Estrategias y procedimientos de protección de datos personales en productos que contienen información sanitaria

Palermo, María Cecilia[1]; Bardauil, Ariana[2]; Nanton, María Cristina[3]; López, Sabrina Laura[4]; Islas, María Belén [5]

[1] Ministerio de Salud, GCABA. https://orcid.org/0000-0002-8132-0705.
[2] Ministerio de Salud, GCABA. https://orcid.org/0009-0000-5020-7331.
[3] Ministerio de Salud, GCABA. https://orcid.org/0000-0003-0426-2879.
[4] Instituto de Cálculo, UBA, CONICET. https://orcid.org/0000-0003-1572-1815.
[5] Ministerio de Salud, GCABA. https://orcid.org/0009-0008-5200-339X.

Abstract. Desde 2016, en la Ciudad Autónoma de Buenos Aires (CABA) se lleva adelante la implementación de Sistemas de Información de Salud (SIS) en el subsistema público, lo cual resulta en la producción de un gran volumen de datos. Estos datos son fundamentales para la gestión del sistema sanitario, la investigación y la difusión de información pública. Entre las funciones de la Gerencia Operativa de Gestión de Información y Estadísticas en Salud (GOGIES) se encuentra el tratamiento de los datos provenientes de los SIS y la respuesta a solicitudes de información emitidas por diversos actores. Este artículo presenta diferentes estrategias desarrolladas durante 2023 para garantizar la protección de datos personales y/o sensibles en los productos de información en salud. Durante dicho año, se recibieron mediante la Mesa de Ayuda -plataforma utilizada por el Ministerio para servicios de gestión de información y solución de incidencias- 586 solicitudes de información sanitaria. Aquí se expondrá el desarrollo de una herramienta de clasificación y evaluación que comprende los tipos de información requerida, los perfiles de solicitantes y objetivos de uso; y la aplicación de procedimientos para tratar aquellas solicitudes que requieren información sensible y/o nominalizada.

Palabras clave: datos personales, datos sanitarios, datos sensibles, salud pública, ética y uso responsable, anonimización.

1 Introducción

En la Ciudad Autónoma de Buenos Aires (CABA) se lleva adelante desde 2016 la implementación de un Sistema de Información de Salud (SIS) en el ámbito del subsistema público. La red de efectores públicos cuenta con 34 hospitales, 47 Centros de Salud y Acción Comunitaria (CeSAC), 2 Centros de Especialidades Médicas de Referencia (CEMAR), 2 Centros de Cuidado Integral (CCI) y 17 Centros Médicos Barriales (CMB). Progresivamente, en ellos se incorporó el uso del Sistema de Gestión Hospitalario (SIGEHOS), el cual se compone de módulos que abarcan múltiples aspectos de la

gestión y atención sanitaria tales como: la Historia de Salud Integral (HIS) para el registro de las consultas; el Gestor de Encuentros (GDE) o Gestor Episódico (GE) para la gestión de turnos, el apartado del Padrón para el empadronamiento de la población y la asignación de un número de HIS, Laboratorio, Prescripciones, entre otras aplicaciones. La información que resulta de su uso consiste en un insumo fundamental para el seguimento, control, gestión y toma de decisiones sobre salud pública.

La implementación de (SIS) –en el caso aquí abordado, SIGEHOS– da lugar a múltiples desafíos éticos y legales para el acceso a la información que en ellos se registra. Esto alcanza a los diferentes usos posibles –que van desde tareas de gestión, seguimiento clínico, insumo para investigaciones científicas, y demás–, a su manipulación y a los modos en que ésta circula. En este marco, resulta necesario debatir las pautas de acceso, actores habilitados, tipos de datos disponibles y procesos adecuados que garanticen la seguridad y confidencialidad de la información. La Gerencia Operativa de Gestión de Información y Estadísticas en Salud (GOGIES) es el área gubernamental responsable del tratamiento de los datos provenientes de los SIS y de dar respuesta a solicitudes de información realizadas por diversos actores, tales como el personal asistencial de los efectores, profesionales del nivel central de gestión, la ciudadanía y personas investigadoras internas o externas al sistema sanitario.

El aumento en la demanda y disponibilidad de datos sobre salud poblacional impone la necesidad de estandarizar circuitos asociados a su solicitud, recepción, evaluación, procesamiento y disponibilización. Dado que los datos de salud de las personas son considerados datos sensibles, resulta indispensable el desarrollo de estrategias que garanticen la confidencialidad y seguridad. En este sentido, el objetivo de este artículo es presentar las estrategias desarrolladas por GOGIES durante 2023 para garantizar la protección de datos personales y/o sensibles en la circulación de productos basados en información del ámbito de la salud y evaluar su eficacia. Se hará foco en dos dispositivos de diagnóstico y procedurales. En primer lugar, un registro de solicitudes según los perfiles de solicitantes de información sanitaria, los tipos de información solicitada y sus objetivos de uso, elaborado en base a una sistematización y análisis de los pedidos realizados a la gerencia. Esta herramienta permitió delimitar procedimientos adecuados al uso ético y responsable de la información y un adecuado seguimiento de las solicitudes. En segundo lugar, se elaboró un instrumento denominado Evaluación de Riesgo Inicial (ERI) con el propósito de caracterizar y evaluar las solicitudes de información sanitaria e identificar aquellas que requieren modificaciones en el tipo de información -o en su nivel de agregación-, la utilización de documentación adicional -como la firma de un convenio de confidencialidad-, o la aplicación de técnicas de anonimización o de-identificación que faciliten el cumplimiento de los objetivos de los pedidos de información garantizando la protección de los datos personales.

2 Ética y tratamiento responsable de los datos personales sanitarios

En la era digital, la protección de datos personales en el ámbito público es una cuestión de suma relevancia, ya que los organismos son las entidades responsables de manipular y salvaguardar una cantidad significativa de información sensible de los/as ciudadanos/as. A nivel internacional, existen documentos que refieren a la ética en el uso de

datos sanitarios. La Declaración de Helsinki (De Helsinki & World Medical Association, 1975) y la Guía Internacional de Ética para Investigaciones Biomédicas que involucren Seres Humanos (OPS y Consejo de Organizaciones Internacionales de las Ciencias Médicas, 2016) contienen principios éticos para la investigación médica en seres humanos y coinciden al destacar la necesidad de incluir estrategias para salvaguardar la confidencialidad de la información. Varios organismos internacionales han emitido recomendaciones sobre la seguridad de la información en los que la confidencialidad consiste en una dimensión central. La OMS (2021) sugiere que los datos sanitarios deben clasificarse como datos personales sensibles o como información de identificación personal y ello requiere de un marco sólido jurídico y códigos éticos que protejan, entre otras cuestiones, la privacidad y la confidencialidad de los datos sanitarios personales. Por su parte, la Organización Internacional para la Estandarización sugiere aspectos técnicos relativos a estrategias de confidencialidad. Particularmente, la norma 27001 incluye aspectos del rango informático y pautas para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) que permitiría identificar las amenazas y vulnerabilidades -entre las cuales se encuentran la pérdida de confidencialidad- y establecer una evaluación de riesgos. Por último, la norma 27799, que refiere a la informática sanitaria, destaca la necesidad de proteger la información y mantener la privacidad de los sujetos. Como aspecto transversal, los organismos internacionales referidos mencionan a la confidencialidad como una dimensión relevante asociada a la seguridad de la información. Entre las recomendaciones efectuadas, se encuentra la generación de un marco normativo local sólido, que aluda a un uso ético y seguro de los datos.

En cuanto a Argentina, cuenta con un vasto marco legal que refiere a datos –tipificación, limitantes y habilitantes para el acceso–, condicionamientos para su uso y obligaciones en torno a la seguridad de los mismos. La protección de los datos personales está garantizada en la Constitución Nacional (artículo 43), en donde se regula el recurso especial de "Habeas Data" a fin de proteger los derechos constitucionales y se establece la protección de los datos personales a la categoría de derecho fundamental. A nivel nacional, la ley 25.326 define los tipos de datos, los derechos de las personas en relación a su información, las obligaciones y responsabilidades de quienes acceden y tratan los datos y los principios para el tratamiento de datos personales en Argentina. El artículo 2 contiene definiciones fundamentales que permiten categorizar tipos de datos, funciones y acciones, sistematizadas en la Tabla 1:

Tabla 1. Definiciones provistas por la ley 25.326.

Datos personales	Refieren a información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
Datos sensibles	Constituyen datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
Datos informatizados	Son aquellos datos personales sometidos al tratamiento o procesamiento electrónico o automatizado-
Titular de los datos	Es la persona física cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

Usuario de datos	Es toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.
Archivo, registro, base o banco de datos	Es el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. El responsable es la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.
Tratamiento de datos	Son las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

El artículo 7 establece que ninguna persona puede ser obligada a proporcionar datos sensibles, y que estos pueden ser recolectados y objeto de tratamiento cuando haya razones de interés general autorizadas por ley, por finalidades estadísticas o científicas siempre y cuando no puedan ser identificados sus titulares. En el caso específico de los datos de salud, se instituye el principio de secreto profesional en establecimientos sanitarios, el cual debe ser respetado por los profesionales vinculados a las ciencias de la salud que recolectan o utilizan datos personales relativos a la salud de individuos que estén o hubieren estado bajo tratamiento de aquéllos (artículo 8). Los artículos 9 y 10 brindan lineamientos para el tratamiento de la información: quien sea responsable o utilice el archivo de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales; quienes intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Por último, en relación a la cesión de los datos, el artículo 11 establece que los datos personales objeto de tratamiento pueden ser cedidos para fines directamente relacionados con el interés legítimo del cedente y del cesionario, y con el previo consentimiento del titular de los datos (el cual es revocable). Entre otros casos, éste no será necesario cuando se trate de datos personales relativos a la salud y la cesión sea necesaria por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.

La ley N°26.259 aporta cuestiones específicas relativas al campo de la salud, señalando aspectos relativos a los derechos del paciente en términos de intimidad y confidencialidad. En cuanto a la intimidad en la actividad médico-asistencial, se debe observar el estricto respeto por la dignidad humana y la autonomía de la voluntad[1], así como el debido resguardo de la intimidad del mismo y la confidencialidad de sus datos sensibles. Particularmente, la confidencialidad refiere al derecho del paciente a que toda persona que participe en la elaboración o manipulación de la documentación clínica guarde la debida reserva, salvo expresa disposición o demanda de autoridad judicial

[1] Definido en esta misma ley como el derecho del paciente a aceptar o rechazar determinadas terapias o procedimientos médicos o biológicos.

competente o autorización del propio paciente (para lo cual se precisa expresamente el consentimiento informado).

En base al marco normativo expuesto, en este artículo se considera como datos personales a aquellos que permiten identificar a la persona individual, ya sea de manera directa o indirecta, mediante uno o varios elementos característicos de su identidad, ya sea físicos, biológicos, fisiológicos, económicos, culturales, genéticos. A su vez, aquellos relativos a opiniones políticas, origen étnico, convicciones religiosas, información referente a la salud, la orientación sexual, datos genéticos y biométricos son categorizados como sensibles.

3 Instrumentos

En esta sección se presentan los instrumentos elaborados en GOGIES para la gestión de los requerimientos de información sanitaria: el registro de solicitudes y la Evaluación de Riesgo Inicial (ERI).

3.1 Registro de solicitudes

La herramienta de registro de solicitudes fue elaborada en dos etapas durante el año 2022: la primera implicó la delimitación de dimensiones para categorizar perfiles de usuarios, objetivos de uso y tipos de información solicitada a GOGIES; la segunda, la realización de un mapa de correspondencias entre estas dimensiones que estableciera criterios para definir quién puede acceder a qué tipo de información y de acuerdo a qué propósitos de uso (qué perfiles de usuarios pueden acceder a qué tipo de información y con qué condicionantes relativos a los objetivos de uso declarados).

En la Tabla 2 se puede visualizar la estructura de las categorías de descripción general de una solicitud:

Tabla 2. Categorías de solicitudes de información.

General						
Id seguimiento	Solicitante	Tipo de Solicitante	Fecha de recepción	Fecha de respuesta	Tipo de información	Objetivo de uso

a. *Tipo de Solicitante*. Tras relevar a los/as usuarios/as que han solicitado información a GOGIES, se establecieron los siguientes agrupadores de acuerdo a su pertenencia:
   - Ministerio de Salud del Gobierno de la Ciudad de Buenos Aires: comprende a profesionales de efectores de salud del subsistema público y a aquellas personas que pertenecen al nivel central (oficinas de gobierno dentro del organigrama del ministerio).
   - Áreas de gobierno externas al Ministerio de Salud: abarca a las personas que trabajan en otras áreas de gobierno, sean del ámbito municipal, provincial o nacional, externas al Ministerio de Salud.

- Investigadores/as: personas que se encuentran desarrollando una investigación aprobada por un Comité de Ética en Investigación (CEI), sean éstas externas o internas al Ministerio de Salud.
- Sociedad civil: personas del ámbito de la comunidad que solicitan acceso a información pública.

b. *Objetivos de uso*. Comprende los propósitos de uso de la información declarados por la persona solicitante. Se establecieron los siguientes agrupadores:
   - Gestión: incluye el monitoreo y la evaluación de programas, la solicitud y asignación de recursos, la planificación y organización de servicios, la confección de informes periódicos.
   - Seguimiento clínico: refiere al contacto con la población, el monitoreo de la población, el seguimiento o contacto con personas particulares y las prácticas de intervención.
   - Investigación: aquellas labores que forman parte de protocolos o proyectos (sean o no patrocinados) aprobados por Comités de Ética en Investigación (CEI), de la elaboración de tesis de grado, maestría o doctorado, de trabajos finales en el marco de residencias o de ponencias para jornadas científicas o artículos para revistas académicas.
   - Judiciales: requerimientos en el marco de oficios o demandas judiciales o que responden a informes de auditoría.
   - Divulgación: esta categoría no se desagrega en componentes ya que, de acuerdo a la normativa que rige las solicitudes de información por Ley N°104, no se deben explicitar los motivos que subyacen a los pedidos realizados por dicha vía.

c. *Tipos de información*. Considerando las definiciones provistas por el marco legal, se establecieron los siguientes agrupadores:
   - Sanitaria: refiere a información que contenga datos de salud, tanto agrupados como asociados a individuos particulares (identificados o no identificados).
   - Padrón: datos de personas escindidos de condiciones sanitarias específicas.
   - Producción: se centra en el uso de los diversos aplicativos de SIGEHOS (por ejemplo, historia clínica, turnos, agendas) por parte de los/as profesionales y administrativos/as que trabajan en los efectores de salud.

     Cabe destacar que, al interior de cada agrupador, se distingue entre la información nominalizada -que contiene identificadores directos o indirectos- y no nominalizada.

A partir de esta tipificación, se diseñaron procedimientos que regulan el acceso a datos sanitarios agrupados y/o a datos sanitarios nominalizados por parte de los diferentes perfiles solicitantes, de acuerdo a sus diferentes pertenencias institucionales (o comunitarias) y a los objetivos de uso explicitados.

3.2 Evaluación de Riesgo Inicial (ERI)

La Evaluación de Riesgo Inicial (ERI) se desarrolló teniendo en cuenta literatura especializada en la materia sobre usos éticos de los datos sanitarios y evaluación de riesgos

de identificación de personas (El Emam & Arbuckle, 2013; Agencia Española de Protección de Datos, 2016; Agencia de Acceso a la Información Pública y Unidad Reguladora y de Control de Datos Personales, 2020). La metodología de creación de la herramienta, desarrollada en trabajos anteriores (López, Palermo y Nanton, 2023), consistió en un relevamiento normativo y bibliográfico, un posterior análisis y caracterización de las solicitudes y pedidos de información, la identificación de los factores riesgo y la aplicación piloto de la herramienta a solicitudes reales. Una vez aprobada por evaluadores, la misma fue incorporada en la labor diaria de gestión y seguimiento de pedidos de información sanitaria de GOGIES. Actualmente, se completa de manera periódica como parte de la labor diaria de los/as analistas de datos.

Este instrumento busca clasificar y distinguir los pedidos a partir del impacto que pueden tener los datos solicitados sobre la vida de las personas, en caso de filtraciones o de reidentificación. [2] La distinción propuesta se fundamenta en:

a. *Cumplimiento normativo* que busca minimizar los riesgos y ajustarse a la normativa vigente en la materia.
b. *Eficiencia en la resolución de pedidos*: dado que gran parte de las solicitudes no requieren del uso de técnicas específicas de anonimización sino la modificación en la formulación de las variables, se puede satisfacer la demanda de información resguardando los datos y sin necesidad de realizar procesamientos más complejos.

El proceso de trabajo implica una serie de evaluaciones secuenciales llevadas a cabo por los/as analistas, teniendo en cuenta las variables y el volumen de información requerida para abordar una solicitud específica. Estas evaluaciones configuran un árbol de decisiones en el que el resultado final determina los pasos a seguir o las herramientas de anonimización adecuadas para tratar la solicitud.

Considerando el grado de sensibilidad de los datos tratados en GOGIES, la ERI permite analizar si atender la solicitud de información involucra la divulgación de texto libre, no estructurado, ingresado por profesionales en la HIS. Esto abarca, entre otros, los registros de evolución de las consultas médicas, los campos abiertos en las fichas de salud y cualquier área donde los profesionales puedan dejar notas redactadas.

En términos de impacto, se considera el riesgo de *filtración* de la información solicitada o la posibilidad de identificación de los pacientes cuyos datos están presentes, ya sea de forma directa o indirecta, en el reporte que se está elaborando. Para clarificar esta categorización, se estableció la siguiente clasificación:

- ➔ Impacto medio: información compuesta por indicadores demográficos agrupados.
- ➔ Impacto alto: información compuesta por indicadores demográficos agrupados que pueden incluir indicadores agrupados referidos a nacionalidad o domicilio en barrios vulnerables, datos que incluyen domicilio, e indicadores agrupados de un efector o grupo de efectores referidos a datos sanitarios (como cantidad de consultas, cantidad de motivos de consulta, cantidad de dispensas de una medicación, etc.).

[2] Agencia Española de Protección de Datos, 2016; Agencia de Acceso a la Información Pública y Unidad Reguladora y de Control de Datos Personales, 2020.

- ➔ Impacto crítico: información en formato de texto libre o datos sanitarios referidos a temáticas sanitarias especialmente sensibles (salud mental, interrupción voluntaria del embarazo, uso problemático de sustancias, HIV, etc.).

Por último, se verifica si la información a ser divulgada contiene identificadores directos, es decir, datos que por sí solos permiten identificar a una persona. También se evalúa la presencia de identificadores indirectos, datos que podrían, potencialmente, llevar a la identificación de una persona al combinarse con otros.

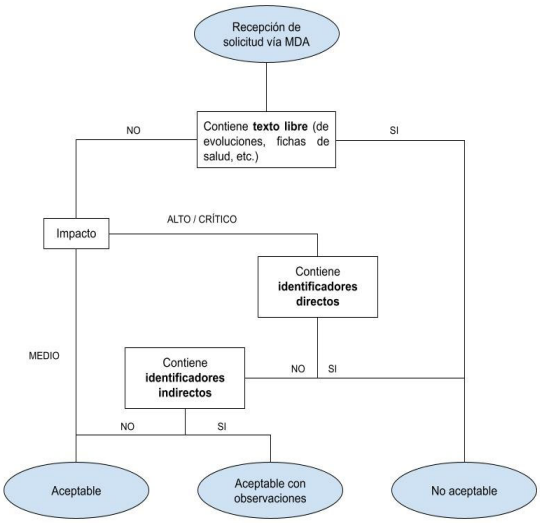

Diagrama 1. Evaluación de Riesgo Inicial (ERI)

Como se indica en el Diagrama 1, la evaluación de estos cuatro nodos puede resultar en tres posibles conclusiones para la ERI:

a. Aceptable: se procede a elaborar y proporcionar la información requerida según las especificaciones del solicitante.
b. Aceptable con observaciones: se procede a solicitar modificaciones en la solicitud, ya sea en el tipo de información solicitada o en su grado de agrupación.
c. No aceptable: no resulta ético y/o seguro brindar la información requerida según las especificaciones del solicitante.

Este instrumento permite evaluar el riesgo de re-identificación de una solicitud de información y generar un tratamiento de información que permita cumplir con los objetivos de la solicitud minimizando los riesgos. En este marco, forma parte de un circuito complejo (Figura 1) en el que la suceden distintos instrumentos técnicos y evaluaciones sucesivas que permiten asegurar la seguridad y confidencialidad en el manejo de la información.

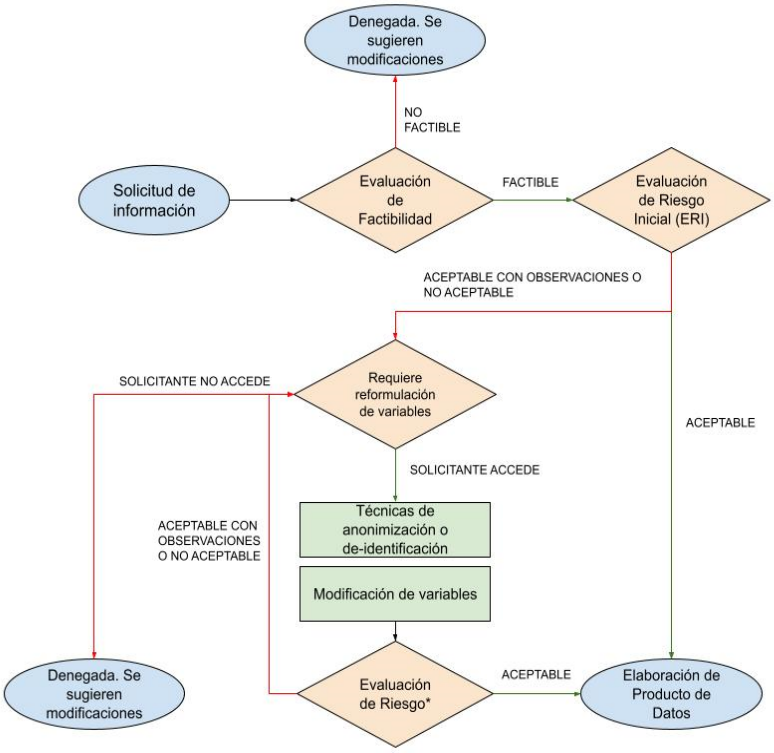

Diagrama 2. Proceso de Evaluación de Solicitudes.

*La segunda Evaluación de Riesgo es una instancia iterativa que se repite tantas veces como sea necesario para reducir el riesgo, hasta un umbral tolerable con la menor pérdida de información posible en cada una de las iteraciones.

4 Metodología

El análisis de la aplicación de los instrumentos durante 2023 se realizó mediante un enfoque sistemático de tres fases con el propósito de evaluar su efectividad en la clasificación y distinción de los pedidos de información, de acuerdo con el riesgo asociado al manejo de datos sanitarios.

El envío, recepción y distribución de pedidos de información se centraliza en la Mesa de Ayuda (MDA), una plataforma utilizada en el Ministerio de Salud para servicios de gestión de información y solución de incidencias.[3] En primer lugar, se llevó a cabo un relevamiento exhaustivo de los 490 pedidos de información recibidos a través de dicho aplicativo e incorporados al registro durante el año 2023. En cada solicitud, se identificó

[3] El siguiente link (https://buenosaires.gob.ar/salud/direccion-operativa-de-operaciones-y-mesa-de-ayuda) contiene mayores precisiones sobre el aplicativo, al cual se puede acceder desde la red privada de gobierno.

la pertenencia institucional u organizacional de la persona solicitante, el objetivo de uso explicitado en el pedido y la firma de documentación adicional -convenio de confidencialidad-. Este proceso permitió recopilar datos detallados sobre: las características de las solicitudes, el ámbito institucional de origen, el propósito de la solicitud y el tipo de usuario solicitante.

En segundo lugar, a partir de los resultados de la ERI para dichas solicitudes, se identificaron aquellas que requerían información con identificadores directos o indirectos, así como el tipo de datos sensibles involucrados. Por último, se analizaron las medidas adicionales de seguridad y confidencialidad aplicadas para garantizar la protección de los datos sensibles.

5 Resultados

Al recibir las solicitudes vía MDA, se realiza una primera evaluación relacionada con la factibilidad, en la que se corrobora que los datos solicitados se encuentren disponibles. De ser positiva, se distingue entre los pedidos que requieren procesamiento de datos y la consecuente elaboración de un producto y los que contienen consultas o solicitudes de acceso a reportes estandarizados que son compartidos con personal específico de acuerdo al cargo y función en los efectores o en el nivel central del ministerio. De los 590 pedidos recibidos, 177 consisten en consultas que no requieren de elaboración de productos de datos. Éstas fueron excluidas del análisis aquí presentado. Además, se excluyeron aquellos pedidos que fueron archivados por falta de respuesta por parte de los/as solicitantes. El total de pedidos incluidos en el análisis es de 302.

En el Gráfico 1 se observa la cantidad de pedidos de información según el objetivo de uso del reporte.

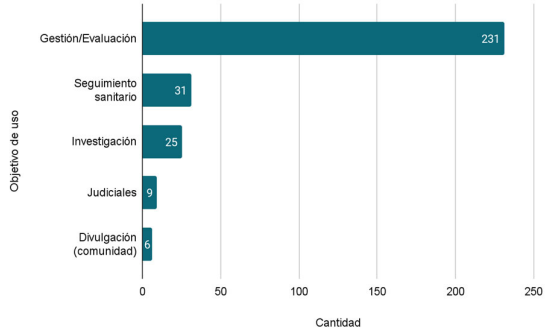

Gráfico 1. Cantidad de solicitudes por objetivo de uso en 2023. Fuente: elaboración propia.

El Gráfico 2 muestra el porcentaje de pedidos de información por tipo de solicitante. Principalmente, las salidas de reportes desde GOGIES se destinan a efectores del subsistema público y para el nivel central.

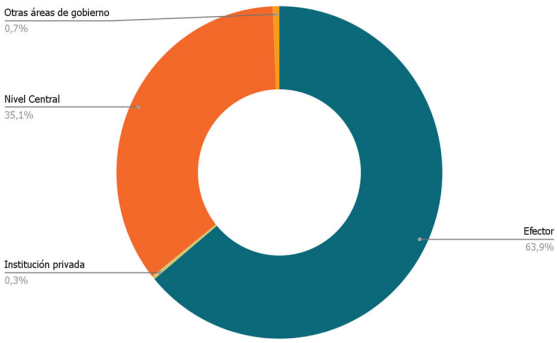

Gráfico 2. Pedidos de información por tipo de solicitante en 2023. Fuente: elaboración propia.

En relación al impacto de la generación del reporte de las solicitudes de información, en el Gráfico 3 se detalla el porcentaje de pedidos que fueron catalogados con un impacto crítico y con impacto medio.

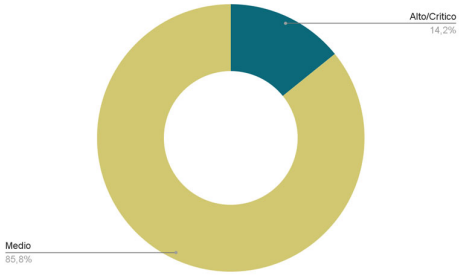

Gráfico 3. Solicitudes según impacto en 2023. Fuente: elaboración propia.

En cuanto a los tipos de identificadores que se requirieron para realizar los informes, en el Gráfico 4 se observa que la mayoría de los pedidos no requirieron identificadores tanto directos como indirectos.

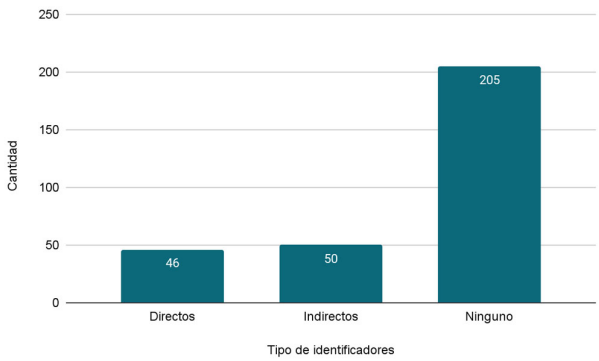

Gráfico 4. Solicitudes según tipo de indicadores en 2023. Fuente: elaboración propia.

De las 46 solicitudes que requerían identificadores directos de la población, solamente 4 involucraron la firma de un convenio de confidencialidad. El resto, como será presentado en el siguiente apartado, fueron redefinidas por parte de los/as solicitantes o se acudió a diferentes técnicas de de-identificación o anonimización (por ejemplo, reemplazo del número de DNI por un identificador de fantasía).

Por último, el Gráfico 5 muestra el resultado de la ERI. De los 46 casos en los que había identificadores directos, solo 19 no tuvieron una ERI aceptable, lo que implicó la redefinición del pedido (10 solicitudes) o el envío de un acuerdo de confidencialidad (4 solicitudes) -las 5 restantes fueron archivadas por falta de respuesta-.

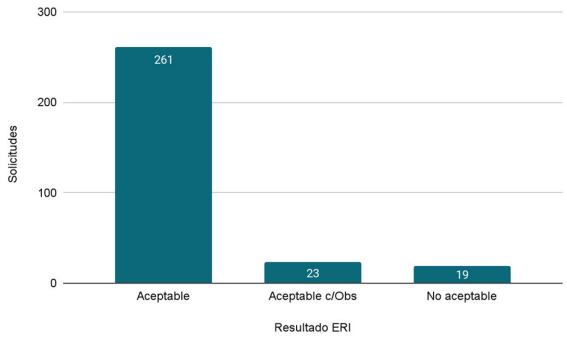

Gráfico 5. Solicitud conforme al resultado de la ERI en 2023. Fuente: elaboración propia.

6 Análisis

La mayoría de las solicitudes de información realizadas por profesionales de los efectores (63.9%) responde a necesidades de información que implican la elaboración de un producto específico, que generalmente consiste en reportes y/o tableros. Estas necesidades están vinculadas a objetivos de planificación por parte de las áreas o equipos

de trabajo, o al seguimiento sanitario. Este último objetivo es el que más se beneficia de la aplicación de la ERI dado que puede operarse sobre las solicitudes de información mediante herramientas como la remoción de variables, recodificación de la información -reemplazo de identificadores directos por identificadores de fantasía- o agrupación de indicadores de modo tal que el riesgo de reidentificación disminuya sensiblemente. Las solicitudes por parte de nivel central (35.1%), en cambio, suelen estar vinculadas casi exclusivamente a objetivos de gestión y evaluación de políticas sanitarias. Si bien estas necesidades pueden satisfacerse con reportes agrupados de baja granularidad, la ERI permite en estos casos transparentar los procedimientos internos de GOGIES que enmarcan las condiciones que permiten la resolución de las solicitudes de información, y orienta a los analistas hacia métodos de remoción y agrupación de variables en la confección de reportes.

El instrumento de registro de solicitudes y el flujo de trabajo estipulado permite, para los casos en los que no hay una ERI aceptable, la redefinición de los pedidos de información y la identificación de los casos en los que es necesaria la solicitud de un acuerdo de confidencialidad para continuar con el circuito y proteger los datos personales y sensibles de la población. De este modo, a partir de la ERI se logró que, en varias instancias, las personas solicitantes redefinieran el contenido de sus solicitudes, ya que no siempre se necesitan datos nominalizados o con identificadores directos para los propósitos enunciados.

Por último, en relación al marco legal vigente contemplado para la elaboración de los instrumentos, cabe destacar ciertas ambigüedades y vacancias en relación a la implementación de SIS y el uso ético y responsable de la información, principalmente en lo que atañe a la cesión de datos dentro del ámbito de gestión y de gobierno -que se autoriza cuando los propósitos de uso sean adecuadamente fundamentados, sin brindar lineamientos para evaluarlos-, para la aplicación del uso del convenio -no se prevee quiénes deben firmarlo, con qué periodicidad, dónde deben archivarse, quién es el ente encargado de auditar el cumplimiento de tal acuerdo de confidencialidad y el buen uso de los datos- y para el adecuado uso de técnicas de anonimización.

7 Conclusiones

El análisis de la implementación del registro de solicitudes y de la ERI consiste en un insumo fundamental para caracterizar los pedidos de información sanitaria recibidos por GOGIES y desarrollar estrategias adecuadas para el tratamiento de la información sanitaria, personal y sensible. Este trabajo permite tener un panorama general de la articulación entre diferentes perfiles de usuarios de la información de acuerdo a su pertenencia institucional, académica o comunitaria; con los diferentes tipos de información, clasificada según su contenido y grados de identificación de personas individuales; de acuerdo a diferentes objetivos de uso. Este último punto tiene especial relevancia en tanto la confidencialidad, aspecto central en recomendaciones de organismos internacionales y en el marco legal vigente, implica respetar el propósito que sustenta cada pedido de información, e inhabilita su uso secundario en proyectos o tareas no especificadas al momento de solicitar los datos.

De acuerdo a los resultados obtenidos, es posible afirmar que el registro de solicitudes y la ERI son herramientas eficientes e implementables en un entorno que lidia de forma cotidiana con solicitudes de información sanitaria y benefician el tratamiento ético y responsable de los datos. El análisis de su implementación permitió identificar usos regulares de la información y generar procesos periódicos para la disponibilización de la misma, y proponerlas como modelo para otros circuitos de solicitudes de información en el campo de la salud.

Tras identificar vacancias en los lineamientos provistos por el marco normativo en relación a los procedimientos que se encuentran en curso, queda pendiente formalizar las instancias analizadas en este trabajo en una normativa ministerial publicada y definir criterios para el circuito de archivo de la documentación secundaria, tales como los convenios de confidencialidad. En este sentido, cabe afirmar que la tensión entre la accesibilidad y la protección de los datos personales y sensibles de los pacientes no ha sido resuelta aún. La construcción de herramientas que permitan a los/as investigadores/as, tomadores de decisión y a los equipos técnicos que procesan y analizan la información, tener reglas claras de accesibilidad que resguarden los derechos de los pacientes es crítica para un desempeño eficiente y eficaz del sistema de salud de la ciudad de Buenos Aires y para su interacción que otras áreas de gobierno y del ámbito civil.

Bibliografía

1. Agencia Española de Protección de Datos: Orientaciones y garantías en los procedimientos de anonimización de datos personales (2016). https://www.aepd.es/documento/guia-basica-anonimizacion.pdf
2. Agencia de Acceso a la Información Pública de Argentina y la Unidad Reguladora y de Control de Datos Personales de Uruguay: Evaluación de Impacto en la Protección de Datos. Ciudad Autónoma de Buenos Aires (2020). https://www.argentina.gob.ar/sites/default/files/guia_final.pdf
3. Agencia Española de Protección de Datos: Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD. Agencia Española de Protección de Datos, (2021). https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf
4. Agencia Española de Protección de Datos: Diez malentendidos relacionados con la anonimización (2021). https://www.aepd.es/guias/10-malentendidos-anonimizacion.pdf
5. Consejo Federal para la Transparencia: Lineamientos para la formulación de un Plan de Protección de Datos Personales. Buenos Aires: Agencia de Acceso a la Información Pública (2023)
6. de Helsinki, D., & World Medical Association: Declaración de Helsinki. Principios éticos para las investigaciones médicas en seres humanos. Tokio-Japón: Asociación Médica Mundial (1975).
7. El Emam, K., & Arbuckle, L.: Anonymizing health data: case studies and methods to get you started. O'Reilly Media, Inc. (2013).
8. Ley 25.326 de 2000: Protección de los datos personales. 2 de noviembre de 2000. Boletín Oficial de la República Argentina No. 29517.
9. Ley 104 de 1998: De acceso a la Información Pública. 29 de diciembre de 1998. Boletín Oficial de la Ciudad de Buenos Aires No. 600.
10. López, S.; Alonso Alemany, L.; Dias, J.M.; Ación, L. y Xhardez, V.: Guía práctica para la protección de datos personales en salud. Buenos Aires: Fundar (2023).
11. López, S., Palermo, M. C. y Nanton, M. (2023). Tratamiento estandarizado de solicitudes de información de salud basado en evaluación de riesgos. En II Congreso de ética en investigación - Ética de las nuevas inteligencias. Comité Central de Ética en Investigación, Ministerio de Salud - GCBA.
12. Organización Mundial de la Salud (2021). Proyecto de estrategia mundial sobre salud digital 2020–2025. https://www.who.int/es/publications/i/item/9789240020924
13. Organización Panamericana de la Salud y Consejo de Organizaciones Internacionales de las Ciencias Médica: Pautas éticas internacionales para la investigación relacionada con la salud con seres humanos, Cuarta Edición. Ginebra: Consejo de Organizaciones Internacionales de las Ciencias Médicas (CIOMS) (2016).