialmente en contextos de pandemia y en áreas remotas. Este artículo explora los aspectos bioéticos y legales de esta práctica, destacando la necesidad de directrices claras para garantizar una práctica ética y segura. Se trata de una revisión de la literatura centrada en publicaciones relevantes sobre ética, bioética, tecnologías de la información y la comunicación, protección de datos y responsabilidades legales asociadas a la telemedicina. Se identificaron y analizaron diversos desafíos y beneficios de la telemedicina, con énfasis en cuestiones éticas, protección de datos y responsabilidades legales. La legislación brasileña fue comparada con regulaciones internacionales. Los resultados refuerzan que la consolidación de la telemedicina como una práctica segura y socialmente legítima depende de la integración entre regulación, principios bioéticos y un compromiso ético permanente con los derechos y el bienestar de los pacientes.

Palabras clave: Telemedicina. Bioética. Seguridad computacional. Ética médica. Legislación. Brasil.

Resumo

Aspectos bioéticos da telemedicina no Brasil: análise abrangente

A telemedicina tem ganhado destaque no Brasil, especialmente em contextos de pandemia e áreas remotas. Este artigo explora os aspectos bioéticos e legais dessa prática, especialmente a necessidade de diretrizes claras para garantir uma prática ética e segura. Trata-se de revisão de literatura focada em publicações relevantes sobre ética, bioética, tecnologias da informação e comunicação, proteção de dados e responsabilidades legais associadas à telemedicina. Foram identificados e analisados diversos desafios e benefícios da telemedicina, com ênfase em questões éticas, proteção de dados e responsabilidades legais. A legislação brasileira foi comparada com regulamentações internacionais. Os resultados reforçam que a consolidação da telemedicina como prática segura e socialmente legítima depende da integração entre regulamentação, princípios bioéticos e compromisso ético permanente com os direitos e o bem-estar dos pacientes.

Palavras-chave: Telemedicina. Bioética. Segurança computacional. Ética médica. Legislação. Brasil.

Abstract

Bioethical aspects of telemedicine in Brazil: comprehensive analysis

Telemedicine has gained prominence in Brazil, especially in pandemic contexts and in remote areas. This article explores the bioethical and legal aspects of this practice, emphasizing the need for clear guidelines to ensure ethical and safe practice. This is a literature review focused on relevant publications addressing ethics, bioethics, information and communication technologies, data protection, and legal responsibilities associated with telemedicine. Various challenges and benefits of telemedicine were identified and analyzed, with emphasis on ethical issues, data protection, and legal responsibilities. Brazilian legislation was compared with international regulations. The results reinforce that the consolidation of telemedicine as a safe and socially legitimate practice depends on the integration of regulation, bioethical principles, and a continuous ethical commitment to patients' rights and well-being.

Keywords: Telemedicine. Bioethics. Computer security. Ethics, medical. Legislation. Brazil.

Los autores declaran que no existe ningún conflicto de interés.

La telemedicina, definida como el uso de las tecnologías de la información y la comunicación (TIC) para la prestación de servicios de salud a distancia, se ha adoptado ampliamente en los últimos años como una solución innovadora a diversos desafíos en el sector de la salud. En Brasil, destaca como una herramienta esencial para mejorar el acceso a los servicios de salud, especialmente en zonas remotas, y para aumentar la eficiencia de la atención médica. Sin embargo, esta práctica plantea importantes cuestiones éticas que deben considerarse cuidadosamente para asegurar que la telemedicina beneficie realmente a los pacientes y respete los principios fundamentales de la bioética.

La rápida adopción de la telemedicina en Brasil ha traído consigo una serie de preocupaciones bioéticas relacionadas con la privacidad de los datos de los pacientes, la calidad de la atención médica a distancia y la equidad en el acceso a los servicios de salud. Autores como Corrêa, Zaganelli y Gonçalves¹ enfatizan que, a pesar de los avances tecnológicos, es esencial asegurar que la telemedicina no comprometa la calidad del cuidado médico y que se utilice de manera ética y responsable. El objetivo de la telemedicina siempre debe estar en línea con los principios bioéticos, priorizando el bienestar del paciente y la justicia en el acceso a los servicios de salud².

Este estudio utiliza un enfoque bibliográfico exploratorio y descriptivo para analizar las cuestiones bioéticas asociadas a la telemedicina en Brasil. Esta investigación se basa en una revisión de la literatura existente, con el objetivo de proporcionar una visión integral de los desafíos y las mejores prácticas para la implementación ética de la telemedicina, así como reflexionar sobre los efectos de las TIC y de la globalización en la salud desde una perspectiva ética, contribuyendo al desarrollo de prácticas más seguras y equitativas en la telemedicina.

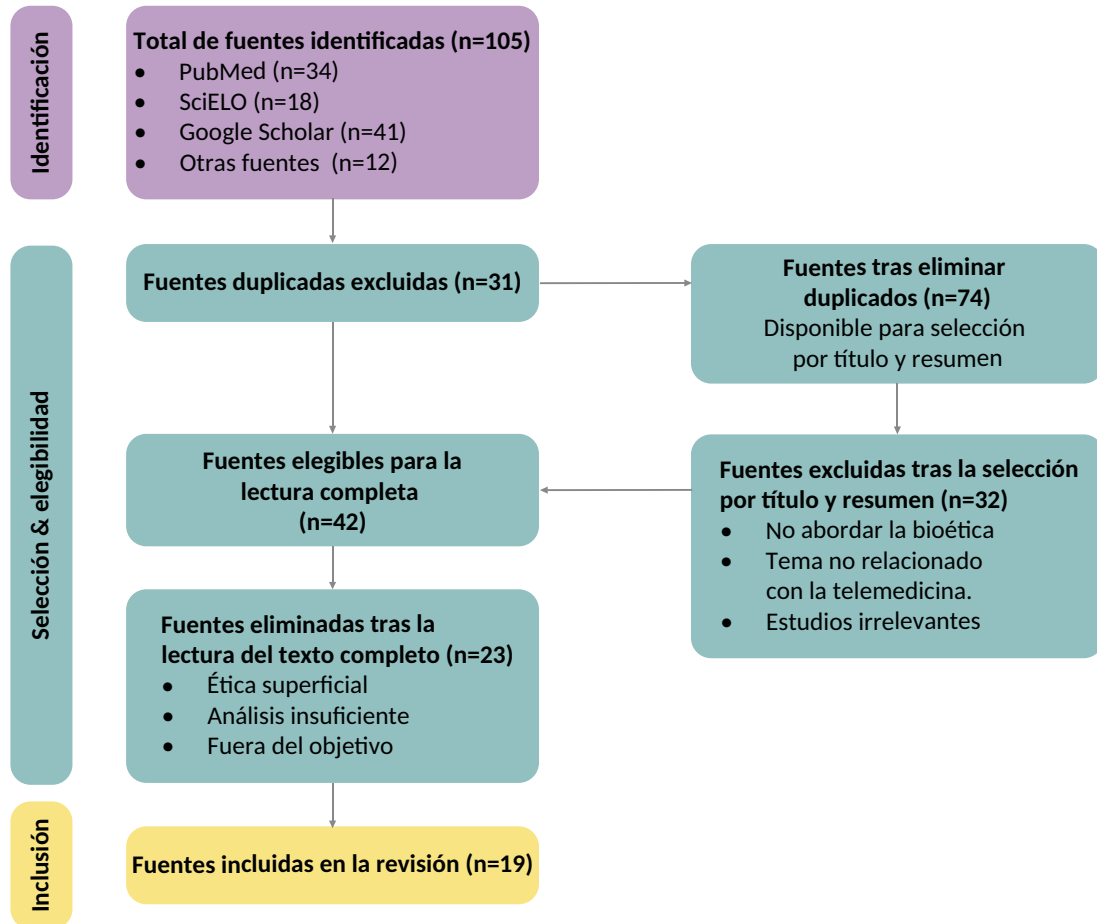
Método

Los procedimientos metodológicos siguieron las directrices propuestas por Köche³ y por Prodanov y Freitas⁴ para un enfoque de revisión bibliográfica de carácter exploratorio y descriptivo. El proceso de revisión siguió, de manera orientadora y deductiva, las recomendaciones de PRISMA 2020⁵, con miras a la transparencia y a la organización lógica del proceso de selección de fuentes, sin pretender una sistematicidad estricta.

La etapa de identificación arrojó 105 registros, procedentes de las bases de datos PubMed, SciELO y Google Scholar, así como de otras fuentes documentales relevantes, como la legislación nacional e internacional y los documentos normativos institucionales. Tras eliminar los duplicados, se seleccionaron 74 registros por título y resumen, y se excluyeron 32 porque no abordaban aspectos éticos o bioéticos, tenían un enfoque exclusivamente técnico o no estaban relacionados con la telemedicina.

En la etapa de elegibilidad, se evaluaron 42 documentos en su totalidad, de los cuales 23 se excluyeron debido a un enfoque ético superficial, falta de análisis bioético estructurado, redundancia conceptual o insuficiencia para el ámbito brasileño o la comparación internacional. Finalmente, el cuerpo analítico de la revisión estuvo conformado por 19 estudios, entre los que se incluyen artículos científicos, legislación, tesis, disertaciones y documentos institucionales, generalmente disponibles en diarios oficiales y repositorios normativos. El análisis y la síntesis de los datos se llevaron a cabo de manera crítica e interpretativa, lo que permitió construir una comprensión sistematizada y bien fundamentada de los principales aspectos bioéticos que impregnan la telemedicina en el contexto brasileño.

La Figura 1 presenta el diagrama de flujo del proceso de identificación, selección, elegibilidad e inclusión de los estudios, desarrollado de acuerdo con las recomendaciones PRISMA 2020.

Figura 1. Diagrama de flujo de búsqueda

Discusión

Definición de ética y bioética

La ética es la rama de la filosofía que estudia los valores morales y los principios que rigen el comportamiento humano en la sociedad. Según Araújo⁶, se trata de juicios relacionados con el bien y el mal que guían la conducta humana, promoviendo el bienestar personal y social. Implica reflexiones sobre lo que es moralmente correcto o incorrecto, justo o injusto, en diferentes contextos.

La bioética, por otra parte, es una extensión de la ética centrada en cuestiones morales relacionadas con la vida y la salud. Es el estudio de las dimensiones éticas de las ciencias de la vida, que abarca puntos de vista, decisiones, conductas y políticas en estos campos, buscando guiar prácticas que respeten la dignidad y los derechos humanos⁷.

En la práctica médica tradicional, la ética y la bioética guían las acciones de los profesionales de la salud. La ética médica, un subcampo de la ética profesional, evalúa el riesgo, los méritos y los impactos sociales de las actividades médicas, asegurando una práctica responsable y el respeto por los derechos y la dignidad de los pacientes⁸.

Los principios éticos fundamentales que guían la práctica médica incluyen la beneficencia, la no maleficencia, la autonomía y la justicia. La beneficencia exige acciones que promuevan la salud y el bienestar. La no maleficencia busca evitar el daño. La autonomía respeta el derecho de los pacientes a tomar decisiones informadas, mientras que la justicia exige equidad en la distribución de recursos y tratamientos⁸.

La aplicación de estos principios en la práctica médica conlleva diversas responsabilidades. Los médicos deben informar claramente a los pacientes, asegurar decisiones informadas, preservar la confidencialidad y tratar a todos de forma

justa, independientemente de factores personales o socioeconómicos⁸.

La bioética, como disciplina más amplia, extiende estos principios para incluir preocupaciones sobre la justicia social y la equidad en el acceso a los cuidados de salud. Se ocupa de las condiciones sociales y ambientales que afectan a la salud, y aboga por enfoques integrados. Esto incluye evaluar los determinantes sociales de la salud y defender políticas que aseguren el acceso equitativo a los servicios para todos⁷.

Ética médica en la telemedicina

Los principios éticos que sustentan la práctica médica tradicional aseguran una relación basada en la confianza, el respeto y la justicia. La beneficencia exige que los médicos prioricen el bienestar del paciente tratando y previniendo enfermedades, así como ofreciendo consejos para mejorar su calidad de vida². Complementando la beneficencia, la no maleficencia requiere que los médicos eviten causar daño evaluando rigurosamente los riesgos y beneficios de las intervenciones, asegurando, así, que los beneficios superen los riesgos².

La autonomía reconoce el derecho de los pacientes a decidir sobre su cuidado. Los médicos deben proporcionar información clara y completa, que permita decisiones conscientes. El respeto a la autonomía es esencial para una práctica ética y humanizada². La justicia exige equidad en la distribución de los recursos e igualdad en el trato con los pacientes, independientemente de factores socioeconómicos o personales. Este enfoque promueve el acceso justo a los cuidados de salud para todos².

Estos principios refuerzan la confianza entre médicos y pacientes, lo cual es esencial para la adherencia al tratamiento. La práctica médica ética también implica mantener la confidencialidad de los pacientes. Esto significa que toda la información personal y de salud de los pacientes debe mantenerse confidencial, salvo cuando el paciente dé su consentimiento para su divulgación o cuando la ley lo exija. La confidencialidad es fundamental para generar confianza entre médicos y pacientes².

Por último, la práctica ética requiere profesionalismo e integridad. Los médicos deben tratar a todos con dignidad, comunicarse con honestidad y evitar la discriminación o los prejuicios, promoviendo un cuidado respetuoso e inclusivo².

Sin embargo, la telemedicina plantea nuevos desafíos éticos, especialmente en lo que respecta

a la confidencialidad de los datos de los pacientes. La transmisión electrónica aumenta el riesgo de violaciones de la privacidad, lo que exige que las plataformas adopten medidas de seguridad sólidas para proteger esta información¹.

El consentimiento informado también supone un reto, ya que es fundamental que los pacientes comprendan los riesgos y beneficios de los tratamientos, lo cual puede resultar más difícil de forma virtual. Los médicos deben explicar los tratamientos en detalle y dejar espacio para preguntas e inquietudes⁹.

La relación médico-paciente, fundamental en la práctica médica, puede verse perjudicada por la mediación tecnológica. La distancia dificulta la conexión empática y la confianza, lo que hace necesario que los profesionales se esfuercen por mantener una comunicación clara y humanizada, utilizando recursos que promuevan la interacción visual y auditiva².

Otro desafío es la equidad en el acceso a la telemedicina, ya que no todo el mundo tiene acceso a la tecnología o a una conexión a internet de calidad, un hecho que genera desigualdades. Las políticas públicas deben asegurar que todos, independientemente de su ubicación o estatus socioeconómico, puedan utilizar estos servicios⁹.

La seguridad de los datos sigue siendo una prioridad, y las plataformas deben cumplir con estándares estrictos como el cifrado y la autenticación multifactor¹. Finalmente, la aceptación de los pacientes varía, y los médicos deben respetar sus preferencias, así como ofrecer apoyo para que la telemedicina sea una opción viable y cómoda⁹.

Para abordar los desafíos éticos de la telemedicina y asegurar el mantenimiento de los principios éticos tradicionales, se necesitan directrices específicas que orienten la práctica de la medicina a distancia. En primer lugar, las plataformas de telemedicina deben implementar medidas avanzadas de ciberseguridad, como el uso de cifrado, cortafuegos y autenticación multifactor, además de auditorías periódicas, para asegurar la seguridad y la confidencialidad de los datos de los pacientes, identificando y corrigiendo vulnerabilidades¹.

Las directrices deben asegurar un acceso equitativo a la telemedicina, con una atención de calidad para todos, independientemente de su ubicación o situación socioeconómica, incluyendo apoyo técnico y equipos para quienes los necesiten¹. En consecuencia, la telemedicina debe ser monitoreada continuamente para asegurar estándares éticos y de calidad, incluyendo revisiones

de seguridad, evaluaciones de satisfacción del paciente y análisis de resultados, con sistemas de feedback para la mejora continua².

La adopción de tecnologías avanzadas puede contribuir a mejorar la seguridad y la eficacia de la telemedicina. Esto incluye el uso de inteligencia artificial para apoyar el diagnóstico, la telemonitorización para el seguimiento continuo del paciente y la integración de dispositivos de salud conectados. Las directrices deben fomentar la innovación tecnológica, a la vez que aseguran que estas tecnologías se implementen de forma ética y segura¹.

Los profesionales de la salud también necesitan formación continua en telemedicina, que abarque aspectos técnicos, éticos y de comunicación, para asegurar una atención ética y de alta calidad. Las instituciones deben ofrecer programas de actualización periódicos sobre tecnologías y directrices². Además, deben humanizar la atención en la telemedicina mediante una comunicación clara y empática; las videollamadas ayudan a mantener la conexión visual y emocional, acercando la experiencia a la de la atención presencial⁹.

La transparencia es fundamental para la práctica ética de la telemedicina. Los pacientes deben ser informados sobre cómo se utilizarán y protegerán sus datos, y cualquier incidente de seguridad debe comunicarse de forma clara y oportuna. La comunicación abierta ayuda a generar confianza y a asegurar que los pacientes conozcan sus derechos y las medidas de protección implementadas⁹.

Los pacientes deben participar activamente en el desarrollo y en la implementación de los servicios de telemedicina. Esto incluye consultarlos sobre sus necesidades y preferencias, incorporar sus perspectivas en el diseño de los servicios y brindarles el apoyo adecuado para ayudarlos a utilizar las tecnologías de telemedicina. La participación de los pacientes ayuda a asegurar que los servicios sean accesibles, comprensibles y adecuados a sus necesidades².

A su vez, el consentimiento informado debe ser claro, estar documentado y asegurar que los pacientes comprendan el tratamiento, los riesgos, los derechos y el uso de sus datos. Los médicos deben explicar las opciones y responder a todas sus dudas⁹.

Las tecnologías de la información y sus impactos en la medicina

La evolución de las TIC ha transformado profundamente la medicina, ofreciendo nuevas herramientas y

métodos para diagnosticar, tratar y gestionar la salud. Desde la década de 1960, las TIC han progresado desde la eficiencia administrativa hasta los sistemas de apoyo a la toma de decisiones clínicas, los registros electrónicos de salud y la telemedicina⁸.

La digitalización de los registros ha facilitado el acceso y el intercambio de información entre profesionales, mejorando la continuidad y la calidad de la atención⁷. Los sistemas de telemetría y monitoreo remoto permitieron el seguimiento remoto, con intervenciones más rápidas y personalizadas⁷.

La pandemia de COVID-19 aceleró el uso de las TIC en la medicina, demostrando la importancia de las soluciones digitales para mantener la atención médica durante el distanciamiento social. Las consultas y tratamientos remotos redujeron el riesgo de infección y aseguraron el cuidado necesario⁶.

Entre las principales tecnologías utilizadas en la telemedicina se encuentran las videoconferencias, las plataformas digitales y los dispositivos móviles. Las herramientas de videoconferencia permiten realizar consultas, diagnósticos y tratamientos a distancia en tiempo real. Promueven la interacción visual y auditiva, que es fundamental para generar confianza entre médico y paciente¹⁰. Plataformas como Zoom, Microsoft Teams y Google Meet están adaptadas para asegurar la privacidad y satisfacer las demandas específicas del sector sanitario.

Las plataformas de salud digital ofrecen funciones como la programación de citas, registros electrónicos, comunicación segura y acceso a información médica. Estas herramientas optimizan la gestión de los cuidados, una vez que facilitan el intercambio de información y mejoran la coordinación entre los profesionales de la salud⁸.

A su vez, los dispositivos como los teléfonos inteligentes y las tabletas son esenciales en la telemedicina, ya que permiten a los pacientes supervisar su salud en tiempo real. Las aplicaciones y los dispositivos conectados, como los medidores de glucosa y los monitores de presión arterial, ayudan en la monitorización continua y la recopilación de datos, lo que permite un seguimiento médico más preciso y personalizado⁷.

Las TIC ofrecen diversos beneficios al campo médico, como una mayor accesibilidad a los cuidados de salud, especialmente para pacientes con movilidad reducida o que viven en zonas remotas. La telemedicina elimina la necesidad de desplazamientos, lo que supone un ahorro de tiempo y recursos para pacientes y profesionales¹⁰. Además,

estas tecnologías facilitan la comunicación entre los profesionales de la salud, promoviendo un cuidado más integrado y eficiente⁸.

A pesar de sus beneficios, las TIC presentan desafíos, como los relacionados con la seguridad y la privacidad de los datos de los pacientes. La transmisión digital de información aumenta el riesgo de ciberataques y violaciones, lo que compromete la confidencialidad⁸. También existen preocupaciones sobre las desigualdades en el acceso, ya que los pacientes sin recursos tecnológicos pueden quedar excluidos⁶.

Adaptarse a las tecnologías digitales es otra barrera. Muchos profesionales de la salud no están familiarizados con estas herramientas, lo que puede afectar la efectividad de la atención⁷. Si bien las consultas a distancia son útiles, presentan limitaciones, como la imposibilidad de realizar exploraciones físicas, lo que puede afectar a los diagnósticos y tratamientos.

Datos en entornos de salud virtuales

Proteger los datos de salud de los pacientes es crucial para la confianza en el sistema de salud digital y el cumplimiento de regulaciones como la Ley General de Protección de Datos (LGPD) en Brasil y el Health Insurance Portability and Accountability Act (HIPAA), en los Estados Unidos (EE. UU.)⁸. Para prevenir accesos no autorizados y ciberataques, son esenciales medidas como el cifrado, la autenticación multifactor, los cortafuegos y la supervisión continua¹⁰.

Las plataformas de telemedicina deben cumplir estrictamente con las normas legales de seguridad y privacidad. Paralelamente, es esencial cultivar una cultura de seguridad entre los profesionales de la salud mediante formación regular y concienciación sobre la protección de datos⁷. La transparencia con los pacientes sobre cómo se utilizarán y protegerán sus datos también es fundamental para mantener la confianza en el sistema de salud digital.

La responsabilidad de la seguridad de los datos debe ser compartida entre los desarrolladores de tecnología, las instituciones sanitarias y los médicos, con esfuerzos conjuntos para asegurar prácticas seguras y eficaces¹.

Aspectos de la Ley General de Protección de Datos

La LGPD establece un marco legal para el tratamiento de datos personales en Brasil y se aplica tanto

a personas físicas como jurídicas, públicas o privadas. En la telemedicina, donde se manejan datos de salud sensibles, la LGPD desempeña un papel esencial y exige una protección rigurosa y seguridad¹¹.

El tratamiento de datos personales en telemedicina debe seguir los principios de la LGPD, como la finalidad, la transparencia, la seguridad y la responsabilidad (art. 6)¹¹. Estos principios guían las prácticas éticas y seguras para la recopilación, el almacenamiento y el uso de datos, promoviendo la confianza del paciente y el cumplimiento legal¹. El consentimiento informado es fundamental y debe otorgarse libremente, de forma explícita y detallada, informando sobre la finalidad del uso de los datos, los métodos de intercambio y las medidas de seguridad (art. 7)¹¹. Este proceso educa a los pacientes sobre sus derechos y la importancia de la protección de datos¹.

La LGPD exige una protección adicional para los datos sensibles, como la información de salud, debido al riesgo de discriminación en caso de uso indebido. El tratamiento de estos datos solo está permitido con consentimiento explícito o para proteger la vida o la integridad física del titular o de terceros (art. 11)¹¹.

La transparencia es otro principio clave de la LGPD, que exige que los responsables del tratamiento de datos proporcionen información clara y accesible a los titulares sobre cómo se utilizan sus datos (art. 9)¹¹. En la telemedicina, esto implica que los pacientes también sean informados sobre sus derechos, como el derecho de acceso, rectificación, supresión y portabilidad de sus datos. Corrêa, Zaganelli y Gonçalves¹ destacan que la transparencia fortalece la relación de confianza entre pacientes y proveedores de servicios de salud.

El tratamiento de datos personales en telemedicina también debe incluir medidas de seguridad apropiadas para proteger los datos contra el acceso no autorizado, la destrucción, la pérdida, la modificación, la comunicación o cualquier forma de tratamiento inapropiado o ilícito (art. 46)¹¹. Estas medidas incluyen la implementación de controles de acceso, el cifrado de datos y la realización de auditorías de seguridad periódicas. La responsabilidad se comparte entre empresas, profesionales y desarrolladores de tecnología¹.

El nombramiento de un responsable de protección de datos (*data protection officer*, DPO) es obligatorio para asegurar el cumplimiento de la LGPD y para ayudar a los pacientes y a las organizaciones con dudas e inquietudes (art. 41)¹¹.

Finalmente, la LGPD prevé sanciones estrictas por incumplimiento, como multas y eliminación de

datos (art. 52), fomentando prácticas de cumplimiento y reforzando la confianza pública¹¹. En telemedicina, el cumplimiento de la LGPD es vital para evitar sanciones y proteger a los pacientes.

Seguridad de la información en plataformas de telemedicina

La seguridad de la información es fundamental para proteger los datos de los pacientes y asegurar la fiabilidad de los servicios de telemedicina. Las plataformas deben implementar medidas sólidas para prevenir accesos no autorizados, la pérdida, la modificación o la divulgación indebida de datos, asegurando el cumplimiento legal y la confianza del usuario en el sistema².

El cifrado es una medida esencial para proteger los datos en tránsito y en reposo, ya que los hace inaccesibles para terceros sin la clave de descifrado. Esta práctica es fundamental para la protección de información sensible, como datos de salud, durante la transmisión y el almacenamiento².

Los controles de acceso también son esenciales, ya que limitan el acceso únicamente a los profesionales autorizados. La autenticación multifactor, que combina métodos como contraseñas y códigos enviados a dispositivos móviles, es crucial para prevenir el acceso indebido y los ciberataques, protegiendo la integridad de los datos de los pacientes⁹.

Las auditorías de seguridad periódicas identifican y corrigen vulnerabilidades, asegurando el cumplimiento de normativas como la LGPD. Estas auditorías mantienen las plataformas actualizadas y efectivas, reforzando la seguridad y confiabilidad de los servicios². Además, la formación continua de los profesionales sanitarios es vital para promover una cultura de seguridad. Deben estar capacitados para reconocer amenazas y proteger datos, asegurando prácticas coherentes con las políticas organizacionales y las regulaciones⁷.

La gestión de incidentes es otro pilar de la seguridad. Los procedimientos claros para la detección, respuesta y recuperación de incidentes minimizan los daños y aseguran la notificación de violaciones de seguridad según lo exige la LGPD. Un plan de respuesta bien diseñado refuerza la confianza del paciente².

Deben implementarse políticas de seguridad integrales para regular todas las etapas del procesamiento de datos, desde la recopilación hasta la eliminación. Las revisiones periódicas de estas políticas aseguran su eficacia frente a cambios en las amenazas o regulaciones¹.

La colaboración entre desarrolladores, proveedores de servicios y profesionales médicos es esencial para integrar prácticas de seguridad en todos los niveles. La protección de datos es una responsabilidad compartida que requiere el compromiso de todos los involucrados⁹.

Por último, la transparencia con los pacientes respecto a las medidas de seguridad adoptadas refuerza la confianza en el sistema de telemedicina. Informarles sobre la protección de sus datos y derechos es un aspecto central de una práctica segura y ética².

Consentimiento informado y protección de la privacidad del paciente

El consentimiento informado es un principio fundamental de la LGPD y de la ética en la telemedicina. Debe ser libre, informado y claro, para que los pacientes comprendan cómo se utilizarán, almacenarán y compartirán sus datos. La LGPD asegura el derecho a información clara sobre el tratamiento de datos personales (art. 7, §1)¹¹, exigiendo que los pacientes sean informados sobre el propósito específico, las entidades involucradas y las medidas de seguridad adoptadas.

Obtener el consentimiento informado es un desafío, pero resulta esencial para educar a los pacientes sobre sus derechos y la protección de datos. Los profesionales de la salud deben explicar las opciones de tratamiento y los riesgos, para que se puedan tomar decisiones informadas. Además, los pacientes pueden revocar su consentimiento en cualquier momento, sin perjuicio de su atención¹.

La privacidad del paciente es fundamental en la telemedicina. Únicamente los profesionales autorizados deben acceder a los datos, y exclusivamente con fines médicos. Cualquier vulneración de la privacidad debe ser tratada con transparencia, reforzando la ética y la confianza en el sistema⁹. Las plataformas de telemedicina deben adoptar políticas de privacidad claras que detallen cómo se protegen los datos, los derechos de los pacientes y los procedimientos para denunciar las violaciones. La transparencia fortalece la confianza entre los pacientes y los proveedores de servicios². Las medidas técnicas, como el cifrado y los estrictos controles de acceso, son esenciales para proteger los datos sensibles. Estas prácticas aseguran que los pacientes compartan información con confianza².

La formación periódica sobre el consentimiento informado y la protección de la privacidad son fundamentales para los profesionales de la salud.

La protección de datos es una cuestión técnica y ética que requiere el compromiso de todo el equipo⁷.

La gestión eficaz del consentimiento y la privacidad incluye un plan de respuesta ante incidentes, que detalla las acciones para las violaciones de datos, como la notificación inmediata a las autoridades y a los pacientes, según lo dispuesto en la LGPD (art. 48)¹¹. Una gestión eficaz de los incidentes es crucial para mantener la confianza del paciente y la integridad de los servicios de telemedicina².

La privacidad debe ser una prioridad en todas las etapas de las plataformas de telemedicina, desde su concepción hasta su operación. Los desarrolladores, los proveedores de servicios y los profesionales médicos deben adoptar prácticas alineadas con las mejores prácticas internacionales y la LGPD. Proteger la privacidad es una responsabilidad compartida y esencial para la confianza en los servicios¹.

Teoría del delito e imputación en la telemedicina

La teoría del delito en la telemedicina aplica los principios del derecho penal a las prácticas médicas digitales. La Ley 14.510/2022¹² y la Resolución 2.314/2022 del Consejo Federal de Medicina (CFM)¹³ definen las directrices para esta práctica, incluida la responsabilidad penal y civil de los profesionales. La acusación formal exige verificar la conducta delictiva, su tipicidad, su ilegalidad y la culpabilidad.

La conducta delictiva puede incluir diagnósticos incorrectos, prescripciones inapropiadas e incumplimiento de protocolos. La tipicidad analiza si la conducta se ajusta al tipo delictivo, como negligencia, impericia e imprudencia, punibles según el Código Penal brasileño¹⁴.

La ilegalidad se produce cuando una conducta es contraria a la ley, sin justificación legal, como por ejemplo actuar con negligencia y causar daño. La culpabilidad evalúa la capacidad del profesional para comprender el carácter ilícito del acto y actuar en consecuencia, teniendo en cuenta su formación en tecnologías digitales y telemedicina.

La responsabilidad objetiva exige que el daño sea consecuencia directa de la acción u omisión del médico, estableciendo así un vínculo causal. La Resolución CFM 2.314/2022¹³ exige el estricto cumplimiento de los protocolos para garantizar la seguridad y la eficacia en la atención.

La Ley 14.510/2022¹² destaca la responsabilidad de los profesionales en telemedicina, reforzando el consentimiento informado y la transparencia con los pacientes. También prevé sanciones, incluida la suspensión o la revocación de la inscripción profesional, para quienes no cumplan con la normativa legal.

Los errores médicos en la telemedicina pueden acarrear responsabilidad civil, penal y administrativa. La responsabilidad civil exige una indemnización por los daños causados por negligencia, imprudencia o impericia, y los profesionales deben garantizar la calidad y la seguridad en la atención remota, según la resolución del CFM¹³.

La responsabilidad penal abarca delitos como lesión corporal culposa, homicidio culposo y omisión de socorro, según lo estipulado en el Código Penal, que requieren prueba de culpa. La Ley 14.510/2022¹² refuerza la necesidad de seguir las normas para evitar errores médicos y sus consecuencias legales.

En el ámbito administrativo, los consejos profesionales aplican sanciones tales como advertencias, multas, suspensión y revocación de registro para aquellos que no cumplan con las normas éticas y técnicas de la telemedicina, de acuerdo con la resolución CFM¹³. El estricto cumplimiento de estas normas es fundamental para garantizar la seguridad y la eficacia en la atención remota.

Los profesionales y las instituciones deben adoptar medidas preventivas, como la actualización continua en tecnologías digitales, capacitación y sistemas de calidad y seguridad, tal como lo refuerza el marco legal^{12,13}, para minimizar los riesgos de la telemedicina.

La transparencia en la comunicación con los pacientes es fundamental. Los profesionales deben informar claramente a los pacientes sobre los riesgos y beneficios de la atención remota, asegurando el consentimiento informado, de conformidad con la Ley 14.510/2022¹² y la Resolución CFM 2.314/2022¹³.

La vulneración del secreto profesional en la telemedicina tiene graves consecuencias legales, éticas y profesionales para los médicos y las instituciones. El secreto profesional es un deber ético y legal que obliga a los profesionales a mantener la confidencialidad respecto a la información confidencial de los pacientes, como se enfatiza en la resolución CFM¹³.

En materia civil, la vulneración puede dar lugar a acciones indemnizatorias por daños morales y materiales, ya que los pacientes tienen derecho a una compensación por la divulgación no autorizada de información. Los profesionales y las instituciones

deben adoptar medidas para proteger estos datos, tal como se establece en la legislación¹².

En el ámbito penal, la vulneración es un delito definido en el Código Penal (art. 154)¹⁴, con penas de prisión de tres meses a un año, o una multa. La Resolución CFM 2.314/2022¹³ establece sanciones penales y administrativas para los infractores. Administrativamente, las sanciones incluyen advertencia, censura, suspensión y revocación del registro, lo que subraya la necesidad de un estricto cumplimiento de los principios éticos y legales en la telemedicina^{13,14}. Además de las sanciones, la vulneración compromete la confianza entre médico y paciente, que es fundamental para el éxito terapéutico y la integridad de la práctica médica, como lo destaca el CFM¹³.

Los profesionales y las instituciones deben implementar medidas rigurosas, como el uso de tecnologías seguras, políticas de privacidad y capacitación periódica, de conformidad con la Ley 14.510/2022¹² y la Resolución CFM 2.314/2022¹³, para prevenir vulneraciones. La transparencia sobre la protección de la información es vital para la confianza en la telemedicina. Los pacientes deben ser informados claramente sobre las medidas de seguridad y sus derechos, para asegurar una comunicación abierta y la protección de la privacidad^{12,13}.

El ejercicio ilegal de la medicina por medio de la telemedicina supone un riesgo para la salud pública y la seguridad de los pacientes. La legislación establece directrices estrictas para que solo los profesionales cualificados y registrados puedan trabajar utilizando tecnologías digitales^{12,13}.

Se considera ejercicio ilegal cuando una persona no cualificada o sin registro realiza consultas, diagnósticos, prescripciones o tratamientos sin autorización. El Código Penal (art. 282)¹⁴ prevé una pena de prisión de seis meses a dos años para este delito. Los profesionales deben estar registrados en el CRM de su jurisdicción y deben cumplir con los requisitos legales y éticos. Las instituciones sanitarias deben garantizar que solo profesionales cualificados trabajen en telemedicina¹³.

Las consecuencias son severas: sanciones civiles, penales y administrativas. Los pacientes pueden reclamar una indemnización por los daños causados por profesionales ilegales y estos pueden enfrentarse a penas de prisión. Las instituciones que permitan o faciliten el ejercicio ilegal también serán responsables administrativamente.

Las instituciones son responsables de garantizar que sus plataformas sean utilizadas únicamente

por profesionales cualificados, con verificación constante de registros y medidas de seguridad para evitar el acceso no autorizado, según lo determine la ley¹².

Regulación de la telemedicina en Estados Unidos y en la Unión Europea

En Estados Unidos, la protección de datos y la telemedicina están reguladas por leyes federales y estatales. La principal legislación federal es el Health Insurance Portability and Accountability Act (HIPAA)¹⁵, promulgado en 1996, que establece normas nacionales para garantizar la privacidad y la seguridad de la información de salud de los pacientes¹⁵.

El HIPAA exige que las entidades cubiertas, como los planes de salud, los proveedores y los intermediarios de datos, implementen medidas rigurosas, que incluyen cifrado, controles de acceso, autenticación multifactor y auditorías de seguridad. También asegura a los pacientes el derecho a acceder y corregir su información¹⁵.

En el caso de la telemedicina, el HIPAA impone requisitos para proteger los datos durante las consultas remotas, exigiendo que las plataformas garanticen la seguridad de las comunicaciones electrónicas y de los datos de los pacientes. El cumplimiento es obligatorio para todos los proveedores que utilizan tecnología digital¹⁵.

Además del HIPAA, el Health Information Technology for Economic and Clinical Health Act (HITECH)¹⁶ refuerza sus disposiciones y promueve el uso de registros de salud electrónicos (*electronic health records*, EHR). El HITECH prevé sanciones severas para infracciones y exige la notificación a los pacientes y al Departamento de Salud y Servicios Humanos (HHS) en casos de vulneraciones significativas¹⁶.

A su vez, la Unión Europea (UE) tiene un enfoque armonizado en materia de protección de datos y regulación de la telemedicina, basado en la General Data Protection Regulation (RGPD)¹⁷, que entró en vigor en mayo del 2018. La RGPD establece un conjunto exhaustivo de normas para la protección de datos personales, aplicables a todas las organizaciones que procesan datos de ciudadanos de la UE, independientemente de dónde estén ubicadas dichas organizaciones.

La RGPD exige el consentimiento informado, la transparencia y la minimización de datos, y garantiza derechos a los titulares, como el acceso,

la rectificación, la supresión y la portabilidad. Las organizaciones deben adoptar medidas técnicas y organizativas, como la pseudonimización, el cifrado, las evaluaciones de impacto y la notificación de infracciones dentro de las 72 horas¹⁷.

En lo que respecta a la telemedicina, la RGPD exige a los proveedores de servicios que garanticen que la información sanitaria de los pacientes se trate con la máxima confidencialidad y seguridad. Esto incluye la adopción de tecnologías seguras para la transmisión y el almacenamiento de datos, así como la implementación de políticas y procedimientos claros para la protección de datos. El cumplimiento de la RGPD es esencial para cualquier organización que ofrezca servicios de telemedicina a ciudadanos de la UE¹⁷.

Además de la RGPD, la UE cuenta con la NIS Directive¹⁸, que establece requisitos para la seguridad de las redes y los sistemas de información, incluidos los sistemas utilizados para la prestación de servicios sanitarios. La NIS Directive exige a los operadores de servicios esenciales, como hospitales y clínicas, que implementen medidas de seguridad apropiadas y notifiquen a las autoridades competentes cualquier incidente de seguridad que pueda afectar significativamente la prestación de servicios¹⁸.

La Estrategia Europea para la Salud Digital¹⁹ también proporciona directrices para promover la telemedicina y la salud digital en la UE. Esta estrategia tiene como objetivo mejorar la interoperabilidad de los sistemas sanitarios, promover la innovación en la salud digital y garantizar que los servicios de salud digital sean accesibles y seguros para todos los ciudadanos de la UE. La estrategia destaca la importancia de la protección de datos y la privacidad como fundamentales para la confianza de los ciudadanos en la salud digital¹⁹.

Comparación entre Brasil, Estados Unidos y la Unión Europea

Al comparar la legislación brasileña con las regulaciones de Estados Unidos y de la Unión Europea, se observa que los tres sistemas legales tienen como objetivo principal la protección de datos personales y la seguridad en la prestación de servicios de salud digital. Sin embargo, existen diferencias significativas en los enfoques y en los requisitos específicos.

En Brasil, la LGPD establece directrices exhaustivas para la protección de datos personales, aplicables a todas las organizaciones que procesan datos de ciudadanos brasileños. La LGPD es similar a la RGPD de la UE en cuanto a rigor y alcance, ya que exige el consentimiento informado, la transparencia y la implementación de medidas de seguridad adecuadas. Sin embargo, la LGPD presenta peculiaridades, como el requisito de un DPO y sanciones específicas por incumplimiento de las normas¹¹.

En Estados Unidos, la regulación está más fragmentada: el HIPAA establece normas federales para la protección de datos de salud, complementadas por leyes estatales específicas para la telemedicina. El cumplimiento del HIPAA es obligatorio para todos los proveedores de servicios de salud, pero la aplicación y los requisitos específicos pueden variar según el estado. El enfoque estadounidense está más orientado a la práctica y es menos centralizado que el enfoque armonizado de la UE^{15,16}.

La Unión Europea, por medio de la RGPD y de la NIS Directive, adopta un enfoque altamente regulado y armonizado en materia de protección de datos y seguridad de la telemedicina. La RGPD impone requisitos estrictos en materia de consentimiento, transparencia y seguridad de los datos, aplicables a todas las organizaciones que procesan datos de ciudadanos de la UE. La estrategia de la UE para la salud digital también promueve la interoperabilidad y la innovación, garantizando que los servicios de salud digital sean seguros y accesibles^{17,18}.

En conclusión, si bien existen diferencias en los enfoques y en los requisitos específicos entre Brasil, Estados Unidos y la Unión Europea, los tres sistemas legales reconocen la importancia de la protección de datos y de la seguridad en la telemedicina. El cumplimiento de la regulación local es fundamental para asegurar la confianza de los pacientes y la eficacia de los servicios de salud digitales. Las mejores prácticas internacionales pueden servir de referencia para la mejora continua de las regulaciones y de las prácticas de protección de datos en la telemedicina.

Consideraciones finales

Los resultados de esta revisión bibliográfica exploratoria y descriptiva indican que la telemedicina, en el contexto brasileño, debe analizarse más

allá de sus aspectos técnicos y normativos, por lo que requiere una reflexión ética y bioética constante. La literatura especializada demuestra que la incorporación de las TIC en la práctica médica reconfigura la relación médico-paciente, el cuidado en salud y la gestión de datos sensibles, lo que demanda una resignificación de los principios bioéticos clásicos.

La protección de datos personales emerge como un eje ético central, directamente vinculado a la dignidad humana y al principio de no maleficencia. Los estudios analizados indican que la confidencialidad, en el entorno digital, depende no solo del cumplimiento de la ley, sino también del compromiso moral de los profesionales y las instituciones para prevenir los riesgos y daños derivados del uso indebido de la información sanitaria. En ese sentido, un análisis comparativo entre la legislación brasileña y los marcos internacionales revela una convergencia en cuanto a la importancia

central de la privacidad, aunque destaca que las normas, por sí solas, no garantizan prácticas éticamente apropiadas.

En lo que respecta a la autonomía, la literatura indica que el consentimiento informado en telemedicina debe entenderse como un proceso continuo de comunicación ética, que abarca no solo los aspectos clínicos, sino también los riesgos tecnológicos y el procesamiento de datos. La beneficencia se asocia con el potencial de ampliar el acceso a la salud, mientras que la justicia impone la necesidad de abordar las desigualdades digitales que pueden comprometer la indicación ética de la telemedicina.

Por lo tanto, los resultados refuerzan la idea de que la consolidación de la telemedicina como una práctica segura y socialmente legítima depende de la integración entre la regulación, los principios bioéticos y un compromiso ético permanente con los derechos y el bienestar de los pacientes.

Referencias

1. Corrêa JCB, Zaganelli MV, Gonçalves BD. Telemedicina no Brasil: desafios ético-jurídicos em tempos de pandemia da Covid-19. *Humanit Tecnol (FINOM)* [Internet]. 2020 [acesso 21 maio 2025];25(1):200-18. Disponível: <https://bit.ly/4dHEuLw>
2. Garcia EF, Oliveira SM, Reis JG. Bioética e telemedicina. *Rev Bioética Cremego* [Internet]. 2020 [acesso 10 jun 2025];2(1):61-6. Disponível: <https://bit.ly/48Cxx4r>
3. Köche JC. Fundamentos de metodologia científica. Petrópolis: Vozes; 2015.
4. Prodanov CC, Freitas EC. Metodologia do trabalho científico. 2ª ed. Novo Hamburgo: Feevale; 2013.
5. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD *et al.* The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ* [Internet]. 2021 [acesso 18 maio 2025];372:71. DOI: 10.1136/bmj.n71
6. Araújo RCV. Direito versus bioética em tempos de pandemia: que desafios? *Rev Ang Ciênc Saúde* [Internet]. 2022 [acesso 21 maio 2025];1:1-4. DOI: 10.54283/RACSaude.v3i1edsupl1.2022.p1-4
7. Oliveira EL, Soares A, Lima J, Santos RM. Falhas de comunicação e epistemológicas limitam a abordagem da bioética na formação e na prática em saúde. *Interface (Botucatu)* [Internet]. 2021 [acesso 21 maio 2025];25:e200679. DOI: 10.1590/interface.200679
8. Cohen C, Gobbetti G, Oliveira RA. Breve discurso sobre ética, moral, estética e bioética das relações. *Rev Bras Psicanál* [Internet]. 2021 [acesso 21 maio 2025];55(2):41-57. Disponível: <https://bit.ly/4njFLN1>
9. Sánchez MVC, Costa FG, Bossio P, Fàbrega C, Abejas AG, Vergès AS. Telemedicina y eSalud: reflexiones desde la bioética. Barcelona: Institut Borja de Bioètica; 10 nov 2022. Disponível: <https://bit.ly/4wapuhs>
10. Sganzerla AS, Zanella DC, Paulo Neto A, Good C. A bioética como ética aplicada: a saúde em destaque. *Rev Inst* [Internet]. 2023 [acesso 21 maio 2025];5(2):59-78. Disponível: <https://bit.ly/4cZButq>
11. Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União* [Internet]. Brasília, nº 154-A, p. 1, 15 ago 2018 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4w7whs6>
12. Brasil. Lei nº 14.510, de 27 de dezembro de 2022. Altera a Lei nº 8.080, de 19 de setembro de 1990. Autoriza e disciplina a prática da telessaúde em todo o território nacional, e a Lei nº 13.146, de 6 de julho

- de 2015; e revoga a Lei nº 13.989, de 15 de abril de 2020. Diário Oficial da União [Internet]. Brasília, nº 244, p. 1, 28 dez 2022 [acesso 21 maio 2025]. Disponível: <https://bit.ly/42eG5mG>
13. Conselho Federal de Medicina. Resolução nº 2.314, de 20 de abril de 2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. Diário Oficial da União [Internet]. Brasília, p. 227, 5 maio 2022 [acesso 21 maio 2025]. Disponível: <https://tinyurl.com/hyrzwr3f>
 14. Brasil. Decreto-Lei nº 2 848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União [Internet]. Brasília, p. 23911, 31 dez 1940 [acesso 21 maio 2025]. Disponível: <https://bit.ly/3OJpDI1>
 15. United States. Health Insurance Portability and Accountability Act (HIPAA). To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes. Federal Register [Internet]. Washington, 20 ago 1996 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4w9dEUT>
 16. United States. Health Information Technology for Economic and Clinical Health Act (HITECH). Federal Register [Internet]. Washington, v. 74, n. 209, 30 out 2009 [acesso 21 maio 2025]. Disponível: <https://bit.ly/3QQVfMj>
 17. European Union. General Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR). Off J Eur Union [Internet]. 2016 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4n6oRBj>
 18. European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union. [Internet]. Brussels, 27 abr 2016 [acesso 21 maio 2025]. Disponível: <https://bit.ly/4wbaiRe>
 19. eHealth - digital services in health and care [Internet]. Brussels: European Commission; 2025 [acesso 21 maio 2025]. Disponível: <https://bit.ly/3OJpJzn>

Juracy Barbosa dos Santos – Estudante de doctorado – drjuracybarbosa@gmail.com

 0009-0009-1729-9778

Guilhermina Rego – Doctora – guilherminarego@med.up.pt

 0000-0002-8590-9832

Rui Nunes – Doctor – ruinunes@med.up.pt

 0000-0002-1377-9899

Correspondencia

Juracy Barbosa dos Santos – Faculdade de Medicina da Universidade do Porto. Alameda Prof. Hernâni Monteiro, 4200-319. Porto, Portugal.

Contribución de los autores

Juracy Barbosa dos Santos: concepción del estudio; análisis de datos; redacción del manuscrito. Guilhermina Rego: revisión del manuscrito. Rui Nunes: análisis crítico; revisión final del manuscrito.

Disponibilidad de los datos: Todos los datos utilizados o generados en la investigación se describen y presentan íntegramente en el cuerpo del artículo.

Editora responsable: Dilza Teresinha Ambrós Ribeiro

Recibido: 28.4.2025

Revisado: 5.6.2025

Aprobado: 13.1.2026