

La ciberseguridad en telemedicina

Según el Ministerio de Salud de Chile, entre 2020 y 2022 se registraron más de 10 millones de consultas médicas virtuales, lo que evidencia no solo el potencial de esta modalidad, sino también su consolidación como un pilar de la atención sanitaria en el país.

Sin embargo, esta expansión acelerada ha planteado un nuevo desafío: ¿están estas plataformas de telemedicina preparadas para proteger los datos sensibles de los pacientes y garantizar servicios confiables y seguros?

Uno de los principales problemas que enfrentan las plataformas de telemedicina es la protección de los datos personales y sensibles de los pacientes. La información médica es, por naturaleza, extremadamente sensible.

Su exposición no solo pone en riesgo la privacidad de los individuos, sino que también puede dar lugar a situaciones de extorsión o fraude. En un mundo donde los ciberataques son cada vez más frecuentes, la seguridad no es un lujo, es una necesidad, y nuestro país no está ajeno a esta problemática.

En 2022, el Centro de Respuesta a Incidentes de Seguridad Computacional de Chile (CSIRT) reportó un aumento del 300% en incidentes cibernéticos, afectando tanto al



La certificación, como la obtenida recientemente por el Grupo Cetep con el Sello CENS otorgado por FONASA, es un paso importante en esta dirección. Este sello avala a la plataforma como una herramienta segura, confiable, de alta calidad y disponibilidad. No obstante, este tipo de certificaciones deben ser la norma, no la excepción.

sector público como privado. Este aumento en los ataques cibernéticos también ha golpeado a las plataformas de telemedicina, exponiendo vulnerabilidades que, en muchos casos, aún no han sido abordadas de manera efectiva.

La legislación también juega un papel crucial en la protección de los datos de salud. En Chile, la Ley N° 19.496 de protección de datos personales regula el tratamiento de datos sensibles, incluyendo aquellos relacionados con la salud. Sin embargo, la realidad es que el 70% de las empresas no cumplen completamente con las normativas de ciberseguridad vinculadas a la protección de datos médicos, según estudios de la Cámara Chilena de Comercio. Esta brecha en el cumplimiento es alarmante.

Uno de los mayores peligros que enfrentan las plataformas de telemedicina es la filtración de datos a través de redes no seguras. La información médica de los pacientes podría ser interceptada durante la transmisión entre los diferentes sistemas de atención, poniendo en riesgo la confidencialidad de la misma. Además, la interoperabilidad entre distintos sistemas de gestión hospitalaria y la integración de servicios con terceros, si no se realiza mediante conexiones adecuadamente protegidas, puede generar puntos de vulnerabilidad

que los ciberdelincuentes pueden explotar.

Además, las estafas denominadas "phishing", en los que los atacantes se hacen pasar por entidades legítimas para obtener credenciales de acceso, son cada vez más sofisticadas y frecuentes.

Este tipo de ataques pone en evidencia la fragilidad de los mecanismos de seguridad en muchos sistemas de telemedicina, lo que deja abiertas las puertas a intrusos con fines maliciosos. En este contexto, es crucial que las instituciones de salud y las plataformas de telemedicina adopten medidas robustas de seguridad y protección de datos.

En un mundo cada vez más digital, donde las amenazas cibernéticas son una constante, la protección de la información médica no puede ser una opción. La confianza de los pacientes en estas plataformas depende directamente de nuestra capacidad para garantizar que sus datos estén protegidos de manera efectiva. Es una responsabilidad que debemos asumir con seriedad.

La telemedicina tiene un enorme potencial para mejorar la atención sanitaria, pero solo si es capaz de ofrecer no solo accesibilidad, sino también seguridad. Solo así podremos avanzar hacia un sistema de salud más eficiente, confiable y, sobre todo, seguro para todos.



CLAUDIA BARRERA
MÉDICO PSIQUIATRA