Aspectos legales de la ruta crítica para una plataforma integrada de gestión de casos de violencia contra la mujer en el Estado de Chile

PATRICIA REYES

WORLD BANK GROUP

TABLA DE CONTENIDO

ANTECEDENTES Y METODOLOGÍA

Existe una visión compartida entre las distintas instituciones del Estado de Chile, que se interrelacionan para atender las situaciones de violencia contra la mujer (VCM), que señala que es necesario hacer seguimiento y monitorear la ruta crítica que recorren las mujeres, ya que sólo a partir de ello se alcanzará el logro de los siguientes objetivos:

1. Coordinar e interoperar en tiempo real un conjunto de servicios que incluyen salud, seguridad/policía, vivienda, apoyo económico/fortalecimiento de los medios de vida, apoyo psicosocial y justicia.
2. Responder de manera adecuada a las personas sobrevivientes de la violencia de género, desde la ocurrencia del fenómeno para su atención psicosociojurídica, protección y reparación.
3. Fortalecer redes primarias y secundarias, tales como: instituciones públicas y privadas, organizaciones de la sociedad civil y de base.
4. Fortalecer la coordinación estrecha y oportuna dentro y entre las instituciones.

Sin embargo, junto con esta visión compartida, existe también el diagnóstico de la falta de una plataforma integrada e interoperable de gestión de los casos referidos a VCM, en virtud de lo cual, el Banco Mundial se encuentra realizando una asistencia técnica destinada a:

1. Optimizar la coordinación interinstitucional para brindar un mejor servicio a las personas que han sufrido violencia y contribuir a la eliminación de la violencia de género
2. Formular una hoja de ruta para la creación de una Plataforma Integrada de Gestión de Casos para personas que sufren violencia de género, con las siguientes características:
    - Que sea interoperable por las instituciones involucradas
    - Que facilite el análisis y gestión interinstitucional del Estado
    - Que permite la agregación/desagregación de datos a nivel nacional, regional y local, según sexo, ubicación geográfica y pertenencia o no a pueblos originarios, como mínimo.

Dentro de esta asistencia técnica del Banco Mundial, el presente informe aborda los aspectos legales de la hoja de ruta y es complementado con los informes de Procesos[1], Tecnologías de Información[2] y Ruta Crítica[3].

Como antecedente del informe, y dentro del proceso que da origen al resultado que se presenta, se destacan los siguientes aspectos metodológicos:

1. Elaboración y revisión de cuestionario legal entregado y respondido por cada uno de las y los participantes en la ruta crítica, el que tuvo por objeto situar la consultoría.
2. Reuniones para entrevistas con cada una de las instituciones y servicios públicos que hacen parte de la ruta, para realizar un diagnóstico cuyos principales hallazgos fueron: identificación del marco normativo que rige a la institución en materia de gestión de datos de VCM; identificación de los instrumentos de intercambio de información con otras instituciones vigentes; levantamiento de las principales barreras legales internas o externas, reconocidas por las y los actores involucrados, para compartir información. Los diagnósticos pormenorizados se desarrollan en el capítulo correspondiente.
3. Reuniones de revisión de los diagnósticos con el mandante y con cada una de las instituciones para validarlo y compartir con ellos estándares nacionales e internacionales en materia de intercambio de información personal, tema que constituyó la principal barrera levantada.
4. Taller general con todas las instituciones y servicios públicos con el fin de revisar los nudos críticos definidos con las instituciones individualmente y cocrear en conjunto la propuesta.

---

[1] Matamala Soto, Constanza (2020). *Análisis del Proceso de Gestión de casos de VCM*. Documento Banco Mundial.
[2] Beltrán, José (2020). *Diagnóstico de soluciones digitales utilizadas por las Instituciones vinculadas a violencia contra la mujer en Chile*. Documento Banco Mundial.
[3] Universidad de Chile (2020). *Estudio cualitativo: Actualización de Ruta Crítica de Violencia contra la Mujer*.

MARCO CONCEPTUAL

REGISTROS ADMINISTRATIVOS Y PLATAFORMAS INTEGRADAS

La VCM constituye una violación grave a los derechos humanos de mujeres y niñas y por tanto existe consenso global en que debe ser erradicada, así se constituye en un ODS 2030 de las Naciones Unidas (UN).

Para avanzar en este objetico se requiere actuar decididamente sobre la prevención, atención y reparación en las situaciones de VCM. Lo anterior, supone necesariamente gestionar correcta y eficazmente los servicios y programas, mantener registros y mediciones del progreso y esfuerzos realizados y proteger la seguridad y protección de los datos de quienes están involucrados.

Lo anterior refuerza la recomendación de los organismos internacionales al Estado de Chile, origen de la Asistencia Técnica del Banco Mundial, en orden a disponer de un registro único de víctimas de violencia (denominada plataforma integrada de gestión de casos de VCM), destinado a dar seguimiento a quienes han sufrido esta situación, independientemente de la instancia por la que hayan solicitado intervención pública y que permitirá también generar estadísticas y aportar a la prevención (DIPRES, 2017: 101).

De acuerdo con el último informe de ONU Mujeres (UN Women, 2020:6) sobre evidencia de recolección y uso de datos administrativos sobre VCM, la necesidad de datos, que incluyan los de fuentes administrativas, ocupa actualmente un lugar destacado en la agenda mundial. Sin embargo, señala el mismo informe, a pesar de la importancia potencial de estos datos administrativos para mejorar las políticas y los programas, beneficiar a las y los supervivientes y garantizar la rendición de cuentas, en general se carece de una síntesis de buenas prácticas y orientación para su recopilación y uso por parte de diferentes sectores.

Atendido lo anterior, consideramos relevante, para efectos de este marco conceptual, determinar en primer lugar qué entendemos por datos o registros administrativos y sus requisitos, para luego referirnos a las condicionantes de una plataforma integrada de gestión de estos registros.

Según el informe de UN Women citado, los datos administrativos se definen como cualquier dato generado a través de operaciones de rutina. Por lo general, se obtienen de registros basados en los servicios o de los procesos administrativos internos de una organización. En consecuencia, en el caso de VCM se recopilan (o podrían) recopilarse como parte de la prestación de servicios y apoyo a una sobreviviente o desde la respuesta institucional a la persona, agresor presunto o condenado, por las autoridades y diferentes tipos de proveedores de servicios, como la policía, fiscales, tribunales, agencias de bienestar social, proveedores de servicios sociales, protección infantil, albergues para mujeres, líneas directas de violencia y el sector salud.

Estos registros administrativos de VCM permiten, de acuerdo con el mismo informe:

- Proporcionar información sobre el número de mujeres que utilizan los servicios de VCM;
- Estimar la necesidad de tales servicios y sus costos;
- Contribuir a comprender las respuestas del sector público a la violencia y las necesidades insatisfechas;
- Cuantificar la necesidad de formación para quienes proveen los servicios; y
- Brindar información valiosa para evaluar programas y políticas, así como para informar la necesidad de legislación y políticas nuevas o mejoradas y procedimientos para responder a la VCM. (UN Women, 2020: 9).

Establecida la relevancia de estos registros, parece obvio y necesario establecer o fortalecer los registros de datos administrativos, así por lo menos se ha establecido en varias otras jurisdicciones y se ha recomendado a los Estados. Así, por ejemplo, en marzo de 2015 la Comisión Interamericana de Derechos Humanos (CIDH) emitió el informe titulado "Acceso a la información, violencia contra las mujeres y la administración de justicia en las Américas". En dicho informe, la CIDH examina los desafíos que enfrentan las mujeres para tener un acceso adecuado y efectivo a la información controlada por el Estado en materia de la prevención y protección frente la violencia y la discriminación basadas en el género, así como del acceso a la justicia para las víctimas, sistematiza las obligaciones de los Estados en la materia y los estándares desarrollados por el Sistema Interamericano de Derechos Humanos, formulando varias recomendaciones a los Estados, entre las que se encuentran varias referidas a los registros de este tipo de hechos y que se pueden revisar en extenso en el documento. En mayo de 2020, a partir de información recopilada sobre las acciones implementadas por los Estados para avanzar en el cumplimiento de esas recomendaciones, la Relatoría Especial para la Libertad de Expresión circuló un cuestionario público de consulta a los Estados y la sociedad civil que permitió profundizar en las recomendaciones. Más adelante en este informe se revisan los estándares que deben alcanzar estos registros en el ámbito legal, teniendo en cuenta esos documentos.

Como señalan las recomendaciones allí contenidas, un elemento relevante en la materia de este informe lo constituyen las plataformas integradas de servicios de VCM. A continuación, nos referimos a este elemento desde un punto de vista conceptual.

Una de las mayores exigencias que debe enfrentar actualmente el Estado para mejorar la calidad de vida de las personas es la integración de los servicios que presta a sus ciudadanos, especialmente si consideramos el desarrollo que han tenido las tecnologías de información y comunicaciones (TIC) y la extensión de su uso en la administración y en la población. Es prácticamente incomprensible que cada entidad haya incorporado TIC a sus procesos sin tener en cuenta la necesaria integración de su información para un resultado con mayor valor público, cuestión que evidenció un estudio de la Comisión Económica para América Latina y el Caribe (CEPAL) que constata que "cada agencia gubernamental incorporó tecnologías de información y las comunicaciones considerando únicamente sus necesidades particulares dando lugar a lo que hoy se conoce como islas informáticas que se caracterizan por un manejo ineficiente y descoordinado de la información, que prácticamente imposibilita la interacción entre ellas e impide que los trámites del Estado los pueda realizar el ciudadano en un solo sitio"(CEPAL, 2007: 8).

En respuesta a esta situación nacen las iniciativas de plataformas integradas de servicios, es decir, una infraestructura tecnológica capaz de integrar procesos de negocio, para aumentar la eficiencia en su ejecución y aumentar la satisfacción con los resultados para los beneficiarios. Para la misma Comisión se trata de un "desarrollo informático que incorpora las definiciones de la arquitectura de interoperabilidad y que se construye con el objetivo de facilitar el intercambio de información" (CEPAL, 2007: 14). Idealmente se trata de una plataforma tecnológica encargada de interconectar datos e información que administran distintos órganos e instancias públicas, de modo que se posibilite el intercambio eficiente de información entre los entes interconectados con la finalidad de agilizar y facilitar la prestación de los servicios públicos a los ciudadanos. En relación con lo anterior, es de gran relevancia remarcar que la plataforma no se limita a intercambiar información - duplicando y enviando registros o mediante interconexión para consulta, sino que se transmite información para integrar procesos administrativos. Esto quiere decir que el intercambio de datos que provee la plataforma se realiza con una finalidad específica, que corresponde a un proceso de negocio vinculado directamente con la prestación de un servicio. De este modo, según Ochoa, los factores organizacionales, técnicos, semánticos y de gobernanza responden a un objetivo, dotar de la mayor eficiencia y agilidad la prestación de un servicio, lo que para el caso de la administración pública que la utiliza, se relaciona con el principio de eficiencia administrativa y la búsqueda de la mejor vía para lograr la satisfacción del interés general (2009: 136).

Otras características de las plataformas integradas es su horizontalidad y neutralidad en la ejecución de los procesos, de modo que no establecen por sí mismas jerarquías en la priorización del intercambio de información. Lo anterior, no significa que no sea recomendable dotarla de una institucionalidad mínima de manera que cuente con responsables, con competencia y funciones definidas dentro de la estructura del Estado para liderar la coordinación interinstitucional, reclutar personal y recursos para garantizar su independencia funcional, todo esto con el objetivo de avanzar en aras de alcanzar cada vez mayores niveles de integración y en consecuencia eficiencia organizacional.

MARCO LEGAL NACIONAL PARA EL INTERCAMBIO DE INFORMACIÓN

En lo referido al marco normativo de sistemas de información de VCM solo existen unas cuantas disposiciones en el ordenamiento jurídico nacional, de aplicación restringida a determinados procesos y servicios de la administración pública chilena.

En las convenciones internacionales, ratificadas por Chile y por tanto parte de nuestro ordenamiento[4], solo aparecen como recomendaciones a los Estados firmantes el adoptar medidas progresivas tendientes a garantizar la recopilación de estadísticas y demás información pertinente sobre las causas, consecuencias y frecuencia de la violencia contra la mujer, con el fin de evaluar la eficacia de las medidas para prevenir, sancionar y eliminar la violencia contra la mujer y de formular y aplicar los cambios que sean necesarios (Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia Contra la Mujer, "Convención de Belem do Pará", artículo 8).

En materia de normas de rango legal, la Ley 20.066 de Violencia Intrafamiliar (VIF), en su artículo 3 autoriza a *"Crear y mantener sistemas de información y registros estadísticos en relación con la violencia intrafamiliar"* y en el 12 establece el *"Registro de sanciones y medidas accesorias. El Servicio de Registro Civil e Identificación deberá llevar un Registro Especial de las personas que hayan sido condenadas, por sentencia ejecutoriada, como autoras de violencia intrafamiliar, así como de las demás resoluciones que la ley ordene inscribir".* Por su parte la Ley 19.968 que Crea los Tribunales de Familia, contiene normas sobre los registros y datos de los procesos que se llevan a cabo en dichos tribunales, algunos de los cuales se refieren a VIF.

Muy interesante al objeto de este informe resulta ser la norma publicada el 5 de enero de 2021, pero aún no vigente hasta que se dicten normas de aplicación, la Ley N° 21.302 que crea el Servicio Nacional de Protección Especializada a la Niñez y Adolescencia, que dispone la creación de un sistema integrado de información, seguimiento y monitoreo, en su artículo 31, y los deberes de reserva y confidencialidad en los artículos 32 a 34, que bien podría servir de modelo a una norma de la misma naturaleza para la protección de mujeres (no solo niñas y adolescentes como es el caso) en situación de violencia. Las nuevas normas disponen:

"Artículo 31.- Sistema integrado de información, seguimiento y monitoreo. El Servicio creará y administrará un sistema integrado de información, que tendrá como objetivo el seguimiento de los niños, niñas y adolescentes sujetos de atención del Servicio y de sus familias, y el monitoreo de las prestaciones que reciben. Dicho sistema deberá ser seguro, interoperable, de fácil acceso y encontrarse actualizado.

La finalidad del sistema integrado de información será proveer los datos necesarios para el seguimiento de los niños, niñas y adolescentes sujetos de atención del Servicio, y el monitoreo de las medidas que se apliquen, para tomar las más adecuadas respecto a la situación particular de cada uno

[4] El presente informe no recoge el marco internacional en materia de violencia contra la mujer, para esa información remitirse al Informe de Actualización de la Ruta Crítica desarrollado por la Universidad de Chile.

de ellos. Asimismo, se podrá utilizar por los órganos del Estado con competencias en materias de infancia o presupuestarias que hayan celebrado un convenio de transferencia de datos con el Servicio, para la asignación y racionalización de las prestaciones financiadas por el Estado, el estudio y diseño de políticas, planes, programas y prestaciones, y el análisis estadístico que la gestión del Servicio requiera.

El sistema de información deberá posibilitar la construcción del historial del niño, niña y adolescente, y registrará, a lo menos, la siguiente información asociada a fechas:

a) Individualización de niños, niñas y adolescentes ingresados como beneficiarios de programas de protección especializada.

b) Antecedentes pertinentes sobre las familias y/o cuidadores de los niños, niñas y adolescentes a quienes se refiere la letra a).

c) Programas de protección especializada a los que han accedido los niños, niñas y adolescentes, y sus familias, en los casos que corresponda.

d) Individualización de las medidas que ordenan su ingreso, su ejecución, sus modificaciones si las hubiere, y el término de las mismas, incluyendo antecedentes respecto a medidas de protección anteriores, en caso de que las hubiere.

e) Los antecedentes de salud pertinentes a la intervención y situación de salud actual de los niños, niñas y adolescentes beneficiarios, con especial énfasis en el cumplimiento de los controles de salud primaria y atenciones de salud mental, según corresponda, y en el hecho de estar en lista de espera para la atención de salud o tener tratamientos médicos inconclusos.

f) La situación escolar de los niños, niñas y adolescentes beneficiarios, considerando al menos matrícula, asistencia y, en caso que corresponda, situación de repitencia y deserción escolar.

g) Situación de discapacidad y su inscripción en el Registro Nacional de Discapacidad, según corresponda.

h) Inscripción en el Registro Social de Hogares y la recepción de beneficios del sistema de protección social, según corresponda.

i) Situación de pertenencia a un grupo de especial atención, como por ejemplo los migrantes, refugiados y pueblos indígenas, según corresponda.

Los colaboradores acreditados estarán obligados a proporcionar la información necesaria que el Servicio les solicite para el sistema a que se refiere este artículo y para el cumplimiento de sus funciones.

Asimismo, los órganos del Estado, en el marco de sus competencias, estarán obligados a proporcionar la información necesaria que el Servicio les solicite para el sistema a que se refiere este artículo y para el cumplimiento de lo establecido en el inciso tercero del artículo 16.

La información contenida y administrada por este sistema estará disponible únicamente para los órganos del Estado que tengan funciones o competencias en protección de la niñez y la adolescencia, que hayan firmado un convenio de transferencia de datos con el Servicio, y para los colaboradores acreditados, para fines de administración y registro de las intervenciones realizadas, y para efectos de lo dispuesto en el inciso segundo del presente artículo, siempre resguardando la confidencialidad de los datos que aquí se registren, de conformidad a lo dispuesto en la ley N° 19.628, sobre Protección de la Vida Privada. En los convenios que suscriban los órganos públicos se deberán especificar sus fundamentos legales, los fines concretos con los cuales se acuerda dicha transferencia y la precisión del tipo de datos a transferir.

El sistema integrado de información del Servicio formará parte del Sistema de Información de Protección Integral, que será administrado por la Subsecretaría de Evaluación Social del Ministerio de Desarrollo Social y Familia, del que deberá recibir información cuando ello sea necesario, así como proveerla, en los casos que la ley expresamente lo autorice.

El sistema integrado deberá ser interoperable, al menos, con el Registro de Información Social del Ministerio de Desarrollo Social y Familia, con el sistema que lleven los tribunales de familia, con el sistema de información del Servicio de Registro Civil e Identificación y con el sistema de información que lleve el Servicio Nacional de Reinserción Social Juvenil, cualquiera sea su denominación legal.

Un reglamento expedido por el Ministerio de Desarrollo Social y Familia regulará la estructura y contenido del sistema, y las normas respecto a los requerimientos de información, y toda otra

disposición que resulte necesaria para su adecuada administración y funcionamiento, incluyendo normas sobre seguridad de la información y actualización de la misma.

Artículo 32.- Causal de reserva legal. Los datos personales de los niños, niñas o adolescentes insertos en los distintos programas del Servicio, sean ejecutados directamente o a través de colaboradores acreditados, revisten para todos los efectos legales el carácter de sensible y, salvo las disposiciones legales que autorizan su tratamiento, no podrán ser comunicados a terceras personas.

Artículo 33.- Deber de reserva y confidencialidad. Los funcionarios de los órganos del Estado que tengan acceso al sistema de información a que se refiere el artículo 31, los funcionarios del Servicio, los miembros del Consejo de Expertos a que se refiere el artículo 9, el personal de los colaboradores acreditados, y toda persona que desempeñe cargos o funciones en tales instituciones, cualquiera sea la naturaleza del vínculo, sea o no remunerado, que traten datos personales de niños, niñas o adolescentes o de sus familias, deben guardar secreto o confidencialidad a su respecto y abstenerse de utilizar dicha información con una finalidad distinta de las funciones legales que les corresponda desempeñar o utilizarla en beneficio propio o de terceros.

Se encuentran especialmente sujetos a reserva y confidencialidad todo informe, registros jurídicos y médicos, actas de audiencia, historial de vida, y los documentos relacionados con la forma, contenido y datos de los diagnósticos o intervenciones a las que está o estuvo sujeto el niño, niña o adolescente.

Para efectos de lo dispuesto en el inciso segundo del artículo 125 de la ley N° 18.834, que aprueba Estatuto Administrativo, cuyo texto refundido, coordinado y sistematizado fue fijado por el decreto con fuerza de ley N° 29, de 2004, del Ministerio de Hacienda, se estimará que los hechos que configuren infracciones a esta disposición vulneran gravemente el principio de probidad administrativa, sin perjuicio de las demás sanciones y responsabilidades que procedan.

El que revelare información confidencial que tuviere en razón de su función, o consintiere en que otro acceda a ésta, será sancionado con la pena de presidio menor en su grado mínimo a medio. Si la conducta fuere cometida por un funcionario público, éste incurrirá, además, en las penas de suspensión de su cargo de conformidad a la ley.

Artículo 33 bis.- La información calificada como confidencial y reservada de acuerdo al artículo anterior será accesible a los tribunales de familia que conozcan de las causas relativas a los niños, niñas y adolescentes. Asimismo, tal información será accesible a los abogados que los representen, y a sus padres y/o madres, familia extensa o cuidadores que comparezcan, en calidad de parte en tales procesos judiciales, incluso cuando lo hagan sin patrocinio letrado.

Toda la información que el Servicio o sus colaboradores acreditados pretendan incorporar como prueba en el proceso deberá ser presentada ante el tribunal que corresponda con, a lo menos, cinco días hábiles de anticipación a la fecha de celebración de la respectiva audiencia, a fin de que las personas referidas en el inciso anterior puedan ejercer debidamente su respectivo derecho a la defensa.

Artículo 34.- Responsables del tratamiento de los datos personales. El tratamiento de los datos personales por parte del Servicio y de los colaboradores acreditados quedará sujeto a lo dispuesto en la ley N° 19.628, sobre Protección a la Vida Privada, considerándose al jefe superior del Servicio y a los representantes legales de los colaboradores acreditados como los responsables del tratamiento de datos".

Debemos reiterar, que, salvo esta norma reciente, aún ni siquiera vigente y solo aplicable a niñas y adolescentes, no existe otra que establezca un Sistema Unificado de Registro de VCM.

Analizamos ahora el marco legal actualmente vigente para una plataforma integrada de gestión de casos de VCM.

Al respecto, no podemos dejar de tener en cuenta los temas de gobernanza y el sistema regulatorio vigente que otorga las facultades para oficializar los mecanismos de colaboración interinstitucional para lograr el acuerdo organizacional, semántico y técnico para intercambiar información, cuestión que no reviste mayor conflicto en nuestro ordenamiento dado los principios constitucionales de eficiencia y eficacia de la Administración que les permiten desarrollar todas aquellas actividades que les permitan cumplir con su finalidad pública. Del mismo modo entran en juego aspectos legales vinculados a la protección de datos personales, en cuanto se trata de información propia de los

ciudadanos y por tanto se debe prever los posibles efectos, positivos o negativos, que esta actividad genere sobre derechos fundamentales de las personas, y por supuesto los aspectos referidos a la seguridad de la propia información tanto cuando esta se encuentra en poder de la institución, tanto en el proceso de intercambio.

Otro elemento que también debe ser revisado en el ámbito legal es la protección de los derechos de propiedad intelectual relativos a sus componentes físicos, lógicos y a la información que se intercambia, cuestión a la que nos referiremos en la propuesta, dado que no apareció como una barrera reconocida por los servicios, debido probablemente a que desde hace tiempo las entidades públicas han venido desarrollando estos servicios y las herramientas legales de que disponen resultan suficientes para no estimarlo un problema.

A continuación, revisamos los principales elementos a tener en cuenta en la construcción de una plataforma integrada de gestión de casos de VCM, a la luz de la legislación nacional. En general, en Chile los organismos públicos no requieren autorización legal expresa para elaborar bases de datos en el ámbito de sus competencias, es decir, pueden y deben recolectar información relevante para cumplir con los fines públicos a ellas asignadas. Podrá en consecuencia almacenar datos de diferente naturaleza, como, por ejemplo:

a) Información o datos personales[5] de acceso público, cuyo régimen de protección es menor, ya que se encuentran en fuentes de uso público;
b) Datos personales sensibles[6], que deben tener un alto grado de protección y que requerirán siempre autorización legal o de su titular para utilizarse en cualquier plataforma, y
c) Datos personales generales que, sin tener ese resguardo especial, deben también protegerse.

Como vemos, la problemática jurídica se traslada y toma nuevos matices en el marco de una plataforma integrada a los datos personales almacenados, pues el Estado en el caso se transforma en el principal recolector y proveedor de información sobre las personas.

Lo anterior permite explicar por qué el intercambio de información en este tipo de infraestructura se enmarca y está regido por los principios y normas jurídicas en materia de protección de datos personales. Se trata en consecuencia, como señala Moya, de "determinar en función de qué fundamentos un organismo público puede mantener bases de datos con información personal. Su naturaleza instrumental determina que sea decisión soberana de cada servicio público el determinar si desea tener bases de datos y de ellas, en particular las de datos personales. Sólo se exigirá que cumpla con los requisitos que establece la ley, que efectúe el tratamiento de estos en función del principio de legalidad y dentro del ámbito de su competencia y que cumpla las obligaciones que se derivan de su mantención. Ahora bien, importa precisar que sí se requiere de autorización legal para la conformación de registros de los cuales se puedan desprender derechos u obligaciones para las personas, que emanan de su condición de pertenecer al mismo. En tal sentido una base de datos personales puede ser el instrumento sobre el cual se genere un registro público, el cuál sí requiere fundamento legal para existir" (Moya, 2007: 4).

Aclarado lo anterior, y no tratándose de un registro público, debemos precisar que cualquier operación que refiera a la recolección de datos personales, la elaboración de registros internos o bases de datos por cada una de las entidades del Estado, como la creación de una infraestructura tecnológica que permita el intercambio de información personal entre sus organismos e incluso los privados contratados por estos, es a todas luces materia que incumbe y se enmarca en la temática de protección de datos personales, pues todas las actividades antes descritas se encuentran contenidas dentro del concepto de tratamiento de datos personales que establece la Ley N° 19.628 de Protección de la Vida Privada. Resulta claro que el funcionamiento de una plataforma integrada requiere tomar

[5] Datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables
[6] Datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

información de los ciudadanos desde los sistemas y bases de datos que poseen los diversos organismos públicos e intercambiarlos entre ellos, lo cual debe realizarse ajustándose a los límites que la protección de datos personales y la seguridad de la información imponen.

Al respecto, podemos afirmar categóricamente que es posible realizar intercambio de información personal a través de este tipo de plataformas, pero es preciso ajustar su funcionamiento a los principios establecidos en la normativa de protección de datos vigente, y que destacamos:

1. **Principio de Legalidad Administrativa:** para su cumplimiento, el intercambio de información, como actividad que implica tratamiento de datos personales, requiere norma legal habilitante, con fundamento en el interés público de los servicios que se ofrecen a las y los ciudadanos, o a través del consentimiento expreso de las y los titulares de los datos para el tratamiento de su información. En el ámbito subjetivo este principio implica también competencia del ente que envía y el que recibe los datos para realizar el intercambio de esta información, así como correspondencia con la finalidad del tratamiento que se va a realizar. La competencia se extrae de las facultades y funciones de su normativa orgánica por lo que, para este estudio fue revisado y validado en conjunto con las instituciones en el diagnóstico realizado con ellas. La finalidad del tratamiento por su parte se refiere a la intervención de las entidades en trámites y procesos públicos validados previamente, en nuestro caso la prevención, atención o reparación de VCM. Para el caso de particulares que ejecuten tratamiento de datos personales en condición de colaboradores de la Administración, como por ejemplo los entes colaboradores de SENAME, el acuerdo con estos les facultará para ejercer estas funciones a nombre de la respectiva entidad pública, debiendo prever en los contratos cláusulas relativas a la confidencialidad, integridad y responsabilidad frente al tratamiento de la información personal que se trata.
   Esta legalidad administrativa exige también que la transmisión e intercambio de datos personales se formalice a través de la suscripción de convenios que regulen los aspectos técnicos y legales de la relación entre la entidad proveedora/receptora de información y el órgano responsable de la plataforma.

2. **Principio de Proporcionalidad**: Se relaciona también con la finalidad del tratamiento, pues la entidad receptora y el funcionario que solicitan los datos no tienen legitimación ni justificación para conocer más datos sobre las personas que los que estrictamente les interesan. Lo anterior es manifestación de la necesaria razonabilidad y pertinencia de los datos que son objeto de procesamiento.

3. **Principio de transparencia**: Al aplicarlo a los intercambios que se realicen en el marco de la plataforma, el tratamiento de datos personales que se realice debe encontrarse disponible a aquellos que requieran conocer para que fines se ejecutaron esas acciones. No debe confundirse el deber de transparencia del procesamiento con la entrega de información personal a terceros no legitimados, pues el mismo deber de probidad que exige a los funcionarios transparencia, se complementa con la confidencialidad y respeto por la información personal de los ciudadanos.

4. **Principio de Eficiencia Administrativa**: Se debe entender, no solamente en cuanto a la obligación de brindar el servicio de la forma más adecuada, ágil y rápida al ciudadano, para lo cual la plataforma colabora con incorporación de TIC en la simplificación de los tramites y mayor rapidez en la obtención de resultados en los servicios públicos que se ofrecen; sino que también se hace referencia a otra faceta, relacionada con la seguridad de la información personal que almacena. Deben asegurar la conservación y custodia de la información personal que se utiliza para ofrecer los servicios públicos, resguardando los mismo de intentos de acceso por terceros no autorizados.

Expuesto los principios, revisaremos a continuación las implicaciones que la regulación jurídica que establece la Ley 19.628, tendrían en el marco de las actividades que involucren tratamiento de datos personales por parte de entidades que concurran a una plataforma integrada de gestión de casos.

Al respecto, el artículo 20 de la Ley 19.628 dispone lo siguiente:

"Artículo 20. El tratamiento de datos personales por parte de un organismo público solo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitara el consentimiento del titular".

Como vemos, la ley opta por la fórmula de establecer una disposición especifica que sustenta al autorizar el tratamiento de datos personales por parte de los entes del sector público, determinando dos presupuestos o requisitos para que esas actividades puedan considerarse legitimas:

a) Que el organismo público realice el tratamiento conforme al ámbito de competencias que el ordenamiento jurídico ha definido para que este realice sus funciones en pos de la finalidad pública asignada a este.
b) Que el tratamiento se realice conforme a las reglas generales para la recolección, transmisión y utilización de datos personales que la Ley 19.628 establece para cualquier otra forma de tratamiento de información de carácter personal, recogidas en los primeros artículos de ese cuerpo normativo. Esto último significa que somete el intercambio a las obligaciones legales de los encargados de ficheros de datos, con especial mención al artículo 5 de la Ley 19.628 respecto del funcionamiento de la plataforma, en cuanto regula las obligaciones en el caso de transmisión de información, y que le corresponde también tomar las medidas tecnológicas, administrativas y jurídicas correspondientes para garantizar la seguridad y privacidad de los datos y, por ende, la protección de los derechos de los titulares de los datos, los famosos derechos ARCO (acceso, rectificación, cancelación y oposición).

Como podemos observar, se establece para los organismos públicos un tratamiento diferenciado al de los privados, ya que se les permite actuando dentro de su competencia y por supuesto, en tanto se respete la normativa, tratar datos sin consentimiento del titular. Lo anterior implica que en esta categoría de datos la autorización previa del titular de los datos para efectuar tratamiento de ellos, en principio, no se requiere, pues es de suyo propio que los órganos públicos actúen dentro de su competencia, y en caso de no hacerlo, son los tribunales y la Contraloría los llamados a pronunciarse, pues no hay una definición específica de la competencia en esta materia y por tanto, se requerirá de una interpretación sistémica de la normativa, lo cual comprende para este caso concreto, valorar el ámbito en que ejercen su tareas y fines las entidades, así como apreciar la finalidad del tratamiento de datos personales que realizaría. Como veremos, para las instituciones involucradas en la ruta crítica de VCM esta interpretación legal es compleja, lo que hace que clasifiquen de manera no uniforme y a veces inadecuada la información que tratan, convirtiendo a la protección de datos personales en la principal barrera para el intercambio.

Si bien el artículo 10 de la Ley N° 19.628, que dispone *"No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares"*, establece una prohibición legal al tratamiento de datos catalogados como sensibles, para el caso de la plataforma sería posible obtener una autorización expresa de la ley o la autorización del titular, en este último caso tanto para la utilización como para la transmisión de los datos.

Un buen ejemplo que encontramos en nuestro ordenamiento de datos sensibles plausibles de tratamiento bajo autorización legal por la Administración, se da con la autorización para tratar los datos de salud, lo cual se autoriza expresamente por el articulo 10 mencionado, complementado por el numeral 127 del Código Sanitario, así como el Decreto con Fuerza de Ley No 1 del 2005 del Ministerio de Salud, que fija el texto refundido de la Ley 18.933 sobre instituciones de salud previsional y que expresamente establece las competencias del Ministerio de Salud y del Fondo Nacional de Salud para el tratamiento de datos personales.

Otro ejemplo se observa en el artículo 21 de la Ley 19.628, el cual dispone la posibilidad del tratamiento de la información relativa a las condenas o penas judiciales, así como de las infracciones administrativas imputadas a las personas las que podrán ser comunicados a los Tribunales de Justicia u otros organismos públicos que demuestren ser competentes para su tratamiento.

Un elemento importante es que, al tener estos datos sensibles una protección adicional, deberá considerarse también los dispositivos de seguridad técnica que garanticen el resguardo especial de esta información.

Otra norma para considerar en este análisis legal de una plataforma integrada es lo dispuesto por el artículo 5 de la Ley N° 19.628 sobre las actividades de transmisión de datos que indica:

"El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.

Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de:

a) La individualización del requirente;

b) El motivo y el propósito del requerimiento, y

c) El tipo de datos que se transmiten.

La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga.

El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

No se aplicará este artículo cuando se trate de datos personales accesibles al público en general…".

La disposición transcrita, es la base normativa principal de una plataforma integrada que maneja datos personales, pues en esencia, la integración de procesos administrativos electrónicamente, consiste en compartir e intercambiar información, en gran parte datos personales de los ciudadanos, a través de una infraestructura de transmisión electrónica informacional, añadiendo cada organismo, bien en su rol de proveedor o destinatario de la información, su cuota de valor al servicio que se ofrece al público.

Conforme a lo anterior, el articulo 5 señalado es el que regula el régimen jurídico y responsabilidades en la transmisión electrónica de datos personales, de modo que los entes de la administración deben considerar lo ahí dispuesto para actuar conforme al ordenamiento nacional.

La norma habilita expresamente a la transmisión electrónica de datos, como una forma más del tratamiento de datos personales. Para realizar esta labor de forma ajustada a la legalidad, la norma impone dos limitaciones: el respeto a los derechos de los titulares de los datos, así como a las competencias de las entidades participantes y a la finalidad con las que se justifica el tratamiento de los datos, principios que ya analizamos anteriormente.

Exige además el artículo 5, que en las solicitudes de trasmisión de datos personales se cumplan y se deje expresa constancia de ciertos elementos esenciales para garantizar los derechos y aspectos señalados en el punto anterior.

En el caso de una plataforma integrada de VCM, se deberá dejar registro por los administradores de la plataforma y los organismos que reciban solicitudes de transmisión de información, como mínimo de los tres aspectos referidos por la ley, a saber:

a) La identificación de la entidad que solicita los datos, si es posible también identificar al funcionario requirente, con la finalidad de validar la pertinencia de la transmisión de información respecto del esquema y niveles de autorizaciones. Para este fin y la seguridad de los datos, es de gran utilidad la implementación de firmas electrónicas avanzadas como mecanismo de autenticación;

b) La razón que origina la solicitud y el propósito con el que será utilizada la información solicitada, esto permitirá la comprobación de la competencia y finalidad del tratamiento, lo cual también podrá ser validado respecto de un esquema que previamente defina los procesos públicos en los que el solicitante interviene, de modo que se garantice al titular de los datos que su información está siendo utilizada en un procedimiento administrativo ajustado a la finalidad publica y a la protección de sus datos personales; y
c) La categoría de los datos que se transmiten, de modo que se pueda determinar la existencia de restricciones y garantías especiales, para el caso de datos personales sensibles.

Aclara también la norma que el órgano que reciba la solicitud se encargara de definir si el requerimiento de información procede o no, será en consecuencia el ente que cuente con la información en su poder quien definirá en última instancia si hace envió o rechaza la solicitud, utilizando la plataforma como medio de intercambio de la resolución tomada, sea esta negativa o positiva, remitiendo los datos al solicitante en el último caso. Lo anterior resulta relevante al objeto de definir las responsabilidades del órgano que tiene la gobernanza de la plataforma, quien actuará como intermediario en el tráfico de solicitudes y datos, recayendo siempre y sin que exista duda, la responsabilidad en la entidad solicitante e incluso en el funcionario que formaliza el requerimiento, y en el ente que entrega la información. En efecto, el receptor solo puede utilizar los datos personales para los fines que motivaron la transmisión, en armonía con el principio de finalidad. La importancia de esto está en la limitación de la reutilización de información personal para fines que no sean los originalmente previstos, exigiendo la responsabilidad a los funcionarios responsables de los requerimientos. Del mismo modo, deberían establecerse mecanismos técnicos y administrativos, que permitan detectar casos en que se soliciten datos a entidades que no son las legitimadas para proveer y tratar esta información, y también deberá aplicarse en sentido inverso, es decir, cuando el proveedor de la información transmita información respecto de la cual no está legitimada para intercambiar, debido a carecer de las competencias suficientes para ese fin.

Por último, es importante para el caso, una de las excepciones que prevé el articulo 5 para la transmisión electrónica de datos personales que consten en registros de acceso al público, que ya hemos definido. En el caso, se atenúan los requisitos y por ende la responsabilidad que puede acarrear a las entidades y los funcionarios que interactúan en la plataforma.

Un último elemento de este análisis, lo constituye precisamente el ámbito de la responsabilidad que podría alcanzar a los órganos públicos intercambian información en el marco de una plataforma integrada. Al respecto, resulta de sumo interés revisar las potestades sancionatorias de los organismos competentes de protección de datos, pues mediante tales potestades se articula una de las principales herramientas de regulación de los agentes públicos y privados que intervienen en actividades de recopilación y tratamiento de datos personales, y se propende a mejorar los niveles de cumplimiento de la normativa de protección de datos. Al pensar en la protección de datos personales, consecuentemente, resulta fundamental no perder de vista nunca la necesidad de que el sistema de protección que se articule contemple mecanismos sancionatorios y sanciones efectivas que permitan disuadir con éxito las violaciones a los derechos de las personas[7].

La responsabilidad se relaciona con temas como los principios de seguridad, tanto jurídica como técnica, así como el deber de reserva o confidencialidad de parte de los entes y funcionarios que intervienen en el tratamiento de datos personales. En primer término, es lógico comprender que un organismo público, como responsable del banco de datos, deba tomar las precauciones que sean necesarias para dar real y efectiva protección a los datos personales que almacena en sus registros,

[7] A pesar de que se describe aquí, tener presente que en Chile el régimen sancionatorio está en deuda, tanto en lo que refiere al procedimiento como en cuanto al tipo y entidad de las sanciones, por lo que se recomienda tener a la vista el catálogo de infracciones y sanciones que contempla el Título VII de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, de España, que constituye un verdadero estándar en materia. Un ejemplo de puede ver en AEPD. Guía Consecuencias administrativas, disciplinarias, civiles y penales de la Difusión de Contenidos Sensibles.

debiendo asumir las acciones para asegurar el cumplimiento de la ley N° 19.628. De otra parte, el deber de secreto, que implica la obligación de reserva respecto del contenido de la información procesada, recae tanto sobre el responsable del banco, como sobre las personas que intervienen directamente los datos personales. Serán aplicables al respecto las normas generales existentes sobre responsabilidad en la Ley Orgánica Constitucional de Bases de la Administración del Estado, en sus artículos 4, 5, 12, 15 y 44 y el Estatuto Administrativo, artículos 124 y 125. De su parte, la ley N° 19.628 contempla normas especiales de responsabilidad civil frente al tratamiento de datos, imponiendo al responsable del banco de datos personales la obligación de indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los mismos, en el artículo 11 de la Ley 19.628, en relación con los artículos 2 inciso n), 5, 7, 9 Y 10. En cualquier caso, la indemnización respectiva será fijada prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos, y en el marco del procedimiento judicial legalmente aplicable en la especie.

Como se indicó anteriormente existen también deberes de transparencia y confidencialidad. En esta línea, es preciso hacer referencia ahora al deber de confidencialidad que establece el artículo 7 de la Ley 19.628, aplicable a los organismos públicos en el tratamiento de datos personales y, por ende, a los intercambios de información que estos realicen en el marco de una plataforma integrada.

En este sentido, el artículo 7 de referencia dispone: "Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo".

Así las cosas, podemos decir que existirá responsabilidad funcionaria por el incumplimiento de esta obligación de confidencialidad respecto de los encargados o aquellos que intervienen en el proceso de tratamiento de datos personales.

Esta responsabilidad puede ser administrativa, civil o incluso penal. Como hemos dicho, esto alcanza a las entidades colaboradoras de los órganos, aun cuando no sean responsables sobre los requerimientos y envíos de información, si lo son respecto de su transmisión y en tanto, estén en una posición que les permita conocer los datos que se transmiten. También se puede precisar que la responsabilidad que se derive, por ejemplo, por el envío de datos personales caducos, erróneos o inexactos corresponde a las entidades y funcionarios encargados de las solicitudes y envíos de información, no a las personas que tienen la gobernanza de la plataforma.

Otro aspecto de medular relevancia en cuanto a la limitación de la responsabilidad y garantía de la seguridad de los datos personales, lo constituye la necesidad de suscripción de convenios de intercambio de información entre las instituciones que la intercambian o con la que gobierna la plataforma. En estos convenios, se establecen los requisitos mínimos que se exigen para el tratamiento de datos personales, así como las características, términos y garantías del intercambio de información, elementos que han sido recogidos en las recomendaciones, como por ejemplo la interoperabilidad. Si bien la ley N°19.628 no establece expresamente la necesidad de formalizar, a partir de la experiencia recabada entre las instituciones, es recomendable que el acto sea documentado, para dejar constancia del hecho y del cumplimiento de los requisitos, particularmente que el tratamiento está dentro de la órbita de competencia del órgano. Como no se exige formalidad alguna entendemos que basta con una resolución exenta, o como observamos en práctica de las instituciones, a través de protocolos, acuerdos o convenios de transferencia de datos.

Para culminar con lo relativo al régimen de responsabilidad y seguridad en el tratamiento de datos personales a través de una plataforma integrada, debemos señalar que esta deberá estar acorde a la normativa en la materia, en específico al Decreto 14 del 2014 y a la Nch 2777, así como a las políticas de seguridad y privacidad aprobadas por cada entidad u organismo público que se interconecte con la plataforma. El Decreto 14 contiene las Normas Técnicas y estándares para los Documentos Electrónicos, Comunicaciones Electrónica e interoperabilidad, las Normas sobre la fijación de esquemas y metadatos de los documentos electrónicos, las Normas Técnicas sobre sitios electrónicos

y plataformas web abiertas, y las Guías Técnicas y de Implementación, aplicables a los órganos de la Administración del Estado. Entre estas últimas se encuentran las siguientes: a) Desarrollo de plataformas web abiertas seguras; b) Publicación de esquemas y metadatos; c) Publicación de datos abiertos; d) Accesibilidad y despliegue de contenidos digitales web; e) Desarrollo e implementación de la interoperabilidad en el Estado; f) Sobre confección y administración de expedientes electrónicos; g) Seguridad de las comunicaciones electrónicas; h) Privacidad en los sitios electrónicos y plataformas web abiertas. Cualquier desarrollo de una plataforma integrada de gestión de casos de VCM deberá tener en cuenta esta normativa.

El déficit en materia de estándares y la relevancia que toma este tema en el Estado chileno queda de manifiesto en la dictación en los últimos dos meses de variada normativa, que, aunque no vigente aún, proporciona lineamientos más claros en materia de digitalización de los procesos del Estado:

La Ley N°21.180 sobre Transformación Digital del Estado, aún no vigente y que sólo tendrá aplicación gradual desde mediados de este año hasta el año 2024, que introdujo modificaciones a las reglas sobre procedimiento administrativo, con el fin de avanzar hacia la digitalización de la gestión administrativa del Estado, mediante la comunicación electrónica entre órganos de la Administración del Estado, el establecimiento de procedimientos administrativos electrónicos, la digitalización de documentos, la notificación electrónica y la implementación del principio de interoperabilidad.

La Resolución 304, publicada el 7 de diciembre de 2020, emanada del Consejo para la Transparencia, que Aprueba Recomendaciones sobre Protección de Datos Personales por parte de los órganos de la Administración del Estado, y contiene el desarrollo de las normas que hemos señalado anteriormente referidas a la protección de datos en poder de la Administración, incorporando herramientas e instrumentos tales como la privacidad desde el diseño, el delegado u oficial de protección de datos y la evaluación de riesgos, entre otros, de acuerdo con los modernos estándares internacionales en materia de protección de datos personales.

ELEMENTOS LEGALES MÍNIMOS EN LA EXPERIENCIA EXTRANJERA

Naciones Unidas y Unión Europea

Respecto a la VCM, diversos instrumentos internacionales del Sistema Universal e Interamericano de Derechos Humanos han enfatizado en la necesidad de recopilar, producir y difundir información sobre estas formas de violencias. La aplicación de estos mecanismos permite comprender la dimensión y evolución del problema, además diseñar y evaluar la eficacia de la legislación, de las políticas públicas y de las medidas implementadas. Se establece como un medio que insta a los Estados a cumplir con su obligación de brindar a las mujeres y personas con identidades de género u orientaciones sexuales no normativas una atención especial y prioritaria.

Debemos resaltar que instrumentos como la Declaración de Naciones Unidas sobre la eliminación de la violencia contra la mujer (1993) y la Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (1994) son tratados internacionales de Derechos Humanos, ratificados por Chile, y por tanto incorporados a nuestro ordenamiento, que comprenden estas obligaciones. El acceso a la información y la obligación del Estado de producir información relativa a la violencia contra las mujeres, la Corte Interamericana de Derecho Humanos también lo ha establecido, y en el mismo sentido lo han hecho tanto la Convención Interamericana para prevenir, sancionar y erradicar la violencia contra las mujeres, conocida como Convención de Belém do Pará como el Comité de Expertas del Mecanismo de Seguimiento a la misma convención (MESECVI), a través de sus informes hemisféricos.

La Unión Europea, el Consejo de Europa y, a nivel internacional, las Naciones Unidas, por su parte, han reconocido la necesidad de una mejor recopilación de datos relacionados con la VCM para cumplir con el compromiso de erradicarla contenido en los ODS, al mismo tiempo, han puesto en relieve la falta de datos disponibles en la materia.

El último estudio realizado por el European Institute for Gender Equality (EIGE) en los años 2017-2018, publicado en 2019, establece como hallazgos en la materia de este informe, los siguientes:

- Los datos administrativos sobre VCM no se recopilan original o principalmente con fines estadísticos, sino para uso interno de las instituciones o agencias con el fin de monitorear sus actividades y por lo tanto, no miden el verdadero alcance de la violencia de género, sin embargo, pueden proporcionar información detallada sobre cómo responden los servicios judiciales, policiales, sanitarios y sociales a la violencia de género, lo que puede apoyar el desarrollo y la evaluación de políticas y medidas adecuadas para prevenir y combatir la violencia de género contra las mujeres en toda la Unión Europea.
- La regulación y recolección de datos administrativos se ve obstaculizada por la falta de mecanismos intersectoriales específicos para la coordinación del proceso. La descentralización de la recopilación, coordinación y compilación de datos sobre incidentes de VCM dificulta la comparación de datos en diferentes niveles. A nivel nacional, a menudo existe una diversidad de organizaciones administrativas encargadas de los registros sin normativa ni directrices claras que establezcan la coordinación de la colección de información relacionada con la VCM.
- Las reglas de confidencialidad representan un obstáculo importante que enfrentan los compiladores de datos, especialmente con la información de los servicios sociales y de salud.
- En general, las agencias públicas no tienen la recopilación de datos como su principal responsabilidad, por lo que estos no se recopilan de forma sistemática y estandarizada, no existe un sistema de codificación aceptado transversalmente entre los registros, dentro y entre sectores. Lo anterior no permite un acceso rápido y fácil a la información y su análisis. Por ejemplo, las diferencias sustanciales en las definiciones legales de las formas de violencia de género.
- La calidad del registro y procesamiento de datos no siempre tiene el estándar necesario para la toma de decisiones, monitoreo y evaluación de la provisión de políticas y servicios en VCM. Estos problemas son el resultado de una formación inadecuada, recursos y capacidad para quienes recolectan datos y la mala coordinación entre agencias y sectores. Es necesario, por tanto, mejorar la calidad de la información recopilada en relación con la violencia de género en toda la Unión Europea.

Como se ha señalado y se puede apreciar también en el diagnóstico incluido en este informe, la mayoría de estos hallazgos son los mismos que presenta nuestra propia realidad.

Considerando los desafíos anteriores, el EIGE sintetiza en otro de sus estudios algunas recomendaciones a partir de las buenas prácticas recogidas en la experiencia analizada por ellos.

1. El compromiso político e institucional en el apoyo recopilación de datos administrativos sobre la VCM. Al efecto, debería asignarse una responsabilidad clara a autoridades y ministerios involucrados. Esto es crucial para garantizar sostenibilidad y recopilación armonizada de datos sobre diferentes formas de violencia. Esto se puede hacer a través de un marco regulatorio que creo o designe una entidad a cargo de la recopilación de datos administrativos sobre VCM o a través de una estrategia nacional que desarrolle planes y programas específicos en este sentido.
2. Recursos financieros dedicados para fortalecer la recopilación de datos administrativos sobre VCM. La falta de recursos puede resultar en la no implementación de las acciones o en la limitación de su implementación a la voluntad de instituciones y organizaciones involucradas.

3. Un enfoque sistemático y multidimensional respecto de las fuentes de datos y partes interesadas. La integración de diferentes fuentes de datos es de especial importancia. Esto incluye el uso simultáneo en colaboración con diferentes partes interesadas en diferentes sectores, incluyendo los observatorios de la sociedad civil.
4. Una buena comprensión del contexto nacional en el que se recopilan datos administrativos. Este contexto refiere tanto a los contenidos, conceptos y definiciones utilizados; la frecuencia y cronogramas; la calidad de la información y su preservación en el tiempo; así como las implicaciones de privacidad de la publicación de información de registros administrativos.
5. Estandarización de los datos. Es imprescindible disponer de ciertos criterios que permitan que los valorar y evaluar la calidad de los datos. La falta de normalización no ayuda en esto.
6. Formación en género y especialmente en VCM a funcionarios que recopilan la información. Las cuestiones de género son muy complejas y, por lo tanto, necesitan una formación específica para ser comprendidos, el estudio determina que es también un factor que afecta la cantidad y calidad de los datos que se recopilan.

Por su parte, en su informe Essential Services Package for Women and Girls Subject to Violence, ONU Mujeres, establece un conjunto de recomendaciones, que constituyen una verdadera hoja de ruta para establecer o fortalecer los registros administrativos en materia de VCM. Al respecto indica los siguientes pasos a seguir:

1. Mapear las instituciones que están proporcionando servicios e interactuando con sobrevivientes y perpetradores de la VCM
2. Establecer un mecanismo de coordinación y gobernanza de la información, tanto en el nivel político como en el nivel operativo.
3. Establece e implementar capacitación para respaldar la calidad y comprensión de los datos administrativos de VCM a la vez que promover un enfoque centrado en la mujer en situación de violencia.
4. Establecer e implementar estándares y sistemas para recopilación, ingreso, validación y análisis de datos que permitan la posterior integración e interoperabilidad con otros sistemas.
5. Informar. Esto es un imperativo ético para apoyar a los sobrevivientes mediante el uso de la información recopilada para mejorar los esfuerzos de prevención y respuesta a la VCM.

Como de observa, en materia de fortalecimiento de los registros la ruta parece clara.

A continuación, se muestran dos experiencias de plataformas integradas de información de VCM que no parece relevante revisar.

Colombia. Sistema Integrado de Información de Violencias por razones de Sexo y Género (SIVIGE)

Según el documento de las entidades coordinadoras del Sistema Integrado de Información sobre Violencias de Género (2015), los antecedentes normativos del SIVIGE se encuentran en el artículo 9 de la ley 1257, de 2008, que obliga a las entidades responsables a aportar la información referente a violencia de genero al sistema de información que determine el Ministerio de Protección Social y a la Consejería Presidencial para la Equidad de la Mujer, Observatorio de Asuntos de Género, para las labores de información, monitoreo y seguimiento; y el artículo 31 de la Ley 1719, de 2014, que faculta a varias entidades para asesorar la incorporación al Sistema de Registro Unificado de Casos de Violencia contra la Mujer contemplado en dichas normas, de un componente único de información, que permita conocer la dimensión de la violencia sexual de que trata la presente ley, monitorear los factores de riesgo de la misma, y aportar elementos de análisis para evaluar las medidas adoptadas en materia de prevención, atención y protección (…).

Posteriormente, la Ley 1761, de 2015, el artículo 12 mandata crear con las entidades vinculadas, un Sistema Nacional de Recopilación de Datos sobre los hechos relacionados con la violencia de género en el país, para establecer los tipos, ámbitos, modalidades, frecuencia, medios utilizados para ejecutar la violencia, niveles de impacto personal, social y el estado del proceso judicial para la definición de políticas públicas de prevención, protección, atención y reparación de las víctimas de la violencia de género.

Dado ese mandado, se crea el Sistema Integrado de Información sobre Violencia de Genero (SIVIGE) con la colaboración y articulación del Ministerio de Salud y Protección Social, el DANE, la Consejería Presidencial para la Equidad de la Mujer, el Instituto Nacional de Medicina Legal y Ciencias Forenses y el Ministerio de Justicia y del Derecho.

En 2019 y por mandato previsto en la Ley 1955 de 2019, se insiste en el fortalecimiento de las capacidades institucionales en transversalización del enfoque de género y crear una articulación que permita consolidar y fortalecer la coordinación interinstitucional e intersectorial en temas de género, para lo cual se considera necesario adoptar una estructura técnica y operativa que cuente con la presencia de la Fiscalía General de la Nación corno ente investigador de los delitos relacionados con la violencia por razones de género, contra niños, niñas, adolescentes y mujeres.

Finalmente, en 2020, mediante Decreto 1710[8], Colombia adopta formalmente el Mecanismo Articulador para el Abordaje Integral de las Violencias por Razones de Sexo y Género, de las mujeres, niños, niñas y adolescentes.

De acuerdo con el artículo 1° el Mecanismo responde a una *"estrategia de coordinación interinstitucional del orden nacional, departamental, distrital y municipal, para la respuesta técnica y operativa dirigida a (i) la promoción del derecho a una vida libre de violencia, (ii) la prevención de esta, (iii) la atención, protección y acceso a la justicia a niñas, niños, adolescentes y mujeres víctimas de la violencia por razones de sexo y género, y (iv) la gestión del conocimiento".*

El artículos 18 por su parte se crea y establece la conformación y funciones del Comité de sistemas de información *"encargado de generar procesos de gestión de conocimiento y fortalecimiento de herramientas de captura de información para el seguimiento, monitoreo y evaluación de la violencia por razones de sexo y género, su abordaje integral y para el direccionamiento de la política pública".* El artículo 19 establece que será *"coordinado por el Ministerio de Salud y Protección Social y el Departamento Administrativo Nacional de Estadística – DANE, alternando la secretaría técnica entre ellos y estará conformado, además, por las personas delegadas de carácter técnico que sean especialistas y encargados del manejo de datos de información cuantitativa*" de las autoridades de todas las instituciones involucradas en los procesos. En el art. 20 se describen sus funciones, que van desde promover los acuerdos intersectoriales, generar los procesos de gestión de conocimiento y fortalecimiento de captura de información y entregar asistencia técnica a las instituciones para la recogida y tratamiento de la información.

Mediante el artículo 30 se formaliza el Sistema Integrado de Información de Violencias por razones de Sexo y Género – SIVIGE, que como señalamos ya existía. La normativa señala expresamente:

"El SIVIGE es el sistema integrado e interoperado que reúne las diferentes herramientas de captura de información a cargo del Ministerio de Salud y Protección Social, que permitirá al Mecanismo Articulador realizar el seguimiento, monitoreo, y la evaluación de las acciones de política pública para la prevención de la violencia por razones de sexo y género, y la garantía en la atención y acceso a la justicia de las víctimas. La información que produzca el Sistema Integrado de Información será consolidada progresivamente, de acuerdo con las formas de violencia que sean priorizadas por el Comité de Sistemas de Información.

[8] Ver texto completo del Decreto 1710, 19 de diciembre de 2020, en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=153846

PARÁGRAFO 1. Las autoridades que cuenten con herramientas de captura de información de violencias por razones de sexo y género, deberán compartir la información al Sistema de Integrado de Información - SIVIGE, a través de la suscripción de convenios o acuerdos de voluntades, acuerdos de confidencialidad, para que de forma expedita y por una sola vez, se facilite la integración de fuentes de información y se establezcan los indicadores sobre el abordaje integral de la violencia por razones de sexo y género, y evaluar la oportunidad en la respuesta en la atención a las víctimas.

PARÁGRAFO 2. En atención a las competencias del Departamento Administrativo Nacional de Estadística - DANE como entidad asesora, productora de estadísticas nacionales, ente rector del Sistema Estadístico Nacional - SEN, y parte del SIVIGE, las entidades competentes que recopilen y administren microdatos relacionados con la violencia por razones de sexo y género a que se refiere el presente Decreto, pondrán a disposición la información requerida para facilitar la asesoría del DANE y se acogerán a los lineamientos técnicos especificados por esta autoridad".

España. Sistema VioGén

De acuerdo con el sitio web del Ministerio de Interior, el Sistema de Seguimiento Integral en los casos de Violencia de Género (Sistema VioGén), de la Secretaría de Estado de Seguridad del Ministerio del Interior, se puso en funcionamiento el 26 de julio del 2007, en cumplimiento de lo establecido en la Ley Orgánica 1/2004, de 28 de diciembre, "de Medidas de Protección Integral contra la Violencia de Género", siendo sus objetivos:

1. Aglutinar a las diferentes instituciones públicas que tienen competencias en materia de violencia de género
2. Integrar toda la información de interés que se estime necesaria
3. Hacer predicción del riesgo
4. Atendiendo al nivel de riesgo, realizar seguimiento y protección a las víctimas en todo el territorio nacional
5. Efectuar una labor preventiva, emitiendo avisos, alertas y alarmas, a través del "Subsistema de Notificaciones Automatizadas", cuando se detecte alguna incidencia o acontecimiento que pueda poner en peligro la integridad de la víctima.
6. Establecer una tupida red que permita el seguimiento y protección de forma rápida, integral y efectiva de las mujeres maltratadas, y de sus hijos e hijas, en cualquier parte del territorio nacional.

Nos parece interesante, para efectos de este informe, el glosario de términos que acompaña a los informes, pues permiten definir algunos elementos de esta plataforma.

- Caso: El concepto de "Caso de violencia de género" es muy similar al de "víctima de violencia de género", aunque no es idéntico. Un Caso contiene toda la información que relaciona a una víctima con un único agresor, incluyendo tantas denuncias (de la víctima, de tercero o de oficio) como se hayan registrado. Igualmente, si una mujer, a lo largo del tiempo, es víctima de violencia de género con más de un agresor, hablaremos de un Caso distinto por cada uno de ellos. Esto mismo es aplicable para los agresores.
- Caso activo: Aquel que es objeto de seguimiento policial. El nivel de riesgo de cada Caso activo, según el momento y las circunstancias que lo rodeen, va evolucionando con el trascurso del tiempo.

1 Se emplean los formularios VPR (Valoración Policial del Riesgo) y VPER (Valoración Policial de Evolución del Riesgo).

2 Los niveles de riesgo son cinco: “NO APRECIADO”, “BAJO”, “MEDIO”, “ALTO” Y “EXTREMO", según lo recoge la Instrucción 4/2019, de la Secretaría de Estado de Seguridad, con entrada en vigor el 13 de marzo de 2019 y cada nivel lleva asociadas una serie de Medidas de Protección y seguimiento, de aplicación obligatoria, que varían en intensidad según el nivel de riesgo del Caso en cada momento.

- Caso inactivo: Aquel que, por determinadas circunstancias, temporalmente, no es objeto de seguimiento policial. El Caso inactivo puede reactivarse en cualquier momento.
- Caso de baja: Aquel en el que se procede a la supresión de datos personales del autor/agresor, una vez estudiadas las características del Caso y siempre que se den alguna de las siguientes circunstancias: sentencia absolutoria firme del interesado; auto de sobreseimiento firme del imputado o procesado; auto de archivo de la causa judicial, siempre que el mismo sea firme; Sentencia condenatoria firme, siempre que se haya ejecutado (cumplimiento de la pena) y haya transcurrido el plazo legal para la cancelación de antecedentes penales.
- Caso valorado conforme al vigente Protocolo (Instrucción 4/2019): Aquellos Casos en los que se ha realizado la Valoración Policial del Riesgo (VPR) o la Valoración Policial de la Evolución del Riesgo con incidencia (VPER-C), conforme al vigente “Protocolo de Valoración policial del riesgo de violencia de género, gestión de la seguridad de las víctimas y seguimiento de los Casos a través del Sistema de seguimiento Integral de los Casos de violencia de género (Sistema VioGén)” regulado por la Instrucción 4/2019 de la SES, con entrada en vigor en fecha 13 de marzo de 2019.
- Caso de ESPECIAL RELEVANCIA: Aquellos Casos en los que, tras la práctica de la valoración policial del riesgo, conforme al vigente Protocolo (Instrucción 4/2019), se detecta una especial combinación de indicadores que aumentan de manera significativa la probabilidad de que el agresor ejerza sobre la víctima violencia muy grave o letal. Esta situación se da únicamente en Casos con riesgo MEDIO, ALTO O EXTREMO.
- Caso con MENORES EN SITUACIÓN DE VULNERABILIDAD: Aquellos Casos en los que, tras la práctica de la valoración policial del riesgo a la víctima, conforme al vigente Protocolo (Instrucción 4/2019), y existiendo MENORES a su cargo, se detecta una especial combinación de indicadores que apuntan a que estos MENORES pueden encontrarse en situación de especial vulnerabilidad. Esta situación se puede dar en todos los niveles de riesgo.
- Caso con MENORES EN SITUACIÓN DE RIESGO: Aquellos Casos en los que, tras la práctica de la valoración policial del riesgo a la víctima, conforme al vigente Protocolo (Instrucción 4/2019), y existiendo MENORES a su cargo, se detecta una especial combinación de indicadores que apuntan a que la violencia ejercida por el agresor sobre la víctima podría extenderse a otras personas cercanas a esta, especialmente hacia los MENORES a su cargo. Esta situación se da únicamente en Casos con riesgo MEDIO, ALTO O EXTREMO.
- En los Casos de ESPECIAL RELEVANCIA, MENORES EN SITUACIÓN DE VULNERABILIDAD O MENORES EN SITUACIÓN DE RIESGO el Sistema VioGén genera para estos Casos una Diligencia Automatizada que se adjunta al informe de valoración policial del riesgo y al Atestado, al objeto de recomendar a la Autoridad Judicial y Fiscal la práctica de evaluación adicional experta en el ámbito forense.

Por último, y para cerrar el análisis conceptual, se consignan a continuación los estándares internacionalmente reconocidos para el diseño legal de plataformas integradas de gestión de los registros de información de VCM que fueron revisados con cada una de las instituciones a fin de hacer conciencia y socializar entre ellos su importancia para el tratamiento de información personal como la que contienen estos registros.

PRINCIPIOS Y ESTÁNDARES INTERNACIONALES PARA LA PROTECCIÓN Y SEGURIDAD DE LA INFORMACIÓN PERSONAL

Como hemos dicho precedentemente en los registros administrativos que pueden ser integrados en una plataforma interoperable se trata información personal, cuyos titulares son los usuarios de los servicios de prevención, atención y reparación de VCM. Lo anterior obliga a los órganos públicos a proteger los datos personales allí contenidos y a asegurar su almacenamiento, gestión y eventual traspaso o comunicación hacia otro servicio.

Con respecto a la protección de datos personales, una de las normas que contiene los estándares más altos en materia de tratamiento de datos personales es el Reglamento General de Protección de Datos Personales (RGPDP) de la Unión Europea, que consigna los siguientes principios:

1. **Licitud, lealtad y transparencia**. Los datos deben ser tratados de manera lícita, leal y transparente en relación con su titular. La ley o el propio titular deben autorizar a tratar esta información. Es interesante hacer notar que este estándar, que considera algunas excepciones amplias en algunos casos, es mucho más estricto cuando se trata de datos sensibles.
2. **Finalidad**. Los datos deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; en todo caso el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales, lo que abre una ventana a posibles usos en materia de prevención y políticas públicas. La referida finalidad, en el caso de órganos de la Administración del Estado, estará determinada en función de las materias propias de su competencia y por la función legal específica que está ejecutando y que justifica el procesamiento de datos personales.
3. **Minimización**. Los datos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. En lo referido a este informe, atendida la finalidad que se persigue con la plataforma integrada, que es el seguimiento de los casos de VCM que permitan generar alertas para la prevención y atención personalizada, no es posible considerar una anonimización completa de la información, sin embargo, en aplicación de este principio, los órganos o servicios públicos deberán optar, de entre los diversos tratamientos que les permitan conseguir los fines pretendidos dentro del ámbito de sus competencias, por aquel que menor incidencia tenga en el derecho a la protección de datos personales y por la utilización de los medios menos invasivos. Los especialistas concuerdan también, que es un error realizar una aplicación del principio de minimización que comprometa la finalidad del tratamiento. Por ejemplo, en el caso de la plataforma de VCM, con relación a la extensión de datos tratados de una mujer, diseñar una pauta que recoja información insuficiente de tal forma que no sea posible obtener detalles del hecho con los niveles de precisión adecuados, no solo no cumpliría con el principio de minimización, sino que iría incluso en contra del principio de lealtad del tratamiento, al ser inviable poder cumplir con el propósito declarado. Por lo tanto, la aplicación del principio de minimización implica un análisis objetivo y racional del tratamiento.
4. **Exactitud o calidad**. Los datos tratados deben ser exactos, adecuados, pertinentes y no excesivos, y deberá ser observado durante la recogida y posterior tratamiento de los datos, incluyendo la purga o eliminación. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
5. **Limitación de la conservación**. Los datos deben ser mantenidos de forma que no se permita la identificación de los interesados durante más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de

investigación científica o histórica o fines estadísticos. Las limitaciones al periodo de conservación están vinculadas con la extensión del tratamiento ya que la conservación de los datos es, en sí, una operación de tratamiento, así los responsables del tratamiento podrían tener razones legales legítimas para conservarlos durante un período mayor al requerido, esto puede darse, por ejemplo, para cumplir otras obligaciones legales o contractuales, o bien para proteger los derechos, la seguridad o los bienes de la persona, por ejemplo, en la situación de VCM los datos ingresados en la plataforma sobre hechos o situaciones anteriores de violencia pueden servir para levantar alertas o acciones de prevención. De todas formas, es preciso tener en cuenta que la aplicación del principio de minimización sobre el periodo de conservación establece que, si un dato personal no se necesita más después de ejecutar una fase del tratamiento, el dato deberá ser suprimido, sea a través del bloqueo, la anonimización o la eliminación.

6. **Seguridad y confidencialidad**. Lo datos deben ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

El conjunto de principios revisados se complementa con estándares que permiten validar o evidenciar que esos principios son observados. Entre ellos destacamos los siguientes.

1. **Consentimiento informado para compartir información**. El titular es dueño de los datos y puede optar por compartir o no sus datos. Es importante, por tanto, especialmente si, como en el caso, existen datos personales sensible obtener este consentimiento previamente.
2. **Políticas de acceso.** Considerando la naturaleza de la información involucrada y la necesidad de asegurar la confidencialidad y seguridad de la misma, será necesario definir niveles de autorización para las entidades y funcionarios en cada trámite y proceso, buscando desagregar información de modo que esta se brinde de la forma más simple y disociada posible respecto de la identidad de las personas en situación de violencia y especialmente de los niños, niñas y adolescentes. , procurando que la arquitectura de la plataforma transmita las respuestas en formato “si” o “no”, cuando sea posible.
3. **Infraestructura de gestión de la información**. A través de estos mecanismos es posible definir elementos de seguridad respecto del almacenamiento, acceso y transmisión de la información. Por ejemplo, el uso de números de identificación para mantener información anónima o un sistema con contraseñas de acceso cifrado.
4. **Evaluación de impacto o riesgo**. Una herramienta que no debe faltar al tratar datos es la elaboración de un informe sobre el impacto que el uso o la transferencia de los datos puede tener y si los riesgos y daños no son excesivos en relación con el impacto positivo de su uso.
5. **Protocolos de intercambio de información, interoperabilidad**. Obviamente disponer de estos protocolos, que pueden quedar consignados en convenios de colaboración entre los distintos agentes públicos que interoperan, es muy beneficioso para establecer las responsabilidades por el tratamiento de la información.
6. **Derecho a la explicabilidad**. Si eventualmente existen decisiones automatizadas, incluida la elaboración de perfiles de los titulares de datos, entregarse a esos titulares información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para su persona.
7. **Minimización, desagregación o anonimización de la información personal.** Como hemos dicho en la situación en estudio no es posible la anonimización, sin embargo, si es posible la desagregación o minimización, especialmente tratándose de su uso para análisis e informes estadísticos. Limitar los riesgos que las personas pueden ser identificadas se puede lograr también eliminando nombres, desagregando datos o disminuyéndolos al mínimo posible. Hay herramientas y directrices técnicas para lograr estos resultados.

Igualmente, revisamos aquí el estándar desarrollado por RGDPD Europeo en lo referido a la protección de datos personales por diseño. En efecto bajo el epígrafe 'Protección de datos desde el diseño y por defecto', incorpora a la normativa de protección de datos la práctica de considerar los requisitos de privacidad desde las primeras etapas del diseño de productos y servicios. De acuerdo con este estándar, aparecen las siguientes orientaciones y recomendaciones a tener en cuente en el diseño, implementación u operación de sistemas que utilicen información personal:

a) **Proactividad y prevención**. Identificar previamente los riesgos al derecho a la protección de datos personales de los titulares, propendiendo a una gestión adecuada, mediante su neutralización o mitigación.

b) **Protección predeterminada**. Proporcionar a los titulares de datos personales el más alto nivel de protección de sus datos por defecto y de manera automática en los sistemas de procesamiento de datos que desarrollen, implementen u operen.

c) **Funcionalidad total.** Comprender los sistemas de procesamiento de datos personales como sistemas funcionales eficaces y eficientes tanto respecto de su propósito principal que es el cumplimiento de su mandato legal, como respecto del derecho constitucional a la protección de datos personales.

d) **Seguridad punta a punta.** Proteger el ciclo completo del procesamiento de datos personales, desde su diseño, adoptando las medidas necesarias para garantizar la seguridad de la información (integridad, confidencialidad y disponibilidad) como el uso de cifrado en todo momento, la anonimización temprana, la definición de roles de acceso a datos, la destrucción segura de datos y el establecimiento de mecanismos para el ejercicio de los derechos de los titulares.

e) **Visibilidad y transparencia**. Adoptar las medidas de transparencia necesarias respecto a sus sistemas de procesamiento de datos personales, informando a los titulares sobre la recolección, procesamiento, eventual comunicación y purga de datos, a través de políticas legibles de protección de datos personales y mecanismos de notificación a titulares.

f) **Enfoque centrado en el usuario**. Esto significa que se deben adoptar sistémicamente todas las medidas necesarias para garantizar un efectivo control por parte del titular de los tratamientos de datos que se realicen y que le conciernan.

Tanto el Comité Europeo de Protección de Datos (EDPB)[9] como la Agencia Española de Protección de Datos (AEPD)[10] han desarrollado una Guías que incluyen técnicas y herramientas para el desarrollo de sistemas que cumplan con los estándares normativos, se recomienda una revisión exhaustiva previa a la construcción de cualquier plataforma que considere el tratamiento de datos personales.

A nivel nacional recogemos el estándar contenido en el numeral 17 de las Recomendaciones del Consejo para la Transparencia[11] sobre Protección de Datos Personales por parte de la Administración del Estado, contenidas en la Resolución N° 304 del año 2020 emanada del mismo Consejo para la Transparencia, en su calidad de órgano competente para promover la protección de datos personales, que señala textualmente:

*"**17. <u>RECOMENDACIONES SOBRE PROTECCIÓN DE DATOS PERSONALES POR DISEÑO</u>**.*

Si bien la Ley N°19.628 no contempla una regla especial que obligue implementar la protección de datos personales por diseño, y teniendo presente los principios de responsabilidad, eficiencia y eficacia en la Administración del Estado, el deber de velar por la eficiente e idónea administración de los medios

[9] EDPB. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.
[10] AEPD. Guía para la Protección de Datos por Defecto.
[11] Consejo para la Transparencia. Ver recomendaciones en:
https://www.consejotransparencia.cl/categoria_publicaciones/recomendaciones/

públicos y por el debido cumplimiento de la función pública, todos contenidos en el decreto con fuerza de ley N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, orgánica constitucional de bases generales de la Administración del Estado; y el derecho fundamental a la protección de datos personales, se recomienda a los órganos de la Administración del Estado desarrollar e implementar sus sistemas de procesamiento bajo los siguientes principios que inspiran la protección de datos personales por diseño:

***17.1. Principio de proactividad y prevención**. Es recomendable que los órganos de la Administración del Estado diseñen, implementen y operen sus sistemas de procesamiento de datos personales identificando previamente los riesgos al derecho a la protección de datos personales de los titulares, propendiendo a una gestión adecuada, mediante su neutralización o mitigación.*

***17.2. Principio de protección predeterminada**. Es recomendable que los órganos de la Administración del Estado proporcionen a los titulares de datos personales el más alto nivel de protección de sus datos por defecto y de manera automática en los sistemas de procesamiento de datos que desarrollen, implementen u operen.*

***17.3. Principio de protección desde el diseño**. Es recomendable que los órganos de la Administración del Estado incorporen la protección de datos personales como un componente esencial e indispensable de los sistemas de procesamiento de datos personales que desarrollen, implementen u operen, desde su diseño.*

***17.4. Principio de funcionalidad total**. Es recomendable que los órganos de la Administración del Estado comprendan sus sistemas de procesamiento de datos personales como sistemas funcionales eficaces y eficientes tanto respecto de su propósito principal (el cumplimiento de su mandato legal) como respecto del derecho constitucional a la protección de datos personales. Esto significa, entre otras cosas, que una aplicación sobre seguridad ciudadana debe ser eficiente y eficaz para ese propósito y a su vez, ser eficiente y eficaz en la protección de los datos personales. Se recomienda la existencia de reglas y mecanismos que permitan una coexistencia balanceada entre el resguardo y protección del derecho, y los objetivos de los mecanismos de procesamiento de datos.*

***17.5. Principio de seguridad punta a punta**. Es recomendable que los órganos de la Administración del Estado protejan el ciclo completo del procesamiento de datos personales, desde su diseño, implementación y operación, adoptando las medidas necesarias para garantizar la seguridad de la información (integridad, confidencialidad y disponibilidad) como el uso de cifrado en todo momento, la anonimización temprana, la definición de roles de acceso a datos, la destrucción segura de datos y el establecimiento de mecanismos para el ejercicio de los derechos de los titulares.*

***17.6. Principio de visibilidad y transparencia**. Es recomendable que los órganos de la Administración del Estado adopten las medidas de transparencia necesarias respecto a sus sistemas de procesamiento de datos personales, informando a los titulares sobre la recolección, procesamiento, eventual comunicación y purga de datos, a través de políticas legibles de protección de datos personales y mecanismos de notificación a titulares.*

***17.7. Principio de enfoque centrado en el usuario**. Es recomendable que los órganos de la Administración del Estado pongan en funcionamiento, en el nivel operacional, el mandato constitucional de tutela del derecho a la protección de los datos personales al momento de diseñar, implementar y operar un sistema de procesamiento de datos personales manteniendo un enfoque centrado en las personas. Esto significa que se deben adoptar sistémicamente las medidas necesarias para garantizar un efectivo control por parte del titular de los tratamientos de datos que se realicen y que le conciernan.".*

DIAGNÓSTICO

Tal como se señaló precedentemente, a partir de las respuestas al cuestionario, entrevista de levantamiento de información y entrevista de validación, se diagnosticó para cada una de las instituciones y servicios públicos, su situación dentro de la ruta crítica en relación con el registro y gestión de información sobre VCM.

Los principales hallazgos de este diagnóstico fueron: identificación del marco normativo que rige a la institución en materia de gestión de datos de VCM; identificación de los instrumentos de intercambio de información con otras instituciones vigentes; y el levantamiento de las principales barreras legales internas o externas, reconocidas por los actores, para compartir información.

Las instituciones involucradas en la ruta, y recogidas en el estudio, fueron:

- Policía de Carabineros de Chile
- Policía de Investigaciones de Chile (PDI)
- Servicio Nacional de la Mujer y Equidad de Género (SernamEG)
- Servicio Médico Legal (ML)
- Poder Judicial (PJ)
- Ministerio Público (MP)
- Subsecretaria de Prevención del Delito (SPD)
- Servicio Nacional de Menores (SENAME)
- Ministerio de Salud

DIAGNÓSTICO GENERAL

No obstante, el diagnóstico pormenorizado para cada entidad que se registra en la ficha individual presentada más adelante, de forma general se pudo establecer el siguiente diagnóstico observado permanentemente en todas o casi todas las instituciones:

1. Existe una visión compartida en los/las entrevistados sobre la importancia, beneficios y oportunidades para las víctimas y la propia labor de la institución en contar con información integrada y de calidad.
2. La disposición positiva para colaborar con el proyecto de las entidades. Algunas instituciones han resultado en mayor complejidad, debido a falta de tiempo o priorización del proyecto, en especial instituciones que resulta clave contar con su apoyo al más alto nivel como el Ministerio Público y Ministerio de Salud.
3. Los sistemas de información disponibles y utilizados por las instituciones para atender la prevención, persecución, reparación a personas sobrevivientes de violencia de género son distintos unos de los otros, tanto en sus formatos, herramientas utilizadas y calidad de la información disponible.
4. La información de las instituciones no se encuentra automatizada y centralizada en un sistema único, lo que conlleva a la existencia de diversos protocolos, criterios de ingreso o de validación, y forma de recuperación de esta.

5. Es necesario fortalecer el sistema de calidad de datos para dar mayor certeza de estos a las instituciones; siguiendo lineamientos internacionales sobre cómo trabajar la calidad de los datos, desde los instrumentos capaces de identificar violencia de género en atención primaria hasta los lineamientos para recopilar, acopiar y compartir data, así como también, elaborar indicadores de gestión.
6. El valor de la información no es compartido o entendido de igual forma por las autoridades de las entidades involucradas.
7. Existe una falta de recurso –humanos, financieros y tecnológicos- para cumplir adecuadamente con la demanda de los servicios y para la integración tecnológica de los sistemas de información.
8. Sería importante considerar la incorporación de Ministerio de Justicia y DD. HH y el Ministerio de Desarrollo Social y de la Familia para integrar información que sería crítica para la Hoja de Ruta de la Plataforma Integrada:
9. Sería importante incorporar en el Circuito o dentro de la asistencia técnica a la Subsecretaría de la Niñez y Subsecretaria de Servicios Sociales.
10. Es fundamental incorporar la percepción de los/as beneficiarios/as del sistema en la toma de decisiones, a través de sondeos de satisfacción usuaria y gestión de casos centrado en sobrevivientes; para que el Estado esté orientado en los clientes.

En el ámbito legal, por su parte y de manera también general, el diagnóstico validado concluyó lo siguiente:

1. Existen criterios de interpretación del marco legal institucional y nacional diversos para el intercambio de datos entre las instituciones.

   No existiendo una norma legal o política pública que obligue u autorice el intercambio o transferencia de datos entre las instituciones públicas involucradas en la atención, protección y reparación en caso de VCM, cada una de ellas, a través de sus unidades jurídicas (fiscalías, departamentos jurídicos, unidades jurídicas) interpreta la normativa vigente que les es aplicable, esto es su normativa orgánica, normas de protección de datos personales, normas de acceso a la información pública, resoluciones e instructivos de órganos fiscalizadores y garantes como la Contraloría General de la Repúblicas y el Consejo para la Transparencia.
2. Hay una opinión extendida de que toda la información de que disponen en sus sistemas es de carácter personal y por tanto no se puede compartir.

   Es una realidad que en los sistemas convive información personal, pero también existe información que tiene el carácter de información pública y por tanto está sujeta a las normas de acceso a la información pública y debe ser entregada cuando se solicita. De las respuestas a cuestionarios y entrevistas con las instituciones se pudo determinar que no tienen internalizada esta realidad y por tanto en general resguardan toda la información como personal.
3. Existen variados convenios de colaboración bilaterales y multilaterales entre las instituciones que acuerdan el intercambio de información en los ámbitos de sus competencias. Las instituciones hicieron constantemente referencia a distintos mecanismos e instrumentos jurídicos utilizados para el intercambio de información entre las instituciones (convenios, reglamentos, protocolos, etc.). Sin embargo, algunos de ellos no son conocidos o no se han implementado.

En efecto, resultó bastante difícil acceder al listado de convenios o acuerdos de colaboración, en general los funcionarios que trabajan en VCM los desconocen y algunos de ellos no han sido implementados. Casi todos nos refirieron al órgano jurídico para que nos enviaran esta información, pero esos órganos disponen de todos los convenios sin discriminación de la materia por lo que fue difícil determinar su vigencia y aplicación. Los convenios no tienen contrapartes especializadas que puedan hacer el debido seguimiento de implementación y resultado.

4. Las barreras legales para el intercambio de la información referidas por las instituciones son en general:

   a. Los tipos de datos que almacenan, datos personales, datos personales sensibles, datos de seguridad[12]. En las entrevistas sostenidas con las instituciones se pudo recoger que reconocen correctamente la tenencia y procesamiento de datos personales de los usuarios de sus servicios, pero solo algunas de ellas distinguen entre datos personales generales y datos sensibles, dado las distintas interpretaciones que hacen de la normativa existente, lo que afecta el nivel de protección, acceso y posibilidad de intercambio de estos. Tal como se señaló a propósito del marco normativo la posibilidad y los requisitos para el intercambio difieren tratándose de uno o de otro tipo de dato.

   b. Las competencias del órgano para compartir esos datos. Algunas de las instituciones aseguran no tener competencia para el tratamiento de datos personales provenientes de VCM por lo que a su juicio no podrían participar del intercambio de esta información. No obstante, el reconocimiento de esta barrera, en algunos casos se vislumbra también que la existencia de convenios de colaboración es una alternativa válida para participar del intercambio.

   c. La etapa del procedimiento en que se encuentra un caso que exige el secreto de las actuaciones. Los organismos con facultades investigativas reconocen como barrera el artículo 182 del Código Procesal Penal, el cual establece el secreto de las actuaciones de la investigación realizadas por el Ministerio Público y por la policía, para los terceros ajenos al procedimiento. A su entender esto impide intercambiar esta información, sin embargo, se debe dejar claro que el impedimento es para terceros ajenos y solo durante la etapa investigativa.

   d. La falta de consentimiento de los titulares de los datos. Como se ha señalado anteriormente el consentimiento es un elemento que habilita el uso y tratamiento de datos personales y constituye por tanto un requisito, no solo desde el punto de vista legal, sino también ético toda vez que los datos personales son de propiedad de sus titulares y no del servicio público que los recopila o intercambia.

   e. La necesidad de autorización por parte de las autoridades superiores del servicio. En alguna de las instituciones, a partir de prácticas o de normas o instructivos internos, se constató que el intercambio de información con otras instituciones debía ser autorizado no sólo por el jefe del servicio, sino por autoridades superiores, tales como Ministro de Estado e incluso en el caso de poder judicial, el propio pleno de la Corte Suprema. Entendemos que lo anterior principalmente al temor que albergan los funcionarios sobre la reserva de la información y a que no cuentan con el consentimiento de los titulares de los datos que almacenan.

5. Varias de las instituciones entrevistadas se encuentran en etapa de modernización o implementación de sistemas de información, pero no se observa un diseño legal de datos, que vele por la protección y seguridad de los datos, especialmente en contextos de intercambio.

[12] Tales como perfiles y claves de acceso

DIAGNÓSTICO POR INSTITUCIÓN

1. Policía de Carabineros de Chile	
Marco Normativo	• Constitución Política • Ley No. 18.961 • Artículo 182 del Código Procesal Penal, el cual establece el secreto de las actuaciones de la investigación realizadas por el Ministerio Público y por la policía, para los terceros ajenos al procedimiento. • Ley No. 19.628 Protección de la vida privada. Artículos 5,7,11,18, 20 y 21 • Ley No. 20.285, Acceso a la información pública • Decreto N° 14/2014 normas técnicas sobre documentos electrónicos, comunicaciones electrónicas e interoperabilidad del Estado de Chile
Convenios interinstitucionales	CONVENIO CIRCUITO INTERSECTORIAL DE FEMICIDIO (2009) CONVENIO TRANSMISIÓN DE INFORMACIÓN INTERINSTITUCIONAL (2016) partes transmisión de policiales, ordenes, contraordenes de detención y medidas cautelares CONVENIO INTERINSTITUCIONAL PROGRAMA 24 HORAS (2009) CONVENIO DE COLABORACIÓN INTERINSTITUCIONAL PARA LA APLICACIÓN DE LA PAUTA UNIFICADA DE EVALUACIÓN INICIAL DE RIESGO (2016) CONVENIO CON MUNICIPIOS POR MENORES EDAD INFRACTORES DE LEY
Principales Hallazgos	**Competencia para el tratamiento de datos**. La Constitución Política y las leyes orgánicas confieren a Carabineros de Chile competencias para el tratamiento de información sobre VCM y contienen obligaciones de secreto, reserva y confidencialidad respecto de datos personales. **Datos en poder de Policía de Carabineros.** Mantiene en sus sistemas información pública, reservada y secreta, con debilidades en el tratamiento de la información que pueden afectar calidad de la información (por ejemplo, registros manuales). **Convenios de colaboración** Tiene convenios de colaboración e intercambio de información con otros poderes públicos en el ámbito de VCM que consignan obligaciones de seguridad de la información y confidencialidad en su tratamiento. **Barreras internas.** Internamente se reconocen como barreras legales para el intercambio de información, el tipo de datos (personales y sensibles) que tratan, y el deber de "secreto de las actuaciones" que afecta a la información que recopilan. **Diseño legal de sistemas.** Se requiere implementación y cumplimiento de principios y estándares de protección de información personal en los sistemas de información disponibles.

2. Policía de Investigaciones de Chile (PDI)	
Marco Normativo	• Constitución Política • Ley Orgánica, Decreto Ley No. 2460, de 1979, en especial artículos 4º, 5º y 7º del establecen que los datos recopilados que contengan información personal de los usuarios sólo podrán ser proporcionados al Ministerio Público, los Tribunales de Justicia que la requieran, a los organismos de la Administración Pública a los cuales la Institución les preste su colaboración dentro del marco de sus competencias, y otros que estén por ley facultados para solicitarla. • Artículo 182 del Código Procesal Penal, el cual establece el secreto de las actuaciones de la investigación realizadas por el Ministerio Público y por la policía, para los terceros ajenos al procedimiento. • Ley No. 19.628 Protección de la vida privada. Artículos 5,7,11,18, 20 y 21 • Ley No. 20.285, Acceso a la información pública • Decreto Nº 14/2014 normas técnicas sobre documentos electrónicos, comunicaciones electrónicas e interoperabilidad del Estado de Chile
Convenios interinstitucionales	CONVENIO TRANSMISIÓN DE INFORMACIÓN INTERINSTITUCIONAL (2016) partes transmisión de policiales, ordenes, contraordenes de detención y medidas cautelares CONVENIO DE COLABORACIÓN INTERINSTITUCIONAL PARA LA APLICACIÓN DE LA PAUTA UNIFICADA DE EVALUACIÓN INICIAL DE RIESGO (2016) CONVENIO CIRCUITO INTERSECTORIAL DE FEMICIDIO (2017)
Principales Hallazgos	**Competencia para el tratamiento de datos**. La Constitución Política y las leyes orgánicas confieren a PDI competencias para el tratamiento de información sobre VCM y contienen obligaciones de secreto, reserva y confidencialidad respecto de datos personales. Jefatura Nacional de Informática y Telecomunicaciones es la responsable de cautelar y proteger la información registrada por los usuarios. **Datos en poder de PDI.** PDI mantiene en sus sistemas información pública, reservada y secreta con medidas de seguridad (política de privacidad, niveles acceso, respaldo etc.) **Convenios de colaboración** Tiene convenios de colaboración e intercambio de información con otros poderes públicos en el ámbito de VCM que consignan obligaciones de seguridad de la información y confidencialidad en su tratamiento. **Barreras internas.** Internamente se reconocen como barreras legales para el intercambio de información personal, los requisitos que deben cumplir las instituciones para suscribir un convenio de interoperabilidad, esto que el órgano requerido debe ser competente legalmente para tratar las materias objeto de solicitud y, por otra parte, para el órgano solicitante también dicha información debe estar dentro del ámbito de su competencia. También se señala como barrara al intercambio el período de "secreto de investigación" que afecta a la información que recopilan. **Diseño legal de sistemas.** Se requiere implementación y cumplimiento de principios y estándares de protección de información personal en los sistemas de información disponibles.

3. Servicio Nacional de la Mujer y Equidad de Género (SernamEG)	
Marco Normativo	• Constitución Política • Ley Orgánica No. 19023 • Ley No. 19.628 Protección de la vida privada. Artículos 5,7,11,18, 20 y 21 • Ley No. 20.285, Acceso a la información pública • Rex 258, de 2020 de Orientaciones Técnicas, contiene indicaciones con referencias al trabajo con registros administrativos y también refiere a la coordinación intersectorial e interinstitucional • Decreto Nº 14/2014 normas técnicas sobre documentos electrónicos, comunicaciones electrónicas e interoperabilidad del Estado de Chile.
Convenios interinstitucionales	CONVENIO CIRCUITO INTERSECTORIAL DE FEMICIDIO (2009) CONVENIO DE COLABORACIÓN INTERINSTITUCIONAL PARA LA APLICACIÓN DE LA PAUTA UNIFICADA DE EVALUACIÓN INICIAL DE RIESGO (2016)
Principales Hallazgos	**Competencia para el tratamiento de datos**. La Constitución Política y las leyes orgánicas confieren a SernamEG competencias para el tratamiento de información sobre VCM y contienen obligaciones de secreto, reserva y confidencialidad respecto de datos personales. **Datos en poder de SernamEG.** SernamEG mantiene en sus sistemas información pública, reservada y secreta, con debilidades de seguridad (planillas Excel) que pueden afectar calidad de la información. Jefes de regiones y jefes de áreas y programas centrales son responsables de cautelar y proteger la información registrada por los usuarios. **Convenios de colaboración** Tiene algunos convenios de colaboración e intercambio de información con otros poderes públicos en el ámbito de VCM que consignan obligaciones de seguridad de la información y confidencialidad en su tratamiento. **Barreras internas.** Internamente se reconocen como barreras legales para el intercambio de información, el tipo de datos, personales y sensibles que tratan como Servicio, por lo que señalan, en su opinión, es indispensable obtener el consentimiento informado. **Diseño legal de sistemas.** Se requiere implementación y cumplimiento de principios y estándares de protección de información personal en los sistemas de información disponibles.

4. Servicio Médico Legal (SML)	
Marco Normativo	• Constitución Política • Ley No. 20.065, en especial sus artículos 7 y 23 referidos al intercambio de información y al sigilo o reserva pericial. • Artículo 182 del Código Procesal Penal (CPP), el cual establece el secreto de las actuaciones de la investigación realizadas por el Ministerio Público y por la policía para los terceros ajenos al procedimiento. • Ley No. 19.628 Protección de la vida privada. Artículos 5,7,11,18, 20 y 21 • Ley No. 20.285, Acceso a la información pública • Decreto Nº 14/2014 normas técnicas sobre documentos electrónicos, comunicaciones electrónicas e interoperabilidad del Estado de Chile.
Convenios interinstitucionales	CONVENIO CIRCUITO INTERSECTORIAL DE FEMICIDIO (2017)
Principales Hallazgos	**Competencia para el tratamiento de datos**. La Constitución Política y las leyes orgánicas confieren al Servicio Médico Legal competencias en el tratamiento de información sobre VCM, pero establecen obligaciones de sigilo o reserva pericial. De acuerdo con su Ley Orgánica corresponde al Director del Servicio autorizar el intercambio de información técnica con otros organismos nacionales o internacionales que desarrollen actividades relacionadas con las funciones del SML, manteniendo la confidencialidad **Datos en poder de Servicio Médico Legal.** SML mantiene en sus sistemas información pública, reservada y secreta, con debilidades de seguridad que pueden afectar calidad de la información, por ejemplo, uso de planillas Excel o información recogida manualmente y transcrita posteriormente. **Convenios de colaboración.** Pertenece al CIF a través de convenio que permite la colaboración e intercambio de información con los otros poderes públicos en el ámbito de VCM y consigna obligaciones de seguridad de la información y confidencialidad en su tratamiento. **Barreras internas.** Internamente se reconocen como barreras legales para el intercambio de información, el tipo de datos, personales y sensibles que tratan como Servicio, el deber de sigilo pericial y de resguardar eventual secreto de la carpeta investigativa que lleva la Fiscalía según Art.182 del CPP. **Diseño legal de sistemas.** Se requiere implementación y cumplimiento de principios y estándares de protección de información personal en los sistemas de información disponibles.

5. Poder Judicial (Pjud)	
Marco Normativo	• Convención para la Eliminación de Todas las Formas de Discriminación en Contra de la Mujer (CEDAW) y de la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia Contra la Mujer (Belém do Pará) que expresamente refieren a la elaboración y difusión de datos estadísticos sobre violencia en contra de las mujeres y su abordaje en la justicia, ya sea por causas conocidas por los Tribunales de Familia o por Tribunales Penales • Política de Igualdad de Género y No Discriminación del Poder Judicial (2018). *"Promover la implementación de estrategias y mecanismos de registro y recolección de información en los sistemas informáticos de administración de causas del Poder Judicial, con perspectiva de género y derechos humanos, a objeto de contar con datos y estadísticas que permitan visibilizar el comportamiento del sistema judicial en relación a fenómenos como la violencia contra la mujer y la violencia y discriminación por orientación sexual y/o identidad de género, entre otros y adoptar las decisiones que correspondan, así como poner los datos a disposición de quienes tienen la iniciativa legislativa para determinar el curso de las políticas públicas en la materia"* • Constitución Política y su ley orgánica • Código Orgánico de Tribunales • Disposiciones orgánicas internas • Ley No. 19.628 Protección de la vida privada. Artículos 5,7,11,18, 20 y 21 • Ley No. 20.285, Acceso a la información pública • Decreto Nº 14/2014 normas técnicas sobre documentos electrónicos, comunicaciones electrónicas e interoperabilidad del Estado de Chile. • Pleno CS Resolución AD-1162-2016, que instruye la obligatoriedad de la anotación de la variable referida al sexo de las personas que intervienen en las causas que conocen los tribunales ordinarios
Convenios interinstitucionales	CONVENIO INTERINSTITUCIONAL PARA EL DISEÑO E IMPLEMENTACIÓN DE BANCO UNIFICADO DE DATOS EN EL MARCO DE PLAN DE SEGURIDAD PÚBLICA CHILE SEGURO (2012) MINISTERIO DE JUSTICIA Y SERVICIOS DEPENDIENTES CONVENIO DE INTEROPERABILIDAD (2014) CONVENIO TRANSMISIÓN DE INFORMACIÓN INTERINSTITUCIONAL (2016) partes transmisión de policiales, ordenes, contraordenes de detención y medidas cautelares Además de los referidos a instituciones que hacen parte de la ruta crítica de VCM, el Poder Judicial mantiene una variedad de convenios de colaboración e intercambios de información con otras múltiples instituciones públicas, como, por ejemplo, e Servicio de Registro Civil e Identificación, la Defensoría Penal Pública, y el Instituto Nacional de Estadísticas, entre otras.

Principales Hallazgos	**Competencia para el tratamiento de datos**. La Constitución Política y las leyes orgánicas otorgan al Poder Judicial competencias para el tratamiento de información sobre VCM y obligaciones de reserva y confidencialidad respecto de datos personales sensibles. De acuerdo con normas orgánicas internas la responsabilidad sobre los sistemas informáticos de administración de causas, el Departamento de Informática de la Corporación Administrativa del Poder Judicial. **Datos en poder de Poder Judicial.** El Poder Judicial mantiene en sus sistemas SITFA y SIAGJ Información pública (sistema penal, salvo excepciones), reservada (causas de familia) y secreta (NNA) con altas medidas de seguridad (niveles de acceso, respaldo, etc.) **Convenios de colaboración** El Poder Judicial mantiene múltiples convenios de colaboración e intercambio de información con los otros poderes públicos, no solo en el ámbito de VCM y consigna obligaciones de seguridad de la información y confidencialidad en su tratamiento. **Barreras internas.** Internamente se reconocen como barreras legales para el intercambio de información disposiciones de reserva en virtud de protección de datos personales y resguardo privacidad de intervinientes, pero se reconoce igualmente que es posible el intercambio de información dentro del ámbito de sus competencias y siempre que se celebran los respectivos convenios interinstitucionales, los que requieren concurrencia de autoridades de las instituciones. Se reconoce como principal proveedor – cliente de información al Ministerio Público, pues la información que mantiene es la que permite mayor trazabilidad en lo que respecta a situaciones de violencia contra la mujer, sin embargo, reconocen falta normativa y voluntad política para la interoperabilidad. **Diseño legal de sistemas.** Se requiere implementación y cumplimiento de principios y estándares de protección de información personal en los sistemas de información disponibles.

6. Ministerio Público (MP)	
Marco Normativo	• Constitución Política y norma orgánica Ley No. 19.640, en especial artículo 8 que deriva la información de los actos relativos a o relacionados con la investigación, el ejercicio de la acción penal pública y la protección de víctimas y testigos, al Código Procesal Penal (CPP). • CPP, en especial artículo 182 el cual establece el secreto de las actuaciones de la investigación realizadas por el Ministerio Público y por la policía para los terceros ajenos al procedimiento. • Ley No. 19.628 Protección de la vida privada. Artículos 5,7,11,18, 20 y 21 • Ley No. 20.285, Acceso a la información pública • Decreto Nº 14/2014 normas técnicas sobre documentos electrónicos, comunicaciones electrónicas e interoperabilidad del Estado de Chile.
Convenios interinstitucionales	CONVENIO CIRCUITO INTERSECTORIAL DE FEMICIDIO (2017) CONVENIO TRANSMISIÓN DE INFORMACIÓN INTERINSTITUCIONAL (2016) partes transmisión de policiales, ordenes, contraordenes de detención y medidas cautelares CONVENIO DE COLABORACIÓN INTERINSTITUCIONAL PARA LA APLICACIÓN DE LA PAUTA UNIFICADA DE EVALUACIÓN INICIAL DE RIESGO (2016)
Principales Hallazgos	**Competencia para el tratamiento de datos**. La Constitución Política, la ley orgánica otorgan al Ministerio público facultades para el tratamiento de información sobre VCM, pero se establecen obligaciones de confidencialidad y reserva. **Datos en poder de Ministerio Público.** MP mantiene en sus robustos sistemas información pública, reservada y secreta, con medidas seguridad. Sin embargo, también dispone de información en planillas Excel que pueden afectar la calidad de la información. **Convenios de colaboración.** Pertenece al CIF a través de convenio que permite la colaboración e intercambio de información con los otros poderes públicos en el ámbito de VCM y consigna obligaciones de seguridad de la información y confidencialidad en su tratamiento. **Barreras internas.** La ausencia de especialización en los distintos actores que deben intervenir en la violencia contra la mujer: Desde la Policía, pasando por la Fiscalía los Tribunales de Familia y Penales. No hay un proceso penal y proteccional especial lo que implica una intervención especializada parcial enfocada en la violencia contra la mujer. Especialmente la falta de una norma general sobre violencia de género reúna toda la normativa, la cual se encuentra muy dispersa, actualmente se tramita en el congreso Ley sobre violencia contra la mujer, que debe ampliar a lo que es género también. **Diseño legal de sistemas.** Se requiere implementación y cumplimiento de principios y estándares de protección de información personal en los sistemas de información disponibles.

7. Subsecretaría de Prevención del Delito (SPD)	
Marco Normativo	• Constitución Política • Ley Orgánica No. 20.502 que establece su responsabilidad en la coordinación en materia de prevención del delito • Ley No. 19.628 Protección de la vida privada. Artículos 5,7,11,18, 20 y 21 • Ley No. 20.285, Acceso a la información pública • Decreto Nº 14/2014 normas técnicas sobre documentos electrónicos, comunicaciones electrónicas e interoperabilidad del Estado de Chile.
Convenios interinstitucionales	CONVENIO CIRCUITO INTERSECTORIAL DE FEMICIDIO CONVENIO INTERINSTITUCIONAL PARA EL DISEÑO E IMPLEMENTACIÓN DE BANCO UNIFICADO DE DATOS EN EL MARCO DE PLAN DE SEGURIDAD PÚBLICA CHILE SEGURO (2012)
Principales Hallazgos	**Competencia para el tratamiento de datos**. La Constitución Política y las leyes orgánicas a la SPD competencias para el tratamiento de información y coordinación de acciones para la prevención del delito y obligaciones de reserva y confidencialidad respecto de datos personales sensibles. **Datos en poder de Secretaría de Prevención del Delito.** SPD mantiene en sus sistemas Información pública, reservada y secreta (NNA), pero falta de estandarización de los sistemas de registro puede afectar la calidad de los datos almacenados. **Convenios de colaboración.** Mantiene convenios de colaboración con otros poderes públicos para el registro de delitos de VCM, estableciendo su rol de coordinación. Los convenios en general consignan obligaciones de seguridad de la información y confidencialidad en su tratamiento. **Barreras internas.** Reconoce como barrera las disposiciones de reserva en virtud del derecho de protección de datos personales y resguardo privacidad de víctimas, se estima que es posible el intercambio de información cumpliendo normativa y tomando resguardos como el consentimiento informado. **Diseño legal de sistemas.** Se requiere implementación y cumplimiento de principios y estándares de protección de información personal en los sistemas de información disponibles.

8. Servicio Nacional de Menores (SENAME)	
Marco Normativo[13]	• Convención sobre Derechos del Niño (D.S. No. 830, de 1990, RREE) • Constitución Política y Decreto Ley No. 2.465, de 1979, que crea el Servicio Nacional de Menores y fija el texto de su ley orgánica (artículos 3 No. 9, 15, 5 No. 10, 8 No. 3) • Ley No. 20.032, que establece Sistema de atención a la niñez y adolescencia a través de la red de Colaboradores Acreditados del Servicio Nacional de Menores, y su régimen de subvención. En él se establecen en artículo 22 obligación de reserva de información. • Ley No. 19.628 Protección de la vida privada. Artículos 5,7,11,18, 20 y 21 • Ley No. 20.285, Acceso a la información pública • Decreto Nº 14/2014 normas técnicas sobre documentos electrónicos, comunicaciones electrónicas e interoperabilidad del Estado de Chile.
Convenios interinstitucionales	CONVENIO CIRCUITO INTERSECTORIAL DE FEMICIDIO (2009) CONVENIO INTERINSTITUCIONAL PARA EL DISEÑO E IMPLEMENTACIÓN DE BANCO UNIFICADO DE DATOS EN EL MARCO DE PLAN DE SEGURIDAD PÚBLICA CHILE SEGURO (2012) CONVENIO DE COOPERACIÓN INTERINSTITUCIONAL CORPORACIÓN ADMINISTRATIVA DEL PODER JUDICIAL, MINISTERIO DE JUSTICIA Y SERVICIO NACIONAL DE MENORES (2014)
Principales Hallazgos	**Competencia para el tratamiento de datos**. La Constitución Política, las leyes orgánicas y sectoriales otorgan al SENAME competencias para el tratamiento de información sobre VCM y obligaciones de reserva y confidencialidad respecto de datos personales sensibles. **Datos en poder de Servicio Nacional de Menores.** SENAME mantiene en sus sistemas Información pública, reservada y secreta (NNA) con problemas de medidas de seguridad producto de la manualidad que pueden afectar la calidad de los datos **Convenios de colaboración.** SENAME Mantiene diversos convenios de colaboración e interoperabilidad con otros poderes públicos. Los convenios en general consignan obligaciones de seguridad de la información y confidencialidad en su tratamiento. **Barreras internas.** Aunque se reconocen las disposiciones de reserva en virtud de protección de datos personales y resguardo privacidad de intervinientes, se estima que es posible el intercambio de información cumpliendo normativa y tomando resguardos. Reconocen también barreras de carácter ético y social, pues el control social a las labores efectuadas por los organismos públicos puede verlo en términos negativos. Se deberían establecer límites claros y objetivos específicos para el uso de esta información, solo en beneficio de las mujeres. **Diseño legal de sistemas.** Se requiere implementación y cumplimiento de principios y estándares de protección de información personal en los sistemas de información disponibles.

[13] Es preciso considerar al respecto la Ley N° 21.302, publicada con posterioridad a las entrevistas y aún no vigente, que crea el Servicio Nacional de Protección Especializada a la Niñez y Adolescencia, órgano sucesor y continuador legal del Servicio Nacional de Menores.
Artículo 31 dispone la creación de un sistema integrado de información, seguimiento y monitoreo.
Artículos 32 a 34 contienen los deberes de reserva y confidencialidad respecto de la información.

9. Ministerio de Salud	
Marco Normativo	• Constitución Política • DFL 1/2005, Salud. Artículo 4 No. 5 regula facultades del Ministro de Salud para tratar datos con fines estadísticos y mantener registros o bancos de datos respecto de las materias de su competencia y tratar datos personales o sensibles con el fin de proteger la salud de la población o para la determinación y otorgamiento de beneficios de salud. • Ley No. 20.584, regula los deberes y derechos que tienen las personas en relación con acciones vinculadas a su atención de salud. Artículo 12 y 13, que señalan carácter sensible de los datos contenidos en la ficha clínica. • Decreto N° 41/2012, Salud, que establece normas referidas a la información contenida en las fichas clínicas, la que puede ser electrónica, en papel o en cualquier otro soporte, siempre que los registros sean completos y aseguren el oportuno acceso, conservación y confidencialidad de los datos, así como la autenticidad de su contenido y de los cambios efectuados en ella. • Ley N° 21.057 que regula entrevistas grabadas en video y otras medidas de resguardo a menores de edad, víctimas de delitos sexuales • Código Procesal Penal artículo 175 d) que establece obligación de denuncia de hechos de violencia • Ley N° 19.628 Protección de la vida privada. Artículos 5,7,11,18, 20 y 21 • Ley N° 20.285, Acceso a la información pública • Decreto Nº 14/2014 normas técnicas sobre documentos electrónicos, comunicaciones electrónicas e interoperabilidad del Estado de Chile.
Principales Hallazgos	**Competencia para el tratamiento de datos**. La Constitución Política y las leyes orgánicas Constitución y leyes orgánicas y sectoriales otorgan al MINSAL competencias para el tratamiento de información sobre VCM y obligaciones de reserva y confidencialidad respecto de datos personales sensibles. **Datos en poder de Ministerio de Salud.** MINSAL mantiene en sus sistemas Información pública, reservada y secreta (NNA). En procesos de atención de salud por exámenes médicos y pericias relacionadas se dispone de entrevistas grabadas en video y, otras medidas de resguardo a menores de edad, víctimas de delitos sexuales, para evitar toda consecuencia negativa, previniendo con ello el proceso de victimización secundaria. **Convenios de colaboración.** Es factible celebrar convenios de colaboración e interoperabilidad, previo análisis y trabajo conjunto que permita definir y describir conjuntos mínimos de datos a los que esperan acceder o recabar. **Barreras internas.** Cumplimiento de obligación de denuncia de hechos de violencia que constituyan delitos constituye en ocasiones una barrera para el levantamiento de información por parte de profesionales dada las cargas legales que impone el sistema (declaración, testimonio, etc.) **Diseño legal de sistemas.** Se requiere implementación y cumplimiento de principios y estándares de protección de información personal en los sistemas de información disponibles.

NUDOS CRÍTICOS AL INTERCAMBIO DE INFORMACIÓN EN EL ÁMBITO LEGAL

A partir del análisis del contexto normativo nacional e internacional, los estándares internacionales recogidos y del diagnóstico expuesto, se definieron los siguientes nudos críticos a ser abordados en la propuesta de solución legal.

1. **Seguridad y calidad de la información.** Se identifican riesgos en la calidad de la información asociados a la manipulación manual de algunos registros, y también al vaciado de información a sistemas para consolidaciones posteriores. Algunos registros no cuentan con sistemas de seguridad de respaldo de la información afectando la calidad y seguridad de la data[14].
2. **Falta de consentimiento de registro de información personal.** No se recoge sistemática ni formalmente el consentimiento de las víctimas para el tratamiento de información personal[15].

A partir de estos nudos críticos se desarrolló en conjunto con las instituciones participantes del diagnóstico, un proceso de cocreación colaborativo y participativo[16], que originó recomendaciones y requerimientos que constituirán la hoja de ruta en la construcción de una plataforma integrada de información de VCM. Al efecto, en consenso se estableció:

- **Que es necesario automatizar y uniformar la carga de datos en los sistemas, generar validaciones automáticas con datos provenientes de bases de datos oficiales**. Se requiere interoperabilidad, trazabilidad y auditorías a los sistemas. Esto se desarrolla también en informe de Tecnologías de la Información.
- **La necesidad de capacitaciones, motivación desde lo ético, lo vocacional y el compromiso institucional y responsabilidad sobre los registros**. Generar protocolos o manuales de ingreso, lenguaje común entre las instituciones, entendimiento de requerimiento de la necesidad de la información. Evitar duplicidades y multiplicidad de datos no requeridos.
- **Se requiere consentimiento escrito e informado para usar y compartir información personal evitando transgredir oposición de mujeres que no desean ser contactadas**. Personas que dan primera acogida deben estar capacitadas y respetar principio de finalidad. Es preciso distinguir la obligación de denuncia del uso de la información para prevención y acompañamiento. También distinguir datos para prevención personalizada y datos para informes estadísticos o medidas de prevención general, lo que deben ser anonimizados.
- **La necesidad de institucionalización para compartir datos**, seguridad de información, trazabilidad, sistema de perfiles y privilegios para acceso o edición, auditorías para establecer responsabilidades, protocolos de intercambio en convenios o normas.

---

[14] Al respecto se copia evidencia recogida en las entrevistas de la consultoría:
"Nuestros sistemas no permiten intercambiar información con otras instituciones e incluso entre nuestros propios sistemas" "Hay veces que las denuncias se recogen en papel y luego cuando hay tiempo se traspasan al sistema" "las denuncias se envían en papel a tribunales" "Llevo una planilla Excel con toda la información consolidada, cuando se requiere traspaso las celdas nuevas al sistema nacional" "Mi planilla está completa, así que me doy cuenta cuando llega información que faltan registros" "son tantas columnas que por ejemplo, hace días me demoré mucho tiempo buscando una información que no encontraba y que se había borrado accidentalmente" "Nosotros no tenemos acceso al sistema por lo que pedimos a otra institución que la registre en el sistema nacional" "La recolección de datos que puede estar disponible para diversos organismos, a través del sistema interoperable, debiese encontrarse delimitada y regulada mediante un convenio, que establezca específicamente los objetivos de dicha plataforma, y cómo ello puede aportar al cumplimiento de las funciones de los organismos involucrados" "Es importante establecer que este sistema interoperable solo funcionaría en beneficio de las mujeres que han sufrido violencia y no tendrá otros efectos de carácter negativo para ellas, como revictimización o como un medio para sufrir otros ataques, ni menos, para denostarlas".

[15] Al respecto se copia evidencia recogida en las entrevistas de la consultoría:
"En la pauta unificada es el único caso en que se pide a las mujeres su autorización para que las contacten para acompañamiento" "No preguntamos a las mujeres si autorizan a compartir la información" "Se debe tener presente que nunca se puede afectar los derechos de las personas, particularmente tratándose de su seguridad, su salud, esfera de la vida privada o derechos económicos entre otros" "Es indispensable informar a las usuarias que accedan a los dispositivos que sus datos serán entregados a un sistema, al que podrán acceder determinadas Instituciones indicando de manera clara y precisa en que se utilizarán dichos datos". "En cuanto a la recopilación de datos, se debe contar con un consentimiento informado firmado por el titular de esos datos, en ese caso no existiría vulneración a las normas de protección de datos de las personas"

[16] Resultados Taller de Trabajo "Hoja de Ruta para la creación de una Plataforma Integrada de Gestión de Casos de Violencia de Género Contra la Mujer", realizado el 23 de noviembre de 2020 con participantes de las 9 instituciones, consultores y mandantes.

PROPUESTA LEGAL DE HOJA DE RUTA PARA LA CONSTRUCCIÓN DE UNA PLATAFORMA INTEGRADA

CONTEXTO DE LA PROPUESTA

La presente propuesta recoge las recomendaciones el proceso de cocreación señalado precedentemente, el marco normativo nacional, los estándares y modelos internacionales recogidos en el informe, así como la experiencia en el diseño legal de plataformas integradas de información.

Como observamos en el diagnóstico de la situación nacional, de manera general, la recogida de datos de VCM en general se realiza, para registrar la prestación de servicios o trámites por cada institución, y por tanto la gestión integral interinstitucional de esos datos para la prevención, el monitoreo, y evaluación de la propia VCM o de los programas asociados presenta debilidades y dificultades (CIF u otros) o no existe.

El proceso de cocreación por su parte insistió sobre la necesidad de avanzar hacia el establecimiento o fortalecimiento de los registros de VCM de manera de convertir, a través de una gestión integral transversal, los datos recopilados por proveedores de servicios y funcionarios de las distintas instituciones que interactúan con mujeres en situación de violencia y perpetradores, en datos útiles especialmente a la prevención. También se concluyó que este proceso debe incluir todo el ciclo de la información (recopilación, almacenamiento, análisis y entrega o traspaso) y todos los actores que desempeñan algún rol en el proceso.

Según señalamos anteriormente, la hoja de ruta de UN Women en materia de fortalecimiento de los registros administrativos sobre VCM propone:

a) Mapear actores y roles
b) Establecer coordinación y gobernanza
c) Capacitar
d) Establecer e implementar estándares y sistemas para recopilación, ingreso, validación y análisis de datos
e) Informar

Revisada la ruta, vemos que responde al trabajo que se ha venido realizando por el conjunto de asistencia técnica del Banco Mundial, así que proponemos insertar esta hoja de ruta en ese contexto.

Desde el punto de vista legal, si bien cada una de estas etapas que se comprenden en el diseño lógico y físico de una plataforma podrían involucrar decisiones que tienen algún componente jurídico, el enfoque que recogemos es la ruta a seguir para establecer e implementar los principios y estándares necesarios para lograr la correcta inserción de una plataforma integrada de gestión de casos de VCM en el ordenamiento jurídico nacional. Se agregan también algunas recomendaciones y sugerencias sobre lineamientos técnico-jurídicos que estimamos necesarios para apoyar la implementación.

HOJA DE RUTA LEGAL PARA UNA PLATAFORMA INTEGRADA

A partir del trabajo realizado, se propone la siguiente hoja de ruta de diseño legal de la plataforma, la que contempla los siguientes pasos:

1. Institucionalización de la coordinación y gobernanza de la información de VCM
2. Formalización de la articulación entre las instituciones para el intercambio de datos
3. Diseño de protocolo del consentimiento de titulares de datos
4. Diseño seguridad de la información y acceso de usuarios
5. Diseño trazabilidad y auditoria de la plataforma

A continuación, se revisan las acciones que las tareas señaladas contemplan y como señalé precedentemente, algunos lineamientos técnico-jurídicos, a modo de recomendaciones a evaluar en el diseño lógico y físico de la plataforma.

1. Institucionalización de la coordinación y gobernanza de la información de VCM

Al respecto, entendemos que la plataforma debe contar con gobernanza que le permita coordinar a los actores, articular firma de convenios o alianzas para el intercambio de la información, participar de las decisiones que requiere la consolidación del sistema y su integración a otras plataformas de monitoreo y seguimiento de la violencia en el país. Con eso en mente, las tareas que deben llevarse a cabo para esta institucionalización son:

- Definir rol y responsabilidad de institución coordinadora
- Definir instituciones actuales y potencialmente colaboradores de la plataforma
- Redactar y formalizar mediante acto jurídico

La recomendación al respecto es usar el modelo de la norma reciente aprobada, Ley N° 21.302, que crea el Servicio Nacional de Protección Especializada a la Niñez y Adolescencia, que dispone la creación de un sistema integrado de información, seguimiento y monitoreo, adecuarlo e incorporarlo en el proyecto de ley en tramitación sobre el derecho de las mujeres a una vida libre de violencia, contenido en el boletín 11077-07.

2. Formalización de la articulación entre las instituciones para el intercambio de datos

El establecimiento y la formalización de esta articulación, a través de convenios de intercambio de información, se hace necesaria, dado el tipo de datos que incluye el intercambio, de igual modo resulta importante para definir responsabilidades de las instituciones que entregan o reciben los datos.

- Definir instrumentos (convenios, resoluciones)
- Definir protocolos de intercambio (normas técnicas del Decreto 14/2014)
- Diseñar modelos de formato de convenio
- Definir y validar comparecientes y responsables de convenio
- Formalizar y difundir
- Hacer seguimiento.

En la práctica, se entiende que el mejor modelo para este intercambio es el de la interoperabilidad, es decir, la puesta en común de la información que recopila y procesa cada institución, mediante la comunicación de datos entre los sistemas de que disponen. Ahora bien, para lograr una arquitectura de interoperabilidad adecuada se requiere la adhesión a estándares comunes y considerar además una arquitectura multicapa, que resuelva y especifique cada uno de los siguientes elementos en detalle:

- Ventanilla única o punto de contacto estandarizado, consistente y eficiente, que permita acceder a la información de un determinado servicio en tiempo real.
- Interoperabilidad organizacional, es decir, coordinación y alineamiento entre los procesos y la información de diferentes instituciones de manera de ojalá no duplicar información.
- Interoperabilidad semántica, para asegurar el entendimiento en el significado de cada componente del proceso de intercambio de información y por tanto la existencia de estructuras estándares. Por ejemplo, que el campo sexo o edad esté categorizado de la misma manera en los sistemas.
- Interoperabilidad técnica, es decir, la definición de los componentes tecnológicos necesarios para lograr el modelo de interoperabilidad adoptado.

Los sistemas actuales de registro de VCM para lograr esta interoperabilidad tienen el desafío de ajustarse a las directrices nacionales en la materia contenidas en el Decreto N° 14, Economía, de 2014, que establece las Normas Técnicas y Estándares para los Documentos Electrónicos e Interoperabilidad de los mismos, las Normas Técnicas para las Comunicaciones Electrónicas, y las Normas sobre la Fijación de Esquemas y Metadatos de los Documentos Electrónicos Empleados por los Órganos de la Administración del Estado, que ya hemos reseñado anteriormente y las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de la Administración del Estado, contenidas en la Resolución N° 304 del año 2020 emanada del mismo Consejo para la Transparencia en su calidad de órgano competente para promover la protección de datos personales.

3. Diseño del protocolo de consentimiento y acceso de usuarios

En el proceso de cocreación se relevó como un factor crucial para la implementación de la plataforma, contar con el consentimiento escrito e informado de los usuarios para usar y compartir su información personal. Personas que dan primera acogida deben estar capacitadas y respetar principio de finalidad informando adecuadamente a los titulares de los datos sobre sus derechos a acceder, rectificar, cancelar u oponerse al tratamiento (derechos ARCO) en cualquier momento. Es preciso distinguir la obligación de denuncia del uso de la información para prevención y acompañamiento.

Como parte del diseño legal de cualquier sistema que involucra datos personales sensibles esta actividad también resulta crucial, pues de no existir consentimiento no es posible tratarlos ni menos intercambiarlos. Al respecto, en consecuencia, se proponen las siguientes tareas:

- Identificar la información personal en la gestión de casos de VCM
- Definir instancias en que se requiere consentimiento (tipo de datos, finalidad)
- Diseñar protocolo para que las personas que dan primera acogida informen y respeten el principio de finalidad informando adecuadamente a los titulares de los datos sobre sus derechos.
- Diseñar modelo de formato de consentimiento que contemple información para el usuario acerca de la finalidad y usos de su información personal.
- Diseñar acceso y ejercicio derechos ARCO de titulares de datos

La finalidad del sistema de gestión integrado de información será proveer los datos necesarios para el seguimiento de las mujeres víctimas de violencia que son atendidas por el respectivo órgano, y el monitoreo de las medidas que se apliquen, para tomar las más adecuadas respecto a la situación particular de cada una de ellas, proveyendo las alertas necesarias para su protección. Asimismo, se podrá utilizar por los órganos del Estado con competencias en materias de mujer, género o presupuestarias que hayan celebrado un convenio de transferencia de datos con el servicio, para la asignación y racionalización de las prestaciones financiadas por el Estado, el estudio y diseño de políticas, planes, programas y prestaciones, y el análisis estadístico que la gestión del organismo requiera.

La sugerencia en esta materia, siguiendo las Recomendaciones del Consejo para al Transparencia sobre Protección de Datos Personales por parte de la Administración del Estado contenida en el numeral 7.2 de la Resolución N° 304 del año 2020[17], es desarrollar una formación en protección de datos personales a funcionarios que forman parte de los equipos de atención y también para quienes forman parte del ciclo de estos datos, pues serán las prácticas adecuadas en la materia las que permitan disponer de los datos para la prevención de VCM, evitar filtraciones ilícitas, pero especialmente asegurar a los titulares la protección y seguridad de su información de manera de evitarles consecuencias indeseadas que conculquen sus derechos fundamentales.

4. Diseño seguridad de la información y acceso de usuarios

Para evitar las posibles derivaciones de la responsabilidad en el tratamiento de datos personales por organismos públicos, que involucra el intercambio electrónico de información, se requiere tomar medidas que garanticen la seguridad jurídica y técnica de la información y de la infraestructura tecnológica involucrada. Estas medidas implican el establecimiento de un esquema de seguridad que contemple:

- Revisar roles y responsabilidades levantadas en los procesos asociados a datos para identificar qué entidades autorizadas para intervenir en un proceso o actividad de tratamiento de datos a través de la plataforma, a partir de sus competencias y la finalidad que motiva el requerimiento y utilización de los datos (tipos de datos, finalidad del tratamiento).
- Definir los funcionarios que estarán autorizados para ejecutar las tareas relacionadas con el intercambio de información personal, para establecer los accesos asociados a esos roles.
- Definir nivel de "identificabilidad" de los datos: identificable (nombre), codificado (seudónimo o número de caso separado del nombre) y anonimizado (agregado sin nombres) de manera de identificar los datos para prevención personalizada y datos para informes estadísticos o medidas de prevención general, lo que deben ser anonimizados o al menos codificados.
- Establecer medidas obligatorias de ciberseguridad para los datos y responsabilidad y sanciones por la pérdida o deterioro.
- Definir tiempos de conservación de la información y métodos de eliminación.
- Establecer obligaciones y deberes de confidencialidad de acuerdo con rol y acceso.
- Formalizar los roles, sus derechos, obligaciones y responsabilidad mediante acto jurídico.

[17] 7.2 Requerimientos para el tratamiento de datos. Los órganos o servicios públicos deben sujetarse para el tratamiento de los datos, según el artículo 20, a las reglas establecidas en la Ley N°19.628. En consecuencia:
f) Los órganos o servicios públicos deberán formar, capacitar y entrenar a sus funcionarios en el cumplimiento de las disposiciones de la Ley N°19.628 y respecto del nuevo derecho fundamental a la protección de datos personales, de manera de cumplir con el mandato constitucional de promover y proteger efectivamente los derechos consagrados en la Constitución y en los tratados internacionales ratificados por Chile y que se encuentren vigentes.

Como vemos, es clave para el funcionamiento adecuado de la operación de intercambio de información la definición de las entidades, procesos y tramites en que se integran servicios a través de un esquema de administración de autorizaciones y usuarios; por lo que la recomendación es examinar en cada caso las competencias y la finalidad de cada tratamiento de datos, sin que esto obste para la modificación o incorporación de nuevos criterios respecto a procesos o entidades que se sumen a la iniciativa. También se deben definir plazos para mantener la información en los sistemas y los métodos de eliminación o envío a registros históricos.

A un nivel técnico recomendamos desagregar información de modo que esta se brinde de la forma más simple y disociada posible respecto de los datos de identidad de los ciudadanos, como por ejemplo separar RUT de otros datos que pueden o no identificar a una persona, como sexo, edad, domicilio.

Se recomienda también definir un oficial o delegado de protección de datos personales para los sistemas de información que interoperen, el que deberá acompañar y apoyar el tratamiento de datos una vez implementada la plataforma. Actualmente existe en el Congreso Nacional el proyecto de ley número de boletín 11144-07 que exige esta figura a instituciones que realizan actividades de tratamiento de datos personales y del mismo modo lo recomienda el numeral 16 de las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de la Administración del Estado contenida en el numeral 7.2 de la Resolución N° 304 del año 2020[18].

5. Diseño de la trazabilidad y auditoria de la plataforma

Dado los objetivos relevantes que una plataforma integrada de gestión de casos de VCM cumpliría y de lo importante que resulta la calidad de la información procesada e intercambiada para la vida presente y futura de las mujeres, resulta imprescindible definir herramientas e instrumentos que permitan hacer trazabilidad y auditoria a la misma en cualquier instancia, sea para mejora continua de la misma, o sea para determinar la responsabilidad objetiva respecto de su uso y funcionamiento.

En esto contexto, creemos relevante establecer algunas tareas orientadas a esto logro.

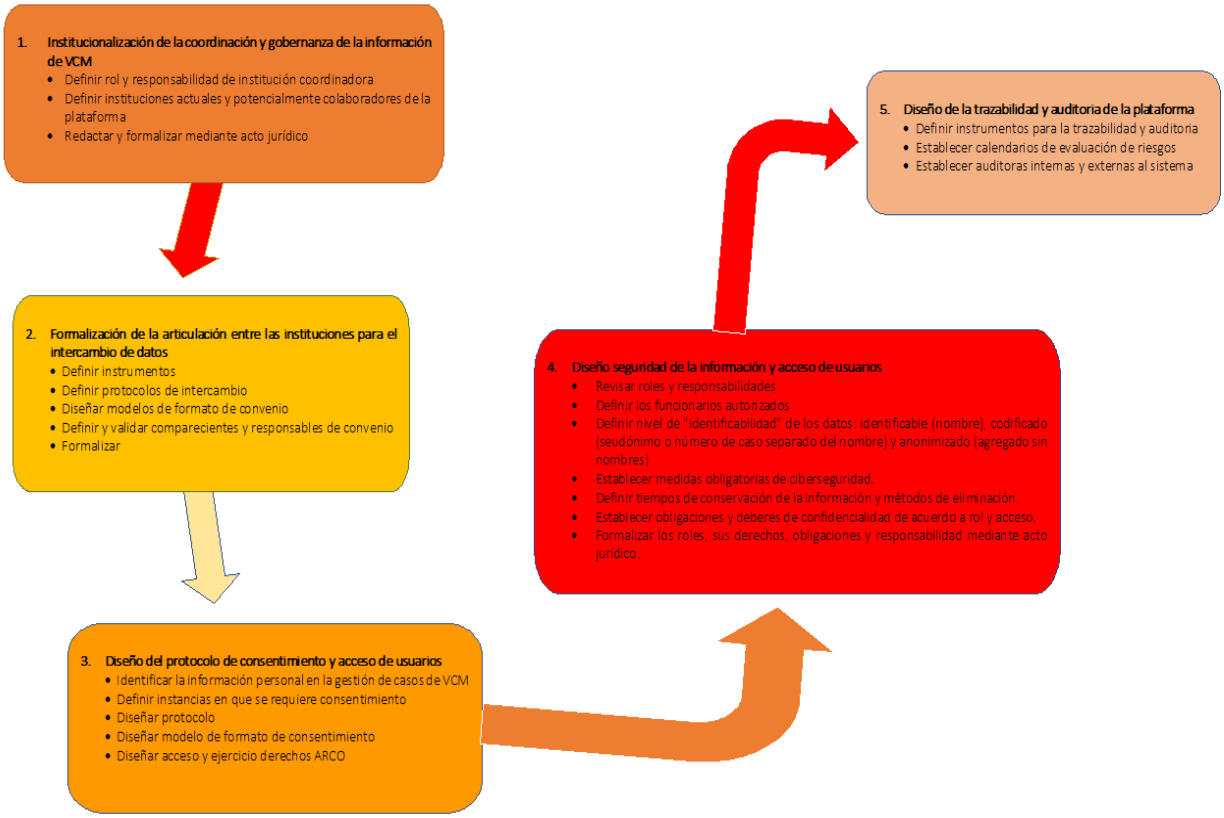
- Definir instrumentos para la trazabilidad y auditoria
- Establecer calendarios de evaluación de riesgos
- Establecer auditoras internas y externas al sistema

Estas tareas permitirán demostrar la responsabilidad objetiva de cada una de las instituciones en el tratamiento de los datos que debe recoger y resguardar.

La recomendación en la materia es avanzar en Compliance de Protección de Datos, herramienta que también está ad-portas de ser incorporada en el marco normativo de protección a través del proyecto de ley en actual tramitación.

[18] DELEGADO DE PROTECCIÓN DE DATOS. Para facilitar el cumplimiento de las obligaciones establecidas en la Ley N°19.628 y una mejor observancia de las presentes Recomendaciones, se sugiere que las distintas autoridades, jefaturas o jefes superiores de los órganos o servicios de la Administración del Estado, designen a un funcionario o funcionaria de dicha repartición para desempeñarse como delegado o delegada de protección de datos.

DIAGRAMA HOJA DE RUTA LEGAL



REFERENCIAS BIBLIOGRÁFICAS

TEXTO BIBLIOGRÁFICOS

AEPD. Agencia Española de Protección de Datos (2020). *Guía para la Protección de Datos por Defecto.* Disponible en: https://www.aepd.es/es/documento/guia-proteccion-datos-por-defecto.pdf

AEPD. Agencia Española de Protección de Datos (2019). *Guía Consecuencias administrativas, disciplinarias, civiles y penales de la Difusión de Contenidos Sensibles.* Disponible en: https://www.aepd.es/es/documento/consecuencias-administrativas-disciplinarias-civiles-penales.pdf

CEPAL. Comisión Económica para América Latina y el Caribe y otros (2007). *Libro Blanco de Interoperabilidad de Gobierno Electrónico para América Latina y el Caribe*. Santiago, Chile

CIDH. Comisión Interamericana de Derechos Humanos, Relatoría sobre los Derechos de las Mujeres (2015). *Acceso a la información, violencia contra las mujeres y la administración de* justicia *en las Américas.* Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/mujer_y_LE/D%C3%ADa%20Internacional%20de%20AIP/Documento%20Acceso%20a%20la%20informaci%C3%B3n%20-%20Final%20(con%20conclusiones%20y%20recomendaciones)%20(3).pdf

COLOMBIA. Ministerio de Salud y Protección Social. (2015). *Sistema unificado de información para violencias de género con énfasis en violencia sexual*. Disponible en: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VS/PP/suivge-sispro-minsalud.pdf

COLOMBIA. Entidades coordinadoras del Sistema Integrado de Información sobre Violencias de Género (2015) *SIVIGE. Sistema unificado información violencias de Género con énfasis en violencia sexual. Marco Normativo, Conceptual y Operativo.* Disponible en: https://www2.unwomen.org/-/media/field%20office%20colombia/documentos/publicaciones/2016/sivige_final_web.pdf?la=es&vs=1633

DIPRES. Dirección de Presupuesto (2017). *Informe final de evaluación programa de prevención integral de la violencia contra las mujeres y programa de atención, protección y reparación integral de violencias contra las mujeres ministerio de la mujer y equidad de género servicio nacional de la mujer y equidad de género*. Disponible en: http://www.dipres.gob.cl/597/articles-163129_informe_final.pdf

EDPB. European Data Protection Board (2020). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Disponible en: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

EIGE. European Institute for Gender Equality (2019). *Improving police and justice data on intimate partner violence against women in the European Union.* Disponible en: https://eige.europa.eu/gender-based-violence/data-collection#2017

EIGE. European Institute for Gender Equality (2016). *Administrative data collection on violence against women −Good practices.* Disponible en: https://eige.europa.eu/publications/administrative-data-collection-violence-against-women-good-practices

MOYA, Rodrigo (2007). *Informe sobre Tratamiento de Datos Personales por Organismos Públicos*. Minuta de Trabajo para la Superintendencia de Seguridad Social, documento proporcionado por el autor. Santiago, Chile.

OCHOA, Sergio y otros (2009). *Documentación electrónica e interoperabilidad de la Información.* Santiago, Chile: Universidad de Chile.

UNIÓN EUROPEA (2016). *Reglamento General de Protección de Datos Personales.* Disponible: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

UN WOMEN. United Nations Entity for Gender Equality and the Empowerment of Women (2020). *Background paper: A synthesis of evidence on the collection and use of administrative data on violence against women.* Disponible en: https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/synthesis-of-evidence-on-collection-and-use-of-administrative-data-on-vaw-en.pdf?la=en&vs=4056

UN WOMEN. United Nations Entity for Gender Equality and the Empowerment of Women (2015) *Essential Services Package for Women and Girls Subject to Violence.* Disponible en: https://www.unwomen.org//media/headquarters/attachments/sections/library/publications/2015/essential-services-package-en.pdf?la=en&vs=720

TEXTOS LEGALES NACIONALES

CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE CHILE. Disponible en: https://www.leychile.cl/Navegar?idNorma=242302

CONVENCIÓN INTERAMERICANA PARA PREVENIR, SANCIONAR Y ERRADICAR LA VIOLENCIA CONTRA LA MUJER (BELEM DO PARÁ). Disponible en: http://www.oas.org/juridico/spanish/tratados/a-61.html

CONVENCIÓN SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACINÓ CONTRA LA MUJER (CEDAW). Disponible en: https://www.ohchr.org/sp/professionalinterest/pages/cedaw.aspx

CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO. Disponible en: https://www.ohchr.org/sp/professionalinterest/pages/crc.aspx

CÓDIGO PROCESAL PENAL. Ley N° 19.696. Disponible en: https://www.leychile.cl/Navegar?idNorma=176595

CÓDIGO SANITARIO. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=5595

LEY SOBRE PROTECCIÓN DE LA VIDA PRIVADA. Ley N° 19.628. Disponible en: https://www.leychile.cl/Consulta/Navegar?idNorma=141599

LEY SOBRE ACCESO A LA INFORMACIÓN PÚBLICA. Ley N° 20.285. Disponible en: https://www.leychile.cl/Consulta/Navegar?idNorma=276363

LEY SOBRE TRANSFORMACIÓN DIGITAL DEL ESTADO. Ley N° 21.180. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1138479 (Aún no vigente)

LEY QUE CREA LOS TRIBUNALES DE FAMILIA. Ley N° 19.968. Disponible en: https://www.leychile.cl/Navegar?idNorma=229557

LEY DE VIOLENCIA INTRAFAMILIAR. Ley N° 20.066. Disponible en: https://www.leychile.cl/Consulta/Navegar?idNorma=242648

LEY QUE CREA EL SERVICIO NACIONAL DE PROTECCIÓN ESPECIALIZADA A LA NIÑEZ Y ADOLESCENCIA. Ley N° 21.302. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1154203 (Aún no vigente)

LEY ORGÁNICA CONSTITUCIONAL DE BASES GENERALES DE LA ADMINISTRACIÓN DEL ESTADO. DFL N° 1, 2001, Ministerio Secretaría General de la Presidencia, que refunde a la Ley N° 18.575. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=191865

ESTATUTO ADMINISTRATIVO. DFL N° 29, 2005, Ministerio de Hacienda, que refunde a la Ley N° 18.834. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=236392

DECRETO N° 14, 2014, Ministerio de Economía. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1059778

RESOLUCIÓN N° 304, 2020, Consejo para la Transparencia. Disponible en:https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/12/N%C2%B0304-Aprueba-el-texto-actualizado-y-refundido-de-las-recomendaciones-del-CPLT-sobre-Proteccio%CC%81n-de-Datos-Personales.pdf