Resumen ejecutivo: Diálogo sobre la Seguridad y Privacidad de los Datos en Salud Sexual y Reproductiva

Introducción

Este resumen ejecutivo presenta los puntos clave del diálogo virtual “Salud Sexual y Reproductiva: desafíos y oportunidad para garantizar la seguridad y privacidad de los datos sensibles”, organizado por la Asociación por los Derechos Civiles (ADC) con el apoyo de la Embajada Británica en Argentina el 27 de febrero de 2025. Cabe señalar que las ideas y conclusiones aquí presentadas emanan directamente de las discusiones y aportes de los y las participantes en la jornada, y no necesariamente reflejan las opiniones de la ADC ni de la Embajada Británica.

El evento reunió a especialistas de diversos sectores en un espacio de intercambio seguro y respetuoso para analizar los riesgos a la privacidad y seguridad asociados con la recopilación, almacenamiento y gestión de datos de salud sexual y reproductiva en el contexto del uso de tecnologías de la información y las comunicaciones en la atención médica. Además, se evaluó la efectividad del marco normativo vigente en Argentina y se discutieron estrategias concretas para resguardar los derechos de las personas usuarias de estos servicios, en especial de las mujeres.

Panorama Normativo y Protección de Datos en Salud Sexual y Reproductiva

La inclusión del habeas data en la Constitución Nacional en 1994 marcó un hito en la defensa del derecho a la privacidad, seguido por la promulgación de la Ley N° 25.326 de Protección de Datos Personales en el año 2000 y su reglamentación en 2001. Esta ley establece principios fundamentales como licitud, calidad, minimización, proporcionalidad y seguridad, aplicables tanto a los datos personales como a los considerados sensibles, como los de salud.

Durante el diálogo quedó resaltado que los artículos 7 y 8 de la Ley N° 25.326 establecen restricciones clave sobre la recolección y tratamiento de datos sensibles, sin embargo, su implementación y fiscalización aún enfrentan ciertas limitaciones. Un aspecto clave en la protección de estos datos es el consentimiento informado, que debe ser libre y expreso, asegurando que las personas comprendan las implicancias de la información proporcionada. La necesidad de reforzar el marco regulatorio quedó evidenciada con la última propuesta de actualización de la Ley 25.326, que contemplaba mejoras en la protección de datos sensibles pero que, lamentablemente, perdió estado parlamentario.

Se resaltó también la importancia de apoyar un cambio de paradigma que desplace el enfoque centrado en la protección del dato hacia la protección de la persona. La adhesión al Convenio 108 y su versión actualizada, el Convenio 108+, representa una oportunidad para fortalecer el marco jurídico local con estándares internacionales de protección de datos. Además, normativas complementarias, como la Resolución 255/2022 de la Agencia de Acceso a la Información Pública (AAIP), han avanzado en la definición de datos genéticos como datos sensibles, aunque aún falta incorporar disposiciones más específicas sobre otros datos como los genómicos.

Otras leyes relacionadas, como la Ley de Protección Integral de las Mujeres y la Ley de Derechos del Paciente, así como la legislación de historia clínica electrónica en la Ciudad Autónoma de Buenos Aires, aportan elementos valiosos al marco normativo, pero requieren una integración más efectiva con la normativa de protección de datos personales. En este sentido, también se destacan la Ley N° 27.610 y la Ley N° 26.150 de Educación Sexual Integral, ambas fundamentales para garantizar derechos en materia de salud sexual, reproductiva y no reproductiva. La actualización del marco regulatorio de protección de datos debe incorporar evaluaciones de impacto y gestión de riesgos, promover la responsabilidad proactiva de quienes manejan estos datos y garantizar mecanismos efectivos de control. Finalmente, se destacó que la generación de espacios de diálogo, como el presente encuentro, resulta clave para impulsar la incidencia en políticas públicas y lograr reformas legislativas que protejan los derechos de las personas usuarias de los servicios de salud sexual y reproductiva.

Respecto al consentimiento expreso e informado, durante el diálogo se manifestó cierta preocupación respecto a alfabetización en la población y la comprensión de los términos y condiciones para su implementación efectiva. Asimismo, se evidenció que existen marcadas desigualdades a lo largo del país, donde muchas instituciones y profesionales del sistema de salud aún operan con registros en formato papel o con sistemas tecnológicos básicos y poco integrados. No se trata únicamente de una falta de normativas adecuadas, sino de la necesidad de mejorar su aplicación e interpretación armónica. En este sentido, resulta fundamental desarrollar estrategias de sensibilización y capacitación tanto para la ciudadanía como para quienes trabajan en el ámbito de la salud, asegurando que los derechos vinculados a la privacidad y la protección de datos sean comprendidos y respetados de manera efectiva.

Ciberseguridad y Seguridad de la Información

La ciberseguridad juega un papel fundamental en la protección y seguridad de los datos de salud. A nivel gubernamental y organizacional, las políticas de ciberseguridad están estrechamente vinculadas a la protección de los datos personales. Sin embargo, en Argentina, la ciberseguridad nunca ha sido realmente una prioridad en la agenda pública, incluso frente al aumento de ataques de ransomware.

Actualmente, el país carece de una ley marco en la materia, pero cuenta con una Dirección Nacional de Ciberseguridad con facultades y recursos limitados. Además, existe una Agencia Federal de Ciberseguridad bajo la órbita de la SIDE (Servicio de Inteligencia), cuya función no está claramente definida. También se ha creado, mediante resolución, un programa de ciberseguridad y cibercriminalidad en el ámbito de seguridad, pero sigue sin resultar preciso en la práctica cuál es el órgano rector en la materia.

La Dirección Nacional de Ciberseguridad ha identificado al sector de la salud entre las infraestructuras críticas. No obstante, esto no implica que todos los establecimientos de salud sean reconocidos como infraestructuras críticas ni que existan estrategias definidas al respecto. Para abordar esta problemática, durante el encuentro surge que será clave la colaboración de organismos rector en la materia

con los entes reguladores, como la Superintendencia de Servicios de Salud, para desarrollar políticas de protección de las infraestructuras críticas y seguridad de la información alineadas con estándares vigentes y ofrecer modelos de implementación.

A nivel nacional, existen antecedentes de ataques de ransomware a instituciones de salud que han comprometido bases de datos, alterando información personal y poniendo en riesgo la seguridad de los y las pacientes. Además, la cooperación entre organismos públicos y privados es deficiente, especialmente en lo que respecta a los reportes de incidentes. La seguridad de la información es esencial para prevenir accesos no autorizados, fugas de datos y ataques cibernéticos, que no solo afectan la privacidad de los y las pacientes, sino también la integridad de los sistemas de salud. Al respecto, quedó evidenciada la necesidad de un enfoque integral en ciberseguridad, que contemple tanto la protección de los sistemas de almacenamiento y gestión de datos como la capacitación continua de los y las profesionales en el uso seguro de la información.

Ciberseguridad y Protección de Datos en Salud Sexual y Reproductiva

A lo largo del intercambio se señaló que la ciberseguridad en el ámbito de la salud no puede limitarse a la protección de sistemas e infraestructuras; debe centrarse en la protección de los datos personales y, en consecuencia, en la seguridad y los derechos de las personas. Esto implica un enfoque basado en la gestión de riesgos, que permita identificar vulnerabilidades, mitigar amenazas y garantizar que la información sensible no sea utilizada en perjuicio de quienes acceden a servicios de salud sexual y reproductiva.

La ciberseguridad, en esencia, consiste en gestionar riesgos. En el cruce entre salud, protección de datos personales y ciberseguridad se presentan múltiples riesgos, que van desde filtraciones de información y accesos no autorizados hasta la discriminación, la violencia por razones de género y la persecución legal. El mayor peligro no es solo que una organización sufra un incidente de seguridad, sino que los datos expuestos puedan ser utilizados en contra de las personas, afectando su privacidad, dignidad y derechos.

Para gestionar estos riesgos de manera efectiva, es necesario que las organizaciones de salud realicen un inventario detallado de los datos que manejan, identifiquen qué tipo de información poseen, cómo la almacenan y qué medidas aplican para su resguardo. La gobernanza de datos es un componente clave de la ciberseguridad, ya que, sin un conocimiento preciso de la información existente, su ubicación y su nivel de sensibilidad, es imposible diseñar estrategias de protección adecuadas.

En Argentina, la ciberseguridad no ha sido una prioridad en la agenda pública y la regulación actual no articula de manera efectiva la seguridad de la información con la protección de los datos personales. Esto deja expuestos los registros de salud sexual y reproductiva a vulnerabilidades críticas, especialmente en un contexto donde muchas instituciones de salud operan con sistemas fragmentados, obsoletos o insuficientemente protegidos. Los recientes ataques de ransomware a hospitales y centros médicos en el país han demostrado la debilidad de la infraestructura digital del sector, afectando tanto la privacidad de pacientes como la continuidad de la atención médica.

A pesar de estos desafíos, existen buenas prácticas que han surgido de procesos de autorregulación en distintos sectores. Algunas instituciones han implementado medidas avanzadas de seguridad, como cifrado de datos por defecto, anonimización de información sensible y mecanismos de acceso restringido basados en principios de necesidad y proporcionalidad. Del mismo modo, han comenzado a incorporar estándares de privacidad más robustos, ofreciendo opciones de gestión de consentimiento más claras y transparentes para las personas usuarias.

Para abordar esta problemática de manera estructural, resulta fundamental que la ciberseguridad en el sector salud se enfoque en la protección efectiva de los datos personales, garantizando el cumplimiento de principios clave como la minimización de datos, el consentimiento informado, la privacidad por defecto y la seguridad de la información. Esto implica la implementación de auditorías permanentes y protocolos claros para la gestión de incidentes. A su vez, la cooperación entre el sector público y privado debe ser fortalecida para establecer estándares homogéneos y estrategias de respuesta eficaces ante amenazas cibernéticas.

Desde una perspectiva de derechos, la ciberseguridad en salud sexual y reproductiva no puede analizarse sin considerar los riesgos diferenciados que enfrentan mujeres y diversidades. La ausencia de un enfoque de género en las políticas de seguridad digital ha dejado expuestas a muchas personas a vulneraciones graves, en particular cuando su información de salud puede ser utilizada como herramienta de control, discriminación o violencia.

La filtración de esta información puede exponer a las personas a persecución legal, violencia de género y vulneraciones de derechos fundamentales. Para mitigar estos riesgos, es fundamental no solo que haya estrategias de ciberseguridad, sino que éstas incorporen una perspectiva de género que reconozca los impactos diferenciados de la exposición de datos personales. Esto implica diseñar directrices específicas y garantizar la implementación de medidas de seguridad avanzadas en la gestión de la información.

Además, surge como una posibilidad para ello, repensar el concepto de infraestructura crítica incorporando servicios esenciales para la vida y el bienestar de mujeres y diversidades.

El diálogo evidenció la urgencia de abordar la ciberseguridad desde un enfoque integral, donde la protección de la información no sea vista únicamente como una cuestión técnica, sino como un componente central de la garantía de derechos. A medida que los sistemas de salud se digitalizan y el uso de tecnologías en la atención médica se expande, es crucial que las estrategias de seguridad prioricen la protección de las personas, asegurando que la información sensible vinculada a la salud sexual y reproductiva no sea utilizada en su contra.

Consideraciones finales

El diálogo evidenció que la implementación del marco normativo argentino para la protección de datos en el sector salud enfrenta desafíos. La digitalización y la falta de medidas de seguridad exponen a las personas usuarias de servicios de salud sexual y reproductiva a riesgos diferenciados, demandando una revisión y armonización normativa que incorpore las mejores prácticas surgidas de la

autorregulación y fortalezca los controles. La ciberseguridad, con regulaciones fragmentadas y escasa prioridad en la agenda pública, sigue siendo una deuda pendiente. La falta de coordinación interinstitucional genera riesgos para la protección de los datos sensibles, lo que puede resultar en violaciones de privacidad y discriminación.

En este contexto, y como resultado de las reflexiones surgidas del diálogo, es esencial priorizar la protección de las personas. Esto implica adoptar un enfoque de derechos con perspectiva de género, fortalecer la cooperación público-privada e impulsar la mejora de prácticas y regulaciones alineadas con estándares internacionales. La seguridad de la información en salud sexual y reproductiva debe ser un componente central en la garantía de derechos. Este resumen busca reflejar preocupaciones y reflexiones frente al estado de situación actual y fomentar la continuidad del diálogo para la construcción de estrategias conjuntas y por qué no la exploración de posibles alianzas.

***