Consejo Federal
para la Transparencia

Lineamientos para la formulación de un

Plan de Protección de Datos Personales

Año 2023

AAIP
Transpa rencia
Acceso a la Información Pública
Protección de Datos Personales

Argentina
Presidencia

Autoridades
del Consejo Federal para la Transparencia:

Beatriz de Anchorena
Presidenta

María Lucrecia Escandón
Vicepresidenta

Analía Zimmermann Sánchez
Secretaria Ejecutiva

Comisión de trabajo
“Gobernanza de Datos y Protección de la privacidad”:

Jorge Piccoli (Buenos Aires)
Coordinador

Ángel Vázquez (Neuquén), Bruno Rezzoagli (Santa Fe), Carolina Zelko (San Juan), Cintia Aguado (Tierra del Fuego), Claudia Pereyra (Chaco), Diego De Francesco (CABA), Eduardo Irigoyte (Buenos Aires), Eduardo Peduto (CABA), Flavia Goldcher (CABA), Gastón Fingerman (Buenos Aires), Gerardo Cambiagno (Córdoba), Laura Chamia (La Rioja), Mariela Dolce (Chaco), Marcelo Augusto Caliva (La Rioja), Marina Briongos (Neuquén), Matías Paniagua (Chaco), Nicolás Caballero (Tierra del Fuego), Pablo Martos (CABA), Rocío Valiente (Chaco), Tania Álvarez (Santa Fe), Yanina Vallejos (Chaco).
Integrantes

Lineamientos para la formulación de un

Plan de Protección de Datos Personales

Año 2023

Autoría:

Consejo Federal para la Transparencia.

Redacción del documento:

Jorge Orovitz y Anastasia Dozo.

Colaboración:

Representantes del CFT y de la Comisión “Gobernanza de Datos y Protección de la privacidad”

Dirección Nacional de Protección de Datos Personales
Violeta Paulero

Dirección de Promoción del Derecho a la Privacidad
Anastasia Dozo
Guadalupe Mercado

Consejo Federal para la Transparencia
Sara Iuliano.

Diseño y arte de tapa:

Vanina Farías.

¿Cómo citar este material?

Consejo Federal para la Transparencia (2023), Lineamientos para la formulación de un Plan de Protección de Datos Personales. Buenos Aires: Agencia de Acceso a la Información Pública.

Índice

1. Introducción

El Consejo Federal para la Transparencia (CFT) es un organismo que está constituido por un representante de cada una de las provincias y un representante de la Ciudad Autónoma de Buenos Aires, este tiene como objetivo la cooperación técnica entre las distintas jurisdicciones y la concertación de políticas públicas de transparencia y de protección de datos personales a nivel federal.

La creación del Consejo fue determinada a partir del artículo 29 de la Ley 27.275 de Acceso a la Información Pública, que contempla que el Consejo tendrá su sede en la Agencia de Acceso a la Información Pública (AAIP), de la cual recibirá apoyo administrativo y técnico para su funcionamiento, a partir de un enfoque integral a fin de lograr una mejor calidad de vida de la ciudadanía.

En el estatuto del Consejo se detalla que este organismo interjurisdiccional de carácter permanente será presidido por el director de la Agencia de Acceso a la Información Pública y este deberá convocar al menos semestralmente a una Asamblea Ordinaria en donde se evaluará el grado de avance en materia de transparencia activa, acceso a la información y protección de datos personales en cada una de las jurisdicciones.

En ese marco, durante la IX Asamblea General Ordinaria del CFT celebrada en el Salón de los Pueblos Originarios de la Casa Rosada en la Ciudad Autónoma de Buenos Aires, se votaron y conformaron tres comisiones de trabajo: Transparencia, Gobernanza de Datos y Protección de la Privacidad, y Formación, Comunicación y Participación Ciudadana.

En la Comisión de Gobernanza de Datos y Protección de la Privacidad el primer desafío fue elaborar un Informe sobre la actualización de la Ley de Protección de Datos Personales desde una perspectiva federal, que permitió que las jurisdicciones del Consejo puedan brindar aportes y comentarios sobre las necesidades y desafíos a la hora de llevar a cabo la gobernanza de los datos personales a nivel jurisdiccional.

La actualización de la Ley de protección de Datos Personales propone dar respuestas a los desafíos constantes que presenta la actualización tecnológica y la brecha digital, a su vez pretende armonizar estándares regionales e internacionales, desde una mirada situada y soberana, afianzando un camino hacia una Argentina más federal.

Durante el año 2023 la comisión se enfocó en la construcción de este segundo documento con eje en la formulación de un Plan de protección de datos personales para el sector público.

El Estado en sus distintos niveles y el conjunto del sector público son hoy los actores que mayor cantidad de datos personales recopilan, almacenan o procesan. Cada vez más, las organizaciones públicas reconocen en los datos personales un activo estratégico. Nadie puede concebir una Estado inclusivo, eficaz, eficiente sin un tratamiento masivo de datos personales. El tratamiento de estos datos permite mejorar las prestaciones, acortar los tiempos, ser más eficientes y, en general, dota de mayor capacidad para lograr impactos sociales, económicos y ambientales para el bienestar de los ciudadanos.

Cuando hablamos de tratamiento de datos personales cada vez más lo estamos asociando a las nuevas tecnologías disponibles, como la inteligencia artificial y la inferencia de datos, que permiten no sólo mejorar la calidad de los servicios sino formular con más precisión el tipo y el alcance de las políticas públicas, proyectar incidencias y resultados.

Al mismo tiempo que abre enormes oportunidades para el mejoramiento de las políticas públicas, implica también enormes responsabilidades y riesgos, pues el tratamiento de datos personales tiene implicancias en lo que hace a la seguridad, privacidad, y potenciales sesgos discriminantes. Es por eso que para el sector público es clave seguir los lineamientos legales y de responsabilidad pro activa. Al representar al conjunto de la comunidad, tiene mayor responsabilidad y pone en juego, a cada paso, su legitimidad, reputación y credibilidad. En este sentido, hay mucho por hacer. Nos proponemos con este documento avanzar hacia la formulación de planes de protección de datos personales que contribuyan y faciliten la implementación de una cultura de la privacidad en cada uno de los organismos públicos.

2.
Marco legal

El marco legal que brinda la base del ordenamiento jurídico en materia de protección de datos personales es la ley 25.326 del año 2000. Aunque es importante su actualización, sin embargo, nos da las herramientas para poder implementar un "Plan de protección de datos personales". A eso le tenemos que sumar el decreto reglamentario 1558 del 2001, y todas las resoluciones de la Agencia de Acceso a la Información Pública en tanto autoridad de aplicación, así como las disposiciones de la Dirección Nacional de Protección de Datos Personales previa a la conformación de la Agencia. En particular, la Resolución 40/18 sobre la política modelo para organismos públicos; la resolución 47/18, sobre medidas de seguridad recomendadas; y la resolución 255/22, que reúne el criterio orientador de mejores prácticas respecto a los datos genéticos.

La protección de datos personales y su marco normativo es obligatorio tanto al sector privado como público. Pero en lo que respecta a la realización de un Plan de protección de datos personales, el sector público tiene características propias que es necesario tomar en cuenta a la hora de su formulación.

La diferencia fundamental reside en que el Estado se encuentra facultado para tratar los datos personales en el marco de las funciones propias del organismo. Por lo tanto, la base legal para el tratamiento de datos personales no es el consentimiento como en el caso de los responsables privados sino el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, o una relación contractual, entre otras.

Pero es necesario remarcar que este hecho no implica de ninguna manera relativizar o disminuir la obligación del sector público y de cada uno de sus organismos de cumplir con la ley. Al revés, por sus propias funciones, tiene un deber legal y ético de cumplir y hacer respetar la ley y sus normas complementarias, y mostrarle a la sociedad que realiza un debido tratamiento de los datos personales.

Cumplir con la ley incluye, por ejemplo, el deber de informar, de adoptar medidas de seguridad, de proteger de manera reforzada los datos sensibles, de notificar incidentes de seguridad, de registrar las bases de datos en el Registro Nacional, entre otras.

3.
Definición de dato personal

Los datos son personales cuando permiten identificar a la persona, ya sea de manera directa o indirectamente, mediante uno o varios elementos característicos de su identidad, ya sea físicos, biológicos, fisiológicos, económicos, culturales, genéticos, etc. En estos casos se aplica la ley 25.236. Estos datos personales pueden ser muy variados. Puede ser el nombre y apellido, profesión, datos de contacto, correo electrónico, información financiera. O cualquier información que permita llevar adelante la ejecución del contrato, como el nombre y apellido, número de cuenta bancaria, condición frente al IVA, etc.

También hay datos personales como los relativos a opiniones políticas, origen étnico, convicciones religiosas, información referente a la salud y la orientación sexual, que son un tipo especial de datos personales, llamados sensibles. También los datos genéticos y biométricos, que tienen una relevancia creciente, son datos sensibles. El sistema de inteligencia artificial involucra en muchos casos datos genéticos o datos biométricos como el reconocimiento facial. La resolución 255/22 de la AAIP establece que los datos genéticos se consideran datos personales de carácter sensible, siempre que identifiquen de manera unívoca a una persona física y de ellos se pueda desprender o revelar información que sea relativa a la salud o a la fisiología del titular o cuyo uso pueda resultar potencialmente discriminatorio para su titular.

4.
La protección de los datos personales como un derecho humano

Hoy en día consideramos la protección de datos personales como un derecho humano. Esto no siempre fue así. En la ley 25.326 se incorpora en el artículo 1 a las personas jurídicas además de las personas físicas, lo que creó una confusión. En las legislaciones más modernas y en el Proyecto de ley queda aclarado el asunto al establecer que la protección de la ley se centra en las personas y se establece que es un derecho humano.

Y el otro cambio paradigmático que tiene el proyecto de ley, es que la ley vigente apunta hacia la protección del dato personal que esté asentado en archivos. El proyecto de ley encara la protección de las personas titulares de los datos. Ya no se enfoca en el dato, sino en la persona titular de los datos. No es una ruptura con la ley 25.326, pero sí es una actualización acorde a los cambios de la realidad, de la tecnología y del enfoque que hoy se tiene del tema.

Por lo mismo, el proyecto de ley también ahonda en la **autodeterminación informativa** como un concepto fundamental en la protección de datos personales, que se refiere al derecho que tienen las personas de tener control sobre la información que comparten y cómo se utiliza esa información. Este principio se basa en la idea de que las personas tienen el derecho de tomar decisiones informadas y conscientes sobre el manejo de su información personal.

5.
Plan de protección de datos personales en el sector público

Una Plan de protección de datos personales en el sector público establece las políticas, procedimientos y prácticas que un organismo debe seguir para gestionar los datos personales de manera responsable y ética. Se trata de un documento integral que guía a una organización en la gestión adecuada de los datos personales que maneja, asegurando el cumplimiento de las normas y especificando las medidas de responsabilidad pro activa que tomará para asegurar el manejo adecuado y seguro de los datos personales.

El mismo debe estar documentado y ser revisado y auditado de manera periódica. El Plan debería:

- Definir los objetivos específicos del organismo en la materia.
- Identificar las leyes y normativas de protección de datos personales que son aplicables.
- Establecer las vías de recolección los datos personales, qué tipo de dato personal se recopila y el flujo interno de los mismos, identificando las áreas y responsables.
- Definir las bases legales del tratamiento de los datos personales.
- Describe las medidas técnicas y organizativas que se implementarán para proteger los datos personales.
- Establecer los plazos de conservación.
- Detallar la forma en que el organismo garantizará de manera práctica que los titulares de los datos puedan ejercer sus derechos.
- Definir las modalidades de capacitación del personal en el manejo seguro y responsable de datos personales y cómo se promoverá la concienciación sobre la privacidad.
- Establecer un plan de acción para el caso de un incidente de seguridad, que incluya notificación a las autoridades y a las personas afectadas.
- Definir los procesos de supervisión interna y la forma en que se garantizará el cumplimiento continuo de las políticas y procedimientos establecidos.
- Implementar la responsabilidad pro-activa: enfoque preventivo y cultura de la privacidad. Implica la designación de un Delegado de Protección

de Datos, la realización de una evaluación de impacto cuando se requiera, elaboración de un plan de respuesta a incidentes, formación y concienciación, monitoreo y auditoría, revisión del Plan y mejora continua.

- Implementación de una política de privacidad. Se trata de un documento redactado de manera clara y sencilla que un organismo produce y divulga para informar a los titulares de los datos cómo se recopilan, utilizan, procesan y protegen sus datos personales, así como los derechos que los asisten y otra información que también debe estar disponible para las personas. La política de privacidad es fundamental para cumplir con las regulaciones y establecer una base de confianza con los titulares de los datos.

Un Plan debe comenzar por la pregunta sobre qué datos tratamos, para qué los recolectamos y para qué los usamos. Estas preguntas nos dan las herramientas para determinar si realmente esa cantidad de datos son necesarios para el objetivo que se tiene o el plazo de conservación. Si se solicitan más datos que los necesarios para el fin establecido no estamos cumpliendo con el principio de minimización, que nos exige recolectar sólo los datos estrictamente necesarios para cumplir las funciones que nos impone la ley. Cuando se formula una Plan desde el sector público, es muy importante tener esta mirada estratégica, la capacidad del organismo para definir qué datos son los necesarios y cuál es la finalidad.

Al mismo tiempo, el plan debe tener un diseño que incluya el flujo de los datos personales. Esto es, se debe conocer el recorrido de los datos a través de los sistemas y procesos de la empresa. Generalmente sigue un proceso que implica la recopilación, el almacenamiento, el procesamiento y la eventual eliminación o retención de estos datos. Es importante saber por dónde entran, podría ser por un formulario en la web, registros de clientes, interacciones personales o cualquier otro medio en el que se recopile información personal. Por lo general en un organismo hay múltiples entradas de distintos datos personales con distintas finalidades. Es importante, entonces, conocer el flujo completo. También es necesario saber quiénes reciben y procesan los mismos, qué personal está en contacto con ellos, quiénes son los responsables de cada una de esas áreas, en resumen, conocer toda la cadena de valor de los datos personales y su ciclo de vida. Esto nos ayuda a construir un Plan adecuado, conociendo al detalle todas las etapas del tratamiento de los datos personales. Las organizaciones deben ser transparentes sobre cómo recopilan, almacenan y utilizan estos datos, y esta actitud pro activa facilita tomar medidas proactivas para proteger los datos de posibles riesgos y amenazas.

Respecto a los plazos de conservación mencionados anteriormente, por ley puede establecerse la necesidad de conservación de la documentación por cierta cantidad de años, como sucede con los datos personales en el sistema

financiero. En ese sentido, una vez cumplida una finalidad, se puede, eventualmente, conservar por más tiempo los datos personales. Pero el plazo establecido debe ser congruente y proporcional a los establecido por la ley y por los objetivos propuestos. Y estos objetivos y los plazos de conservación deben estar justificados ante la autoridad de aplicación.

Otro tanto sucede con los derechos de acceso, supresión o rectificación, que pueden ser denegados en función de una ley superior, por ejemplo de Defensa Nacional, o si hay una investigación judicial en curso. En estos casos la denegación de los derechos del titular debe estar fundada y comunicada.

Sin cumplir esta exigencia, no se alcanza el objetivo final que es tener política pública de calidad.

En el caso de los archivos que guardan documentación de interés público pueden conservar los datos personales, siempre que cumplan con todas las restantes exigencias de la ley.

Otro tema que en el Estado tiene relevancia es la investigación científica o estadística, porque en la medida que haya algún procedimiento de disociación de los datos, pueden ser utilizados. Si las actividades estadísticas están realizadas conforme la ley de censos, no aplica la ley de protección de datos personales.

Toda la información que se debe ofrecer al titular de los datos se reúne en lo que se denomina **política de privacidad**.

6.
Política de privacidad

La política de privacidad es un componente fundamental de un plan de protección de datos en el sector público. Es la forma de cumplir con el deber de informar, es el documento que nos permite darle esa información al titular de los datos. Para el privado también es la forma más importante, por naturaleza, para recoger su consentimiento.

La información debe incluir las finalidades del tratamiento, los datos que se recolectan, los derechos que asisten a los titulares y cómo se pueden ejercer, el derecho de iniciar un reclamo ante la Agencia de Acceso a la Información Pública, los plazos de conservación, aclarar que se toman medidas de seguridad acordes al tratamiento de los datos, el registro de la base de datos, las cesiones que se hagan, si hacemos transferencias internacionales, los datos de contacto para la formulación de reclamos, el derecho de iniciar una acción frente a la Agencia de Acción de la Información Pública.

Para su formulación, recomendamos tomar como guía la resolución 40/18 referida a la política modelo de protección de datos en el sector público. La Resolución establece una serie de pautas para la elaboración de una política de privacidad en el sector público. Se trata sólo de una guía que obviamente puede y debe ser adaptada a las condiciones específicas de cada organismo. El mismo se presenta como un formulario genérico a ser completado por cada organismo.

Las pautas son:

1. Objeto: informa que la política de privacidad aplica a todo el tratamiento del organismo público.

Aplica a todo el tratamiento de los datos personales y se debe detallar de qué organismo se trata.

2. Identificación de tratamientos: informa el canal o los canales por los que se recopilan los datos.

La forma de recolectar información puede ser diversa, personalmente en mesa de entradas o por otros canales, como formularios, por vía telefónica, mediante sistemas informáticos y/o sitios en Internet, cesión de terceros, entre otros. También hace referencia al tipo de datos que se utilizan ¿Qué datos uso? ¿Para qué los uso?

3. Inscripción: informa que las bases de datos personales a su cargo se encuentran inscriptas ante el Registro Nacional de Base de Datos (RNBD).

El Registro es obligatorio por la ley 25.326, y se implementó desde el 2006. Dispone que todo archivo, registro, base o banco de datos personales público o privado debe inscribirse en el Registro. La Resolución 132 de 2018 establece que se realiza por única vez mediante la plataforma "Trámites a Distancia" (TAD) o sistema de Gestión Documental Electrónica (GDE). Se debe registrar tanto la base de datos como el responsable del mismo. Los organismos públicos pueden tener muchas bases de datos, por ejemplo, una de recursos humanos, otra de videovigilancia, una base de datos de proveedores, de usuarios, etc. Es necesario inscribir cada una de ellas.

4. Finalidad y calidad: informa las bases legales sobre las que se apoya el tratamiento de los datos y el compromiso del organismo de velar por la calidad de los mismos.

Aunque un organismo público puede recabar el consentimiento de los titulares de los datos, la base legal para su tratamiento es el interés público normado por la legislación vigente. Por lo tanto, se debe informar el ámbito de su competencia, las leyes y normas complementarias sobre las que se apoya para el cumplimiento de sus competencias. Puede suceder que el tratamiento de los datos se realice también para el cumplimiento de una obligación legal, que sea necesario para la ejecución de un contrato o que resulte necesario para salvaguardar la vida de la persona.

En cuanto a la calidad de los datos personales, la ley plantea que los mismos deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

5. Caducidad: informa el plazo de conservación por el que serán tratados y luego destruidos o archivados los datos conforme a la normativa específica del organismo. Una vez que los fines para el que fueron recolectados los datos han finalizado, estos deben eliminarse. Es fundamental que en cada organismo se estudie en detalle los plazos de conservación y eliminación o archivo de cada una de las bases de datos.

Pueden conservarse durante períodos más largos siempre que se trate exclusivamente de fines estadísticos, de archivo en interés público, de investigación científica o histórica, pero siempre teniendo en cuenta la aplicación de las medidas técnicas y organizativas apropiadas con el fin de proteger los derechos de los titulares. También pueden conservarse por imposiciones legales.

6. Confidencialidad: informa la existencia de convenios de confidencialidad con parte del personal, o terceros que presten servicios y accedan al contenido de las bases de datos.

Cada organismo debe adoptar medidas de confidencialidad y medidas técnicas de seguridad, que están asociadas. Por ejemplo, puede ser que un organismo deba convenir con los empleados que trabajan con bases de datos sensibles, cláusula de confidencialidad, donde hay un compromiso de no revelar datos, ni copiarlos, ni usarlos con otros fines, etc. También hay un aspecto educativo, para capacitar al personal respecto de la necesidad de cuidar sus claves, y de todo lo que hace a la preservación de la información y de la base de datos.

7. Seguridad: informa que el organismo adopta medidas necesarias para garantizar la seguridad de los datos personales. También informa que en caso de detectarse un incidente de seguridad que implique un riesgo significativo, se comunicará sin dilación con la autoridad de aplicación y que tomará medidas correctivas y paliativas.

Garantizar la seguridad y confidencialidad de cada dato es un aspecto central del tratamiento de los datos personales. Uno organismo debe tomar medidas para evitar la pérdida de la información, la consulta o tratamiento no autorizado, y detectar acciones no permitidas, ya sean intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

La resolución 47/ 2018 de la AAIP, plantea una lista de medidas recomendadas de seguridad que se pueden implementar, relacionadas a la seguridad y la completitud e integridad de los datos recolectados, la minimización de errores, la limitación del acceso no necesario para asegurar la confidencialidad; el control de los accesos definiendo responsables y responsabilidades, verificación y aplicación de controles, gestión de accesos, asignación de permisos, verificación de identidad, monitoreo, establecer procedimientos para el respaldo y la recuperación, gestión de vulnerabilidades, detección de incidentes de seguridad, y gestión de los mismos, entre otras medidas.

Las medidas de seguridad deben ser implementadas en relación al riesgo de seguridad que corren esos datos, y que dependen de su volumen y del tipo de datos que sean. Una vez que se establece la categoría de datos a tratar, se deben diseñar las medidas de seguridad acordes que se deben implementar. También debe tener un plan de contingencia y de diseño de políticas y procedimientos frente a un incidente para implementar medidas de mitigación del daño.

En el caso de que un organismo sufra una brecha de seguridad en su organización, se debe notificar a la Dirección Nacional de Ciberseguridad. Pero, en la medida que haya datos personales involucrados, se debe también no-

tificar a la autoridad de aplicación y es recomendable que se notifique a los titulares de los datos, de modo tal de darle herramientas para minimizar los daños. En la resolución 47, también hay una pequeña guía que explica en qué forma hay que notificar esas incidencias, que la Agencia está actualizando.

La política de privacidad no debe tener un listado de las medidas que un organismo ha diseñado en su plan de protección de datos personales. Basta con informar al titular que se implementó medidas acordes para cuidar sus datos personales.

8. Cesión de datos personales: informa que los datos podrán ser cedidos a otros organismos del Estado en forma directa, en la medida que el cesionario lo requiera en el marco de su competencia y que el tratamiento sea compatible con sus funciones. También informa cuando haya cesiones a particulares y de qué tipo, y que se dará a publicidad los convenios existentes con terceros.

Definimos a las cesiones como cualquier mecanismo que proporcione acceso a una base de datos a un tercero. La Ley 25.326 menciona específicamente las cesiones de datos en el artículo 11, inciso 1, cuando permite que los datos personales pueden ser cedidos siempre que se cumpla con los fines que están relacionados con los intereses legítimos del cedente el responsable y del cesionario encargado. En el caso de los privados, sólo se pueden ceder con el previo consentimiento del titular. En el caso de los organismos públicos, como ya hemos visto, la base legal del tratamiento es otra, por ejemplo, el interés público fundado en una ley, o por razones de salud pública, de emergencia o de investigaciones epidemiológicas, etc.

Todas las cesiones que realice el organismo en tanto responsable a un encargado de tratamiento deben ser informadas a los titulares, incluida la finalidad y quién es el cesionario y toda otra información relevante.

Para tener políticas públicas de calidad, van a ser necesarias las sesiones entre organismos. Es la base, por ejemplo, de la interoperabilidad. Pero deben realizarse en el marco de las competencias. Es una buena práctica firmar convenios de colaboración entre organismos donde se determinen todas las cuestiones referidas a los fines, medidas de seguridad, base legal y toda otra información relevante. Este convenio, por lo tanto, debería incluir una cláusula que establezca que ambos organismos respetan la ley 25.326 e implementan medidas de seguridad y confidencialidad.

El artículo 18 del proyecto de ley menciona las cesiones entre organismos del sector público mediante un acuerdo o contrato de por medio que debe explicitar la finalidad de la sesión entre los organismos, qué categoría de datos se van a ceder, cuál va a ser la base que legitime ese tratamiento, los plazos de conservación, las medidas de seguridad y cualquier tipo de información que la autoridad de aplicación solicite.

El Registro Nacional de Base de Datos exige que el responsable mencione si realiza cesiones de datos. Las mismas son lícitas -de hecho, es una de las formas del tratamiento de los datos- siempre que cumplan con los requisitos mencionados más arriba. Y es importante remarcar que ambas partes -responsable y encargado- son corresponsables por la protección de los datos personales.

9. Transferencia Internacional: informa si se prevé alguna transferencia internacional de datos personales, indicando el país u organismo destinatario, la normativa que la admite y las garantías previstas.

El desarrollo de actividades en un mundo globalizado implica un flujo internacional creciente de datos personales. En el artículo 12 de la ley 25.326 se prohíben las transferencias internacionales de cualquier tipo, con cualquier país u organización internacional o supranacional que no proporcione niveles de protección adecuados. Pero también menciona excepciones, por ejemplo, cuando existan colaboraciones judiciales internacionales, cuando una persona por un tratamiento médico necesite realizar las transferencias o cuando existan investigaciones epidemiológicas, transferencias bancarias, acuerdos o tratados internacionales en los cuales el país sea miembro.

En el proyecto de actualización de la ley, se permite las transferencias internacionales si el organismo o el país al que se transfiere datos personales tiene o proporciona un nivel de protección adecuado, o si el exportador brinda garantías adecuadas. El proyecto actualiza la legislación adecuándose a la realidad actual de un flujo internacional de datos creciente, al nivel de otras leyes de la región, como Brasil o Uruguay, basados en el principio de extraterritorialidad, que implica que la protección de la regulación viaja con el dato a otro país o a otro Estado, permitiendo que la ley alcance a los responsables o encargados aunque estos no se encuentren físicamente en el país pero traten datos personales de ciudadanos o residentes locales.

¿Qué significa esta decisión de adecuación respecto de un país? Es que la Agencia como autoridad nacional analiza la legislación de otro país y el conjunto de su normativa para determinar si en ese país se respetan los mismos principios y se reconocen los mismos derechos de los titulares que en Argentina. En función de este análisis, define a un país como adecuado o no. Los países que cuentan con legislación adecuada se pueden encontrar en la página web de la Agencia. La última vez que se actualizó fue en el 2019 y quizás sea necesaria una revisión prontamente. Japón y Corea del Sur, por ejemplo, podrían estar incluidos en el listado de países adecuados. Brasil, un país de la región socio-estratégico para la Argentina tiene una disposición nueva en materia de protección de datos personales y es necesario analizar, porque las legislaciones en los países van cambiando, y requieren una actualización.

En casos como los de Google o Meta, empresas extranjeras cuyos servidores se encuentran fuera del territorio nacional y en países que no cuentan con legislación adecuada, se deben implementar medidas adicionales que provean garantías adecuadas que permitan reconocer los derechos de los titulares al mismo nivel que tenemos en la Argentina. Estas medidas pueden ser cláusulas contractuales modelo. La Agencia tiene la Disposición 60 que provee cláusulas contractuales modelo que pueden servir de guía. Y en octubre pasado, la AAIP, mediante la Resolución 198/23 aprobó la Guía de Implementación de Claúsulas Contractuales Modelo para la Transferencia Internacional de Datos Personales (TIDP), propuesta por la Red Iberoamericana de Protección de Datos Personales. Una es útil cuando se hacen transferencias internacionales de un responsable a otro responsable. La segunda es un modelo de contrato entre el responsable y el encargado de tratamiento. En cuanto a transferencias internacionales entre organismos públicos, otro mecanismo para elevar las garantías son los acuerdos internacionales en los que la República Argentina sea parte, y que contengan cláusulas de protección de datos donde se establezcan cuestiones como el principio de finalidad, marco legal que permite la transferencia, plazos de conservación, etc. También tiene que garantizarse el ejercicio de derechos a los titulares y contar con una instancia de revisión administrativa y judicial. Otro mecanismo para el sector privado son las normas corporativas vinculantes, que se utilizan dentro de un grupo económico que tiene presencia en diferentes países, donde algunos de los países pueden tener legislación adecuada y otros no.

En el proyecto de ley se propone también el mecanismo de certificación, siempre que estén aprobados por la Agencia.

Muchas empresas extranjeras ofrecen la firma de un contrato genérico y no dan espacio para su modificación. En esos casos es importante observar si contiene una cláusula de protección de datos personales y qué dice sobre las transferencias internacionales, poniendo el foco en la posibilidad del ejercicio de derechos de los titulares. El ejemplo clásico son los contratos de empresas internacionales que tienen una cláusula modelo que establece los estándares del reglamento europeo y que es la misma línea que sigue la legislación argentina.

10. Prestaciones de servicios de terceros: se se informa si se contratan servicios de terceros, y el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento de datos, el tipo de datos personales, las categorías de titulares de los datos y las obligaciones y responsabilidades del organismo y de los terceros contratados.

Cuando una organización contrata a un tercero para prestar servicios que involucran datos personales, ambas partes comparten la responsabilidad de

proteger esos datos. El organismo que proporciona los datos sigue siendo responsable de garantizar que se cumplan las leyes de privacidad y seguridad de datos. Antes de contratar a un tercero, es importante llevar a cabo una evaluación exhaustiva de su capacidad para cumplir con los estándares de protección de datos. Este tercero es guardián y corresponsable del correcto tratamiento de los datos personales que el organismo le cede. Esto implica verificar sus políticas de privacidad, medidas de seguridad y prácticas de manejo de datos. El Estado en sus distintos niveles tiene un papel fundamental que cumplir hacia el conjunto de la sociedad. Se relaciona con las buenas prácticas y cómo los ciudadanos ven al Estado, la forma en que hace uso de esos datos personales, cuestiones que hacen a la legitimidad y responsabilidad en la defensa y fortalecimiento de lo público y sus valores.

Es esencial seleccionar proveedores confiables y que cumplan con los requisitos legales, ya que existe una responsabilidad solidaria entre cedente y el cesionario. Una parte importante de la responsabilidad proactiva es seleccionar servicios de terceros sólo entre aquellos que valoran y toman con responsabilidad la protección de los datos personales. Debe establecerse un acuerdo contractual sólido entre la organización y el tercero que detalle claramente las responsabilidades y obligaciones en relación con los datos personales. Esto incluye cláusulas que establezcan medidas de seguridad, restricciones en el uso de datos y procedimientos para notificar y manejar incidentes de seguridad.

11. Derechos de los titulares: se informa los derechos y la forma de ejercerlos.

La protección de datos personales implica una serie de derechos que las leyes y regulaciones de privacidad otorgan a las personas para garantizar que sus datos personales se utilicen de manera justa y transparente. En la ley 25.326 se establecen:

- **Derecho de acceso:** el titular de los datos tiene derecho a saber si se están tratando sus datos personales y de acceder a ellos, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento
- **Derecho de rectificación:** los titulares pueden solicitar la rectificación de sus datos personales cuando estos resulten ser inexactos, falsos, erróneos, incompletos o desactualizados.
- **Derecho de supresión:** los titulares pueden solicitar que se eliminen sus datos personales en ciertas circunstancias, como cuando los datos ya no son necesarios para el propósito original de su recopilación.
- **Derecho de actualización:** este derecho permite a las personas solicitar la corrección o actualización de datos personales inexactos o desactualizados que un organismo tenga sobre ellos.

Por su parte el proyecto de actualización de la ley de protección de datos personales, así como otras legislaciones de la región vienen incorporando nuevos derechos que se suman a los ya planteados. Entre ellos están:

- **Derecho a la portabilidad:** el titular tiene derecho a obtener una copia de los datos de medios electrónicos o automatizados y solicitar que sus datos personales se transfieran directamente de responsable a responsable.
- **Derecho de limitación:** la persona interesada tiene derecho a la limitación del tratamiento de sus datos personales si el tratamiento es ilícito y la persona interesada se opone a la supresión de los datos personales y solicita en su lugar la limitación de su uso; si el responsable ya no necesita los datos personales para los fines del tratamiento, pero la persona interesada los necesita para la formulación, el ejercicio o la defensa de sus derechos o mientras se verifica si los motivos legítimos del responsable de tratamiento prevalecen sobre los de la persona interesada. En ese caso se abre un periodo de tiempo donde se limita el tratamiento de esos datos mientras se verifica si son correctos o no.

El organismo público debe analizar cuando algunos de esos derechos proceden o no. Y facilitar el pedido de ejercer esos derechos, por ejemplo, mediante mail de contacto, etc. La ley establece un determinado plazo para responder esos pedidos. Si no hay respuesta del organismo, el titular puede denunciar ante la AAIP, y puede ser pasible de una sanción si la base de datos es de jurisdicción federal.

12. Designación de un Delegado de Protección de Datos: se informa si se ha designado a un delegado su nombre y apellido y la forma de contactarse con el mismo.

La designación de un delegado de protección de datos no está contemplada en la ley actual, pero es parte de la cultura de privacidad que se está instalando cada vez más en las legislaciones modernas y que está planeado como de cumplimiento obligatorio en el proyecto de actualización de la ley.

Los responsables y encargados de tratamiento deben designarse cuando el tratamiento requiera un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades. Para el caso de los organismos públicos se recomienda en todos los casos elegir un delegado. En el caso en que se trate de una autoridad u organismo público con dependencias subordinadas, se puede designar un único delegado teniendo en consideración su tamaño y estructura organizativa.

La designación debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones.

Dicho puede ser desempeñado por un empleado del organismo puede ejercer otras funciones siempre que no den lugar a conflictos de intereses, y debe ejercer sus funciones de manera autónoma y libre de interferencias, sin recibir instrucciones, y solo debe responder ante el más alto nivel jerárquico del organismo y no puede ser destituido ni sancionado por desempeñar sus funciones.

Sus funciones son las de informar y asesorar a los funcionarios jerárquicos tanto como a los empleados, promover y participar en el diseño y aplicación de una política de tratamiento de datos personales, supervisar y asignar responsabilidades, concientizar, realizar las auditorías ofrecer asesoramiento para hacer una evaluación de impacto y cooperar y actuar como referente ante la Autoridad de Aplicación.

13. Datos sensibles: se informa si se tratan datos sensibles y que se lo hace mediante una autorización legal expresa fundada en interés general.

El sector público puede tratar datos personales sensibles, siempre que haya razones de interés general que son autorizadas por ley. Un caso que puede servir de ejemplo es el manejo de datos personales referidos a la salud y a la geolocalización de los titulares durante la pandemia. En estos casos el Estado tiene la obligación de cuidar los derechos a la salud de las personas y por lo tanto está autorizado a tratar datos personales.

En todos estos casos, cuando el sector público, sus organismos, tratan este tipo de datos tienen la obligación de implementar la responsabilidad reforzada. Esto significa que hay que establecer salvaguardas adicionales, entornos de protección más seguros, con protocolos de acceso, con control del personal que accede y con cláusulas de confidencialidad, con plazos de eliminación en el caso que pueda establecerse un plazo. Aunque no está en la ley actual, las buenas prácticas en materia de protección de datos sugieren realizar una evaluación de impacto, tener protocolos de mitigación frente a una brecha de seguridad, auditorías periódicas, capacitación permanente y compromiso del personal.

14. Capacitación: se informa si los agentes relacionados con el tratamiento de datos personales están capacitados.

Las capacitaciones desempeñan un papel esencial en la protección de datos personales al crear conciencia, fomentar el cumplimiento normativo, mejorar las prácticas de seguridad, reducir los riesgos, promover un cambio cultural y preparar a los empleados para responder adecuadamente a los incidentes de seguridad. Es importante que las organizaciones inviertan en programas de capacitación efectivos y continuos como parte integral de su estrategia de protección de datos.

15. Sitios en Internet: se informa que los sitios web del organismo pueden contener enlaces a sitios de terceros, cuyas políticas de privacidad son ajenas al mismo.

Los organismos públicos deben informar claramente que están abandonando su sitio web y accediendo a un sitio web de terceros. Los sitios de terceros deben tener sus propias políticas de privacidad que describan cómo recopilan, utilizan y protegen los datos personales de los usuarios. Una buena práctica de protección de datos es enlazar a estas políticas o proporcionar información sobre cómo los usuarios pueden acceder a ellas. También es importante verificar regularmente la validez de los enlaces y actualizarlos según sea necesario. Aunque los datos personales pueden ser manejados por el sitio de terceros, los ciudadanos pueden asociar cualquier problema de privacidad con el sitio web del organismo. Por lo tanto, es importante supervisar y garantizar que los sitios de terceros cumplan con las normativas de privacidad y brinden seguridad a los datos personales de los usuarios.

El deber de informar es una obligación legal que se puede cumplir mediante la política de privacidad ubicada en la web del organismo. Es una forma práctica y accesible de cumplir con la ley. Todo organismo tiene que tener una política de privacidad formal para cumplir con la ley, pero los lineamientos que establecemos pueden superar los mínimos requeridos.

El modelo que propone la Resolución 40 no es exhaustivo, siempre puede haber alguna información adicional que se pueda desarrollar, y esto depende de cada organismo y de las políticas proactivas que tenga cada uno de ellos.

Así como hoy en día se habla de que la cadena de valor, los proveedores, tienen que ser sostenibles medioambientalmente, podemos también plantear que deben proteger los datos personales. No es un requisito legal hoy en día, pero es parte de las buenas prácticas que permiten ampliar derechos y proteger a los titulares y adelantarse a cualquier incidente de seguridad.

7.
Alojamiento en la nube

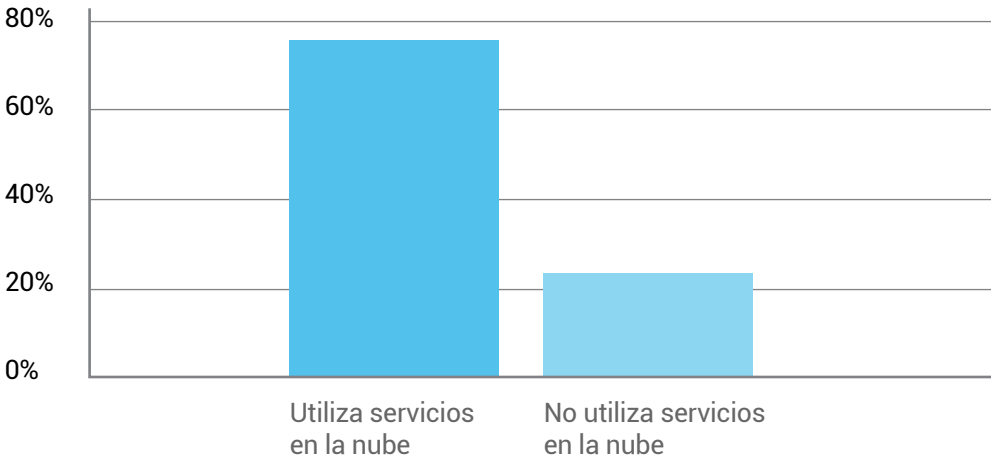
El cloud hosting o alojamiento en la nube es un tipo de servicio en el que uno o más servidores virtuales son utilizados para permitir que las aplicaciones o sitios web estén disponibles en Internet. Se trata de un servicio cada vez más requerido para el tratamiento de datos personales, por lo que tiene una relevancia cada vez mayor para la privacidad de las personas. Al seleccionar un proveedor de servicios en la nube, es fundamental investigar y elegir uno que ofrezca altos estándares de seguridad y cumpla con las regulaciones de privacidad.

En el país no hay muchos prestadores del servicio, por lo que la mayoría de los proveedores son extranjeros y, por lo tanto, puede involucrar transferencias internacionales de datos personales.

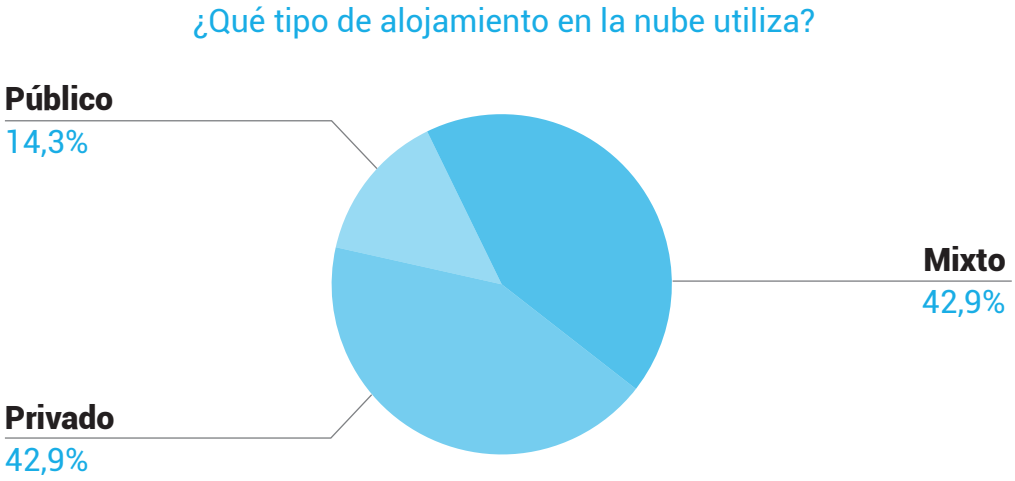
Los prestadores pueden ser públicos o privados. El servidor de origen público por excelencia es Arsat. Es un prestador de servicio que forma parte del Estado. Empresas nacionales privadas hay muy pocas. Por lo tanto, en la mayoría de los casos se termina contratando servicios privados extranjeros. Para ello es necesario un acuerdo con el encargado de tratamiento, que debe detallar el objeto y el alcance del acuerdo, el plazo, la ubicación, la naturaleza y la finalidad, qué categoría de datos personales serán tratados. Algunos encargados sostienen que al alojar datos en la nube no tratan datos personales. Es importante destacar que para nuestra administración el alojamiento es una parte del tratamiento. Si no modifican esos datos y solo los almacenan, debe figurar como su finalidad en el acuerdo. También debe tener una previsión respecto al deber de confidencialidad, y deben figurar las medidas de seguridad, que varían según el tipo de tratamiento y la categoría de los datos tratados. El contrato de servicios debe contemplar también los derechos de los titulares.

Esto implica una responsabilidad compartida entre el responsable y el encargado. Este último también puede contratar un sub-encargado, basado en un contrato con las mismas obligaciones y responsabilidades. El sub-encargado puede ser seleccionado de una lista previa dada por el responsable, basado en un análisis previo sobre qué tipo de encargados se pueden contratar, y va a realizar el mismo procedimiento de implementar cláusulas contractuales antes establecidas entre responsable y encargado. Estas cláusulas permiten al responsable controlar las condiciones en que se va a brindar el servicio independientemente del lugar en que se aloje el encargado y el sub-encargado. En el proyecto de actualización de la ley el subcontratado asume el carácter de encargado de tratamiento en términos y condiciones de la ley, y para el supuesto que incumpla las obligaciones y responsabilidades, asume la calidad de responsable del tratamiento, es decir, asume las obligaciones y el peso de la ley.

Un relevamiento a referentes claves del Consejo Federal para la Transparencia sobre el uso por parte del sector público provincial de servicios de almacenamiento en la nube, obtuvo, con casi la mitad de respuestas, el siguiente resultado:



Respecto a la contratación de la prestación de los servicios a empresas privadas, ARSAT o ambos la encuesta arrojó el siguiente resultado:



Aunque es importante profundizar en el relevamiento por jurisdicción y por área del Estado, los gráficos estarían indicando una situación de creciente utilización de servicios en la nube y una importante heterogeneidad respecto a la fuente pública o privada de los servicios, un claro indicador de la necesidad urgente de promover una mayor conciencia respecto a la protección de los datos personales, al tipo de contrato que se firma y las salvaguardas que deben incorporar los organismos, teniendo en cuenta que muchas veces involucra transferencia internacional de datos personales.

8.
Avances y desafíos en las jurisdicciones

La experiencia aprendida en el transcurso de los talleres y cursos realizados durante 2023 con la intervención activa de las jurisdicciones, se destaca:

La gran mayoría puede identificar el flujo de los datos personales y trata datos sensibles. También se realizan habitualmente cesiones a otros organismos y una proporción considerable utiliza servicios en la nube.

Esta situación evidencia la necesidad, en gran parte de las jurisdicciones, de avanzar en que cada organismo posea un plan de protección de datos personales, un manual de procedimiento interno, una política de Privacidad, y un DPO encargado del tema, así como en lo que respecta a protocolos de seguridad, capacitaciones internas y campañas de sensibilización. Sensibilización e información que debe ser extendida al conjunto de la población y en particular a grupos vulnerables.

Por último, se destaca la relevancia en todos los organismos del sector público de enfocar la protección de los datos personales desde el diseño de las políticas públicas y durante todo el ciclo.

Estos lineamientos para la formulación de un plan de protección de datos personales se proponen contribuir a estas tareas y ser de utilidad para la formulación del mismo, teniendo en claro que solo puede servir de guía, dado que cada provincia y cada organismo tiene su propia realidad y sus propias necesidades, lo que exige adecuar y adaptar estos lineamientos a los problemas concretos que cada sector enfrenta.

9.
Consideraciones finales

Hemos plasmado en este documento unos lineamientos generales que sintetizan un conjunto de políticas, procedimientos y prácticas diseñadas para garantizar la privacidad y la seguridad de la información personal que cada organismo trata. El Estado juega un papel crucial en la creación de un entorno en el que las personas puedan confiar en que sus datos personales serán manejados de manera segura. También posee la responsabilidad ética frente a la sociedad de proteger la privacidad de las personas, cuestión que va más allá del cumplimiento estricto de las leyes y regulaciones, y exige una responsabilidad pro activa, tomando medidas que pueden ser movilizadoras para la protección de datos en el conjunto de la sociedad.

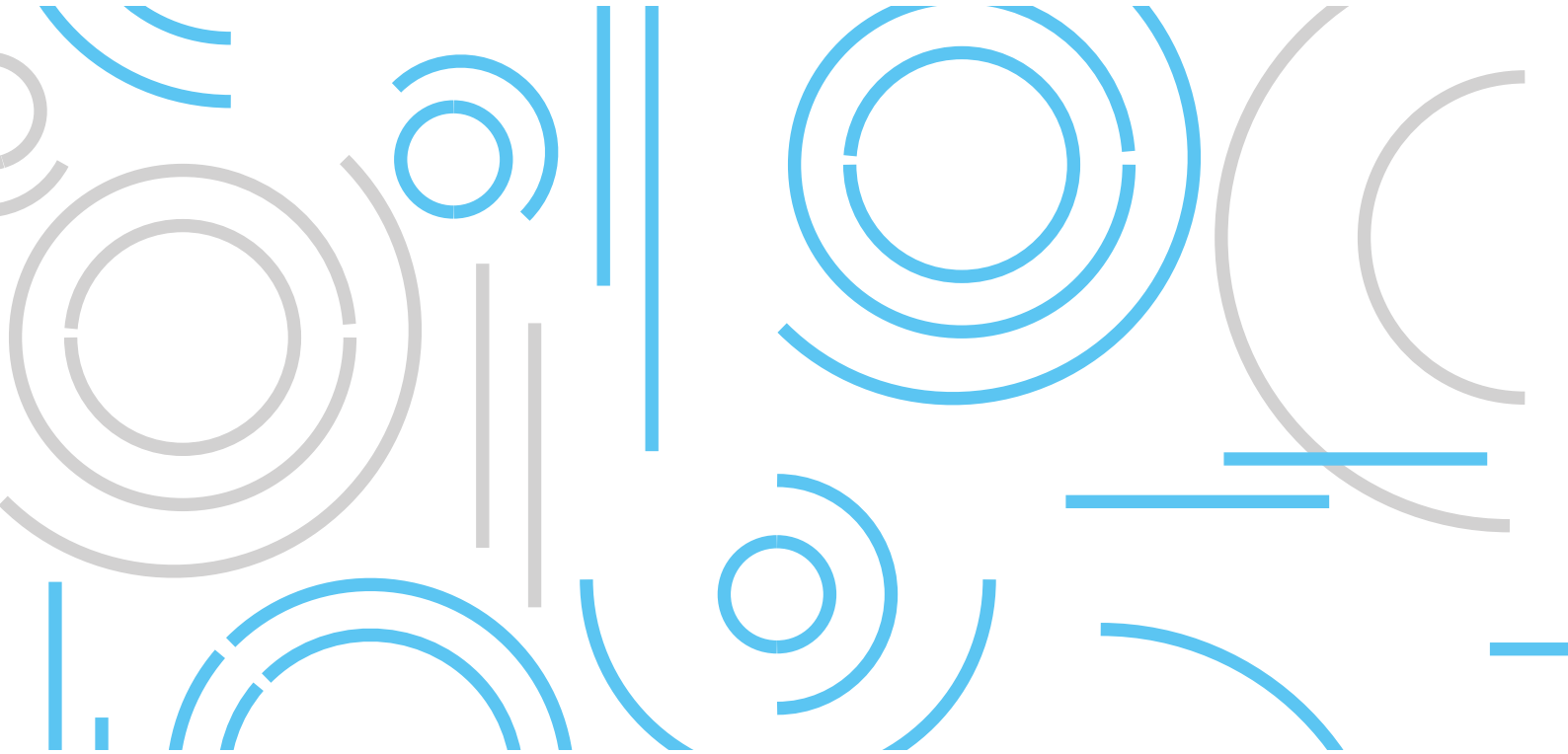
En ese sentido, cabe destacar la necesidad de modernizar los marcos normativos con nuevos principios y derechos. El proyecto de Ley de Protección de Datos Personales elaborado desde la Agencia de Acceso a la Información Pública ya fue elevado al Congreso de la Nación, y comenzó a ser debatido en comisiones en la Cámara de Diputados. Además, Argentina, junto con otros 30 países, ratificó el convenio 108+ del Consejo de Europa. En este sentido, el proyecto recupera éste y otros estándares regionales e internacionales, así como también los principales antecedentes en la materia. En ese sentido, el proyecto propone un cambio de paradigma: pasar de un modelo de protección de registros de datos, a uno que garantice el derecho humano de las personas.

A 40 años de democracia, construir capacidades estatales en diálogo con la ciudadanía y desde una perspectiva federal y soberana, nos permite contar con un mayor consenso en las políticas públicas.

10.
Referencias bibliográficas

- Anchorena, B. “Protección de Datos Personales: una oportunidad para impulsar el desarrollo”, Télam, 08-09-2023. Disponible en: https://www.telam.com.ar/notas/202309/639603-proteccion-datos-personales-opinion.html
- Convenio 108 modernizado https://rm.coe.int/convenio-para-la-proteccion-de-las-personas-con-respecto-al-tratamient/1680968478
- Guía de Evaluación de Impacto en la Protección de Datos, Agencia de Acceso a la Información Pública. Disponible en: https://www.argentina.gob.ar/sites/default/files/guia_final.pdf
- Guía de Implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales (TIDP). Red Iberoamericana de Protección de Datos Personales.Disponibleen:https://www.redipd.org/sites/default/files/2022-09/guia-clausulas-contractuales-modelo-para-tidp.pdf
- Ley 25.326/ 2000 de Protección de datos Personales. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm
- Proyecto de Ley de Protección de Datos Personales. Disponible en: https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf
- Resolución 40/ 2018 Agencia de Acceso a la Información Pública, Política Modelo de Protección de Datos Personales para Organismos Públicos. Disponible en: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-40-2018-312130
- Resolución 47/ 2018. Medidas de Seguridad - Tratamiento y conservación de los datos personales en medios Informatizados. Disponible en: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-47-2018-312662

Esta guía se terminó de imprimir y encuadernar en el mes de noviembre de 2023
en la imprenta de la Secretaría de Gestión y Empleo Público de
la Jefatura de Gabinete de Ministros de la Nación.



Consejo Federal
para la Transparencia

AAIP
Transpa rencia
Acceso a la Información Pública
Protección de Datos Personales

Argentina
Presidencia