INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"GUÍA PRÁCTICA-OPERATIVA PARA QUE LOS SERVIDORES PÚBLICOS QUE REALICEN TRATAMIENTO DE DATOS PERSONALES EN CUMPLIMIENTO DE SUS FUNCIONES LO HAGAN APEGADO AL MARCO NORMATIVO APLICABLE"

PROPUESTA DE INTERVENCIÓN

Que para obtener el grado de MAESTRA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Elizabeth Grace Jiménez Vázquez

Asesora:

Maestra Evelyn Téllez Carvajal

Ciudad de México, a 01 de junio de 2022

Autorización de Impresión

Agradecimientos

A **Dios**, por todo lo que me das, por ser siempre mi guía en todo momento.

A mis hijos **Diego y Damián**, por impulsarme cada día a ser mejor persona, por ser mis motores de vida, porque me inspiran a concluir este logro, porque con ustedes todo lo que hago es para mejorar en todos los sentidos. Solo con verlos, sentirlos y olerlos me ensañan lo maravilloso que es la vida.

A **Cristian**, mi esposo y mejor amigo, porque siempre me alientas a dar un paso extra para superarme, porque siempre confías en mí; mis metas también las haces tuyas, por tu ayuda, todo tu amor y cariño. Porque siempre me has acompañado en este camino en pareja, haciendo el uno-dos y alentándome en todo momento.

A **Hilario** y **Gloria**, mis padres, por siempre ser mis ejemplos de vida, por todo su amor y procuración; porque su valentía, lucha y esfuerzo me dan la fuerza para seguir adelante. Porque me han enseñado y educado que la vida se gana con esfuerzo y dedicación. Simplemente porque sin ustedes, nada de lo que soy podría ser.

A mi hermano **Hugo**, porque eres mi gran ejemplo para salir adelante.

A mi familia **Vázquez**, porque la bondad y valores que tenemos como familia refuerzan mi convicción de que sin familia, nada de esto tendría sentido.

Tabla de contenido

Índice de Figuras

Índice Gráficos

Índice de Cuadros

Introducción

La protección de la vida privada es un derecho joven, el cual se encuentra en proceso de madurez, sin embargo, no por ello las normas que la protegen son laxas, sino lo contrario, se instauran como un instrumento que permite salvaguardar dicho derecho.

Resulta entonces oportuno, distinguir entre lo que es considerado como privado y lo que se considera como lo público, siendo el primer ámbito una creación del Estado a través de una ley, lo que no es del interés público, y que no se trata de actividades estrictamente individuales, lo cual se delimita con la injerencia que de ellas puede tener el Estado,[1] constituyéndose éste, el ámbito a proteger.

Ahora bien, estando dentro de lo que es privado refirámonos a lo que es la intimidad, vista ésta desde el punto de vista psicológico, el que se entiende, desde una perspectiva pasiva, como "el sentimiento que una persona tiene de que los demás deben ser excluidos de algo que sólo a él concierne, así como el reconocimiento de que los demás tienen derecho a hacer lo mismo",[2] y desde una perspectiva activa, entendida como "el control de la interacción, la libertad de elegir el momento y el lugar de la privacidad".[3]

No obstante ello, por diversas circunstancias, resulta necesario que, aquello que nace en lo privado y en lo íntimo, sea conocido por otros, sin embargo, cada persona también tiene el derecho de decidir lo que ocurre sobre los mismos, lo que veremos más adelante como autodeterminación informativa.

Ahora bien, la necesidad de exponer a lo público lo que nació en el ámbito privado, debemos contextualizarlo en la época en que vivimos, esto es, desarrollándonos en un entorno de lo que se denomina la sociedad de la información, la que se define como "un nuevo modelo de organización industrial,

---

[1] Escalante Gonzalbo, Fernando, *El derecho a la privacidad*, México, IFAI, Cuadernos de Transparencia, 2013, pp. 8 a 14. Disponible en *https://sontusdatos.org/wp-content/uploads/2013/04/c2-ifai-derecho-a-la-privacidad.pdf*, última fecha de consulta el 20 de agosto de 2019.
[2] Rebollo Delgado, Lucrecio, *El derecho fundamental a la intimidad*, Madrid: Dykinson, 2005, p. 26.
[3] *Ibidem*.

cultural y social caracterizado por el acercamiento de las personas a la información a través de las nuevas tecnologías de la comunicación".[4]

En razón de lo anterior, resulta importante tener en cuenta que cada vez que la tecnología tiene mayores avances, es mayor del número de amenazas y riesgos a la privacidad de personas,[5] por lo tanto, en la nueva era de la tecnología, "es posible que la publicación/distribución de los contenidos o información controvertida en la red suponga en vez de una intromisión en la intimidad del sujeto —o además de aquella— un tratamiento inadecuado de datos personales".[6]

Los riesgos sobre la privacidad de las personas los vemos latentes en dos sectores, tanto por los particulares y el Estado. En este último caso, el ciudadano —o bien, otras entidades del sector público o privado, proporciona a la Administración Pública la información referente a una persona, la que puede ser utilizada para "la práctica de modelos y simulaciones para la toma de decisiones",[7] sin embargo, "la seguridad de actuar siempre dentro de la normatividad aplicable, que en nuestra época es una maraña compleja. […] Asimismo, el uso de la informática en manos tanto del Estado como en manos de particulares, crea diversos riesgos que pueden suponer una amenaza de agresión a la intimidad de los gobernados o usuarios de los servicios".[8]

En razón de lo anterior, en nuestro Estado mexicano, contamos con instrumentos normativos que garantizan la vida privada de las personas, sin embargo, al ser normas en proceso de madurez, se ve necesario que los operadores del Estado, esto es, los servidores públicos, cuenten con instrumentos que, en primer lugar, garanticen el cumplimiento del derecho a la vida privada de las personas, y que además protejan la labor diaria de los servidores públicos.

---

[4] Campuzano Tome, Herminia, *Vida privada y datos personales*, Madrid, Tecnos, 2000, p. 20.
[5] Méjan, Luis Miguel C., *El derecho a la intimidad y la informática*, México, Porrúa, 1994, pp. 45 a 49. Se refiere a algunos riesgos, como lo son, la clasificación de personas y perfiles, la etiquetación y predicción de conductas, la agregación de datos.
[6] López Martín, Gemma Ana y Chichón Álvarez, Javier, *Nuevos retos y amenazas a ala protección de los derechos humanos en la era de la globalización*, España, Tirant lo Blanch, 2016, p. 86.
[7] Meján, Luis Miguel, *El derecho a la intimidad y*, *op. cit*., nota 5, p. 48.
[8] *Idem*.

En razón de lo anterior, el presente documento tiene la intención de que se garantice el cumplimiento de las normas aplicables en materia de protección de datos personales, lo que tendrá como consecuencia inmediata, la protección del ejercicio de funciones de los servidores públicos, evitando con ello sanciones que pueden dañar el ejercicio de su carrera profesional, e incluso tener consecuencias de otra índole en su persona, como pueden ser cuestiones económicas, o de privación de la libertad por considerarse que alguna actividad pudiera configurar un hecho delictuoso.

Ahora bien, las normas aplicables en materia de protección de datos personales contienen diversas obligaciones que deben ser cumplidas por los sujetos a los que obliga, sin embargo, el no tener una estructura que sirva como base para dar cumplimiento, tiene dos consecuencias: (i) La primera, que es la inobservancia de la norma, cuya consecuencia expone la privacidad de los titulares de quienes se tratan datos personales, y (ii) El inicio de procedimientos que pueden reparar en sanciones administrativas e incluso hasta penales, para quiénes no observaron las disposiciones normativas.

Es por ello, que se identifica que al interior de cada sujeto obligado en materia de protección de datos personales, se debe contar con un instrumento que permita de manera sencilla y específica atender el cumplimiento de cada uno de los supuestos normativos, que al final se convierten en obligaciones para cada sujeto obligado.

De ahí deriva la propuesta de intervención, pues formando parte del servicio público, la autora ha podido identificar que los supuestos normativos no son cumplidos por varias razones, dentro de las cuales se encuentra la falta de instrumentos que guíen al obligado a cumplir con sus obligaciones.

De esta manera, estando dentro del Instituto Mexicano del Seguro Social, en específico en la Dirección de Innovación y Desarrollo Tecnológico, se identificó que son diversos los roles que deben organizarse para dar cumplimiento a la norma en materia de protección de datos personales, es por ello, que a efecto de facilitar dicha labor, se pensó en la guía que aquí se presenta, la que ha sido diseñada en dos secciones.

La primera sección se refiere a todos los aspectos que norman la protección de datos personales en posesión de sujetos obligados, los cuales se

convierten en el andamio de conocimiento para el debido cumplimiento de la norma.

En la segunda sección, se proponen formatos y plantillas, a través de las cuales, los servidores públicos de la Dirección de Innovación y Desarrollo Tecnológico podrán documentar el cumplimiento de cada supuesto normativo.

El instrumento propuesto, en este sentido, permitirá por un lado que el área cuente con su arquitectura de procesos, en la que se deberán indicar los procesos y subprocesos del área, con lo que se evita dejar fuera cualquier tratamiento de datos personales. Por otro lado, por cada uno de los subprocesos mapeados, se deberá documentar: (i) La identificación de los datos personales involucrados, categorizándolos e indicando el titular al que pertenecen, el medio por los que fueron obtenidos e indicando si los mismos son sensibles o no; (ii) Documentar el marco normativo que justifica el tratamiento de los datos al interior del área; (iii) Por cada uno de los datos, deberá justificarse su utilización, esto es, las finalidades del tratamiento, identificando el cumplimiento de que las mismas sean concretas, lícita y explícitas; (iii) Para cumplir con la lealtad, deberán documentarse los medios de obtención y tratamiento, así como las acciones para cumplir la expectativa razonable de privacidad de su titular; (iv) Se deberá indicar cómo se obtuvo el consentimiento del titular para el tratamiento de sus datos, en caso de no configurarse alguna excepción; (v) Por otro lado, se deberá indicar las acciones que se ejecutan para que los datos sean, por una parte, completos, correctos, actualizados y exactos y por otra adecuado, relevantes y necesarios; (vi) Se deberán indicar los plazos de conservación y bloqueo para la posterior supresión de datos personales; (vi) Asimismo, se deberán indicar los avisos de privacidad que se generen, refiriéndose a la modalidad en que están disponibles y las evidencias que se relacionan con su puesta a disposición; (vii) Se indicarán las medidas ejecutadas para que los datos sean conservados de manera segura, confidencial, integral y disponibles, y (vii) Se deberá documentar cada remisión y transferencia de datos realizada.

Capítulo 1

La protección de datos personales

Capítulo 1 La protección de datos personales

En este primer capítulo haremos una breve referencia a lo que históricamente ha dado lugar a que en nuestros días contemos con un marco normativo nacional e internacional cuya intención es proteger la privacidad de las personas.

1.1 Antecedentes de la protección de datos personales

Veremos a continuación la génesis de los que hoy conocemos como la protección de datos personales, desde una perspectiva histórica e internacional, para llegar a lo hoy conocido internacionalmente como la protección de los datos personales.

1.1.1 "The Right to be alone"

La expresión "el derecho a estar solo", proviene del derecho inglés con el principio "*a man´s house as his castle*", esto es, la casa o el castillo de cualquier persona es la máxima protección personal. El primero en utilizar el término fue el juez Thomas M. Cooley en 1879.[9]

De acuerdo con el texto titulado "El derecho a la Privacidad en los Estados Unidos" de la autora María Nieves Saldaña, este término ya había alcanzado un reconocimiento oficial constitucional en el año de 1791, y con el fin de dar un panorama histórico, señala la autora, que el término se configuró como una garantía de la Tercera Enmienda, como un principio básico respecto de la prohibición de confiscación de domicilios particulares por parte de soldados en tiempos de paz. Aunado a lo anterior, también en la Cuarta Enmienda se protege a los ciudadanos frente a registros y requisas arbitrarios o injustificados, limitando la intrusión del gobierno en las personas, domicilios, documentos y efectos personales. Finalmente, la Quinta Enmienda, que protege al ciudadano a no autoincriminarse, pues impide que el gobierno le obligue a revelar información personal y reservada,[10] diferenciándose del concepto del "derecho

[9] Véase Gay Wood, Addison Horace, *A Treatise of the Law of Torts*, Estados Unidos de América, Arkose Press, 1789.
[10] Saldaña, María, "Derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales", *Revista UNED. Teoría y Realidad Constitucional*, España, 2011, núm. 28, pp. 283. Disponible en *https://dialnet.unirioja.es/descarga/articulo/3883001.pdf* y *http://revistas.uned.es/index.php/TRC/article/view/6960*, consultado el 13 de junio de 2019.

a estar solo", pues el primer término hace referencia a no revelar información propia, y en el segundo a proteger al titular a que un tercero entre a su vida privada.

Entonces la expresión de "el derecho a estar solo" es básico para la protección de la información, así como de los bienes, amparados por la constitución de los Estados Unidos, la cual, ha sido considerada como una buena base para lo que posteriormente conoceríamos como la protección de los datos personales, pues aquí surge lo que se conoce como privacidad.[11]

1.1.2 El derecho a la privacidad. Warren y Brandeis

Los juristas norteamericanos, Samuel D. Warren y Louis D. Brandeis, publicaron el 15 de diciembre de 1980 una monografía titulada "*The Right to Privacy*",[12] a través de la cual, se hace una clara referencia a la importancia que tiene la privacidad o la protección individual de las personas, dando origen al derecho a la privacidad.[13]

El artículo remonta a los tiempos donde no se garantizaba la protección individual de las personas respecto de su privacidad, entendida ésta como "el rechazo a todo intromisión no consentida"[14] en distintos aspectos de la vida, donde la ley no se aplicaba de manera explícita para que este derecho no fuera dañado, precisando así, la importancia que tiene su protección y concibiendo a la privacidad como un derecho.

Dentro de su artículo mencionan las diferentes calumnias, mentiras y demás acciones que perjudicaban a los individuos, siendo que los mismos no

---

[11] Véase Garriga Domínguez, Ana, *Nuevos retos para la protección de datos personales. En la era del Big Data y la computación ubicua*, Madrid, Dykinson, 2016, Disponible en *https://books.google.com.mx/books?id=qxkJDAAAQBAJ&pg=PA75&lpg=PA75&dq=derecho+a+estar+s%C3%B3lo+cooley&source=bl&ots=kbIJe9DxxT&sig=ACfU3U1H-aUDFrJNQBpi-ZdEzJkvj1Jc5A&hl=es-419&sa=X&ved=2ahUKEwiF-efai8nhAhVPtZ4KHb7JB2UQ6AEwAnoECAkQAQ#v=onepage&q=derecho%20a%20estar%20s%C3%B3lo%20cooley&f=false*, última fecha de consulta el 13 de junio 2019

[12] Warren, Samuel D. y Brandeis, Louis D., "The Right to Privacy", *Revista Harvard Law Review*, vol. 4, núm. 5, 1890, pp. 193 a 220. Disponible en *https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf*, última fecha de consulta el 4 de junio 2019.

[13] Murillo de la Cueva, Pablo Lucas, *El derecho a la autodeterminación informativa*, España, Tecnos, 1990, p. 57.

[14] Garriga Domínguez, Ana, *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, *op. cit*., nota 11, p. 76.

tenían una protección clara de sus derechos, comenzando desde sus propios bienes hasta de su persona.

Los juristas dejan claro la importancia que tiene ubicar el derecho a la intimidad como principio que ampara a la persona y lo que a ella le rodea, como son sus bienes, sus escritos, "su apariencia personal, a los dichos, a los hechos y a las relaciones personales, domésticas o de otra clase y los pensamientos, emociones y sensaciones".[15]

El impacto del texto en mención fue grande, pues no se quedó en solo una publicación teórica, pues 12 años más tarde de su publicación, la Corte de Apelación de Nueva York adoptó la doctrina propuesta por los juristas Warren y Brandeis, lo cual fue el inicio de resoluciones con sustento en la misma.

1.1.3 La protección de datos personales en el ámbito internacional

Tal y como se ha hecho la anotación anteriormente, si bien es cierto que la concepción del derecho a la privacidad es un derecho nuevo, también es cierto que de manera general diversos instrumentos internacionales, protegían ya al individuo y su esfera privada, la cual sirvió como base para la perfección como derecho y que incluso las legislaciones lo denominaran como tal, en su evolución más perfecta como datos personales. A continuación, se presentan los documentos internacionales que refieren a dicha protección.

1.1.3.1 *Declaración Universal de los Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos*

La Declaración Universal de Derechos Humanos[16] proclamada por la Asamblea General de la Organización de las Naciones Unidas el 10 de diciembre de 1948, aceptado por la mayoría de los países, incluyendo México,[17] se convierte en el instrumento que se refiere a la protección que tiene cada uno de los individuos por el hecho de ser humanos.

---

[15] *Ibidem*, p. 77.

[16] Declaración Universal de Derechos Humanos. Disponible en *https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf*, última fecha de consulta el 13 de junio de 2019.

[17] México ratificó la Declaración desde su proclamación, esto es, el 10 de diciembre de 1948.

La Declaración, tal y como se menciona en su introducción, se formuló con el fin de que la protección de los países participes garanticen una protección a la población con leyes y legislando para que el instrumento tuviera efectos tangibles y de protección a los humanos.

En materia de protección a los individuos, es importante destacar su artículo 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Resultando éste, el primer texto internacional que protege a los humanos en su vida privada, señalando también la protección a su familia,[18] su domicilio y correspondencia, protegiendo su honra y reputación de ataques, pero no se convierte solo en un buen deseo, sino que cuida la vida privada de los humanos pues les concede el derecho de que la ley les proteja cuando los mismos son vulnerados.

El texto garantizado en la Declaración Universal de Derechos Humanos, fue reforzado[19] por el Pacto Internacional de Derechos Civiles y Políticos[20] en su artículo 17.

> "Artículo 17
> 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

[18] Cabezuelo Arenas, Ana Laura, *Derecho a la intimidad*, España, Tirant lo Blanch, 1998, p. 200. Indica que se entiende por intimidad familiar a "determinados aspectos de la vida con otras personas, con la que se guarda una especial y estrecha vinculación, como es la familiar, aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo".

[19] Michel, James, *Privacy and Human Rights*, Estados Unidos de América: Dartmouth Pub Co & UNESCO, 1994, p. 19.

[20] Pacto Internacional de Derechos Civiles y Políticos. Disponible en *www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D47.pdf*, última fecha de consulta el 13 de junio de 2019.

1.1.3.2 *Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales*

También conocido como la Convención Europea de Derechos Humanos,[21] es un instrumento vigente desde 1953 para los países integrantes del Consejo de Europa[22] y con la tendencia de asegurar el reconocimiento y de la aplicación universal y efectiva de los derechos que se contienen en la misma. La Convención Europea, al igual que la Declaración Universal, hace énfasis en la protección de los derechos fundamentales de los seres humanos, tales como lo son la vida, la igualdad, la seguridad, entre otros.

En el ámbito de la protección de la privacidad, la Convención dispone de su artículo 8o., el que a la letra indica:

> Derecho al respeto a la vida privada y familiar.
>
> 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

En la primera parte del artículo, podemos ver que la misma se encuentra en el mismo sentido que la Declaración Universal, esto es, protege la vida privada y familiar de los individuos, así como su domicilio y correspondencia, sin embargo, la segunda parte del artículo 8o. antes referido, además protege a los individuos, indicando que no puede haber injerencia por la autoridad en dicha protección, a menos de que la misma esté prevista en la ley, esto es, las injerencias deben estar basadas en el principio de legalidad.

---

[21] Convenio Europeo de Derechos Humanos. Disponible en *https://www.echr.coe.int/Documents/Convention_SPA.pdf*, última fecha de consulta el 13 de junio de 2019.

[22] Consejo Europeo. Disponible en *https://www.coe.int/es/web/about-us/our-member-states*, última fecha de consulta el 13 de junio de 2019.
Del Consejo de Europa son países miembro: Albania, Alemania, Andorra, Armenia, Austria, Azerbaiyán, Bosnia y Herzegovina, Bulgaria, Bélgica, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Federación de Rusia, Finlandia, Francia, Georgia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Liechtenstein, Lituania, Luxemburgo, Macedonia del Norte, Malta, Montenegro, Mónaco, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República de Moldavia, Rumanía, San Marino, Serbia, Suecia, Suiza, Turquía y Ucrania.

1.1.3.3 *Convención Americana de Derechos Humanos*

También conocida como el "Pacto de San José Costa Rica",[23] adoptada por México el 18 de diciembre de 1980,[24] la cual contiene un apartado de derechos civiles y políticos de las personas, y en especial el artículo 11 concede la protección a la honra y a la dignidad,[25] cuyo numeral 2 se refiere a la vida privada, como a continuación se indica: "2. Nadie puede ser objeto de ingerencias (sic) arbitrarias o abusivas en su vida privada, en la de su familia en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación".

De lo anterior podemos destacar que el instrumento protege a las personas en su vida privada y de su familia, tanto en su domicilio y su correspondencia, sin embargo, protege también la honra y la reputación de los mismos, sumando el numeral 3 del artículo en cita, que, de existir injerencias o ataques, las personas tienen derecho a ser protegidas a través de la ley.

1.1.3.4 *Acciones de la Organización para la Cooperación y el Desarrollo Económico (OCDE)*

Nos referiremos a continuación a las Directrices emitidas en 1980 y el Marco de Privacidad de 2013.

1.1.3.4.1 Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales (23 de septiembre de 1980)[26]

Ante la necesidad de una expansión de la vida económica y social dentro de un entorno tecnológico, la Organización para la Cooperación y el Desarrollo Económico[27] advirtió la necesidad de recomendar a sus países miembros tener

---

[23] Convención Americana sobre Derechos Humanos. Disponible en *http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D1BIS.pdf*, última fecha de consulta el 14 de junio de 2019.

[24] Antes del texto de la Convención Americana de Derechos Humanos en el continente europeo eran ya dos las constituciones que adoptaban el derecho a la intimidad, es el caso de la Constitución Portuguesa de 1976 en su artículo 26.1 y después, en 1978, la Constitución Española en su artículo 18. Cfr. Murillo de la Cueva, Pablo Lucas, *El derecho a la autodeterminación…, op. cit.*, nota 13, p. 74.

[25] Laje, Agustín, *Derecho a la intimidad*, Buenos Aires-Bogotá, Astrea, 2014, p. 14. No deja ver la importancia que el precepto normativo realiza, dado que "la dignidad humana se presenta como la fuente de donde brotan todos los derechos, reemplazando la autonomía de los Estados como el origen de los sistemas jurídicos locales e incluso del sistema jurídico internacional".

[26] Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Disponible en *https://www.oecd.org/sti/ieconomy/15590267.pdf*, última fecha de consulta el 13 de junio de 2019.

[27] Conocida por sus siglas OCDE y fundada en 1961, está conformada por 36 países miembro, los que tienen como misión "promover políticas que mejoren el bienestar económico y social de

en cuenta en su legislación interna los principios relativos a la protección de la privacidad, con base en lo establecido en las Directrices de dicha organización que regulan la protección de la privacidad y el flujo transfronterizo de datos personales.

Las Directrices están estructuradas en cinco grandes apartados. El primer apartado se refiere a cuestiones generales en la materia, de las que son importantes destacar que aporta la definición de flujo transfronterizo de datos personales, entendido como "los desplazamientos de datos personales más allá de las fronteras nacionales".[28] Asimismo, en el apartado se establece el alcance del instrumento, resultando aplicable para los sectores público y privado de los Estados.

El segundo apartado se refiere a los principios en materia de protección de datos personales, los cuales son: (i) Principio de limitación de recogida;[29] (ii) Principio de calidad de los datos;[30] (iii) Principio de especificación de los fines;[31] (iv) Principios de limitación de uso;[32] (v) Principio de salvaguarda de la seguridad;[33] (vi) Principio de transparencia;[34] (vii) Principio de participación individual;[35] y (viii) Principio de responsabilidad.

---

las personas alrededor del mundo". Los miembros de la OCDE son: Australia, Austria, Bélgica, Canadá, Chile, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Islandia, Irlanda, Israel, Italia, Japón, Corea, Lituania, Luxemburgo, Letonia, México, Países Bajos, Nueva Zelandia, Noruega, Polonia, Portugal, República Eslovaca, Eslovenia, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos, tal y como se advierte de los sitios *https://www.oecd.org/centrodemexico/laocde/* y *https://www.oecd.org/centrodemexico/laocde/miembros-y-socios-ocde.htm*, última fecha de consulta el 16 de junio de 2019.

[28] Véase inciso c) de la directriz.

[29] La directriz 7a. se refiere a lo que la legislación mexicana refiere como a los principios de legalidad y consentimiento, toda vez que, indica que la recolección de datos personales debe realizarse a través de medios legales y con el consentimiento del sujeto de datos, esto es, del titular.

[30] El principio además de referirse a que los datos personales deben ser correctos, completos y actualizados, deben cumplir con lo que en la legislación mexicana se conoce como el principio de proporcionalidad, esto es, los datos obtenidos deben ser correspondientes a los fines de su recolección.

[31] Al igual que en la legislación mexicana, se indica que los fines para los que se utilizarán los datos personales, deben ser indicados al momento de la recolección de los datos.

[32] Los datos no deben revelarse, a menos de que exista consentimiento del titular, o bien, una ley lo permita.

[33] Se consideran las medidas de seguridad como un principio y no como un deber, el cual se refiere a la protección de los datos.

[34] Lo que hoy conocemos como el principio de información, tal y como lo conocemos en la legislación mexicana.

[35] El principio se refiere a lo que hoy la legislación mexicana dispone como el derecho de acceso.

En la tercera parte, las directrices se refieren al flujo de datos entre los miembros de la organización, pues el mismo no debería restringirse, si cada estado garantiza que el flujo es seguro y los miembros dan cumplimiento al instrumento en comento.[36] En la sección cuarta se expresan las medidas legales y administrativas que cada Estado debería adoptar para el cumplimiento de las directrices y el quinto apartado complementa el círculo virtuoso refiriéndose a la cooperación internacional para garantizar el flujo transfronterizo de datos personales.

1.1.3.4.2 Marco de Privacidad de la OCDE (11 de julio de 2013)[37]

En virtud de que habían transcurrido más de treinta años a la emisión de las Directrices de 1980 y que el entorno actual ha cambiado, el Grupo de Trabajo de la OCDE sobre la Seguridad de la Información y Privacidad, convocó a grupos de expertos en el tema de privacidad de los datos, quienes pertenecían a diversos sectores, como lo son gobierno, autoridades de protección de datos, instituciones académicas, empresas y técnicos.

En dicha reunión, se identificó que debía modernizarse el enfoque sobre el flujo de datos transfronterizos, rendición de cuentas y aplicación de la privacidad.[38]

El instrumento prevé los siguientes principios para la protección de los datos personales: (i) Principio de limitación en la recolección, esto es, la obtención debe realizarse a través de medios legales; (ii) Principio de calidad de los datos; (iii) Principio de especificación del propósito; (iv) Principio de limitación del uso, referido también al que hoy conocemos como deber de confidencialidad; (v) Principio de seguridad; (vi) Principio de apertura, si bien no se refiere expresamente a contar con un aviso de privacidad, se refiere a que el titular de los datos, debe contar con medios a través de los cuales obtenga de manera fácil información sobre el uso de sus datos, y (vii) Principio de responsabilidad.

[36] Véanse directrices 16 y 17.
[37] The OECD Privacy Framework. Disponible en *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*, última fecha de consulta el 16 de junio de 2019.
[38] *Cfr*. Prólogo del Marco de Privacidad de la OCDE 2013.

Es importante destacar que los numerales 16 y 17 del instrumento se refieren al libre flujo de datos entre los Estados que sigan lo dispuesto en las directrices contenidas en el marco que nos ocupa.

1.1.3.5 *Marco de privacidad del Foro de Cooperación Económica Asia Pacífico (APEC)*

El Marco es un instrumento no vinculante, a través del cual, las economías miembro del Foro de Cooperación Económica Asia Pacífico establecen los principios bajo los cuales cada una de ellas debe proteger la privacidad de la información, con el objetivo de lograr el libre flujo de la misma, en la región Asia Pacífico[39].

En este nuevo instrumento, se definen los siguientes principios: (i) Previniendo el daño, esto es, tomar en cuenta los intereses del titular y los daños a los que sus datos se exponen; (ii) Aviso, lo que en nuestra legislación mexicana se conoce como principio de información; (iii) Limitación de recolección, el que se refiere a que datos deben ser tratados previo consentimiento, así como que la recolección debe estar limitadas conforme a los propósitos de tratamiento; (iv) Usos de la información, esto es, se debe cumplir con los propósitos que originan el tratamiento; (v) Elección, esto es, el titular tenga opciones para decidir sobre el tratamiento de sus datos; (vi) Integridad de la información personal, referida a lo que hoy conocemos como calidad de los datos; (vii) Medidas de seguridad; (viii) Acceso y corrección, y (ix) Responsabilidad.

1.1.3.6 *Convenio Nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*

Con el objetivo de reforzar lo que ya se iniciaba en los países miembro del Consejo de Europa, con las directrices mencionadas en el numeral anterior, y dado que la circulación de datos de carácter personal se había intensificado en las fronteras, el Consejo de Europa emitió el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto al

[39] Marco de Privacidad del Foro Cooperación Económica Asia Pacífico. Disponible en *https://sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf*, última fecha de consulta el 17 de junio de 2019.

tratamiento automatizado de datos de carácter personal,[40] las cuales tienen el objeto del respecto de la vida privada, ello con respecto del tratamiento de sus datos personales.[41]

El alcance del Convenio, tal y como se indicó anteriormente es el tratamiento de datos automatizados, tanto por el sector público como privado de cada miembro. El Convenio se refiere a cinco principios en materia de protección de las personas: (i) Compromiso de las partes, esto es, el compromiso de las partes para adoptar en su legislación lo mandatado por el convenio; (ii) Calidad de los datos, el cual recoge diversos principios actuales, el de consentimiento, finalidad, proporcionalidad y calidad, esto es, que los datos sean exactos y actualizados, y basados en procesos de conservación; (iii) Categorías particulares de los datos, definiendo la prohibición del tratamiento de ciertos datos[42]; (iv) Seguridad de los datos, y (v) Garantías complementarías, los que se refieren a los derechos actuales de acceso y rectificación.

1.1.3.7 *Protocolo adicional de Convenio No. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos (08 de noviembre de 2001)*[43]

El protocolo se refiere sustancialmente a que cada Estado prevea una o más autoridades responsables de asegurar el cumplimiento del Convenio 108. Dichas autoridades deben tener facultades totalmente independientes de investigación e intervención frente a reclamaciones sobre violaciones respecto del tratamiento de datos personales.

---

[40] Convenio No. 108 del Consejo de Europa, para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal. Disponible en *http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf*, última fecha de consulta el 17 de junio de 2019.

[41] Véase artículo 1o. del Convenio 108.

[42] Los datos de una persona que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, estrictamente, no podrían ser tratados automáticamente a menos que el derecho interno prevea garantías apropiadas de su protección.

[43] Protocolo Adicional del Convenio No. 108 para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos. Disponible en *http://transparencia.udg.mx/sites/default/files/Protocolo%20adicional%20del%20convenio%20No.%20108.pdf*, última fecha de consulta el 13 de junio de 2019.

Por otro lado, el artículo 2o. del protocolo se refiere a la excepción de transferencias de datos personales a Estados que no formen parte del convenio, siempre y cuando el receptor asegure un adecuado nivel de protección.

1.1.3.7.1 Adhesión de México al Convenio

Con fecha 12 de junio de 2018, se publicó en el Diario Oficial de la Federación el "Decreto por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente",[44] lo que representa para el Estado Mexicano adoptar legislación interna para garantizar la protección de datos personales y abrir fronteras a efectos de que exista flujo transfronterizo de datos residentes en estados miembros del Consejo de Europa y México.

1.1.3.8 *Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*[45]

El objetivo de la Directiva, es que los Estados miembro de la Unión Europea garanticen la protección del derecho a la intimidad de las personas, en lo que respecta al tratamiento de sus datos personales.[46] Si bien es cierto no resultó directamente aplicable para México, ahora hacemos referencia a la misma, pues su contenido y lenguaje sirvieron de base para la legislación mexicana. Cabe destacar que, con fecha 23 de octubre de 2018, el Parlamento Europeo y el Consejo de la Unión Europea, adoptaron el Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta

[44] Decreto por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente. Disponible en *http://www.dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018*, última fecha de consulta el 13 de junio de 2019.

[45] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML*, última fecha de consulta el 17 de junio de 2019.

[46] *Cfr*. Artículo 1o. de la Directiva 95/46/CE.

al tratamiento de datos personales y a la libre circulación de estos datos,[47] el cual en esencia se refiere a lo establecido por la Directiva, sin embargo, el Reglamento tiene el carácter de obligatorio para la Unión Europea.

1.1.4 La protección de datos personales en México

Si bien es cierto que en México contamos con legislación específica para la protección de los datos personales, es importante conocer la legislación general que se refiere a la protección de la vida privada.

Tenemos en primer lugar el Código Civil Federal, el que pone a salvaguarda el derecho de cualquier persona a realizar un reclamo por daño moral, el cual se actualiza por tener una afectación, entre otros, en su vida privada.[48]

Por su parte, el Código Penal Federal, contiene diversas tipificaciones delictuosas cuya intención es proteger la vida privada de las personas. Los artículos 173 a 177 se refieren a los tipos penales que se configuran por violar la correspondencia o comunicaciones privadas de una persona. Asimismo, en los artículos 210 a 211 Bis la norma tipifica la revelación de secretos como delito, el que si bien, puede considerarse como un tipo penal muy amplio, precisamente es dicho amplitud, la que nos permite decir que dichos secretos pudieren contener información que se refiera a la vida privada de una persona.

La Ley Federal de Telecomunicaciones establece que los concesionarios y autorizados que presten el servicio de acceso a Internet, entre otras obligaciones, deben preservar la privacidad de los usuarios,[49] y estableciendo de manera general para todos los concesionarios que las comunicaciones privadas son inviolables, excepto la intervención autorizada.[50] Concluyendo la

[47] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) no. 45/2001 y la Decisión no. 1247/2002/CE. Disponible en *https://europass.cedefop.europa.eu/sites/default/files/regulation-es.pdf*, última fecha de consulta el 17 de junio de 2019.
[48] *Cfr*. Artículo 1916 del Código Civil Federal.
[49] *Cfr*. Artículo 145, fracción III de la Ley Federal de Telecomunicaciones.
[50] *Cfr*. Artículo 190, último párrafo de la Ley Federal de Telecomunicaciones.

norma, en su artículo 298 la infracción que conlleva el incumplimiento de lo antes indicado.[51]

La Ley de Información Estadística y Geográfica, en su artículo 5o. establece que dicha ley es garantía para los titulares que entregan datos personales de que los mismos serán resguardados bajo confidencialidad. Por su parte el artículo 37 de dicho instrumento normativo establece el derecho que los titulares o informantes tienen para rectificar la información que hubieren proporcionado. El artículo 42 hace referencia a la obligación que tienen los titulares o informantes de proporcionar información verdadera, por lo tanto, en este precepto "se consagra el principio de veracidad y exactitud de los datos personales, que constituye uno de los más importantes en torno al sistema de protección de datos personales".[52]

El Código Fiscal de la Federación, en su artículo 69 dispone la obligación de los servidores públicos de guardar absoluta reserva respecto de las declaraciones y datos que entrega el contribuyente.

En temas de salud, la Ley General de Salud, establece que los beneficiarios del Sistema de Protección Social en Salud, tienen derecho a ser tratados con confidencialidad.[53]

En salud y seguridad social, la Ley del Seguro Social, establece que los documentos, datos e informes que los trabajadores, patrones y demás personas proporcionen al Instituto Mexicano del Seguro Social, en cumplimiento de las obligaciones que les impone por Ley, serán estrictamente confidenciales y no podrán comunicarse o darse a conocer en forma nominativa e individual. A su vez, declara que no se aplicará lo anterior cuando: I. Se trate de juicios y procedimientos en que el Instituto fuere parte; II. Se hubieran celebrado

---

[51] El artículo referido dispone: "Artículo 298. Las infracciones a lo dispuesto en esta Ley y a las disposiciones que deriven de ella, se sancionarán por el Instituto de conformidad con lo siguiente:
(...)
D) Con multa por el equivalente del 2.01% hasta 6% de los ingresos del concesionario o autorizado por:
(…)
V. No establecer las medidas necesarias para garantizar la confidencialidad y privacidad de las comunicaciones de los usuarios;".

[52] Basterra, Marcela I., *Protección de datos personales*, Buenos Aires, UNAM-EDIAR, 2008, p. 310.

[53] *Cfr*. Artículo 77 BIS 37 fracción X de la Ley General de Salud.

convenios de colaboración con la Federación, entidades federativas o municipios o sus respectivas administraciones públicas, para el intercambio de información relacionada con el cumplimiento de sus objetivos, con las restricciones pactadas en los convenios en los cuales se incluirá invariablemente una cláusula de confidencialidad y no difusión de la información intercambiada; III. Lo soliciten la Secretaría de la Función Pública, la Contraloría Interna en el Instituto, las autoridades fiscales federales, las instituciones de seguridad social y el Ministerio Público Federal, en ejercicio de sus atribuciones, y IV. En los casos previstos en ley.

Por otra parte, esta Ley hace notar que el Instituto puede celebrar convenios de colaboración con los sectores social o privado para el intercambio de información estadística, relacionada con el cumplimiento de sus objetivos y que la información derivada del seguro de retiro, cesantía en edad avanzada y vejez será proporcionada directamente, en su caso, por las administradoras de fondos para el retiro, así como por las empresas procesadoras de información del Sistema de Ahorro para el Retiro; información que señala estará Esta información estará sujeta, en materia de confidencialidad, a las disposiciones de carácter general que emita la Comisión Nacional del Sistema de Ahorro para el Retiro, en términos de la ley correspondiente.[54]

La Ley Federal de Protección al Consumidor, en su artículo 16, concede al consumidor el derecho de acceso a su información, sin embargo, el plazo que concede para dar respuesta a la misma, es de 30 días hábiles.

No obstante lo indicado anteriormente, a continuación realizaremos un recorrido histórico de los acontecimientos que nos han llevado a tener hoy leyes específicas que protegen los datos personales, tanto para el sector público como privado.

1.1.4.1 *Ley Federal de Acceso a la Información Pública Gubernamental (julio 11, 2002)*

Durante el año de 2001, ante la Cámara de Diputados de la Federación se presentaron tres iniciativas de Ley Federal de Acceso a la Información Pública Gubernamental.

[54] *Cfr*. Artículo 22 de la Ley del Seguro Social.

La exposiciones de motivos[55] se refieren al derecho del libre acceso a la información producida por el Estado, el que al garantizarse debe respetar el derecho a la privacidad. Por lo que exponen que, hasta en tanto no se expidiera una ley en materia de datos personales, las iniciativas en comento, contienen disposiciones específicas dedicadas a tal tema, el cual se presentó como una base para legislación futura específica para la protección de datos personales.

En razón de lo anterior, el dictamen correspondiente de junio de 2002,[56] concluye indicando que el derecho de acceso a la información no debe ser ilimitado, dado que acepta alguna reservas, tales y como la protección de la seguridad nacional, la seguridad pública y la protección de la vida privada.

Ahora bien, el 11 de junio de 2002 se publicó en el Diario Oficial de la Federación la Ley Federal de Transferencia y Acceso a la Información Pública Gubernamental (en adelante "LFTAIPG"),[57] la cual tiene como finalidad "proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal".[58]

A fin de lograr un equilibrio entre el derecho a la transparencia y la protección de la privacidad de la personas,[59] la legislación en comento, contiene un apartado dedicado a la "Protección de Datos Personales", esto es, el Capítulo IV. Los datos personales, son definidos por el artículo 3o. fracción II como información concerniente a una persona física identificada o identificable, dando algunos ejemplos de datos personales, tal y como se transcribe a continuación:

> La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté

[55] Exposición de motivos de la Ley Federal de Acceso a la Información Pública Gubernamental. Disponible en *http://legislacion.scjn.gob.mx/Buscador/Paginas/wfProcesoLegislativoCompleto.aspx?q=EI+gQjK83C7L/d/8KCB3tZtIjA0olo1k5kA5s0Az0/3mRsTKKxvwltTA+JdhcERhRMt8zhqTkHuyE1MiNvj8vg==*, última fecha de consulta el 17 de junio de 2019.

[56] Dictamen de la Ley Federal de Acceso a la Información Pública Gubernamental. Disponible en *http://legislacion.scjn.gob.mx/Buscador/Paginas/wfProcesoLegislativoCompleto.aspx?q=EI+gQjK83C7L/d/8KCB3tZtIjA0olo1k5kA5s0Az0/3mRsTKKxvwltTA+JdhcERhEgjwsdDRf54DN/Pn+oG4IQ==*, última fecha de consulta el 17 de junio de 2019.

[57] Ley Federal de Transferencia y Acceso a la Información Pública Gubernamental. Disponible *en https://www.dof.gob.mx/nota_detalle.php?codigo=727870&fecha=11/06/2002*, última fecha de consulta el 17 de junio de 2019.

[58] Véase artículo 1o. de la LFTAIPG.

[59] Tenorio Cueto, Guillermo, *Los datos personales en México*, México, Porrúa y Universidad Panamericana, 2012, pp. 17 a 19.

> referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad;

La LFTAIPG se refiere a los principios de consentimiento, información, calidad y proporcionalidad; así como al deber de seguridad y a los derechos de acceso y corrección de datos personales.

Respecto del principio del consentimiento,[60] la ley prohíbe a los sujetos obligados referidos en el artículo 1o. de la misma, difundir, distribuir o comercializar los datos personales que se contengan en sus sistemas de información,[61] a menos de que exista consentimiento expreso por escrito o por un medio de autenticación de los individuos a que hace referencia dicha información. Previendo las siguientes excepciones: (i) Tratándose de cuestiones médicas o servicios de salud; (ii) Cuando se realice con fines estadísticos, siempre y cuando, los datos estén desasociados; (iii) Cuando los datos se transmiten entre sujetos obligados para el cumplimiento de sus facultades; (iv) Cuando exista una orden judicial; (v) A terceros cuando le sea contratado para la prestación de un servicio, lo que hoy en día se conoce como remisión, y (vi) En los demás casos que así lo establezcan las leyes.

Por cuanto hace al principio de información,[62] la establece como obligación para los sujetos obligados poner a disposición de los individuos, desde el momento en el que recaban los datos, el documento en el que se establezcan los propósitos de su tratamiento.

Sobre el principio de proporcionalidad,[63] se establece la obligación de que los datos personales solo pueden ser tratados cuando sean adecuados, pertinentes y no excesivos relacionados con los propósitos para los cuales fueron obtenidos.

---

[60] Véanse artículos 21 y 22 de la LFTAIPG.
[61] *Ibidem*, artículo 3o. fracción XIII, “Sistema de datos personales: El conjunto ordenado de datos personales que estén en posesión de un sujeto obligado”.
[62] *Ibidem*, artículo 20 fracción III.
[63] *Ibidem*, artículo 20 fracción II.

Del principio de calidad,[64] solamente se indica que los sujetos obligados deben procurar que los datos personales sean exactos y actualizados.

Por lo que se refiere a las medidas de seguridad,[65] se establece que los sujetos obligados deben adoptar las medidas necesarias para evitar que los datos personales sean alterados, perdidos o transmitidos o se tenga un acceso a ellos sin autorización.

Finalmente, la LFTAIPG prevé que los individuos tienen los derechos de acceso y corrección respecto de sus datos personales, sin embargo, solo es respecto del primero, que establece que las reglas para su ejercicio.

1.1.4.2 *Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (junio 11, 2003)*

El Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (en adelante "RLFTAIPG"),[66] tuvo por objeto reglamentar lo dispuesto por la LFTAIPG.

En particular, por cuanto hace a la protección de los datos personales, se contiene un capítulo respecto de la Protección de los Datos Personales.

El Reglamento indica que para el ejercicio del derecho de acceso y el de corrección, se deberá atender a lo dispuesto en los Lineamientos que expidiera el entonces Instituto Federal de Acceso a la Información.[67]

Por otro lado, el mismo Reglamento, dispone que los sistemas de datos personales deben hacerse del conocimiento del Instituto y del público en general, a través de sus sitios en internet.[68]

1.1.4.3 *Lineamientos de Protección de Datos Personales (septiembre 30, 2005)*

Toda vez que el artículo 37 de la LFTAIPG, así como los diversos 2, 47 y 62 del RLFTAIPG disponían que el entonces Instituto Federal de Acceso a la

---

[64] *Ibidem*, artículo 20 fracción IV.
[65] *Ibidem*, artículo 20 fracción VI.
[66] Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Disponible en *http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf*, última fecha de consulta el 13 de junio de 2019.
[67] Véase artículo 47 del RLFTAIPG.
[68] *Ibidem*, artículo 48.

Información debía emitir Lineamientos en materia de Protección de Datos Personales, es que el 30 de septiembre de 2005, se publicaron en el Diario Oficial de la Federación los Lineamientos de Protección de Datos Personales,[69] los cuales tuvieron por objeto

> establecer las políticas generales y procedimientos que deberán (debían) observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.[70]

Los Lineamientos en referencia se refieren a 6 grandes apartados: (i) Principios rectores de la Protección de los Datos Personales; (ii) El tratamiento de los Datos Personales; (iii) La transmisión de los Datos Personales; (iv) La seguridad de los Sistemas de Datos Personales; (v) El Sistema Persona, y (vi) El Instituto Federal de Acceso a la Información.

En los Lineamientos se prevé que son 7 los principios rectores en materia de protección de datos personales: (i) licitud; (ii) calidad; (iii) acceso y corrección; (iv) información; (v) seguridad; (vi) custodia, y (vii) consentimiento para su transmisión.

El lineamiento sexto se refiere al principio de licitud el cual se refiere al cumplimiento de tres condiciones: (i) La posesión de los sistemas de datos personales solo debe atender a las atribuciones legales del sujeto obligado; (ii) Los datos personales deben obtenerse por medios previstos en las disposiciones que regulan su posesión, y (iii) El tratamiento de datos personales deben tratarse para las finalidades para las cuales se obtuvieron, las cuales deben ser determinadas y legitimas.

Respecto de la calidad de los datos personales, el lineamiento séptimo dispone que el tratamiento de los datos personales debe ser, además de exacto, adecuado, pertinente y no excesivo, características que hoy se refieren al principio de proporcionalidad.

---

[69] Lineamientos de protección de datos personales. Disponible en *http://dof.gob.mx/nota_detalle.php?codigo=2093669&fecha=30/09/2005*, última fecha de consulta el 18 de junio de 2019.
[70] Véase artículo 1o. de los Lineamientos de Protección de Datos Personales.

Por cuanto hace al acceso y corrección de los datos personales, el lineamiento octavo disponía que los sistemas de datos personales debían ser almacenados de tal manera que permitan el ejercicio de los derechos de acceso y corrección.

El lineamiento noveno disponía que, al momento de recabar los datos personales, los sujetos obligados, debían de manera escrita, hacer del conocimiento del titular de los datos: (i) El fundamento y motivo de la recolección de los datos, y (ii) propósitos para los cuáles serán tratados los datos personales.

A diferencia de lo que, actualmente, dispone la norma vigente, el lineamiento noveno se refería al deber de seguridad como un principio, el que se traduce en la obligación de los sujetos obligados para garantizar la integridad, confiabilidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

El principio contenido en el lineamiento undécimo se refiere a la custodia y cuidado de la información, el que se refiere a que los responsables,[71] encargados[72] y usuarios,[73] debían garantizar el manejo cuidadoso en el tratamiento de los datos personales.

El último principio se refiere al consentimiento del titular para la transmisión[74] de sus datos personales, el cual debe otorgarse de forma libre, expresa e informada, salvo las excepciones que ya preveía la Ley.

Respecto el segundo apartado de los Lineamientos, esto es, el tratamiento de los datos personales, en el que las disposiciones normativas se

---

[71] Lineamiento tercero fracción "IV. Responsable: El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales".

[72] Lineamiento tercero fracción "II. Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales".

[73] Lineamiento tercero fracción "IX. Usuario: Servidor público facultado por un instrumento jurídico o expresamente autorizado por el Responsable que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido".

[74] Lineamiento tercero fracción "VI. Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita".

refieren a las condiciones específicas del cumplimiento de los principios referidos anteriormente.

- Principio de calidad: Específica lo que debe entenderse por exacto, adecuado, pertinente y no excesivo, tal y como se transcribe a continuación:

> a) Exacto: Cuando los datos personales se mantienen actualizados de manera tal que no altere la veracidad de la información que traiga como consecuencia que el Titular de los datos se vea afectado por dicha situación;
>
> b) Adecuado: Cuando se observan las medidas de seguridad aplicables;
>
> c) Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de las dependencias y entidades que los hayan recabado, y
>
> d) No excesivo: Cuando la información solicitada al Titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubieran recabado.[75]

El lineamiento decimocuarto establecía que los responsables, encargados o usuarios que identificaran que los datos personales fueran inexactos, debían corregirlos de oficio, con la condición de que contaran con los documentos que con los cuales pudiera justificarse su actualización.

Asimismo, respecto del principio de calidad, se establecían las reglas de la conservación de los datos personales, esto es, que los datos personales que no contengan un valor histórico, científico, estadístico o contable, los mismos deben ser dados de baja conforme a los siguientes plazos:[76]

a) El establecido en el formato en el que hubiera sido recabado.
b) El establecido por la ley.
c) El establecido en el convenio entre el titular y el sujeto obligado.
d) Lo que se hubiere señalado en los convenios de transmisión.

- Principio de seguridad: El lineamiento DECIMOSEXTO indica que solamente se podrían tratar los datos personales que reunieran las condiciones de seguridad a las que se hará referencia más adelante.
- Principio de información: Respecto del documento que debe ponerse a disposición en el momento en el que se recaben los datos personales, el

[75] Véase Lineamiento Décimo Tercero.
[76] Véase Lineamiento Décimo Quinto.

lineamiento decimoséptimo establece que los requisitos del mismo, estos son:

a) La mención de que los datos serán protegidos conforme a lo que dispone la Ley.
b) El fundamento legal para el tratamiento.
c) La finalidad del sistema de los datos personales.

Al final del segundo apartado, el lineamiento vigésimo primero refería a lo que en la legislación actual se conoce como remisión de datos personales, el cual estipulaba que la relación con el tercero debía estipularse en un contrato en el que se indicaran las medidas de seguridad y custodia que los lineamientos contenían.

El tercer apartado se refería a la figura de transmisión,[77] la cual en principio podría efectuarse sin consentimiento del titular, para los que casos que se establecían en la Ley de la cual estos Lineamientos emanaron, esto es:[78] (i) Para cuestiones de salud; (ii) Razones estadísticas, científicas o de interés general; (iii) Entre sujetos obligados cuya transmisión se basara en ejercicio de sus facultades; (iv) Por existir una orden judicial; (v) Cuando un tercero es contratado para realizar servicio contemplado dentro del tratamiento[79], y (v) en los demás casos establecidos por las leyes.

Fuera de los supuestos referidos anteriormente, podrían efectuarse transmisiones de datos personales[80], solamente si una disposición legal lo preveía y, mediara consentimiento expreso de su titular.[81]

---

[77] Lineamiento tercero fracción "VI. Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita".
[78] Véase artículo 22 de la LGTAIPG.
[79] Lo que la Ley aplicable actual denomina como remisión de datos personales.
[80] Véase Lineamiento Vigésimo Tercero.
[81] De conformidad con lo dispuesto por el Lineamiento Vigésimo Cuarto, el consentimiento del titular debía otorgarse por escrito incluyendo la firma autógrafa y la copia de identificación oficial, o bien a través de un medio de autenticación. Asimismo, se establecía que el servidor público que estuviera a cargo de recabar el consentimiento del titular, debía entregar al mismo, previo a cada transmisión, la información suficiente acerca de las implicaciones de otorgar su consentimiento. Aunado a ello, de conformidad con lo establecido en el lineamiento subsecuente al comentado, el responsable del tratamiento - servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos

Continuando con el cuarto apartado, el que se refiere a la seguridad de los sistemas de datos personales, tenemos que se establecía como obligación de los titulares de las dependencias y entidades:[82]

- Designar a los responsables en términos de lo entendido como tal y que se ha hecho ya referencia.
- Proponer al Comité de Información, la emisión de criterios en la materia, la difusión de la norma aplicable y, la elaboración de un plan de capacitación.

Resulta necesario destacar que los lineamientos preveían por cada dependencia o entidad, la elaboración de un documento de seguridad,[83] en el que establecieran las medidas administrativas, físicas y técnicas[84] para evitar la alteración, pérdida o acceso no autorizado de los datos personales.

El quinto apartado se refería al denominado Sistema Persona, esto es, la "aplicación informática desarrollada por el Instituto (Federal de Acceso a la Información) para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos",[85] las obligaciones de actualización de la información contenidas en el mismo, debían realizarse los primeros diez días hábiles de los meses enero y julio.[86]

---

personales tenía la obligación de notificar al Instituto Federal de Acceso a la Información las transmisiones de datos personales.

[82] Véase Lineamiento Vigésimo Séptimo.

[83] Véase Lineamiento Trigésimo Tercero.

[84] De conformidad con lo dispuesto por el Lineamiento Trigésimo Cuarto, el documento de seguridad debía cumplir con los siguientes requisitos: "I. El nombre, cargo y adscripción de los Responsables, Encargados y Usuarios; II. Estructura y descripción de los sistemas de datos personales; III. Especificación detallada del tipo de datos personales contenidos en el sistema; IV. Funciones y obligaciones de los servidores públicos autorizados para acceder al sitio seguro y para el tratamiento de datos personales; V. Medidas, normas, procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido en los presentes Lineamientos, las cuales deberán incluir lo siguiente: a) Establecer procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación del Sistema de datos personales; b) Actualización de información contenida en el Sistema de datos personales; c) Procedimientos de creación de copias de respaldo y de recuperación de los datos; d) Bitácoras de acciones llevadas a cabo en el Sistema de datos personales; e) Procedimiento de notificación, gestión y respuesta ante incidentes; y f) Procedimiento para la cancelación de un Sistema de datos personales".

[85] Lineamiento Tercero, fracción III.

[86] Véase Lineamiento Cuadragésimo.

El último apartado, sin embargo, el más importante por el tema que se aborda en el presente, nos referimos a las facultades que se concedían al entonces Instituto Federal de Acceso a la Información, pues nos referimos a su facultad de supervisión del cumplimiento de lo expuesto anteriormente, lo que de no ocurrir, se haría del conocimiento del Órgano Interno de Control que correspondiere, a efecto de que él mismo, aplicare lo conducente, de conformidad con lo dispuesto por la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.[87]

1.1.4.4 *Plan Nacional de Desarrollo (2007)*

El Plan Nacional de Desarrollo 2007-2012,[88] planteó cinco ejes para su política pública: (i) Estado de Derecho y seguridad; (ii) Economía competitiva y generadora de empleos; (iii) Igualdad de oportunidades; (iv) Sustentabilidad ambiental, y (v) Democracia efectiva y política exterior responsable.

Dentro del quinto eje se contiene el objetivo quinto del mismo, el que se refiere a "Promover y garantizar la transparencia, la rendición de cuentas, el acceso a la información y la protección de los datos personales en todos los ámbitos de gobierno", derivado del cual, se desprenden dos estrategias referentes a la protección de los datos personales:

Estrategia 5.2 Fortalecer a los organismos encargados de facilitar el acceso a la información pública gubernamental y de proteger los datos personales.

Estrategia 5.3 Desarrollar el marco normativo que garantice que la información referente a la vida privada y a los datos personales estará protegida.

Para esta última estrategia se destaca que, si bien era cierto que para ese momento se garantizaba la protección de los datos personales en posesión del gobierno, se veía necesario contar con una ley que regulara el tratamiento de los datos en posesión de los particulares, es aquí donde esbozamos el nacimiento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, a la que haremos referencia más adelante.

---

[87] Véanse Lineamientos Cuadragésimo Tercero y Cuadragésimo Cuarto.

[88] Plan Nacional de Desarrollo 2007-2012. Disponible en *http://pnd.calderon.presidencia.gob.mx/pdf/PND_2007-2012.pdf*, última fecha de consulta el 20 de agosto de 2019.

1.1.4.5 *Reforma al artículo 6 de la Constitución Política de los Estados Unidos Mexicanos (julio 20, 2007)*

Con fecha 20 de julio de 2007 fue publicado en el Diario Oficial de la Federación la adición de un segundo párrafo al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, del que es relevante destacar ahora la fracción II:

> Artículo 6o. (…)
>
> Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> (…)
>
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.[89]

La iniciativa[90] que dio origen al texto referido anteriormente, tiene su origen en la garantía que debía brindarse del acceso a la información pública, el cual debía regirse por diversos principios, destacando ahora, el principio se refiere a la inexistencia de derechos ilimitados, referida a la protección de la vida privada de las personas, y en consecuencia, la de sus datos personales, la cual debía adquirir el carácter de confidencial y su acceso debía quedar determinado por la leyes.

1.1.4.6 *Reforma al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (noviembre 25, 2008)*

El 1o. de junio de 2009 se publicó en el Diario Oficial de la Federación la reforma al artículo 16 de la Constitución,[91] el que en la actualidad sigue siendo el mismo texto, tal y como se transcribe a continuación:

> "Artículo 16. (…)

[89] Con fecha 29 de enero de 2016 el párrafo segundo fue reformado para quedar como apartado A del artículo 6o. Constitucional.
[90] Iniciativa que reforma el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos. Disponible en *https://www.ctainl.org.mx/descargas/IniciativaGacetaParlamentaria[1].pdf*, última fecha de consulta el 20 de agosto de 2019.
[91] Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf*, última fecha de consulta el 20 de agosto de 2019.

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
>
> (…)"

1.1.4.7 *Reforma al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos (abril 30, 2009)*

Con fecha 27 de marzo de 2007 fue presentada ante la Cámara de Diputados una iniciativa de reforma al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos,[92] el que se basa en lo dispuesto por el artículo 6o. Constitucional, al cual nos hemos referido anteriormente.

Asimismo, la iniciativa hace referencia a los derechos que se contenían en los artículos 7o. y 16 del nuestra Carta Magna, identificando a la protección de los datos personales como un derecho en construcción, dado que se trataba de garantías del gobernado frente al Estado, sin embargo, se veía nula la protección de dicho derecho frente a los entes de carácter privado.

En razón de lo anterior, se propuso la adición del inciso O) a la fracción XXIX del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, como a continuación se indica: "Artículo 73. El Congreso tiene facultad: […] XXIX-O Para legislar en materia de protección datos personales en posesión de particulares. [...]".[93]

1.1.4.8 *Ley Federal de Protección de Datos Personales en Posesión de Particulares (julio 5, 2010) y su Reglamento (diciembre 21, 2011)*

El 5 de julio de 2010 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley Federal de Protección de Datos Personales en

[92] Puede ser consultado el proceso legislativo de reforma al artículo 73 Constitucional. Disponible en *https://www.sitios.scjn.gob.mx/constitucion1917-2017/sites/default/files/CPEUM_1917_CC/procLeg/185%20-%2030%20ABR%202009.pdf* , última fecha de consulta el 20 de agosto de 2019.

[93] Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_185_30abr09.pdf*, última fecha de consulta el 20 de agosto de 2019.

Posesión de los Particulares[94] (LFPDPPP) y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Resultado de lo anterior, desde entonces se regula que el tratamiento que se realiza de los datos personales por parte de los particulares, se haga de manera legítima, controlada e informada, teniendo ello como consecuencia garantizar la privacidad de los titulares y su derecho de la autodeterminación informativa[95].

Posteriormente, el 21 de diciembre de 2011, se emitió el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[96] (RLFPDPPP), cuyo objetivo ha sido reglamentar la ley emitida en 2010.

De ambos instrumentos normativos se deriva que, los particulares deben tratar los datos personales conforme a mandatos legales, cuyo incumplimiento podría derivar en el inicio de procedimientos administrativos, imposición de sanciones administrativas, y en su caso, la imposición de sanciones penales. A continuación, nos permitimos referirnos brevemente al contenido de dicha normatividad.

1.1.4.8.1 Sujetos regulados

De conformidad con el artículo 2o. de la LFPDPP, quienes deben dar cumplimiento de la protección de los datos personales, son aquéllos particulares, ya sean estos personas físicas o morales, cuya naturaleza es de carácter privado y que llevan a cabo el tratamiento de datos personales y son denominados "responsables del tratamiento".

[94] *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*, última fecha de consulta el 20 de agosto de 2019.

[95] Es importante referirnos a la Sentencia del Tribunal Constitucional Federal Alemán del 15 de diciembre de 1983 sobre la Ley del Censo de 31 de marzo de 1982, en la que configura a la autodeterminación informativa como "la facultad del individuo, (…) de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida. (...)". *Cfr*. Murillo de la Cueva, Pablo Lucas, *El derecho a la…, op. cit*., nota 13, p. 122.

[96] *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares*. Disponible en http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf, última fecha de consulta el 20 de agosto de 2019.

1.1.4.8.2 Datos personales

Los datos personales son definidos por la propia LFPDPPP en su artículo 3o. fracción V, definiéndolos como "cualquier información concerniente a una persona física identificada o identificable". Son ejemplos de datos personales, el nombre, el domicilio, números de teléfono, correo electrónico, características físicas, informes médicos, fotografías, videos, voz, por mencionar algunos.[97]

Ahora bien, existe una clasificación de datos personales, aquéllos llamados sensibles, que se refiere a:

> Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.[98]

Dichos datos personales tienen reglas muy particulares para llevar a cabo su tratamiento, pues como se ha podido advertir, en caso de tratarlos indebidamente podría ocasionar daños graves o poner en riesgo a la persona física de quien pertenecen a quien la ley denomina "titular".

1.1.4.8.3 Tratamiento de datos personales

El tratamiento de los datos personales puede resumirse en cualquier actividad que sea realizada a los datos personales, esto es obtenerlos, usarlos, divulgarlos o guardarlos.

Consecuencia de lo anterior, cualquier particular que realice tratamiento de datos debe observar lo dispuesto en la normatividad en materia de protección de datos personales, que podemos agrupar en tres grandes secciones: principios, deberes y obligaciones.

Ahora bien, cuando dentro del tratamiento se realiza comunicación de datos personales, la misma puede efectuarse como una remisión o una transferencia. La primera, es la que se hace a un "encargado del tratamiento",

---

[97] Murillo de la Cueva, Pablo Lucas, *El derecho a la…*, *op. cit*., nota 13, p. 117. Realiza un análisis sobre la técnica de la protección de los datos que protege la norma, pues no solamente se trata a datos que versan sobre la intimidad, pues se puede tratar de datos ya conocidos por un determinado círculo de personas próximo al titular, ya sea por razones afectivas o profesionales.
[98] Véase artículo 3o. fracción VI de la LFPDPPP.

quien deberá tratar los datos conforme a las instrucciones y por cuenta del responsable del tratamiento. Por otro lado, la transferencia de datos personales es la comunicación que se hace a otro responsable del tratamiento, ello es, porque ese nuevo responsable será quien decida sobre el tratamiento de los datos personales.[99]

1.1.4.8.4 Principios

Los principios son enunciados normativos que rigen el deber actuar de quienes tratan datos personales y son ocho: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

El principio de finalidad, regulado en los artículos 7o. de la LFPDPPP y 10 del RLFPDPPP, y se traduce en que el tratamiento de los datos personales debe llevarse a cabo de conformidad con lo estipulados en las leyes mexicanas y el Derecho Internacional.

El principio de consentimiento[100] se traduce en l*a* aceptación del titular para que el responsable trate sus datos, de conformidad con una o varias finalidades determinadas. El consentimiento puede otorgarse de manera tácita, esto es, cuando no existe oposición y expresa, esto es, que se requiere de un mecanismo en el que se deje constancia de la aceptación, como puede ser verbal, escrita, a través de medios electrónicos, ópticos o cualquier otra tecnología o a través de signos inequívocos. Cuando se trata de datos patrimoniales o financieros, se debe otorgar de manera expresa, sin embargo, cuando se trata de datos sensibles, el consentimiento debe ser expreso y por escrito, ello de conformidad con los artículos 8o. y 9o. de la LFPDPPP.

El consentimiento debe otorgarse observando que su obtención sea:

- Libre. Que no debe exista error, mala fe, violencia o dolo.
- Específica. Se debe referir a una o varias finalidades determinadas que justifiquen el tratamiento.

[99] Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). Disponible en *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF*, última fecha de consulta el 20 de agosto de 2019.

[100] Véase artículo 3o. fracción IV de la LFPDPPP, “Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos”.

- Informada: Previo al tratamiento de los datos, el titular debe tener conocimiento del Aviso de Privacidad, al que nos referimos en breve. Asimismo, debe saber de las consecuencias que traerá el consentimiento otorgado.

Existen excepciones para que el tratamiento deba ser consentido por el titular, las cuales las encontramos en el artículo 10 de la LFPDPPP:

> I. Esté previsto en una Ley;
> II. Los datos figuren en fuentes de acceso público;
> III. Los datos personales se sometan a un procedimiento previo de disociación;
> IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
> V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
> VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o
>
> VII. Se dicte resolución de autoridad competente.

Ahora bien, el principio de información[101] se traduce en el tan afamado Aviso de Privacidad, esto es, el documento a través del cual se da a conocer al titular la información relativa a la existencia y características principales del tratamiento al que sus datos personales serán sometidos. Existen tres tipos de Avisos:

a. El integral que resulta aplicable cuando los datos se obtienen directamente del titular (presencialmente).
b. El simplificado cuando los datos se obtienen del titular, pero a través de medios electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología.
c. El corto que resulta aplicable cuando los datos se obtienen a través de un formato en impresos y cuyo espacio es limitado y mínimo.

[101] Véanse artículos 15 a 18 de la LFPDPPP, 23 a 35 del RLFPDPPP y Lineamientos del Aviso de Privacidad.

El principio de calidad[102] se traduce en que los datos tratados sean exactos, completos, pertinentes, correctos y actualizados de conformidad con la finalidad para la cual son tratados. Asimismo, para cumplir con el principio es necesario observar las reglas de conservación de los mismos, esto es para atender los aspectos administrativos, contables, fiscales, jurídicos e históricos necesarios, por lo que posterior a dicho periodo deben entrar en un periodo de bloqueo, en el que solo podrían ser consultados para determinar posibles responsabilidades derivadas de su tratamiento y pasado dicho periodo, proceder a su posterior supresión.

Ahora bien, el principio de finalidad[103] se refiere a los usos que les será dado a los datos. Las finalidades pueden ser primarias y secundarias, las primeras son las que dan origen a la relación jurídica entre el responsable y el titular y las secundarias se refieren a aquéllas que no dan origen a dicha relación.

El principio de lealtad[104] es que el tratamiento de los datos personales se realice privilegiando la protección a los intereses y su expectativa razonable de privacidad.

El séptimo principio es el de proporcionalidad,[105] que se cumple cuando los datos sujetos a tratamiento resultan ser los necesarios, adecuados y relevantes de conformidad con las finalidades por las que fueron obtenidos.

Finalmente, el principio de responsabilidad es el que se refiere a la vigilancia del cumplimiento de los principios anteriores.

1.1.4.8.5 Deberes

Los deberes en materia de protección de datos personales son dos,[106] el de confidencialidad esto es, que los datos no deben ser divulgados a personas no autorizadas, y el de medidas de seguridad que se traduce en la adopción de medidas físicas, administrativas y técnicas que protejan a los datos personales de sufrir daños, pérdidas, alteraciones, destrucciones o usos, acceso o tratamientos no autorizados.

[102] Véanse artículos 11 de la LFPDPPP y 36 al 39 del RLFPDPPP.
[103] Véanse artículos 12 de la LFPDPPP y 40 a 43 del RLFPDPPP.
[104] Véanse artículos 7o. de la LFPDPPP y 44 del. RLFPDPPP
[105] Véanse artículos 13 de la LFPDPPP y 45 del RLFPDPPP.
[106] Véanse artículos 19 a 21 de la LFPDPPP y 57 a 66 de su Reglamento.

1.1.4.8.6 Obligaciones

Finalmente, las obligaciones se refieren a las acciones que deben ejecutarse para asegurar la protección de los datos personales, las cuales se traducen también en la observancia de los principios y deberes antes mencionados, pero también en las que a continuación se señalan[107]:

a. Designación de la persona o departamento de datos personales.
b. Atención a solicitudes de derechos acceso, rectificación, cancelación y oposición, conocidos como los derechos ARCO.
c. Efectuar acciones de capacitación y concientización al interior de la organización.
d. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable.
e. En caso de existir vulneraciones de seguridad, informarlas inmediatamente.
f. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.
g. Destinar recursos para la instrumentación de los programas y políticas de privacidad.
h. Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.
i. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.
j. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.
k. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.
l. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones.

[107]Véanse artículos 30 de la LFPDPPP y 48 del Reglamento.

m. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

1.1.4.8.7 Remisiones y transferencias

Cuando dentro del tratamiento se realiza comunicación de datos personales, la misma puede efectuarse como a través de una remisión o de una transferencia.

De conformidad con el artículo 2o. fracción IX del RLFPDPPP", la remisión es "la comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano", y por su parte el artículo 3o. fracción IX de la "LFPDPPP", se refiere al encargado como a "la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable" y refuerza lo anterior, lo dispuesto por el diverso 49 del Reglamento de la misma ley, en el que además aclara que el encargado del tratamiento es una persona ajena a la organización y que al tratar datos por cuenta del responsable se presupone la existencia de una relación jurídica que los vincula y que delimita el ámbito de actuación respecto de la prestación del servicio.

Ahora bien, dicha comunicación entre el responsable y el encargado presupone una relación jurídica, la cual debe quedar establecida, ya sea mediante cláusulas contractuales o a través de cualquier otro instrumento jurídico que el responsable decida, con el fin de que a partir de los mismos se pueda acreditar su existencia, alcance y contenido.[108]

Al encargado del tratamiento le han sido conferidas obligaciones legales contenidas en el artículo 50 del RLFPDPPP, el que, por su importancia, ahora me permito trascribir a continuación:

> I. Tratar únicamente los datos personales conforme a las instrucciones del responsable;[109]
> II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
> III. Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables;
> IV. Guardar confidencialidad respecto de los datos personales tratados;
> V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones

[108] Véase artículo 51 del RLFPDPPP.
[109] Dichas instrucciones deben ser acordes al Aviso de Privacidad que corresponda.

del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y

VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente. Los acuerdos entre el responsable y el encargado relacionados con el tratamiento deberán estar acordes con el aviso de privacidad correspondiente…

Ahora bien, en aquéllos casos en los que el encargado destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o realice una transferencia sin cumplir las instrucciones del responsable, el encargado será considerado como responsable, quien deberá responder por sus actos.[110]

Por último, por cuanto hace a la figura de remisión de datos personales, debemos referirnos a la posibilidad que existe de que el encargado del tratamiento realice una subcontratación para llevar a cabo las instrucciones del encargado, sin embargo, dicha subcontratación deberá ser autorizada por el responsable, toda vez que el tratamiento por parte del subencargado deberá realizarse en nombre y por cuenta del responsable.[111]

Por otro lado, es también el artículo 3o. fracción XIX de la LFPDPPP que define a la transferencia como “toda comunicación de datos realizada a personal distinta del responsable o encargado del tratamiento”. Es por lo anterior, que la transferencia se realizar a otra persona, la que adquiere el carácter de responsable.

A diferencia de la remisión de datos personales, las transferencias deben ser informadas y autorizadas por sus titulares,[112] salvo los siguientes casos:

I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

[110] Véase artículo 53 de la LFPDPPP.
[111] Véase artículo 54 del RLFPDPPP.
[112] Véase artículo 36 de la LFPDPPP.

V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.[113]

Las transferencias pueden adquirir el carácter de nacionales o internacionales, lo que depende si el receptor de los datos personales se encuentra o no en territorio nacional.[114] Al igual que en las remisiones, es necesario que las transmisiones sean formalizadas mediante cláusulas contractuales o instrumentos jurídicos, a través de los que se indiquen las condiciones de dicha comunicación de datos.[115]

1.1.4.8.8 Derechos ARCO

Los titulares de datos personales, esto la persona física a la que pertenecen dichos datos, la normatividad mexicana le ha conferido cuatro derechos, de acceso, rectificación, cancelación y oposición, los tan famosos Derecho ARCO.

Tabla 1 Derechos Arco

	Acceso	**Rectificación**	**Cancelación**	**Oposición**
Artículos de la Ley.	Artículos 28, 29 y 32 a 35.	Artículos 28, 29, 31, 32 y 34.	Artículos 28, 29 y 32.	Artículos 28, 29 y 32.
Artículos del Reglamento.	Artículos 87 a 102.	Artículos 87 a 98, 100, 103 y 104.	Artículos 87 a 98, 100 y 105 a 108.	Artículos 87 a 98, 100, 103 y 109 a 111.
¿Qué es?	**La obtención de sus datos personales.**	**La rectificación de sus datos personales, ya sea porque han cambiado o porque los obtenidos no son los correctos.**	**Es la solicitud del cese del tratamiento.**	**Es la solicitud para que el tratamiento no se realice respecto de ciertas finalidades.**

Fuente: Elaboración propia con base en la normatividad nacional vigente en la materia de protección de datos.

[113] Véase artículo 37 de la LFPDPPP.
[114] Véanse artículos 71 y 74 del RLFPDPPP.
[115] Véanse artículos 73 y 75 del RLFPDPPP.

Todo titular de datos personales, ya sea por su propio derecho, o bien, a través de su representante legal[116] puede presentar, ante cualquier responsable del tratamiento, una solicitud para el ejercicio de uno o cualquiera[117] de los derechos ARCO.

De conformidad con lo dispuesto por el artículo 29 de la LFPDPPP, la solicitud debe: (i) Indicar el nombre del titular, así como su domicilio u otro medio para comunicarle la respuesta de su solicitud;[118] (ii) Acompañar los documentos que acrediten la identidad del titular, y en su caso, de su representante legal; (iii) Describir de manera clara y precisa los datos respecto de los cuales se desea ejercer algún derecho ARCO, y (iv) indicar cualquier elemento o documento que facilite la localización de los datos personales.

Una vez que la solicitud es recibida por el responsable del tratamiento, el mismo cuenta con un plazo de 5 días hábiles para revisar la solicitud, y en caso de que se requiera mayor información respecto de la solicitud, requerirla al solicitante, quien contará con el plazo de 10 días hábiles, contado a partir del día siguiente de su recepción, a efecto de atender el requerimiento, pues de no realizarlo, la solicitud se tendrá por no presentada.[119]

Desde el día en que la solicitud es recibida por el responsable, además de atender lo explicado en el párrafo anterior, contará con el plazo de 20 días hábiles para notificar al titular sobre la procedencia de la solicitud, la que de resultar así, deberá hacerse efectiva dentro de los siguientes 15 días hábiles, siguientes al día en que se realice la notificación de procedencia de la solicitud.[120] De conformidad con lo dispuesto por el artículo 97 del RLFPDPPP, los plazos indicados en este párrafo, pueden ser ampliados por el responsable en una sola ocasión, solo por razón justificada, que sea notificada al titular.[121]

---

[116] Véase artículo 89 del RLFPDPPP.
[117] El artículo 87 del RLFPDPPP dispone que, “el ejercicio de cualquiera de los derechos ARCO no excluye la posibilidad de ejercer alguno de los otros, ni puede constituir requisito previo para el ejercicio de cualquiera de estos derechos”.
[118] De no realizar el señalamiento de domicilio u otro medio para comunicar la respuesta de la solicitud, de conformidad con lo dispuesto por el artículo 95 del RLFPDPPP, la solicitud se deberá tener como no presentada.
[119] Véase artículo 96 del RLFPDPPP.
[120] Véase artículo 32 de la LFPDPPP.
[121] Véanse artículos 32 de la LFPDPPP y 97 del Reglamento.

1.1.4.8.9 Autoridades en materia de protección de datos personales

Son dos las autoridades en materia de protección de datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y la Secretaría de Economía.

El INAI es constitucionalmente el órgano garante, esto es, la autoridad que tiene como principal atribución la de vigilar y verificar el cumplimiento de la normatividad mexicana en materia de protección de datos personales.

Por otro lado, tenemos a la Secretaría de Economía, que funge como autoridad reguladora, cuya atribución en la materia es de coadyuvancia con el INAI.

1.1.4.8.10 Incumplimiento de principios, deberes y obligaciones

Son tres los procedimientos administrativos que prevén tanto la LFPDPPP como el Reglamento, a través de los cuales se puede verificar que los sujetos regulados den cumplimiento a los principios, deberes y obligaciones en torno a la protección de datos personales, estos son, el procedimiento de protección de derechos, de verificación y de imposición de sanciones.

El procedimiento de protección de derechos inicia a través de una solicitud que se presenta ante el INAI por considerar que no le ha sido una solicitud de ejercicios de Derechos ARCO.

El procedimiento de verificación, puede iniciar a través de una denuncia que puede ser presentada por cualquier persona física, o bien, de oficio. El objetivo del procedimiento es “verificar” que el sujeto regulado, un particular, esté tratando los datos personales con apego a la normatividad en materia de protección de datos personales.

Por otro lado, el procedimiento de imposición de sanciones, es resultado de los dos anteriores, pues en los casos en los que se identifican incumplimientos, se sigue este procedimiento, cuyo objetivo es identificar que las conductas constituyan infracciones, las que son sancionadas con multas.

Finalmente, también es importante tener en cuenta que la propia ley prevé sanciones en el ámbito penal, pues prevé dos tipos penales, el que se refiere a la provocación de vulneraciones de seguridad y al tratamiento de datos para alcanzar lucros indebidos.

1.1.4.9 *Reforma en materia de transparencia (febrero 7, 2014)*

Si bien es cierto que la reforma se refiera a la transparencia y acceso a la información,[122] obligando a las autoridades de los tres órdenes de gobierno para implementar mecanismos que garanticen tal derecho, también es cierto que se cubre la necesidad de crear un organismo autónomo e independiente para garantizar no solo el acceso a la información, sino también la protección de los datos personales.

El artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos fue una de las disposiciones que resultaron reformadas, la cual indica:

> Artículo 6o. (…)
> A. (…)
> I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.
> (…)
> IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos que se sustanciarán ante los organismos autónomos especializados e imparciales que establece esta Constitución.
> (…)
> VIII. La *Federación* contará con un *organismo* autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, *responsable de garantizar* el cumplimiento del derecho de acceso a la información pública y a *la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley*.
> (Énfasis añadido).

Resulta de suma relevancia hacer referencia al artículo 73, dado que, con ésta reforma se adicionó la fracción XXIX-S, a través de la cual, se faculta al

[122] Reforma en materia de transparencia. Disponible en *https://www.gob.mx/cms/uploads/attachment/file/66464/13_Transparencia.pdf*, última fecha de consulta el 18 de junio de 2019.

Congreso de la Unión para “expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno”,[123] fundamento legal para la expedición de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, a la que referiré a continuación.

1.1.4.10 *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*

El año 2017 fue el año que vio nacer una norma completa que regula la protección de los datos personales en posesión del Estado, sin embargo, en el siguiente capítulo se analizará específicamente.

[123] Véase fracción XXIX-S de artículo 73 de la Constitución Política de los Estados Unidos Mexicanos.

Capítulo 2

Protección de Datos Personales en el sector público

Capítulo 2 Protección de Datos Personales en el sector público

2.1 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Lineamientos Generales de Protección de Datos Personales para el Sector Público

Tal y como se indica en la exposición de motivos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[124], las reformas en materia de transparencia en nuestro país se constituyen como pilar de la protección de datos personales en posesión del Estado, pues él mismo se establece como un contrapeso para el ejercicio del primer derecho mencionado.

El 26 de enero de 2017 fue publicada en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la que de conformidad con su artículo 1o. párrafo cuarto, tiene por objeto "establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados".

De conformidad con el párrafo quinto del artículo 1o. de la LGPDPPSO, son sujetos obligados "en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos".

La LGPDPPSO está integrada por once títulos, con sus respectivos capítulos, los cuales se mencionan a continuación:

- Título Primero. Deposiciones Generales. Capítulo I Del Objeto de la Ley, y Capítulo II Del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- Título Segundo. Principios y Deberes. Capítulo I De los Principios, y Capítulo II De los Deberes.

[124] Exposición de motivos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en *http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Iniciativa.pdf*, última fecha de consulta el 20 de agosto de 2019.

- Título Tercero. Derechos de los Titulares y su Ejercicio. Capítulo I De los Derechos de Acceso, Rectificación, Cancelación y Oposición; Capítulo II Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición, y Capítulo III De la Portabilidad de los Datos.
- Título Cuarto. Relación del Responsable y Encargado. Capítulo Único Responsable y Encargado.
- Título Quinto. Comunicaciones de Datos Personales. Capítulo Único De las Transferencias y Remisiones de Datos Personales.
- Título Sexto. Acciones Preventivas en Materia de Protección de Datos Personales. Capítulo I De las Mejores Prácticas, y Capítulo II De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia.
- Título Séptimo. Responsables en Materia de Protección de Datos Personales en Posesión de los Sujetos Obligados. Capítulo I Comité de Transparencia, y Capítulo II De la Unidad de Transparencia.
- Título Octavo. Organismos Garantes. Capítulo I Del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; Capítulo II De los Organismos Garantes, y Capítulo III De la Coordinación y Promoción del Derecho a la Protección de Datos Personales.
- Título Noveno. De los Procedimientos de Impugnación en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados. Capítulo I Disposiciones Comunes a los Recursos de Revisión y Recursos de Inconformidad; Capítulo II Del Recurso de Revisión ante el Instituto y los Organismos Garantes; Capítulo III Del Recurso de Inconformidad ante el Instituto; Capítulo IV De la Atracción de los Recursos de Revisión; Capítulo V Del Recurso de Revisión en Materia de Seguridad Nacional, y Capítulo VI De los Criterios de Interpretación.
- Título Décimo. Facultad de Verificación del Instituto y los Organismos Garantes. Capítulo Único Del Procedimiento de Verificación.
- Título Décimo Primero. Medidas de Apremio y Responsabilidad. Capítulo I De las Medidas de Apremio, y Capítulo II De las Sanciones.

Por su parte, con el objetivo de desarrollar lo previsto en la LGPDPPSO, con fecha 26 de enero de 2018, se publicaron en el Diario Oficial de la Federación los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPGPSP).[125]

2.1.1 Aspectos generales de la LGPDPPSO

De conformidad con lo establecido por artículo 1o. de la LGPDPPSO, la misma tiene como objeto "establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados". Indicando también que "en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos" así como "los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal" son considerados como sujetos obligados.

Es preciso, por su competencia en materia de protección de datos personales en el sector público, hacer referencia al Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, el que tuvo su nacimiento en la Ley General de Transparencia y Acceso a la Información Pública[126] (LGTAIP), siendo concebido como un conjunto de miembros, procedimientos, instrumentos y políticas, que tienen como finalidad "coordinar y evaluar las acciones relativas a la política pública transversal de transparencia, acceso a la información y protección de datos personales, así como establecer e implementar los criterios y lineamientos" en las tres materias de su competencia, esto es, transparencia, acceso a la información y protección de datos personales.[127]

---

[125] Publicación en el Diario Oficial de la Federación. Disponible en *http://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018*, y texto de los Lineamientos. Disponible en *https://colaboracion.uv.mx/rept/files/2018/08/066/LinamientosGeneralesDatosPersonales.pdf*, última fecha de consulta de ambos enlaces el 20 de agosto de 2019

[126] Publicada en el Diario Oficial de la Federación el 4 de mayo de 2015. Disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf*, última fecha de consulta el 22 de junio de 2019.

[127] Véase artículo 28 de la LGTAIP.

De conformidad con lo dispuesto por el artículo 30 de la Ley en referencia, el Sistema Nacional está conformado por: (i) El INAI; (ii) Los Organismos garantes de las Entidades Federativas;[128] (iii) La Auditoría Superior de la Federación; (iv) El Archivo General de la Nación, y (v) El Instituto Nacional de Estadística y Geografía.

Ahora bien, en materia de protección de datos personales en posesión de sujetos obligados, de conformidad con lo dispuesto por el artículo 10 de la LFPDPPSO, tiene la función de "coordinar y evaluar las acciones relativas a la política pública transversal de protección de datos personales, así como establecer e implementar criterios y lineamientos en la materia", y su objetivo en la materia es el de diseñar, ejecutar y evaluar un Programa Nacional de Protección de Datos Personales, al cual haré referencia más adelante.[129]

Al igual que la norma aplicable en la materia para el sector privado, los datos personales se refieren a información que concierne a una persona física a quien se le denomina titular, esto es, un individuo que adquiere tal calidad desde el momento en que es concebido y hasta el momento de su muerte. Después se tiene que pensar en cualquier información que gira alrededor de dicho individuo y que a través de la misma se identifique o se pueda identificar con certeza al individuo a que pertenecen. La fracción IX del artículo 3o. de la LGPDPPSO establece la siguiente definición:

> Artículo 3. Para los efectos de la presente Ley se entenderá por:
> (…)
> IX. *Datos personales: Cualquier información* concerniente a una *persona física identificada o identificable*. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;
> (Énfasis y subrayado añadido).

Existe, también como el sector privado, una clasificación de los mismos, toda vez que la normatividad en la materia distingue a los datos personales sensibles, esto es aquélla información de identifica o hace identificable a un individuo, pero que se refieren al ámbito más íntimo de dicho individuo o que su

[128] De conformidad con los dispuesto por el artículo 3o. fracción XVI "Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales en términos de los artículos 6, 116, fracción VIII y 122, apartado C, Base Primera, Fracción V, inciso ñ) de la Constitución Política de los Estados Unidos Mexicanos".
[129] Véase artículo 12 de la LGPDPPSO.

indebido uso pueden conllevar a que dicho individuo sea discriminado o lo coloque en una situación de riesgo grave. El mismo artículo 3 antes referido, define a los datos personales sensibles como a continuación se indica:

> Artículo 3. Para los efectos de la presente Ley se entenderá por:
> (…)
> X. Datos personales sensibles: Aquellos que se refieran a la *esfera más íntima* de su titular, o cuya utilización indebida pueda dar origen a *discriminación* o conlleve un *riesgo grave* para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual"
> (Énfasis y subrayado añadido).

En razón de lo anterior, es necesario identificar si los datos personales de que se trate cumple con alguna de las dos características mencionadas anteriormente: (i) que el uso indebido lleve a que su titular pueda ser discriminado, o (ii) que su uso indebido coloque al titular en una situación de riesgo grave.

El artículo antes mencionado realiza un listado de los datos que considera como sensibles:

1) Datos sobre origen racial o étnico.
2) Datos sobre el estado de salud del individuo, ya sea que dichos datos se refieran a su estado de salud presente o futuro.
3) Datos sobre la información genética del individuo.
4) Datos sobre creencias religiosas.
5) Datos sobre creencias filosóficas.
6) Datos sobre creencias morales.
7) Datos sobre opiniones políticas.
8) Datos sobre preferencia sexual.

Sin embargo, es importante resaltar que dicho listado solo es enunciativo y no limitativo, esto es, que si cualquier otro dato cumple con las características de (i) que el uso indebido lleve a que su titular pueda ser discriminado, o (ii) que su uso indebido coloque al titular en una situación de riesgo grave, dichos datos también deben ser considerados y tratados como sensibles.

Ahora bien, el tratamiento de datos personales debe ser entendido como cualquier operación u operaciones realizadas con los mismos a través de procedimientos manuales o automatizados. Dichas operaciones se pueden relacionar con las siguientes acciones: (i) Obtención; (ii) Uso; (iii) Registro; (iv) Organización; (v) Conservación; (vi) Elaboración; (vii) Utilización; (viii) Comunicación; (ix) Aprovechamiento; (x) Difusión; (xi) Almacenamiento; (xii) Posesión; (xiii) Acceso; (xiv) Manejo; (xv) Aprovechamiento; (xvi) Divulgación; (xvii) Transferencia, o (xviii) Disposición.[130]

De lo anterior tenemos que, cualquier actividad realizada a los datos personales se considera que los mismos están siendo sometidos a tratamiento.

El responsable del tratamiento se define como los sujetos obligados que deciden sobre el tratamiento de los datos personales, esto es, quienes disponen sobre acciones que deban ejecutarse sobre los datos personales bajo su tratamiento.[131] Por otro lado, tal y como se indicaba anteriormente, también el tratamiento de datos personales puede ser realizado bajo la figura de encargado del tratamiento, quien es definido como la persona física o moral, ya sea que pertenezca al ámbito público o privado, ajena al responsable que trata datos personales en nombre y por cuenta del responsable.[132]

Al igual que en el ámbito privado, el público, es el INAI el organismo que tiene la atribución de "garantizar el ejercicio del derecho a la protección de los datos personales en posesión de sujetos obligados",[133] lo cual realiza a través de acciones preventivas como son la capacitación y difusión, y de acciones correctivas conociendo y resolviendo los casos de incumplimiento de la norma.

2.1.2 Principios en materia de protección de datos personales en el sector público

En materia de protección de datos personales en posesión de sujetos obligados, la LGPDPPSO establece ocho principios, los cuales deben ser observados tanto por el responsable del tratamiento como, en su caso, por el encargado del

[130] Véase artículo 3o., fracción XXXIII de la LGPDPPSO.
[131] Véase artículo 3o., fracción XXVIII de la LGPDPPSO.
[132] *Ibidem*, fracción XV.
[133] *Ibidem*, fracción I del artículo 89.

tratamiento. Dichos principios, de conformidad con el artículo 16 de la referida Ley, son licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

El principio de licitud se refiere al cumplimiento de las facultades o atribuciones que la normatividad aplicable le confiere al responsable del tratamiento.[134]

Por su parte, de conformidad con el artículo 18 de la LGPDPPSO, el principio de finalidad se refiere a los propósitos, actividades o tratamientos a los que serán sometidos los datos personales. Dichas finalidades deben cumplir con las siguientes características:[135]

1) Concretas, esto es, que la finalidad sea precisa y determinada;
2) Lícitas, lo que significa que la finalidad debe estar apegada a las facultades y atribuciones de la institución;
3) Explícitas, lo que se logra cuando la finalidad es expresada con claridad, y;
4) Legítimas, que se traduce en dar el carácter de legalidad a la finalidad, esto es, no solo basta con justificar normativamente la finalidad, sino ejecutarla con apego a la ley.

El principio de lealtad, como lo establece el artículo 19 de la LGPDPPSO, se observa cuando se privilegia la protección de los intereses del particular y su expectativa razonable de privacidad.[136]

---

[134] *Ibidem*, artículo 17.

[135] El artículo 9o. de los LGPDPSP se ocupa de definir cada una de las características, tal y como se indica a continuación:
"I. Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión al titular; II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad; III. Lícitas: cuando las finalidades que justifican el tratamiento de los datos son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y IV. Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular…".

[136] De conformidad con lo dispuesto por la fracción I del artículo 11 de la LGPDPSP, se privilegian los intereses del particular cuando el tratamiento de los datos no da lugar a discriminación o tratos arbitrarios o injustos para el mismo. Asimismo, la fracción II de la misma disposición, nos indica que la expectativa razonable de privacidad, debe ser entendida como la confianza que el titular deposita en el responsable, para que los datos sean tratados, en lo general, conforme a lo que dispone la ley, y en lo particular, conforme a lo que indica el aviso de privacidad que ampara su tratamiento.

Asimismo, también como lo establece el ya mencionado artículo 19, para observar el principio de lealtad, es necesario que, el tratamiento de los datos personales, el cual incluye su obtención, no se realice ni por medios engañosos ni fraudulentos, esto es, que los datos personales no sean tratados con dolo, mala fe o negligencia.[137]

Ahora bien, el consentimiento, esto es, el siguiente principio que abordaremos, se traduce en la manifestación de la voluntad a efecto de que aceptar una situación que se materializará a partir de dicho reconocimiento, y comprende la oposición del titular para los datos sean utilizados para distintos fines de los que justificaron su existencia.[138]

En materia de protección de datos personales se debe contar con el consentimiento del titular de los datos personales, y tratándose de incapaces, dicha manifestación de la voluntad debe realizarla su representante. Son incapaces: (i) Los menores de edad; (ii) Los mayores de edad disminuidos o perturbados en su inteligencia, aunque tengan intervalos lúcidos, y (iii) Los mayores de edad que padezcan alguna afección originada por enfermedad o deficiencia que no les permita gobernarse u obligarse por sí mismos.[139]

El consentimiento puede ser manifestado de manera tácita o expresa dependiendo de los datos personales que se pretenda obtener; el primero de los casos resultará aplicable para todos los datos personales, excepto los sensibles y los que la ley de manera expresa requiera de consentimiento expreso, y para el segundo de los casos, esto es, consentimiento expreso, será aplicable tratándose de la obtención de datos sensibles, el cual deberá manifestarse a través de: (i) Firma autógrafa; (ii) Firma electrónica avanzada, o (iii) Cualquier mecanismos de autenticación que se establezca.[140]

Se está en presencia de un consentimiento tácito cuando el titular no manifieste oposición para el tratamiento de sus datos,[141] sin embargo, es importante que se le ponga a disposición el correspondiente aviso de privacidad,

---

[137] Véase fracción II del artículo 11 de los LGPDPSP.
[138] Villanueva, Ernesto y Nucci, Hilda, *Comentarios a la Ley Federal de Protección de Daatos Personales en Posesión de los Particulares*, México, Novum, 2012, p. 34.
[139]Véase artículo 450 del Código Civil Federal, lo cual es totalmente acorde a lo que establece el artículo 20 de la LGPDPPSO en su parte final.
[140]Véase artículo 21 de la LGPDPPSO.
[141]Véase párrafo segundo del artículo 21 de la LGPDPPSO.

al que se hace referencia en el principio de información. Por su parte, el consentimiento expreso para configurarse debe contarse con la manifestación de la voluntad de manera verbal, escrita, a través de medios electrónicos u ópticos, signos inequívocos o por cualquier otra tecnología.[142] Es importante en este punto identificar que se debe contar siempre con la prueba de la obtención del consentimiento.

El consentimiento, de conformidad con lo dispuesto por el artículo 20 de la LGPDPPSO, debe ser otorgado dando cumplimiento a las siguientes características:

1) *Libre.* No debe presentarse ninguno vicio en el otorgamiento del consentimiento, los de que de conformidad con lo dispuesto en los artículos 1812 a 1823 del Código Civil son: (i) Error;[143] (ii) Dolo;[144] (iii) Mala fe,[145] y (iv) Violencia.[146]
2) *Específica.* Ésta característica se encuentra íntimamente vinculada con el principio de finalidad, al que ya nos hemos referido, por lo tanto, es importante destacar que la manifestación de la voluntad tiene que referirse a finalidades deben ser:
    a. Concretas. Una finalidad es concreta cuando adquiere la cualidad de ser específica.
    b. Lícitas. Íntimamente relacionado con principio de licitud, esto es, que la finalidad esté apegada a las atribuciones y funciones del responsable del tratamiento.
    c. Explícitas. Entendida como la finalidad que es expresada de manera clara y determinada.
    d. Legítimas. No basta con justificar la finalidad con un supuesto

[142]Véase primer párrafo del artículo 21 de la LGPDPPSO.
[143] Hay error al existir una diferencia entre la voluntad del titular y los alcances que tiene la manifestación de dicha voluntad, esto es, cuando se configura una falsa apreciación de la realidad.
[144] De conformidad con lo dispuesto por el artículo 1815 del Código Civil Federal, existe dolo cuando se emplea cualquier sugestión o artificio para la inducción del titular al error, o bien, mantenerlo en el error en el que se encuentre.
[145] De conformidad con lo dispuesto por el artículo 1815 del Código Civil Federal, se define a la mala fe como la disimulación del error conocido.
[146] Conforme a lo dispuesto por el artículo 1819 del Código Civil Federal, se configura la violencia cuando se emplea fuerza física o amenazas que importen peligro de perder la vida, la honra, la libertad, la salud, o una parte considerable de los bienes del contratante, de su cónyuge, de sus ascendientes, de sus descendientes o de sus parientes colaterales dentro del segundo grado.

normativo, sino su ejecución debe realizarse observando la ley que le da soporte.

3) *Informada.* Característica relacionada con el principio de información, esto es, que previo el tratamiento de los datos personales, se debe poner a disposición del titular el aviso de privacidad correspondiente, ello con el fin de que la manifestación de la voluntad se realice con conocimiento de los datos personales que se recabarán y las finalidades a las que los mismos serán sometidos.

Finalmente, es importante tener en cuenta que, como regla general, para el tratamiento de los datos personales, se requiere del consentimiento conforme ya se ha indicado, sin embargo, la norma establece excepciones, los que de conformidad con lo dispuesto por el artículo 22 de la LGPDPPSO son:

1) Cuando una ley así lo disponga, sin embargo, dicha disposición debe encontrase en armonía con lo dispuesto la LGPDPPSO;
2) Tratándose de transferencias entre responsables, sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
3) El tratamiento debe realizarse derivado de una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
4) El tratamiento deba realizarse para el reconocimiento o defensa de derechos del titular ante autoridad competente;
5) Si los datos personales se requieren para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el Instituto;
6) De existir una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
7) Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
8) Cuando los datos personales figuren en fuentes de acceso público, entendidas las mismas como los datos, los sistemas o los archivos que por disposición de ley puedan ser consultadas públicamente, la que, en

su caso, puede estar condicionada al pago de una contraprestación, tarifa o contribución;[147]

9) Si los datos personales han sido sometidos a un procedimiento previo de disociación, esto es, que los datos personales no puedan ser asociados a su titular ni permitir su identificación,[148] y

10) Si los datos pertenecen a una persona que ha sido reportada como desaparecida, entendida dicha figura como la ausencia de una persona física de su lugar ordinario de residencia.[149]

El quinto principio es el de calidad tiene como objetivo que los datos personales en posesión del responsable del tratamiento no sean alterados en su veracidad, por lo que conforme a lo dispuesto por el artículo 23 de la LGPDPPSO, ello se cumple cuando los datos son: (i) Completos;[150] (ii) Correctos;[151] (iii) Exactos,[152] y (iv) Actualizados.[153]

Es importante destacar que el artículo referido en el párrafo anterior, se refiere a una presunción, dado que los datos que sean proporcionados por el propio titular, se presume que dichos datos cumplen con el principio de calidad.

Ahora bien, en este principio nos encontramos con un procedimiento muy relevante, esto es, la conservación, bloqueo, cancelación y supresión[154] de los datos personales. Lo anterior quiere decir, que una vez que los datos personales dejan de ser necesarios para las finalidades indicadas en el aviso de privacidad

---

[147] La fracción XVII del artículo 3º de la LGPDPPSO define a las fuentes de acceso público.
[148] La fracción XII del artículo 3º de la LGPDPPSO define al proceso de disociación.
[149] Para que una persona sea declarada como ausente, tiene que observase lo dispuesto en el Código Civil Federal a partir de su artículo 648.
[150] Si bien es cierto que la norma no establece cuando se cumple con dichos requisitos, respecto de la completitud, podemos decir que se cumple cuando los datos personales contienen cada uno de los atributos que se requieren, ello es así, dado que la fracción II del artículo 21 de los LGPDPSP dispone que los datos son completos "cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable".
[151] La característica se cumple cuando el dato personal no contiene errores. Véase fracción I del artículo 21 de los LGPDPSP.
[152] La característica de exactitud está relacionada con la anterior característica, esto es, que sean correctos, sin embargo, la exactitud también está relacionada con lo correcto, lo que es cierto.
[153] Finalmente, un dato personal es actualizado, cuando nos referimos al dato más reciente, el último. De conformidad con la fracción III del artículo 21 de los LGPDPSP, la característica se observa "cuando los datos personales responden fielmente a la situación actual del titular".
[154] Para la supresión de los datos personales, de conformidad con lo dispuesto por el artículo 23 de los LGPDPSP, el responsable debe establecer políticas, métodos y técnicas que cumplan con las características de ser: (i) Irreversibles, esto es, que los datos no se puedan recuperar; (ii) Seguros y confiables, y (iii) Favorables con el medio ambiente.

que correspondan, los mismos deben ser bloqueados durante el periodo de conservación necesario, de acuerdo a las norma aplicables de índole administrativo, fiscal, laboral, jurídico, histórico o cualquier otro, y una vez concluido dicho periodo, los datos personales deben suprimirse.[155]

El sexto principio es el de proporcionalidad, el que de conformidad con lo dispuesto por el artículo 25 de la LGPDPPSO, se observa por el responsable del tratamiento cuando los datos personales sujetos a tratamiento resultan ser adecuados,[156] relevantes[157] y los estrictamente necesarios[158] de conformidad con las finalidades por los que fueron obtenidos y justifican su tratamiento.

El siguiente principio, esto es, el de información se traduce en dar a conocer e informar al titular de los datos personales sobre la existencia y características del tratamiento a que serán sometidos sus datos personales, ello con el objetivo de que dicho titular, decida de manera informada las acciones que adoptará al respecto.[159] Dicho principio se materializa en el aviso de privacidad.[160]

A diferencia que, en el sector privado, para el sector público, la norma solo prevé dos modalidades para los avisos de privacidad, el integral y el simplificado,[161] sin embargo, los requisitos tampoco son los mismos que para el sector privado, aunado a que la norma no específica en qué casos debe ser utilizado cada uno de ellos.

El aviso integral debe contener los requisitos que a continuación se indican:[162]

---

[155] Véanse párrafos tercero y cuarto del artículo 23 de la LGPDPPSO.
[156] La característica de adecuados, se refiere a que los datos personales tratados deben los que se ajustan a las necesidades que motivaron su obtención y su posterior tratamiento.
[157] Que los datos personales tratados sean relevantes se refiere a que los datos personales sean los más importantes o significativos para las finalidades que correspondan.
[158] Por último, que sean los estrictamente necesarios, se refiere a que los datos tratados sean los mínimos posibles para el cumplimiento de las respectivas finalidades. La norma se refiere al criterio de minimización contenido en el artículo 46 del RLFPDPPP.
[159] Véase artículo 26 de la LGPDPPSO.
[160] La LGPDPPSO define en su artículo 3o., fracción II al aviso de privacidad como el "documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos".
[161] Véase artículo 27 de la LGPDPPSO.
[162] Ello de conformidad con lo indicado en el artículo 28 de la LGPDPPSO, que incluye los requisitos del aviso simplificado, contenidos en el diverso 27 de la misma ley. Los artículos 30 a

1. La denominación del responsable;
2. El domicilio del responsable;
3. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
4. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
5. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;
6. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar: a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y b) Las finalidades de estas transferencias;
7. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular;
8. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
9. Información sobre la portabilidad de los datos personales;[163]
10. El domicilio de la Unidad de Transparencia, y
11. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

42 de los LGPDPSP contienen las disposiciones específicas a cumplir para cada uno de los requisitos de los avisos de privacidad.

[163] Posteriormente haremos referencia a los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de los datos personales, sin embargo, ahora es importante destacar que los mismos señalan en su artículo 11 “En el aviso de privacidad integral a que se refiere el artículo 28 de la Ley General o los que correspondan en las legislaciones estatales en la materia, el responsable deberá informar al titular sobre la posibilidad que tiene de solicitar la portabilidad de sus datos personales y su alcance; los tipos o categorías de datos personales que técnicamente sean portables; el o los tipos de formatos estructurados y comúnmente utilizados disponibles para obtener o transmitir sus datos personales, así como los mecanismos, medios y procedimientos disponibles para que el titular pueda solicitar la portabilidad de sus datos personales”.

De los anteriores, los numerales 1, 5, 6 y 7, además de indicar el sitio en donde se podrá consultar el aviso de privacidad integral, son los requisitos de los avisos de privacidad en su modalidad de simplificado.

Finalmente, el artículo 30 de la LGPDPPSO se refiere al último principio, el principio de responsabilidad, el que, si bien no es definido, indica ocho mecanismos que debe adoptar el responsable del tratamiento para que el principio sea cumplido. Dichos mecanismos son los siguientes:

> I. Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;
> II. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;
> III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
> IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
> V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
> VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares;
> VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y
> VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley (la LGPDPPSO) y las demás que resulten aplicables en la materia.

2.1.3 Deberes en materia de protección de datos personales en el sector público

Son dos los deberes en materia de protección de datos personales: (i) El deber de seguridad, y (ii) El deber de confidencialidad, integridad y disponibilidad.

El deber de seguridad se refiere a las medidas de seguridad, esto es, tal y como se refiere la fracción XX del artículo 3o. de la LGPDPPSO el conjunto de

acciones, actividades, controles o mecanismos administrativos,[164] técnicos[165] y físicos[166] que protegen los datos personales.

Al igual que en el sector privado, los responsables del tratamiento en el sector público, para determinar las medidas de seguridad aplicables, deben considerar:[167] (i) El riesgo inherente a los datos personales tratados; (ii) La sensibilidad de los datos personales tratados; (iii) El desarrollo tecnológico; (iv) Las posibles consecuencias de una vulneración para los titulares; (v) Las transferencias de datos personales que se realicen; (vi) El número de titulares; (vii) Las vulneraciones previas ocurridas en los sistemas de tratamiento, y (viii) El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Con el propósito de establecer y mantener las medidas de seguridad, el responsable del tratamiento debe realizar las siguientes actividades:[168]

1) Emitir políticas internas para la gestión y tratamiento de los datos personales.
2) A efecto de identificar el rol de cada servidor público involucrado en el tratamiento de datos personales, es necesario documentar el rol y obligaciones que cada uno tiene de ellos.
3) Realizar un inventario de datos personales, así como de los sistemas que realizan tratamiento[169].
4) Se debe realizar un análisis de riesgo[170] de los datos personales.

---

[164] La fracción XXI del artículo 3.o de la LGPDPPSO las define como “Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales”.
[165] La fracción XXIII del artículo 3oº de la LGPDPPSO las define como “Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.”
[166] La fracción XXII del artículo 3o. de la LGPDPPSO las define como “Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento”.
[167] Véase artículo 32 de la LGPDPPSO.
[168] Véase artículo 33 de la LGPDPPSO.
[169] El artículo 58 de los LGPDPPSO contiene los elementos mínimos del inventario de datos personales.
[170] El Manual Administrativo de Aplicación General Aplicable en las Materias de Tecnologías de la Información y las Comunicaciones (MAAGTICSI) las Políticas y Disposiciones para la Estrategia Digital Nacional en materias de tecnologías de la información y comunicaciones (Política TIC), son disposiciones normativas vigentes que, entre otros, son rectoras para el

5) Por otro lado, debe realizarse un análisis de brecha, esto es, documentar las medidas hoy existentes y las medidas faltantes por implementar.
6) Consecuentemente, deberá realizarse un plan de trabajo tanto para la implementación de las medidas faltantes, como para cumplimiento de las políticas emitidas.
7) Será necesario que se realice un monitoreo de las medidas de seguridad implementadas, así como del estado de las amenazas y vulnerabilidades que pudieran giran en torno a los datos personales de que se trate.
8) Asimismo, será necesario que se diseñe y aplique un programa de capacitación para el personal involucrado sobre las medidas de seguridad que deben implementarse.
9) Por último, se debe elaborar un documento de seguridad,[171] el cual contendrá los numerales antes indicados. Dicho documento deberá ser revisado cuando:
    a. Se produzcan riesgos sustanciales en el tratamiento de datos personales y que modifique su nivel de riesgo.
    b. Se identifique la necesidad de su mejora, la cual puede derivar de las actividades de monitoreo y revisión, o bien, para mitigar el impacto de una vulnerabilidad ocurrida.
    c. Requerimiento correctivo derivado de una vulnerabilidad.

Dispone el artículo 38 de la LGPDPPSO que se consideran vulneraciones a la seguridad: (i) La pérdida o destrucción no autorizada; (ii) El robo, extravío o copia no autorizada; (iii). El uso, acceso o tratamiento no autorizado, o (iv) El daño, la alteración o modificación no autorizada. Al ocurrir cualquiera de las anteriores, se deberá:

Instituto en materia de seguridad de la información, por lo tanto, las acciones hoy adoptadas para su cumplimiento son de gran apoyo para el cumplimiento del deber de seguridad establecido en la LGPDPPDO. En particular, el artículo 24 de la Política TIC y el Proceso ASI del MAAGTICSI prevén la elaboración del análisis de riesgo y que es definido por el MAAGTICSI como: “El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a las infraestructuras de información esenciales y/o críticas o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas”.

[171] Esta actividad se encuentra dispuesta en el artículo 36 de la LGPDPPSO.

1) Inscribir la vulneración en la bitácora correspondiente, la cual al menos: (i) La descripción de la vulnerabilidad; (ii) La fecha en que ocurrió; (iii) El motivo de la vulneración, y (iv) Las acciones correctivas que se implementaron para concluir de manera definitiva con dicha vulneración.[172]
2) Si se causara una afectación significativa en los derechos patrimoniales o morales del (de los) titulare (s) afectado (s), notificarle (s) inmediatamente,[173] así como al INAI sobre la vulneración ocurrida.

   La afectación significativa de manera ejemplificativa se refiere a una vulneración relacionada con en el titular y sus sentimientos, afectos, creencias, decoro, honor,[174] reputación, vida privada, configuración y aspectos físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica.[175]

   La notificación de la vulneración debe, al menos, contener la siguiente información, tal y como lo dispone el artículo 41 de la LGPDPPSO:

   a. La naturaleza del incidente;
   b. Los datos personales comprometidos;
   c. Las recomendaciones al titular respecto de las medidas que el mismo pueda adoptar para proteger sus intereses;
   d. Las acciones correctivas que se han realizado, y
   e. Los medios donde puede obtener más información sobre el motivo que dio origen a la notificación.

Las medidas de seguridad implementadas deben tener el propósito de garantizar la confidencialidad, integridad y disponibilidad de los datos personales. La confidencialidad o como también se le conoce, el deber de

[172] Véase artículo 39 de la LGPDPPSO.
[173] El artículo 66 de los LGPDPPSO establece el plazo máximo de 72 horas para realizar dicha notificación, el cual comienza a correr desde el mismo día natural en el que se confirme la vulneración.
[174] Se retoma el concepto de dignidad humana, dado que el honor derivad de la misma, esto es no ser humillado ante uno mismo o los demás, por lo tanto, el honor se clasifica dentro de derechos de proyección social, entendida cono la opinión o estima que de la persona tienen los demás. *Cfr*. Caballero Gea, José Alfredo, Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen. Derecho de Rectificación. Calumnia e Injuria, 2a. ed., España, Dykinson, 2007, p. 21.
[175] Véase último párrafo del artículo 66 de los LGPDPSP.

secreto, es la no divulgación de los datos sometidos al tratamiento, sin embargo, es un deber que se verifica con medidas que aseguren mecanismos bajo los cuales, los servidores públicos que operan los datos, aseguren su custodia y deber de guardarlos, aun así, cuando la relación laboral hubiere terminado.[176]

2.1.4 Derechos de los titulares en el sector público

En materia de protección de datos personales en el sector público, son cinco los derechos que tienen los titulares,[177] los derechos ARCO y el de portabilidad.

El derecho de acceso es la facultad del titular[178] para acceder a sus datos personales, pero además con base en el mismo, puede conocer las condiciones del tratamiento de los mismos.[179] Por su parte, el derecho de rectificación es la corrección de datos personales, cuando los mismos sean inexactos, incompletos o se encuentren desactualizados.[180] El derecho de cancelación se ejerce a efecto de que los datos personales del solicitante, dejen de ser tratados, y tal como lo referimos anteriormente, la cancelación conlleva el bloqueo y posterior supresión de los datos personales.[181] Finalmente, el derecho de oposición implica que los datos personales no se traten, porque de continuar con el mismo, causa o causaría daño o perjuicio al titular.[182]

Los responsables del tratamiento deben definir procedimientos sencillos para que los titulares ejerzan sus derechos, sin embargo, la norma establece plazos que deben ser observados: (i) Para definir la procedencia del derecho, el responsable cuenta con 20 días hábiles contados a partir del día siguiente a la fecha de su recepción. Este plazo se puede ampliar hasta por 10 días hábiles

[176] López-Vidriero Tejedor, Iciar y Santos Pascual, Efrén, Protección de Datos Personales. Manual práctico para empresas, España, FC Editorial e ICEF Consultores, 2000, pp. 63 y 64.
[177] Cabe destacar que, si bien es cierto que la LGPDPPSO solamente se refiere a los derechos de acceso, rectificación, cancelación y oposición, y solo hace referencia a la portabilidad, es importante destacar que, los Lineamientos de Portabilidad, los definen como una prerrogativa de los titulares, es por ello, que este apartado nos referiremos a los cinco derechos. El 12 de febrero de 2018, Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, emitió el Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de los datos personales. Disponible en *dof.gob.mx/nota_to_doc.php?codnota=5512847*, última fecha de consulta el 20 de agosto de 2019.
[178] O de cualquier persona autorizada legalmente para ello.
[179] Véase artículo 44 de la LGPDPPSO.
[180] *Ibidem*, artículo 45.
[181] *Ibidem*, artículos 3 fracción IV, 23 y 46.
[182] *Ibidem*, artículo 47.

más, siempre y cuando, exista causa justificada, y (ii) Para el hacer efectivo el derecho se cuenta con el plazo de 15 días hábiles, contados a partir de la fecha de notificación de la procedencia del derecho.[183]

Los derechos ARCO pueden ser ejercidos, a través de una solicitud, por el titular o su representante acreditando su personalidad.[184] El artículo 52 de la LGPDPPSO establece los requisitos que deben cumplir las solicitudes a que nos hemos referido,[185] de lo que resulta importante destacar, que no cumplirse con alguno de dichos requisitos, es primera obligación del responsable del tratamiento subsanar dicha omisión,[186] y si ello no es posible, se deberá prevenir al titular, para que dentro de los subsane dentro de los diez días hábiles siguientes. Si lo anterior no sucede, la solicitud se tendrá como no presentada.

Las únicas causas para declarar una solicitud como no procedente, son las siguientes:

> I. Cuando el titular o su representante no estén debidamente acreditados para ello;
> II. Cuando los datos personales no se encuentren en posesión del responsable;
> III. Cuando exista un impedimento legal;
> IV. Cuando se lesionen los derechos de un tercero;
> V. Cuando se obstaculicen actuaciones judiciales o administrativas;
> VI. Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;
> VII. Cuando la cancelación u oposición haya sido previamente realizada;
> VIII. Cuando el responsable no sea competente;

---

[183] *Ibidem*, artículo 51.

[184] De conformidad con lo dispuesto por el artículo 49 de la LGPDPPSO, se establecen las excepciones de menores de edad, personas en estado de interdicción o incapacidad y de personas fallecidas.

[185] "Artículo 52. En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes:
I. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones; II. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante; III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud; IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso; V. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso. Tratándose de una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan.
El responsable deberá atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación".

[186] Se debe destacar que, para esta revisión, el responsable del tratamiento cuenta con los primeros cinco días hábiles siguientes a la recepción de la solicitud.

> IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;
> X. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;
> XI. Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o
> XII. Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

Finalmente, nos referiremos al derecho de la portabilidad, el cual se encuentra íntimamente relacionado con el derecho de acceso, dado que, si los datos personales se encuentran en un formato estructurado y comúnmente utilizados, la copia de los datos a obtener, se pueden requerir en un formato estructurado para su posterior utilización. Respecto de este derecho nos referiremos a más detalle al explicar los Lineamientos de Portabilidad.

2.1.5 Comunicaciones de datos personales

La comunicación de los datos personales puede realizarse al interior de la organización del responsable, esto es, con sus unidades administrativas, pero también, pueden realizarse al exterior de la organización. En ese último caso, esto es, al exterior de la organización, la comunicación puede configurarse bajo la figura de remisión de datos personales o de transferencia de datos personales.

La remisión[187] de datos personales es la que se realiza a una persona ya sea física o moral, de carácter público o privado de nacionalidad o mexicana o de cualquier otra, denominada encargado del tratamiento,[188] y cuya obligación es realizar el tratamiento de los datos personales que le son remitidos conforme a las instrucciones del responsable del tratamiento, lo cual significa que el encargado del tratamiento no tiene decisión ni el alcance ni contenido del tratamiento, pues el mismo se define por el responsable del tratamiento y su

[187] La fracción XXVII del artículo 3o. de la LGPDPPSO, define a la remisión como “toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano”.
[188] Véase artículo 3o. fracción XV de la LGPDPPSO.

correspondiente aviso de privacidad,[189] las que de no observarse por dicho encargado, el mismo asume el carácter de responsable del tratamiento.[190]

Resulta importante destacar que, a efecto de delimitar el carácter de cada una de las partes, la relación entre el responsable del tratamiento y el encargado del tratamiento debe constar por escrito a través de cláusulas contractuales o cualquier otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. Destacando el artículo 59 de la LGPDPPSO las cláusulas mínimas de dicho instrumento, las que son:

> I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
> II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
> III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
> IV. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
> V. Guardar confidencialidad respecto de los datos personales tratados;
> VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
> VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
> (Énfasis y subrayado añadido).

A su vez, el encargado del tratamiento puede subcontratar a otro tercero para realizar las actividades que le fueron encargadas, sin embargo, para que ello sea legal, dicha subcontratación, debe ser autorizada por escrito, en el instrumento donde nace el encargo del tratamiento, por el responsable del tratamiento.[191]

Por su parte, la transferencia de datos personales es la comunicación de datos que se realiza a un tercero ajeno al responsable del tratamiento, a diferencia de la remisión de datos personales, en la transferencia el tercero receptor no atiende a instrucciones del responsable del tratamiento, pues el nuevo receptor decide sobre el tratamiento, y las transferencias deben ser

[189] Resulta necesario destacar que el aviso de privacidad no debe contener las remisiones que el responsable de tratamiento realizará, ello de conformidad con lo dispuesto en el artículo 71 de la LGPDPPSO.
[190] Véanse artículos 59 último párrafo y 60 de la LGPDPPSO.
[191] Véase artículo 62 y 63 de la LGPDPPSO.

informadas al titular en el aviso de privacidad correspondiente, y están sujetas al consentimiento del titular, excepto los siguientes casos: (i) Cuando se configure alguna de las excepciones del consentimiento para el tratamiento de datos personales, conforme al artículo 22 de la LGPDPPSO; (ii) Cuando la transferencia es nacional y es en cumplimiento a una disposición legal o ejercicio de atribuciones,[192] (iii) Cuando sea internacional, pero se basa en un instrumento que fundamente dicha comunicación.[193]

Por último, es necesario apuntar que, en las transferencias de datos personales, al igual que en las remisiones, la relación entre el responsable de datos y el receptor, debe constar en un instrumento jurídico en el que conste el alcance, obligaciones y responsabilidades de las partes.[194]

2.1.6 Responsables de la protección de los datos personales. Consecuencias de incumplimiento de responsabilidades

Al interior de cada sujeto obligado, son dos las figuras importantes en materia de protección de datos personales, el Comité de Transparencia y la Unidad de Transparencia.

Los Comités de Transparencia tuvieron su origen en la LGTAIPG, los que deben conformarse y que, en materia de protección de datos personales, tiene la siguiente función:

> Artículo 44. Cada Comité de Transparencia tendrá las siguientes funciones:
> (…)
> VI. Establecer programas de capacitación en materia de transparencia, acceso a la información, accesibilidad y protección de datos personales, para todos los Servidores Públicos o integrantes del sujeto obligado.[195]

Asimismo, el artículo 84 de la LGPDPPSO complementa las funciones del Comité de Transparencia, el que se convierte en el coordinador de las actividades que se tienen que realizar al interior de cada responsable del

[192] Véase *ibidem*, fracción I del artículo 66 y 70.
[193] Véase *ibidem*, fracción II del artículo 67.
[194] Véase *ibidem*, primer párrafo del artículo 66.
[195] Véase artículo 44 de la LGTAIPG.

tratamiento.

Por cuanto hace a derechos ARCO, el Comité tiene dos funciones importantes, pues debe definir procedimientos que aseguren la eficiencia en la gestión de solicitudes y, confirmar, modificar o revocar atenciones a solicitudes en donde se declare la inexistencia de datos personales, o que, se hubiere negado el ejercicio del derecho.

En materia de seguridad, en coordinación con las áreas correspondiente, debe supervisar que se dé cumplimiento al documento de seguridad.

También es el responsable de dar seguimiento al cumplimiento de las resoluciones emitidas por el INAI y los organismos garantes. Pero también, debe dar vista al órgano interno de control de presuntas irregularidades cometidas por los servidores públicos, respecto del tratamiento de datos personales.

Por su parte, las Unidades de Transparencia, es la unidad operadora en materia de protección de datos personales, pues es la unidad que está en contacto con los titulares para auxiliarlos y orientarlos en la materia, así como de gestionar las solicitudes de derechos ARCO.

Asimismo, la Unidad de Transparencia es la encargada de asesorar a las áreas que conforman al sujeto obligado, a efecto de que cada una de ellas cumpla con las normas aplicables a la protección de datos personales.

2.1.7 Incumplimiento de la norma en materia de protección de datos personales

El recurso de revisión resulta aplica de interposición por el titular que, de manera general, no hubiera sido atendido oportuna o completamente en su solicitud de ejercicio de derechos ARCO.[196] Si el titular no está conforme con la resolución del recurso de revisión, dicho titular puede impugnarla, a través del recurso de inconformidad, las que a su vez solo pueden ser impugnadas mediante Juicio de Amparo ante el Poder Judicial de la Federación.[197]

[196] Véase artículo 104 de la LGPDPPSO.
[197] Véanse *ibídem*, artículos 116, 117 y 129.

Ahora bien, el cumplimiento de la norma en materia de protección de datos personales, puede verificarse por el INAI, ya sea de oficio o por denuncia, a través del Procedimiento de Verificación. Si durante la ejecución de dicho procedimiento se identifica el incumplimiento de las siguientes obligaciones, el INAI podrá establecer sanciones al sujeto obligado:

> I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
> II. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;
> III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
> IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;
> V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
> VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
> VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la presente Ley;
> VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;
> IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente Ley;
> X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;
> XI. Obstruir los actos de verificación de la autoridad;
> XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;
> XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y
> XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.[198]

Por lo tanto, si resulta el incumplimiento de dichas obligaciones, el INAI puede imponer al sujeto obligado una amonestación pública o una multa en

[198] Véase artículo 163 de la LGPDPPSO.

cantidad de 150 y hasta 1,500 veces el valor diario de la Unidad de Medida y Actualización.[199]

Sin embargo, las sanciones no concluyen ahí, pues si el infractor tiene la calidad de servidor público, el INAI o el organismo garante, debe hacerlo del conocimiento de la autoridad competente, tal y como se indica en el artículo 167 de la LGPDPPSO, la cual puede ser el Comité de Transparencia o el órgano interno de control del sujeto obligado que corresponda.

2.2 Programa Nacional de Protección de Datos Personales

De conformidad con lo dispuesto por el artículo 32 de la LGPDPPSO, el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, cuenta con un Consejo del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el que, con fecha 26 de enero de 2018, aprobó el Programa Nacional de Transparencia y Acceso a la Información,[200] también conocido como PRONADATOS 2018-2022, y que se advierte como el principal instrumento del Sistema Nacional "para definir y coordinar las bases de la política pública de protección de datos personales en el país, dentro del sector público".[201]

El establecimiento de este primer PRONADATOS advierte que los primeros pasos de su establecimiento son los que serán la base para un programa más sólido, sin embargo, se advierte que, en materia de protección de datos personales en el sector público, son tres principales problemas públicos a los que debe atenderse: "(a) Resolver la utilización de los derechos ARCO orientada a un beneficio concreto para el titular de los datos; (b) Resolver el tratamiento y seguridad de los datos considerando situaciones urgentes, y (iii) Implementar simplificadamente la ley y establecer prioridades en la

[199] Véase artículo 153 de la LGPDPPSO. Asimismo, para calificar las medidas de apremio aplicables, el INAI toma en cuenta: "I. La gravedad de la falta del responsable, determinada por elementos tales como el daño causado; los indicios de intencionalidad; la duración del incumplimiento de las determinaciones del Instituto o los Organismos garantes y la afectación al ejercicio de sus atribuciones; II. La condición económica del infractor, y III. La reincidencia".
[200] Acuerdo mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales. Disponible en *http://www.dof.gob.mx/nota_detalle.php?codigo=5511542&fecha=26/01/2018*, última fecha de consulta el 20 de agosto de 2019.
[201] PRONADATOS, introducción.

administración pública".[202]El programa está conformado por 8 ejes temáticos, planteando para cada uno de ellos líneas objetivos de cumplimientos y líneas de acción específicas, sin embargo, también se establecen tres líneas estratégicas transversales, las cuales se implementan para cada uno de los 8 ejes temáticos.

A continuación, se presenta un diagrama del Programa:

[202] PRONADATOS, I.2 Enfoque inicial del PRONADATOS. Cabe destacar que dichas problemáticas son la conclusión del Documento de Diagnóstico de PRONADATOS, el cual identifica que es necesario atender las siguientes temáticas: (i) Educación y cultura de protección de datos personales entre la sociedad mexicana: a. Desconocimiento general de la protección de datos personales. b. Hay un número reducido de estudios e investigaciones en las materias de protección de datos personales y privacidad en México. c. Hay una preocupación generalizada entre la población sobre el uso de sus datos personales, en especial: información que permite localizarlos, aspectos económicos o de salud. d. Los Organismos Garantes no son ampliamente reconocidos como las instituciones garantes del derecho a la protección de datos personales. e. Las características socioeconómicas de las personas que ejercen su derecho a la protección de datos personales indican que pertenecen a grupos específicos y minoritarios de la población; (ii) Ejercicio de los derechos ARCO y de portabilidad: a. Heterogeneidad de las prácticas para ejercer los derechos ARCO. b. No hay un ejercicio suficiente y adecuado de los derechos ARCO; (iii) Capacitación a los responsables en materia de protección de datos personales: a. Se desconoce el universo de atención. b. La LGPDPPSO ha definido nuevas y más amplias obligaciones y facultades para los responsables, las cuales desconocen. c. Se carece de criterios para identificar necesidades, priorizaciones y sectorizaciones adecuados para atender las necesidades de capacitación en el sector público. d. Las políticas de capacitación no están vinculadas a los programas sustantivos. e. No existen las capacidades técnicas, entre los servidores públicos, en materia de protección de datos personales (profesionalización); (iv) Implementación y mantenimiento de un sistema de gestión de seguridad: a. Pueden darse vulneraciones de seguridad que afecten de manera significativa los derechos de los titulares. b. Las medidas de seguridad y el tratamiento de datos ante las nuevas tecnologías de la información son desconocidos y carecen de un marco de certeza. c. Hay un desconocimiento generalizado de las medidas de seguridad informática; (v) Estándares nacionales, internacionales y buenas/mejores prácticas en la materia: a. No han sido identificados los incentivos que permitan a los responsables adoptar mejores prácticas; (vi) Monitoreo, seguimiento, y verificación de metas: a. Al momento no se evalúa el desempeño de los responsables de carácter público en lo que respecta al cumplimiento de sus obligaciones previstas en la normatividad; (vii) Acciones preventivas en materia de protección de datos personales: a. No existen suficientes herramientas de facilitación para el cumplimiento de las obligaciones por parte de los responsables. b. Los responsables pueden someterse a auditorías voluntarias sin que hasta el momento se hayan desarrollado los medios para su atención, y (viii) Perspectiva normativa con enfoque de política pública: a. La LGPDPPSO y las leyes locales en la materia son muy generales en su redacción y muy vagos para su desarrollo. b. Derivado de la reciente promulgación de la LGPDPPSO no se han desarrollado acciones específicas en las instancias del SNT para promover su aplicación en todo su potencial. c. Los organismos garantes tienen nuevas atribuciones para las cuáles aún no cuentan con los recursos y capacidades necesarias para su cumplimiento.

Figura 1 Programa Nacional de Protección de Datos Personales

Fuente: Elaboración propia con datos del Programa Nacional de Protección de Datos Personales.

Cabe destacar que, para evaluar el cumplimiento del Programa, se establece una serie de indicadores, los cuales pretender medir el cumplimiento de cada una de las líneas de acción, sin embargo, la mayoría de ellos tiene metas aún no definidas.

Capítulo 3

Propuesta de intervención.

“Guía práctica-operativa para que los servidores públicos, que, en cumplimiento de sus funciones, realicen tratamiento de datos personales apegados al marco normativo aplicable”

Capítulo 3 Propuesta de intervención. “Guía práctica-operativa para que los servidores públicos, que, en cumplimiento de sus funciones, realicen tratamiento de datos personales apegados al marco normativo aplicable”

Toda vez que la normatividad aplicable en materia de protección de datos personales en el sector público contiene diversas obligaciones que deben ser observadas por el responsable del tratamiento, y en su caso, por el encargado del tratamiento, es importante tener en cuenta que las consecuencias de su incumplimiento tienen sanciones tanto para la institución responsable, como para el servidor público involucrado en el incumplimiento. Es por ello, que a efecto de complementar las acciones que hoy en día ejecuta el INAI, como una acción preventiva, se sugiere la siguiente Guía, a efecto de minimizar la verificación de algún incumplimiento a las normas en la materia.

En razón de lo anterior, a continuación se presenta la “**Guía práctica-operativa para que los servidores públicos adscritos a la Dirección de Innovación y Desarrollo Tecnológico que, en cumplimiento de sus funciones, realicen tratamiento de datos personales apegados al marco normativo aplicable”**, la que si bien, se presenta para un área específica del Instituto Mexicano del Seguro Social, la misma puede resultar aplicable para cualquier área, dirección o unidad de gobierno que realice el tratamiento de datos personales.

Instituto Mexicano del Seguro Social

Protección de Datos Personales en Posesión de Sujetos Obligados

Guía práctica-operativa para que los servidores públicos adscritos a la Dirección de Innovación y Desarrollo Tecnológico que, en cumplimiento de sus funciones, realicen tratamiento de datos personales apegados al marco normativo aplicable

Presentación

El 26 de enero de 2017 fue publicada en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante LGPDPPSO), la que de conformidad con su artículo 1, párrafo cuarto, tiene por objeto "establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados."

De conformidad con el párrafo quinto del artículo 1o. de la LGPDPPSO, son sujetos obligados "en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos".

Ahora bien, de conformidad con lo dispuesto en el artículo 5 de la Ley General del Seguro Social, la organización y administración del Seguro Social están a cargo de organismo público descentralizado con personalidad jurídica y patrimonio propios, dando origen así, a este Instituto Mexicano del Seguro Social (en adelante IMSS). Ello implica que, conforme a lo establecido por la Ley Orgánica de la Administración Pública Federal, el IMSS forma parte de la Administración Pública, lo que trae aparejado consigo que, este Instituto debe observar lo dispuesto en la LGPDPPSO y la normatividad que de ella emane.

Si bien es cierto que el Comité de Transparencia y la Unidad de Transparencia están ejecutando diversas actividades para dar cumplimiento a la normatividad aplicable en materia de protección de datos personales en posesión de sujetos obligados, se identificó la necesidad en la Dirección de Innovación y Desarrollo Tecnológico de contar con un instrumento que preventivamente le

permita que la ejecución de sus facultades se realice con apego a dicha normatividad.

En razón de ello, esta guía está divida en dos secciones: (I) La sección primera contiene todos los aspectos que norman la protección de datos personales en posesión de sujetos obligados, y que debe ser conocido por todo el personal adscrito a la Dirección de Innovación y Desarrollo Tecnológico, pues estos aspectos contienen las reglas que deben ser observadas durante la ejecución de sus actividades laborales, y (ii) La sección segunda contiene diversos formatos y plantillas que permitirán documentar que cada proceso y subproceso ejecutado en la Dirección de Innovación y Desarrollo Tecnológico, en los que se involucre el tratamiento de datos personales, cumple con lo dispuesto en la normatividad aplicable en materia de protección de datos personales, por lo tanto, una vez adoptados dichos instrumentos, ellos serán los rectores de las actividades ejecutadas por cada servidor público involucrado en el tratamiento de datos personales.

SECCIÓN PRIMERA. LO QUE USTED NO PUEDE DEJAR DE SABER SOBRE LA PROTECCIÓN DE DATOS PERSONALES

3.1.1 La protección de los Datos Personales

Las personas tenemos derecho a la preservación de nuestra privacidad, pues en ese ámbito se encuentra lo que cada uno de nosotros decidimos mantener en lo secreto, sin embargo, en diversas ocasiones es necesario que dichos datos, denominados como **personales** y conformantes de privacidad, deben ser del conocimiento de otras personas con diversos motivos.

Tanto la vida privada como los datos personales, son protegidos por la Constitución Política de los Estados Unidos Mexicanos, pues su artículo 6o. mandata que *"la información que se refiere a la **vida privada** y **los datos personales** será **protegida** en los términos y con las excepciones que fijen las leyes"*. Aunado a ello, el subsecuente artículo 16, párrafo segundo refuerza lo anterior, instituyendo:

> *"Toda persona tiene **derecho** a la **protección** de sus **datos personales**, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".*
> *(Énfasis y subrayado añadido).*

Los datos personales deben ser protegidos, a efecto de que la vida privada de una persona permanezca en dicho ámbito, distinguiendo entonces, que son dos grandes ámbitos de los que habría que protegerlos, esto es, los datos personales en manos del sector privado y el sector público. En el primero de los casos, referidos a particulares, esto es, personas físicas o morales de carácter privado. En segundo de los casos, referido al Estado, de cualquier ámbito territorial y material de competencia.

3.1.2 La protección de los datos personales en el ámbito público[203]

La LGPDPPSO fue publicada en el Diario Oficial de la Federación el pasado 26 de enero de 2017, constituyéndose como la Ley Reglamentaria de los artículos 6o. y 16 constitucionales referidos en el apartado anterior.

Determina esta Ley su obligatoriedad y observancia para lo que ha sido delimitado como sujetos obligados, lo que designa tanto en el ámbito federal, estatal y como municipal a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como a los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad.

De conformidad con lo establecido en el artículo 1o. de la LGPDPPSO, dicha Ley tiene como objeto "*establecer las **bases**, **principios** y **procedimientos** para **garantizar** el derecho que tiene toda persona a la **protección** de sus **datos personales**, en posesión de sujetos obligados*".

Toda vez que de conformidad con lo dispuesto por el artículo 5o. de la Ley del Seguro Social, el Instituto Mexicano del Seguro Social está constituido como un organismo público descentralizado de la Administración Pública Federal, le resulta aplicable lo dispuesto en la LGPDPPSO, y si bien es cierto que en éste Instituto los responsable en materia de protección de datos personales son el Comité de Transparencia y la Unidad de Transparencia, también es cierto que cada uno de los servidores públicos que operan en su día a día con datos personales son quienes están encargados de que lo dispuesto en la LGPDPPSO se cumpla en ese día a día.

En razón de lo anterior, y dada la naturaleza de las funciones de la Dirección de Innovación y Desarrollo Tecnológico, esta **guía tiene como propósito coadyuvar con las acciones implementadas por el Comité y la**

[203]Para el ámbito privado, esto es, particulares sean personas físicas o morales de carácter privado que tratan datos personales, resulta aplicable la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada en el Diario Oficial de la Federación el 5 de julio de 2010, así como la normatividad que deriva de la misma.

Unidad de Transparencia de este Instituto en materia de protección de datos personales y proporcionar a los servidores públicos adscritos a dicha Dirección un instrumento que les permita identificar las medidas que debe ejecutar en su operación cotidiana, a efecto de que la normatividad en materia de protección de datos personales en posesión de sujetos obligados sea observada y aplicada durante el tratamiento de los datos personales que estén involucrados en la operación de sus procesos.

3.1.3 Los datos personales. Definición

Cuando se utiliza la expresión **"datos personales"** debemos pensar, en primer lugar, que la expresión es referida a una persona física a quien se le denomina **"titular"**, esto es, un individuo que adquiere tal calidad desde el momento en que es concebido y hasta el momento de su muerte. Después tenemos que pensar en cualquier información que gira alrededor de dicho individuo y que a través de la misma se identifique o se pueda identificar con certeza al individuo a que pertenecen. La fracción IX del artículo 3o. de la LGPDPPSO establece la siguiente definición:

> *"Artículo 3. Para los efectos de la presente Ley se entenderá por:*
> *(…)*
> *IX. **Datos personales**: **Cualquier información** concerniente a una **persona física identificada** o **identificable**. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;*
> (Énfasis y subrayado añadido).

Pueden constituirse como ejemplos de datos personales: (i) El nombre; (ii) La imagen; (iii) La voz; (iv) El correo electrónico; (v) El domicilio; (vi) Números o claves de identificación como el CURP, el RFC o el número de seguridad social, por mencionar algunos.

Datos personales sensibles: Artículo 3 fracción X LGPDPPSO.

Ahora bien, es importante señalar que, dentro de los datos personales existe una clasificación de los mismos, toda vez que la normatividad en la materia distingue a los **"datos personales sensibles"**, esto es aquélla información que identifica o hace identificable a un individuo, pero que se refieren al ámbito más íntimo de dicho individuo, por lo que, su indebido uso, puede conllevar a que dicho individuo sea discriminado o lo coloque en una situación de riesgo grave. El mismo artículo 3o. antes referido, define a los datos personales sensibles como a continuación se indica:

> *"Artículo 3. Para los efectos de la presente Ley se entenderá por:*
> *(…)*

> *X. Datos personales sensibles: Aquellos que se refieran a la* ***esfera más íntima*** *de su titular, o cuya utilización indebida pueda dar origen a* ***discriminación*** *o conlleve un* ***riesgo grave*** *para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;* (Énfasis y subrayado añadido).

En razón de lo anterior, es necesario identificar si los datos personales de que se trate cumplen con alguna de las dos características mencionadas anteriormente: (i) que el uso indebido lleve a que su titular pueda ser discriminado, o (ii) que su uso indebido coloque al titular en una situación de riesgo grave.

El artículo antes mencionado realiza un listado de los datos que considera como sensibles:

1) **Datos sobre origen racial o étnico.**
2) **Datos sobre el estado de salud del individuo, ya sea que dichos datos se refieran a su estado de salud presente o futuro.**
3) **Datos sobre la información genética del individuo.**
4) **Datos sobre creencias religiosas.**
5) **Datos sobre creencias filosóficas.**
6) **Datos sobre creencias morales.**
7) **Datos sobre opiniones políticas.**
8) **Datos sobre preferencia sexual.**

Sin embargo, es importante resaltar que dicho listado solo es enunciativo y no limitativo, esto es, que si cualquier otro dato cumple con las características de (i) que el uso indebido lleve a que su titular pueda ser discriminado, o (ii) que su uso indebido coloque al titular en una situación de riesgo grave, **dichos datos también deben ser considerados y tratados como sensibles.**

Por lo anterior, por cada una de las dos características anteriores, proporcionaremos elementos que permitan identificar si un dato distinto a los enlistados, podría ser considerado como sensible.

En la legislación mexicana nos encontramos con la Ley Federal para Prevenir y Eliminar la Discriminación que es reglamentaria del último párrafo del artículo 1o. constitucional, la cual es aplicable desde el año 2013 y tiene por objeto prevenir y erradicar cualquier forma de discriminación. Esta disposición normativa define a la discriminación como:

> "*Artículo 1. (…):*
> *(…)*
> *III. Discriminación: Para los efectos de esta ley se entenderá por discriminación toda* ***distinción, exclusión, restricción o preferencia*** *que, por acción u omisión, con intención o sin ella, no sea objetiva, racional ni proporcional y tenga por objeto o resultado* ***obstaculizar, restringir, impedir, menoscabar o anular el reconocimiento, goce o ejercicio de los derechos humanos y libertades****, cuando se base en uno o más de los siguientes* ***motivos****: el origen étnico o nacional, el color de piel, la cultura, el sexo, el género, la edad, las discapacidades, la condición social, económica, de salud o jurídica, la religión, la apariencia física, las características genéticas, la situación migratoria, el embarazo, la lengua, las opiniones, las preferencias sexuales, la identidad o filiación política, el estado civil, la situación familiar, las responsabilidades familiares, el idioma, los antecedentes penales o cualquier otro motivo;*
> *También se entenderá como discriminación la homofobia, misoginia, cualquier manifestación de xenofobia, segregación racial, antisemitismo, así como la discriminación racial y otras formas conexas de intolerancia;*"
> (Énfasis y negritas añadido).

De lo anterior, se desprende que para identificar si un dato puede o no conllevar a que el individuo sea discriminado debemos verificar:

1) Que el uso de los datos distinga, excluya, restrinja o causa preferencia.
2) Que dicha distinción, exclusión, restricción o preferencia puede ser origen de acciones u omisiones.
3) Que las acciones u omisiones pueden o no ser intencionales.
4) Que dicha distinción, exclusión, restricción o preferencia no sea justa, fundada en razones ni equivalente.
5) Que dicha distinción, exclusión, restricción o preferencia tanga por objeto que el reconocimiento, goce o ejercicio de los derechos humanos

y libertades se vea:

a. Obstaculizado;
b. Restringido;
c. Impedido;
d. Menoscabado, o
e. Anulado.

Los derechos humanos son derechos inherentes a todos los seres humanos los cuales son protegidos por la ley, de los que podríamos enlistar los siguientes: (i) Derecho a la vida, libertad y seguridad de su persona; (ii) Reconocimiento de su personalidad jurídica; (iii) Igualdad ante la ley; (iv) Derecho a un recurso efectivo ante los tribunales; (v) Derecho a ser oído públicamente y con justicia ante un tribunal; (vi) Derecho a la vida privada, esto es, no puede ser objeto de injerencias arbitrarias en su familia, domicilio o correspondencia, ni puede ser atacado en su honra o reputación; (vii) Derecho a la libre circulación y elección de residencia; (viii) Derecho de asilo en cualquier país; (ix) Derecho a una nacionalidad; (x) Derecho al matrimonio; (xi) Derecho a la propiedad privada; (xii) Libertad de pensamiento, de conciencia y de religión; (xiii) Libertad de opinión y de expresión; (xiv) Libertad de reunión y de asociación; (xv) Derecho para participar en el gobierno de su país; (xvi) Derecho de acceso a las funciones públicas de su país; (xvii) Libertad del voto; (xviii) Derecho a la seguridad social; (xix) Derecho al trabajo, igual trabajo, igual salario, remuneración equitativa y satisfactoria y a fundar sindicatos y sindicarse; (xx) Derecho al descanso, al disfrute del tiempo libre, a una limitación razonable de la duración del trabajo y a vacaciones periódicas pagadas; (xxi) Derecho a un nivel de vida adecuado; (xxii) Derecho a cuidados y asistencia especiales para la maternidad y la infancia; (xxiii) Derecho a la educación, y (xxiv) Derecho a tomar parte de la vida cultural de la comunidad.

6) Lo anterior, derivado de alguno de los siguientes motivos:
   a. Origen étnico o nacional.
   b. Color de piel.
   c. La cultura.
   d. El sexo.

e. El género.
f. La edad.
g. Las discapacidades.
h. La condición social.
i. La condición económica.
j. El estado de salud.
k. Condición jurídica.
l. La religión.
m. La apariencia física.
n. Las características genéticas.
o. La situación migratoria.
p. El embarazo.
q. La lengua.
r. Las opiniones.
s. Las preferencias sexuales.
t. La identidad.
u. La afiliación política.
v. El estado civil.
w. La situación familiar.
x. Las responsabilidades familiares.
y. El idioma.
z. Los antecedentes penales.
aa. Cualquier otro motivo.

7) O bien, se debe identificar si no se incurre en cualquiera de las siguientes figuras:

a. Homofobia.
b. Misoginia.
c. Cualquier manifestación de xenofobia.
d. Segregación racial.
e. Antisemitismo.
f. Discriminación racial.
g. Otra forma conexa de intolerancia.

Por otro lado, el riesgo grave es un término muy amplio, pues el mismo se puede interpretar con la disminución o pérdida en cualquiera de los ámbitos que rodean al individuo, tales como su libertad, su salud, su patrimonio, su familia, por mencionar algunos.

En razón de lo antes expuesto, los datos personales que pueden ser considerados como sensibles puede tener un amplio espectro por lo que se debe ser muy cuidadoso para identificar si un dato personal debe ser clasificado como sensible.

3.1.4 Del tratamiento de datos personales

El tratamiento de datos personales debe ser entendido como cualquier operación u operaciones realizadas con los mismos a través de procedimientos manuales o automatizados. Dichas operaciones se pueden relacionar con las siguientes acciones: (i) Obtención; (ii) Uso; (iii) Registro; (iv) Organización; (v) Conservación; (vi) Elaboración; (vii) Utilización; (viii) Comunicación; (ix) Aprovechamiento; (x) Difusión; (xi) Almacenamiento; (xii) Posesión; (xiii) Acceso; (xiv) Manejo; (xv) Aprovechamiento; (xvi) Divulgación; (xvii) Transferencia, o (xviii) Disposición.

Tratamiento: Artículo 3, fracción XXXIII LGPDPPSO.

De lo anterior tenemos que, cualquier actividad realizada a los datos personales se considera que los mismos están siendo sometidos a tratamiento. El tratamiento de datos personales que es realizado por los sujetos obligados y en este caso por el Instituto Mexicano del Seguro Social puede realizarse bajo dos figuras, ya sea como responsable del tratamiento o como encargado del tratamiento.

El responsable del tratamiento se define como los sujetos obligados que **deciden** sobre el tratamiento de los datos personales, esto es, quienes disponen sobre acciones que deban ejecutarse sobre los datos personales bajo su tratamiento.

Responsable: Art. 3, fracción XXVIII LGPDPPSO.

Por ejemplo, si el IMSS decide lanzar una aplicación móvil para que los ciudadanos soliciten servicios de salud a domicilio y a través de dicha aplicación se requiere que el individuo registre su nombre, teléfono, correo electrónico, número de seguridad social y domicilio. En este caso el IMSS se convierte en responsable del tratamiento, quien decide que dichos datos personales serán utilizados para realizar con ellos las siguientes acciones:

1) Obtención de datos personales de los suscriptores de la aplicación móvil.
2) Conformar un registro de suscriptores de la aplicación móvil.
3) Brindar el servicio a atención a la salud del individuo en la ubicación que indique.
4) Realizar análisis estadísticos sobre los usos que cada usuario realiza

en la aplicación móvil.

5) Enviarle información publicitaria que genere el Instituto.

Encargado: Art. 3, fracción XV LGPDPPSO.

Por otro lado, tal y como se indicaba anteriormente, también el tratamiento de datos personales puede ser realizado bajo la figura de encargado del tratamiento, quien es definido como la persona física o moral, ya sea que pertenezca al ámbito público o privado, **ajena** al responsable que **trata datos personales en nombre y por cuenta del responsable.**

Continuando con el ejemplo de la aplicación móvil, y si el IMSS tuviera contratado el servicio de arrendamiento para el uso de un centro de datos con el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (en adelante INFOTEC), en donde el centro de datos es administrado por dicha institución pública y es en dicho centro de datos donde se almacenarán los datos personales, INFOTEC adquiere el carácter de encargado del tratamiento, pues el centro de datos es contratado con la finalidad de hospedar, entre otra información, los datos personales obtenidos a través de la aplicación.

Es importante también tener en cuenta que el IMSS puede fungir como encargado del tratamiento, cuando otro sujeto obligado o un particular le solicita realizar el tratamiento de datos personales en su nombre. Por ejemplo, suponiendo que la aplicación a la que hemos hecho referencia fuera adoptada para proporcionar también servicio a los derechohabientes del Instituto de Seguridad y Servicios Sociales para los Trabajadores del Estado (en adelante ISSSTE) para que sea dicho Instituto el que preste los servicios de salud, pero quien sigue administrando la aplicación sea el IMSS, en ese caso, frente a los trabajadores del Estado, el responsable del tratamiento es el ISSSTE, el IMSS fungiría como encargado del tratamiento, y al tener el IMSS subcontratado el servicio de centro de datos con INFOTEC, éste se convierte en **subencargado del tratamiento**.

Ahora bien, durante el tratamiento de los datos personales, el IMSS, **a través de cada uno de los servidores públicos que ejecutan acciones**

concernientes a su tratamiento deben observar el cumplimiento de **principios, deberes y obligaciones**, a los que más adelante nos referiremos.

En razón de lo anterior, es importante que para cada grupo de datos personales concernientes a un titular, derivados de un procedimiento específico, se cuente con la trazabilidad de su tratamiento, pues en caso de que la operación de los datos se realice de manera contraria a lo dispuesto por la normatividad en materia de protección de datos personales, es necesario identificar el área y el servidor público que cometió dicha falta, a efecto de que, en su caso se inicien los procedimientos correspondientes y se finquen las responsabilidades que resulten aplicables, ya sean las mismas del orden administrativo, penal y/o civil.

Figura 2 Ciclo de los datos personales en posesión de sujetos obligados

Fuente: Elaboración propia con datos de flujo de datos en una dependencia o entidad.

La ilustración anterior, explica de gráficamente lo mencionado en párrafos anteriores, esto es:

1) El **inicio** del tratamiento de los datos personales, el cual tiene su origen en la **obtención** de los mismos, ya sea:
    a. Porque el titular del dato hace entrega del mismo;
    b. Porque se recibe el dato de otra institución de carácter público. Pudiendo resultar que dicha comunicación puede derivar de una

remisión o una transferencia, o bien,

c. Porque se recibe el dato de un particular, ya sea a través de una remisión o transmisión, de la que es importante, observar lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares y la normatividad que de dicha ley deriva.

2) Una vez que el dato se encuentra en posesión del IMSS, el mismo puede ser **tratado** al interior de la institución por **una o más unidades administrativas**, y en consecuencias por **uno o más servidores públicos.**

Durante cada uno de los tratamientos realizados sobre el dato personal de que se trate, debe observarse el cumplimiento de principios deberes y obligaciones.

Asimismo, resulta importante el papel que adquieren el Comité de Transparencia y la Unidad de Transparencia. El primero de ellos, que de manera general es el encargado de *coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales*, y la Unidad es la encargada en términos generales de fungir como enlace con los titulares de los datos personales, *auxiliándolos y orientándolos en lo que los mismos requieran con relación a la protección de sus datos personales.*

Comité de Transparencia: Art. 84 LGPDPPSO.
Unidad de Transparencia: Art. 85 LGPDPPSO.

3) Por último, los datos personales tratados al interior del IMSS podrían ser comunicados, al igual que en su obtención, ya sea como una remisión o una transferencia, cuyo destinatario puede ser un particular de carácter privado u otra institución de carácter público.

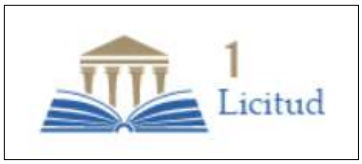
3.1.5 De los principios en materia de protección de datos personales

Un principio puede ser entendido como lo primero o lo primordial para una determinada situación y que son expresados como reglas mandatarias que deben ser adoptadas y observadas durante la misma.

En materia de protección de datos personales en posesión de sujetos obligados, la LGPDPPSO establece **ocho principios**, los cuales deben ser observados tanto por el responsable del tratamiento como, en su caso, por el encargado del tratamiento.

Figura 3 Principios en materia de protección de datos personales

Fuente: Elaboración propia con datos de la LFPDPPP.



El **principio de licitud** es el que se define de manera más sencilla, pues en términos generales se resume en que el tratamiento de los datos personales debe realizarse con apego a lo dispuesto en la normatividad que resulte aplicable, lo cual se materializa cuando:

Principio de licitud: Artículo 17 LGPDPPSO.

1) El tratamiento se realice con sujeción a las facultades y atribuciones de la Institución, esto es del IMSS, y
2) Como ya se ha indicado, el tratamiento debe realizarse conforme a las facultades y atribuciones de cada servidor público involucrado en dicho tratamiento.

Por su parte, el **principio de finalidad** se refiere a los propósitos, actividades o tratamientos a los que serán sometidos los datos personales. Dichas finalidades deben cumplir con las siguientes características:

Principio de finalidad: Artículo 18 LGPDPPSO.

1) Concretas, esto es, que la finalidad sea precisa y determinada;
2) Lícitas, lo que significa que la finalidad debe estar apegada a las facultades y atribuciones de la institución;
3) Explícitas, lo que se logra cuando la finalidad es expresada con claridad, y
4) Legítimas, que se traduce en dar el carácter de legalidad a la finalidad, esto es, no solo basta con justificar normativamente la finalidad, sino ejecutarla con apego a la ley.

El **principio de lealtad** deja de observarse cuando: (i) la obtención y el tratamiento de los datos personales se realice a través de medios fraudulentos o engañosos; (ii) cuando no privilegia la protección de los intereses del titular ni su expectativa razonable de privacidad, esto es, que el titular acude ante el Instituto para la prestación de un servicio público, confiando en que sus datos personales serán utilizados para el tratamiento estrictamente necesario.

Principio de lealtad: Artículo 19 LGPDPPSO.

Ahora bien, el **consentimiento** es la manifestación de la voluntad a efecto de aceptar una situación que se materializará a partir de dicho reconocimiento.

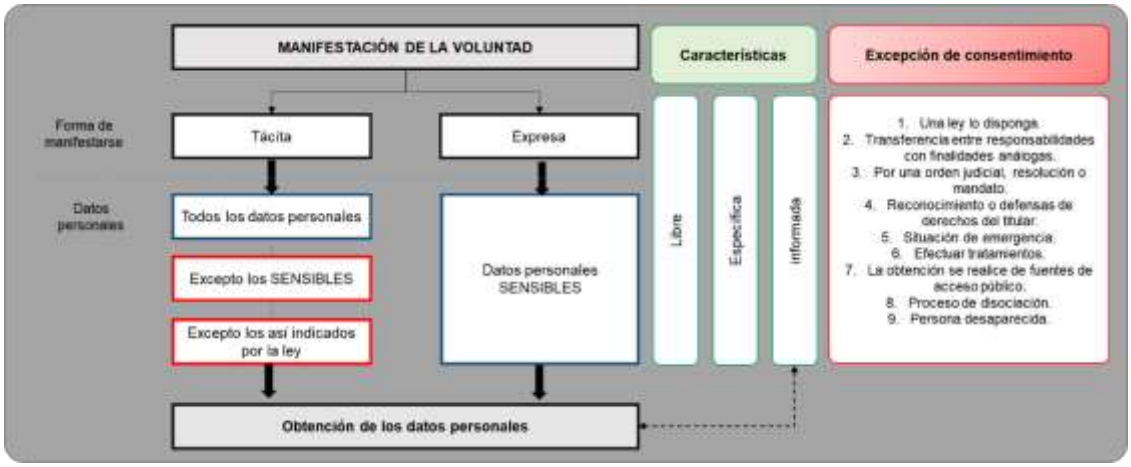
Principio de consentimiento: Artículos 20 a 22 LGPDPPSO.

En materia de protección de datos personales se debe contar con el consentimiento del titular de los datos personales, y tratándose de incapaces, dicha manifestación de la voluntad debe realizarla su representante. Son incapaces: (i) Los menores de edad; (ii) Los mayores de edad disminuidos o perturbados en su inteligencia, aunque tengan intervalos lúcidos, y (iii) Los mayores de edad que padezcan alguna afección originada por enfermedad o deficiencia que no les permita gobernarse u obligarse por sí mismos.

Incapacidad: Artículo 450 Código Civil Federal.

Así, el consentimiento debe cumplir con ciertas reglas, las cuales se diagraman a continuación:

Figura 4 Manifestación de la voluntad



Fuente: Elaboración propia con datos de la LFPDPPP.

Tal y como se desprende del anterior diagrama, el consentimiento puede ser expresado de manera tácita o expresa dependiendo de los datos personales que se pretenda obtener; el primero de los casos resultará aplicable para todos los datos personales, excepto los sensibles y los que la ley de manera expresa requiera de consentimiento expreso, y para el segundo de los casos, esto es, consentimiento expreso, será aplicable tratándose de la obtención de datos sensibles, el cual deberá manifestarse a través de: (i) Firma autógrafa; (ii) Firma electrónica avanzada, o (iii) Cualquier mecanismos de autenticación que se establezca.

Estamos en presencia de un consentimiento tácito cuando el titular no manifieste oposición para el tratamiento de sus datos, sin embargo, es importante que se le ponga a disposición el correspondiente aviso de privacidad, al que se hace referencia en el principio de información. Por su parte, el consentimiento expreso para configurarse debe contarse con la manifestación de la voluntad de manera verbal (decir acepto), escrita, a través de medios electrónicos u ópticos (por ejemplo, una huella digital electrónica), signos inequívocos o por cualquier otra tecnología. Es importante en este punto identificar que se debe contar siempre con la prueba de la obtención del consentimiento.

El consentimiento debe ser otorgado dando cumplimiento a las características que ahora se explican:

1) **Libre**. No debe presentarse ninguno vicio en el otorgamiento del consentimiento:
    f. Error. Hay error al existir una diferencia entre la voluntad del titular y los alcances que tiene la manifestación de dicha voluntad, esto es, cuando se configura una falsa apreciación de la realidad.
    g. Dolo. Existe dolo cuando se emplea cualquier sugestión o artificio para la inducción del titular al error, o bien, mantenerlo en el error en el que se encuentre.
    h. Mala fe. La disimulación del error conocido configura la mala fe.
    i. Violencia. Hay violencia cuando se emplea fuerza física o amenazas que importen peligro de perder la vida, la honra, la libertad, la salud, o una parte considerable de los bienes del titular de los datos personales.

Vicios en el consentimiento: Artículos 1812 a 1823 Código Civil Federal.

4) **Específica**. Esta característica se encuentra íntimamente vinculada con el principio de finalidad, pues la manifestación de la voluntad tiene que referirse a finalidades que cumplan con ser:
    a. Concretas. Una finalidad es concreta cuando adquiere la cualidad de ser específica.
    b. Lícitas. Íntimamente relacionado con principio de licitud, esto es, que la finalidad esté apegada a las atribuciones y funciones de la Institución.
    c. Explícitas. Entendida como la finalidad que es expresada de manera clara y determinada.
    d. Legítimas. No basta con justificar la finalidad con un supuesto normativo, sino su ejecución debe realizarse observando la ley que le da soporte.
5) **Informada**. Característica relacionada con el principio de información, esto es, que previo el tratamiento de los datos personales, se debe poner a disposición del titular el aviso de privacidad correspondiente, ello con el fin de que la manifestación de la voluntad se realice con conocimiento de los datos personales que se recabarán y las finalidades a las que los mismos serán sometidos.

Finalmente, es importante tener en cuenta los supuestos que, de configurarse, constituyen una excepción a la obtención del consentimiento para el tratamiento de datos personales:

Excepciones para la obtención del consentimiento: Artículo 22 LGPDPPSO.

1) Cuando una ley así lo disponga, sin embargo, dicha disposición debe encontrase en armonía con lo dispuesto la LGPDPPSO;
2) Tratándose de transferencias entre responsables, sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
3) El tratamiento debe realizarse derivado de una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
4) El tratamiento deba realizarse para el reconocimiento o defensa de derechos del titular ante autoridad competente;
5) Si los datos personales se requieren para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el Instituto;
6) De existir una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;[204]
7) Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
8) Cuando los datos personales figuren en fuentes de acceso público, entendidas las mismas como los datos, los sistemas o los archivos que por disposición de ley puedan ser consultadas públicamente[205], la que, en su caso, puede estar condicionada al pago de una contraprestación, tarifa

Fuente de acceso público: Artículo 3, fracción XVII LGPDPPSO.

[204] Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en *https://home.inai.org.mx/wp-content/uploads/_GuiaPrincipiosDeberes.pdf*, última fecha de consulta el 20 de agosto de 2019.

[205] SENTENCIA dictada por el Tribunal Pleno de la Suprema Corte de Justicia de la Nación en la Acción de Inconstitucionalidad 158/2017. Disponible en http://diariooficial.segob.gob.mx/nota_detalle.php?codigo=5571264&fecha=04%2F09%2F2019, última fecha de consulta el 20 de agosto de 2019.

o contribución;

9) Si los datos personales han sido sometidos a un procedimiento previo de disociación, esto es, que los datos personales no puedan ser asociados a su titular ni permitir su identificación, y

Disociación: Art. 3, fracción XII LGPDPPSO

10) Si los datos pertenecen a una persona que ha sido reportada como desaparecida, entendida dicha figura como la ausencia de una persona física de su lugar ordinario de residencia.

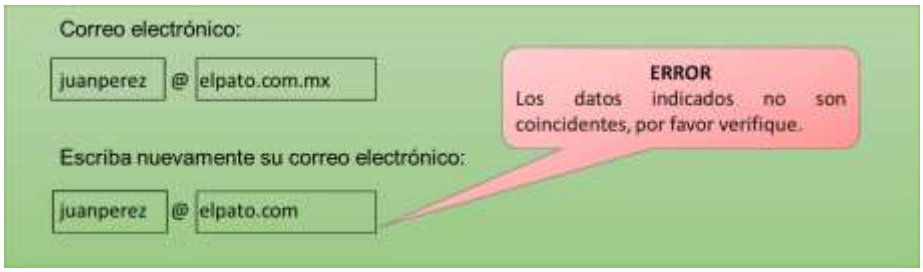
Ausencia: Art. 648 Código Civil Federal.

El siguiente principio es el de **calidad**, el que se cumple cuando se adoptan las medidas necesarias para que los datos se mantengan:

Principio de calidad: Artículos 23 y 24 LGPDPPSO.

1) Completos. Adquieren está característica cuando los datos personales contienen cada uno de los atributos que se requieren, en el mismo ejemplo de requerir el dato de correo electrónico, se puede implementar un procedimiento para verificar que el dato contenga la estructura de un correo electrónico, esto es validar la siguiente estructura: [ ] @ [ ].
2) Correctos. Lo que se traslada en que el dato personal proporcionado no contenga errores, en el mismo ejemplo de requerir el correo electrónico, se puede implementar un mecanismo para escribir dos veces el dato, a efecto de que de no coincidir se solicite al titular la corrección de dicho dato.

Figura 5 Ejemplo para verificar que un dato personal sea correcto



Fuente: Elaboración propia con datos de la LFPDPPP.

3) Exactos. Consta en que los datos personales sean ciertos, por ejemplo,

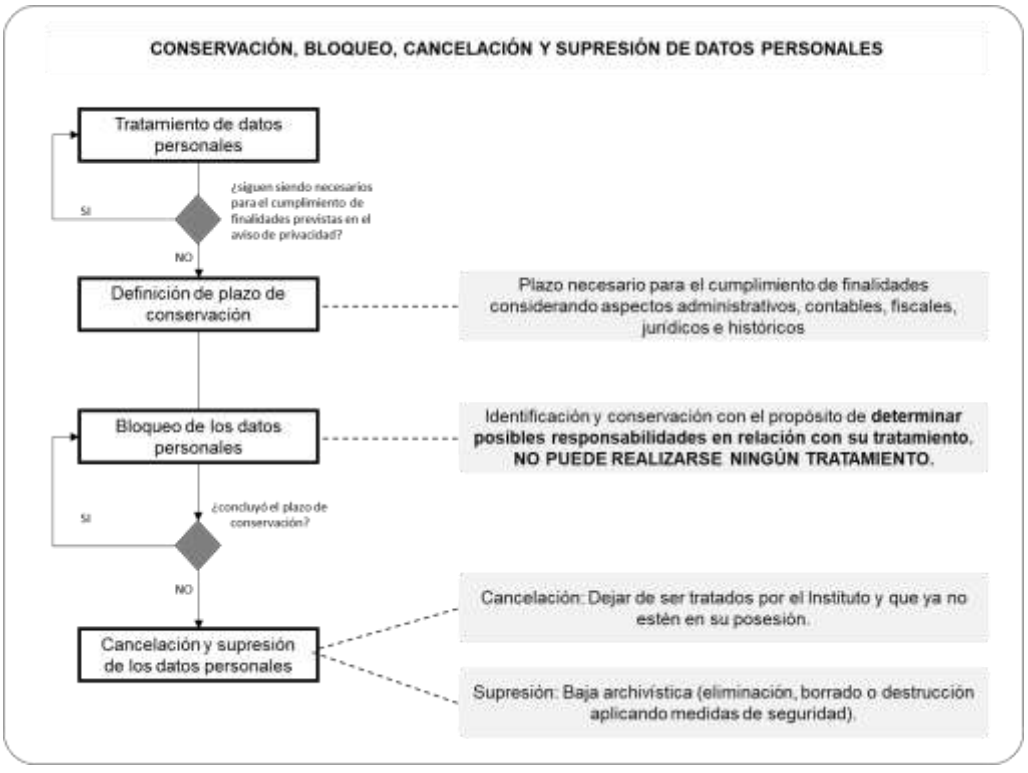
de requerirse el correo electrónico, se puede implementar un procedimiento electrónico que verifique que el correo indicado sea un dato existente.

4) Actualizados. Los datos personales deben ser los más recientes, por ejemplo, en el mismo caso del correo electrónico puede ejecutarse una campaña de actualización que el titular de los datos personales mantenga actualizados sus datos personales.

Cuando los datos son proporcionados por el propio titular de los datos personales, se presume que dichos datos cumplen con el principio de calidad.

Ahora bien, en este principio nos encontramos con un procedimiento muy relevante, esto es, **la conservación, bloqueo, cancelación y supresión de los datos personales.**[206]

Figura 6 Procedimiento de conservación, Bloqueo, Cancelación y Suspensión de datos Personales



Fuente: Elaboración propia con datos de la LFPDPPP.

[206] Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en *https://home.inai.org.mx/wp-content/uploads/_GuiaPrincipiosDeberes.pdf*, última fecha de consulta el 20 de agosto de 2019.

Es necesario que desde la obtención de cada dato personal se identifique el titular al que pertenece y la relación jurídica existente entre el mismo y el Instituto, pues ello facilitará identificar los plazos de conservación que corresponden para la cada uno de ellos. A continuación, se presenta un listado de las obligaciones más comunes para la conservación de los datos personales y que pueden resultar aplicables al IMSS.

Tabla 1. De Artículos

Disposición normativa	**Artículo**	**Acción**	**Tiempo para la conservación**
Ley Federal de archivos.	Artículo 7.	Datos personales conservados por su valor histórico.	30 años.
	Artículo 7.	Datos personales sensibles conservados por su valor histórico.	70 años.
Ley Federal de los Trabajadores al Servicio del Estado, reglamentaria del apartado B) del artículo 123 Constitucional.	Artículo 112.	De manera general, las acciones que nacen de la Ley Federal de los Trabajadores al Servicio del Estado, del nombramiento del trabajador o de las condiciones generales de trabajo.	1 año.
	Artículo 113	Las acciones para pedirla nulidad de un nombramiento. Las acciones de los trabajadores para ejercitar el derecho a ocupar la plaza que hayan dejado por accidente o por enfermedad, contado el plazo a partir de la fecha en que estén en aptitud de volver al trabajo.	1 mes
	Artículo 114	En caso de despido o suspensión injustificados, las acciones para exigir la reinstalación en su trabajo o la indemnización que la Ley concede, contados a partir del momento en que sea notificado el trabajador, del despido o suspensión.	4 meses.

Disposición normativa	Artículo	Acción	Tiempo para la conservación
		En supresión de plazas, las acciones para que se les otorgue otra equivalente a la suprimida o la indemnización de Ley. La facultad de los funcionarios para suspender, cesar o disciplinar a sus trabajadores, contado el término desde que sean conocidas las causas.	
	Artículo 115	Las acciones de los trabajadores para reclamar indemnizaciones por incapacidad provenientes de riesgos profesionales realizados; Las acciones de las personas que dependieron económicamente de los trabajadores muertos con motivo de un riesgo profesional realizado, para reclamar la indemnización correspondiente. Las acciones para ejecutar las resoluciones del Tribunal Federal de Conciliación y Arbitraje.	2 años
Ley del Seguro Social.	Artículo 297	Fijar en cantidad líquida los créditos a favor del Instituto.	5 años.
	Artículo 300	El derecho de los asegurados o sus beneficiarios para reclamar el pago de las prestaciones en dinero, respecto a los seguros de riesgos de trabajo, enfermedades y maternidad, invalidez y vida y guarderías y prestaciones sociales.	1 año.
		Los subsidios por incapacidad para trabajar derivada de un riesgo de trabajo.	2 años.

Disposición normativa	Artículo	Acción	Tiempo para la conservación
	Artículo 302	El derecho del trabajador o pensionado y, en su caso, sus beneficiarios a recibir los recursos de la subcuenta de retiro, cesantía en edad avanzada y vejez	10 años.
		Cualquier mensualidad de una pensión, asignación familiar o ayuda asistencial	1 año.

Fuente: Elaboración propia con datos de la LFPDPPP.

Por lo tanto, para determinar el plazo de conservación para cada caso en específico, será necesario identificar el titular de que se trata y las reglas que le son aplicables. Por ejemplo, si tenemos un sistema que registre y controle todos los movimientos de los derechohabientes del Instituto, y para el sistema dejan de ser visibles los registros de los derechohabientes que causan baja, de conformidad con la tabla anterior, tendremos que conservar los datos conforme a las siguientes reglas:

1. Si el derechohabiente es mayor a 60 años, tendrán que conservarse sus datos por 10 años (artículo 302 Ley del Seguro Social).
2. Para el resto de los derechohabientes, sus datos personales tendrán que conservarse por 2 años, toda vez que, del resto de las reglas indicadas en la tabla relacionadas con la Ley del Seguro Social, es el plazo con mayor duración.

El **principio de proporcionalidad** se cumple cuando los datos sujetos a tratamiento resultan ser adecuados, relevantes y los estrictamente necesarios de conformidad con las finalidades por los que fueron obtenidos y justifican su tratamiento.

Principio de proporcionalidad: Artículo 25 LGPDPPSO.

1) La característica de **adecuados**, se refiere a que los datos personales tratados deben los que se ajustan a las necesidades que motivaron su obtención y su posterior tratamiento.
2) Que los datos personales tratados sean **relevantes** se refiere a que los datos personales sean los más importantes o significativos para las finalidades que correspondan.
3) Por último, que sean los estrictamente **necesarios**, se refiere a que los datos tratados sean los mínimos posibles para el cumplimiento de las respectivas finalidades.

Si continuamos con el ejemplo de la aplicación móvil para que los ciudadanos soliciten servicios de salud a domicilio y se requiera el siguiente dato personal: "*partido político de su preferencia*", evidentemente vemos violado el principio de proporcionalidad, pues el dato no es adecuado, ni relevantes y mucho menos necesario para la prestación del servicio de salud a domicilio.

El **principio de información** se traduce en dar a conocer e informar al titular de los datos personales sobre la existencia y características del tratamiento a que serán sometidos sus datos personales, ello con el objetivo de que dicho titular, decida de manera informada las acciones que adoptará al respecto.

Principio de información: Artículos 3 fracción II y 26 a 28 LGPDPPSO.

Figura 7 Aviso de Privacidad

Fuente: Elaboración propia con datos de la LFPDPPP.

La puesta a disposición del aviso de privacidad tiene que realizarse a través de los medios electrónicos y físicos con que cuente el IMSS, por ejemplo, para administrar todos los aspectos laborales relacionados con los empleados del Instituto se cuenta con un sistema específico, por lo tanto, es necesario contar con un aviso de privacidad dirigido a los empleados del Instituto, el cual deberá ser puesto a disposición de los mismos en los sitios de electrónicos tanto de internet como intranet, así como de manera física en el área de recursos humanos que es donde se obtienen los datos que alimentan al sistema, como en la de tecnologías de la información que es donde se administra dicha información.

También en el ejemplo a que nos referimos sobre la aplicación móvil para prestación de servicios médicos a domicilio, se deberá contar con un aviso de privacidad dirigidos a derechohabientes, en el que uno de las finalidades sea la prestación de este servicio. El aviso de privacidad también deberá ser puesto a disposición en los sitios de internet del Instituto, como en la aplicación móvil y en las instalaciones del Instituto donde se prestan servicios a los derechohabientes.

Si bien es cierto que la normatividad con la que hoy se cuenta no específica los casos en los que deba de ponerse a disposición el aviso de privacidad en la modalidad integral y el aviso de privacidad en la modalidad simplificada, es entonces necesario que para cada titular distinto de los que se traten datos personales, se cuente con ambas modalidades.

Figura 8 Contenido para el aviso de privacidad integral y para el aviso de privacidad simplificado

Contenido	Integral	Simplificado
1) Denominación del responsable.	✓	✓
2) Domicilio del responsable.	✓	
3) Datos personales que serán sometidos al tratamiento.	✓	
4) Identificación de datos sensibles que serán sometidos al tratamiento.	✓	
5) Fundamento legal para llevar a cabo el tratamiento.	✓	
6) Finalidades del tratamiento. Distinguir aquéllas que requieren consentimiento del titular.	✓	✓
7) Indicar transferencias que requieran consentimiento. Indicar destinatario y finalidades de la transferencia.	✓	✓
8) Mecanismos y medios para manifestar la negativa sobre el tratamiento para finalidades y transferencias que requieren consentimiento.	✓	
9) Mecanismos, medios y procedimientos para el ejercicio de derechos ARCO.	✓	
10) Domicilio de la Unidad de Transparencia.	✓	
11) Medios a través de los cuales se comunicará a los titulares los cambios del aviso de privacidad.	✓	
12) El sitio para consultar el aviso de privacidad integral.		✓
13) Portabilidad de los datos.	✓	

Fuente: Elaboración propia con información de los Lineamientos del Aviso de Privacidad.

Principio de responsabilidad: Artículos 29 y 30 LGPDPPSO.

Por último, tenemos el **principio de responsabilidad,** consistente en que el responsable del tratamiento, esto es, el Instituto Mexicano del Seguro Social debe implementar los mecanismos que continuación se señalarán, con el objetivo de acreditar el cumplimiento de principios, deberes y obligaciones que se contienen en la LGPDPSO.

- Destinar recursos para la instrumentación de programas y políticas en materia de protección de datos personales.
- Elaborar políticas y programas en materia de protección de datos personales.
- Poner en práctica un programa de capacitación y actualización del personal.
- Revisar periódicamente las políticas y programas de seguridad de datos personales.
- Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares.
- Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la LGPDPDPSO.
- Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia.

Principio de responsabilidad: Artículos 29 y 30 LGPDPPSO.

Si bien es cierto que lo anteriores mecanismos deben ser implementados de manera general por el IMSS a través del Comité de Transparencia a cada una de las unidades administrativas que conforman el Instituto, también es cierto que, de manera específica, particular y preventiva, esta unidad encargada de las tecnologías de la información, puede adoptar acciones que coadyuven al cumplimiento de dichos mecanismos.

Elaborar políticas y programas en materia de protección de datos personales.


Una política se refiere al conjunto de actividades que se establecen para que las personas a quienes están dirigidas, las adopten y las apliquen. Por su parte, un programa está referido a la planeación que se realiza para ejecutar ciertas actividades, en términos generales, la programación se conforma por el conjunto de actividades marcadas en el tiempo y que deben ser realizadas por las personas que el mismo se especifique.

La política en materia de protección de datos personales para esta área encargada de la adopción y aplicación de las tecnologías de la información y las comunicaciones en el IMSS, puede contener los siguientes rubros:

1) Carácter del IMSS como encargado y responsable del tratamiento, así como la responsabilidad de cada uno de los servidores públicos que en su día a día realizan tratamiento de datos personales.
2) Referencia a las funciones en materia de protección de datos personales del Comité de Transparencia y de la Unidad de Transparencia de este Instituto.
3) La referencia general teórica sobre los aspectos relacionados con la protección de datos personales: (i) De los datos personales; (ii) Del tratamiento de los datos personales; (iii) De los principios en materia de protección de datos personales; (iv) De los deberes en materia de protección de datos personales.
4) Por último, la referencia a las actividades que ésta área debe adoptar para que la normatividad en materia de protección de datos personales sea materializada.

   Respecto de estas actividades definidas, es conveniente definir responsables y fecha(s) para su ejecución.


Revisar periódicamente las políticas y programas de seguridad de datos personales.

En el apartado anterior, se indicó que debería hacerse referencia a las actividades a adoptar para el cumplimiento de los deberes en materia de protección de datos personales, lo que más adelante veremos a detalle, sin embargo, uno de ellos es el deber de seguridad.

Por la delicadeza que representa la seguridad de los datos personales, el documento general de políticas en la materia, puede contener aspectos genéricos sobre el deber, sin embargo, puede contarse con otros instrumentos específicos que detallen las actividades a ejecutar. Sobre este particular, un instrumento auxiliar para su elaboración es el Manual Administrativo de Aplicación General aplicable en las materias de tecnologías de la información y las comunicaciones (en adelante MAAGTICSI), pues dentro de los nueve procesos que contiene, **dos** de ellos están íntimamente relacionados con el deber de seguridad: (i) Proceso de Administración de la Seguridad de la Información (ASI), y (ii) Procesos de Operación y Controles de Seguridad de la Información y del ERISC (OPEC).

Proceso ASI y Proceso OPEC del MAAGTICSI

 Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

De manera preparatoria y preventiva, ésta área de tecnología puede adelantarse en contar con instrumentos que le permitan hacer frente a auditorías, o acciones de supervisión o vigilancia. En la segunda sección de esta guía se sugerirán documentos que podrán ser adoptados para cumplir con la normatividad en materia de protección de datos personales y que de manera proactiva documentarán su cumplimiento para hacer frente a posteriores auditorías, o acciones de supervisión o vigilancia.

 Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la LGPDPDPSO.

Finalmente, la LGPDPPSO dispone que, respecto de sistemas o plataformas electrónica, aplicaciones electrónicas o cualquier tecnología que implique tratamiento de datos personales debe: (i) Cumplir por defecto, esto es, previa a su puesta en operación, esto es, en la fase de planeación y diseño, se debe prever que el producto final cumpla los dispuesto en la normatividad en materia de protección de datos personales que está contenido en esta PRIMERA SECCIÓN, y (ii) Las productos con los que hoy se cuente y que tratan datos personales, también deben cumplir con lo dispuesto en la normatividad en materia de protección de datos personales.

Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia.

En razón de lo anterior, en la SEGUNDA SECCIÓN de esta guía, se proporcionarán formatos y plantillas que podrán ser adoptadas para documentar el cumplimiento de cada disposición normativa en materia de protección de datos personales, los cuales servirán para demostrar que los sistemas o plataformas electrónica, aplicaciones electrónicas o cualquier tecnología que implique tratamiento de datos personales por desarrollar cumplen desde su diseño con dichas disposiciones y las ya existentes se documente su cumplimiento.

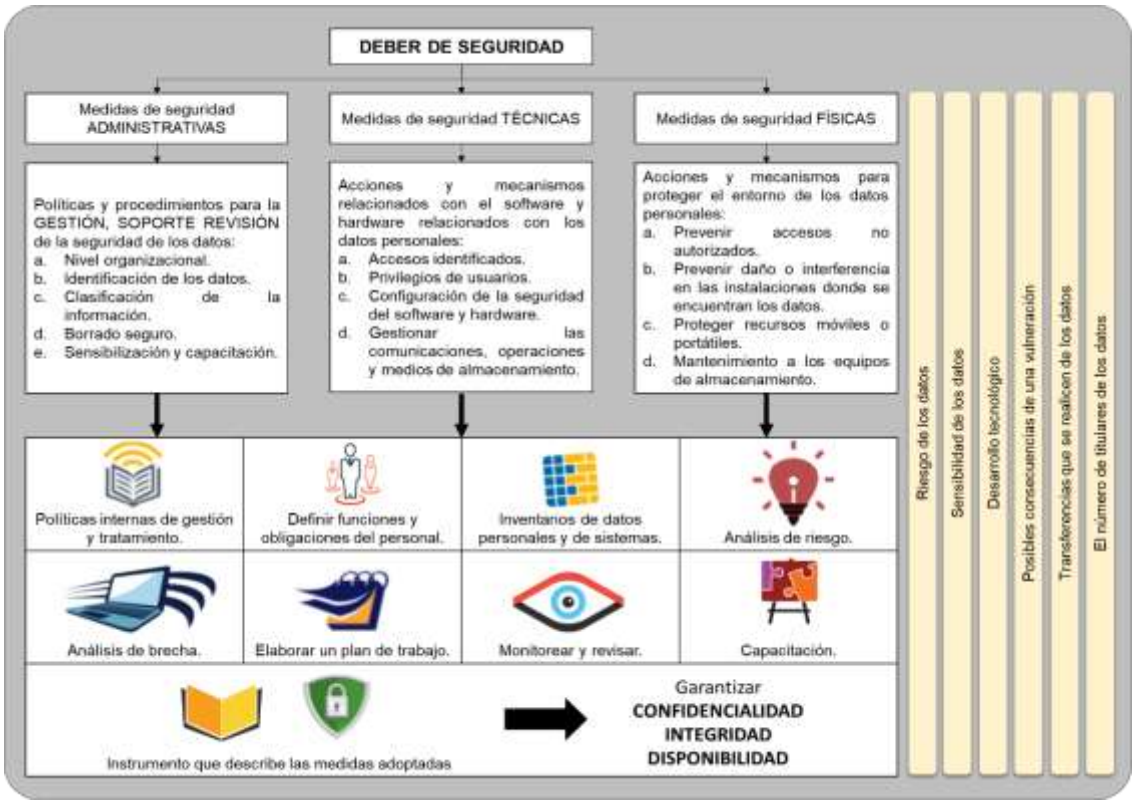
3.1.6 De los deberes en materia de protección de datos personales

Son dos los deberes en materia de protección de datos personales: (i) El deber de seguridad, y (ii) El deber de confidencialidad, integridad y disponibilidad.

Deber de seguridad: Artículos 3 fracciones XVI y XX a XXIII y 31 a 42 LGPDPPSO.

El **deber de seguridad** se refiere a las medidas de seguridad, esto es, el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que protegen los datos personales.

Figura 9 Deber de Seguridad



Fuente: Elaboración propia con datos de la LFPDPPP.

La figura anterior indica la manera en que cada medida deberá materializarse y el objetivo de cada una de ellas. El deber de seguridad indica que deben ejecutarse las siguientes actividades.

1) En complemento a lo indicado en el principio de responsabilidad, se deben emitir políticas internas para la gestión y tratamiento de los datos personales.
2) A efecto de identificar el rol de cada servidor público involucrado en el

tratamiento de datos personales, es necesario documentar el rol y obligaciones que cada uno tiene de ellos. Sobre esta particular, es importante que se tenga en cuenta el Manual de Procedimientos existente en el área.

3) Realizar un inventario de datos personales, así como de los sistemas que realizan tratamiento.
4) Se debe realizar un análisis de riesgo de los datos personales. Tal y como se apuntaba anteriormente, el MAAGTICSI y las Políticas y Disposiciones para la Estrategia Digital Nacional en materias de tecnologías de la información y comunicaciones (en adelante Política TIC), son disposiciones normativas vigentes que, entre otros, son rectoras para el Instituto en materia de seguridad de la información, por lo tanto, las acciones hoy adoptadas para su cumplimiento son de gran apoyo para el cumplimiento del deber de seguridad establecido en la LGPDPPDO. En particular, el artículo 24 de la Política TIC y el Proceso ASI del MAAGTICSI prevén la elaboración del análisis de riesgo y que es definido por el MAAGTICSI como:

   "El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a las infraestructuras de información esenciales y/o críticas o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas."

5) Por otro lado, debe realizarse un análisis de brecha, esto es, documentar las medidas hoy existentes y las medidas faltantes por implementar.
6) Consecuentemente, deberá realizarse un plan de trabajo tanto para la implementación de las medidas faltantes, como para cumplimiento de las políticas emitidas.
7) Será necesario que se realice un monitoreo de las medidas de seguridad implementadas, así como del estado de las amenazas y vulnerabilidades que pudieran giran en torno a los datos personales de que se trate.

8) Asimismo, será necesario que se diseñe y aplique un programa de capacitación para el personal involucrado sobre las medidas de seguridad que deben implementarse.
9) Por último, se debe elaborar un documento de seguridad, el cual contendrá los numerales antes indicados. Dicho documento deberá ser revisado cuando:
    a. Se produzcan riesgos sustanciales en el tratamiento de datos personales y que modifique su nivel de riesgo.
    b. Se identifique la necesidad de su mejora, la cual puede derivar de las actividades de monitoreo y revisión, o bien, para mitigar el impacto de una vulnerabilidad ocurrida.
    c. Requerimiento correctivo derivado de una vulnerabilidad.

Se consideran vulneraciones a la seguridad: (i) La **pérdida** o **destrucción** no autorizada; (ii) El **robo**, **extravío** o **copia** no autorizada; (iii). El **uso**, **acceso** o **tratamiento** no autorizado, o (iv) El **daño**, la **alteración** o **modificación** no autorizada[207]. Al ocurrir cualquiera de las anteriores, se deberá:

1) Inscribir la vulneración en la bitácora correspondiente, la cual al menos: (i) La descripción de la vulnerabilidad; (ii) La fecha en que ocurrió; (iii) El motivo de la vulneración, y (iv) Las acciones correctivas que se implementaron para concluir de manera definitiva con dicha vulneración.
2) Si se causara una afectación significativa en los derechos patrimoniales o morales del (de los) titulare (s) afectado (s), notificarle (s) inmediatamente, así como al Instituto Nacional de Transparencia y de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante "INAI") sobre la vulneración ocurrida.

   La afectación significativa de manera ejemplificativa se refiere a una vulneración relacionada con en el titular y sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, consideración que de sí mismo tienen los demás, o

[207] Diccionario de Protección de Datos Personales Conceptos Fundamentales. Disponible en: http://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf, última fecha de consulta 20 de agosto de 2019.

cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica.

La notificación de la vulneración debe, al menos, contener la siguiente información:

a. La naturaleza del incidente;
b. Los datos personales comprometidos;
c. Las recomendaciones al titular respecto de las medidas que el mismo pueda adoptar para proteger sus intereses;
d. Las acciones correctivas que se han realizado, y
e. Los medios donde puede obtener más información sobre el motivo que dio origen a la notificación.

Las medidas de seguridad implementadas deben tener el propósito de garantizar la **confidencialidad, integridad y disponibilidad de los datos personales.**

3.1.7 De las comunicaciones de datos personales

Remisión y transferencia: Artículos 3 fracciones XV, XVII, XVIII y XXXIII, y 58 a 71 LGPDPPSO.

La comunicación de los datos personales puede realizarse al interior de la organización del responsable, esto es, con sus unidades administrativas, y al exterior de la organización. En ese último caso, la comunicación puede configurarse bajo la figura de remisión de datos personales o de transferencia de datos personales.

Figura 10 Comunicación de los datos personales

Fuente: Elaboración propia con datos del proyecto de intervención.

La **remisión** de datos personales es la que se realiza a una persona ya sea física o moral, de carácter público o privado de nacionalidad o mexicana o de cualquier otra, denominada encargado del tratamiento, y cuya obligación es realizar el tratamiento de los datos personales que le son remitidos conforme a las instrucciones del responsable del tratamiento y no requiere ser informada al titular de los datos personales. Tal y como hemos apuntado anteriormente, puede existir una remisión de datos personales si se cuenta con un contrato de prestación de servicios de almacenamiento, en donde se guardan datos personales cuyo responsable es el IMSS.

La relación entre el responsable del tratamiento y el encargado del tratamiento debe constar por escrito a través de cláusulas contractuales o cualquier otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. Si bien es cierto que dichos instrumentos son responsabilidad del área jurídica del IMSS, también es cierto que resulta conveniente para Dirección de

Innovación y Desarrollo Tecnológico, y siendo más específicos para los administradores y supervisores del contrato, que dichas cláusulas se encuentren presentes en el instrumento que se adopte.

La ley sugiere las siguientes como cláusulas mínimas, sin embargo, es importante mencionar que en la SECCIÓN SEGUNDA de esta guía se presentará una propuesta para el contenido de cada una de ellas.

1. Que el tratamiento de datos debe realizarse conforme a las instrucciones del responsable.
2. Que el encargado no debe tratar los datos personales para finalidades distintas a las indicadas por el responsable.
3. Que debe implementar medidas de seguridad[208].
4. Que debe informar al responsable ante la presentación de una vulnerabilidad a los datos personales.
5. Que debe guardar la confidencialidad sobre los datos remitidos.
6. Que debe suprimir o devolver los datos personales, una vez concluido el tratamiento.
7. Que no debe transferir datos personales, a menos que así se autorice.

Cláusulas contractuales en remisión: Artículo 59 LGPDPPSO.

Ahora bien, si para el cumplimiento de las instrucciones del responsable del tratamiento, el encargado requiere de otro tercero, esto es, de una subcontratación, es el responsable quien debe otorgar dicha autorización. La relación entre el encargado y el subencargado, también debe constar en cláusulas contractuales.

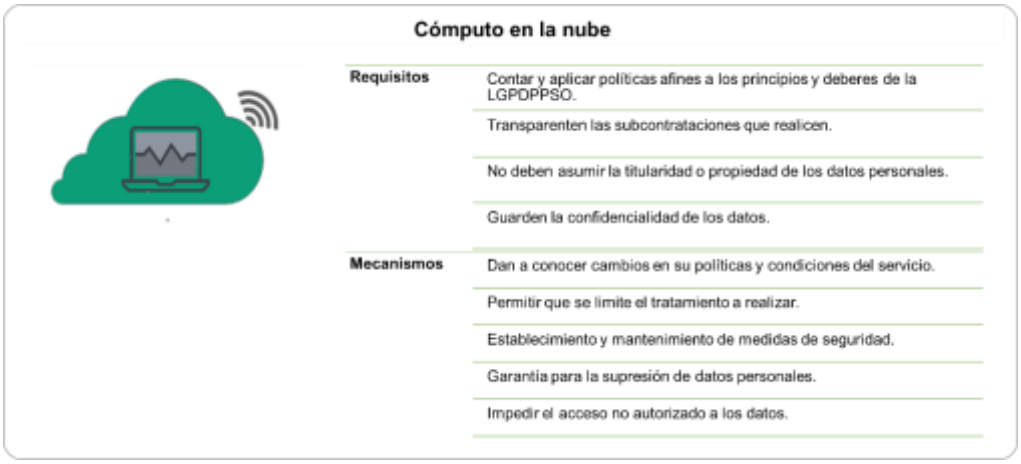
Subencargado: Art. 61 y 62 LGPDPPSO.

[208] Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en *https://home.inai.org.mx/wp-content/uploads/_GuiaPrincipiosDeberes.pdf*, última fecha de consulta el 20 de agosto de 2019.

Cómputo en la nube: Art. 3 fracción VI y 62 y 63 LGPDPPSO.

Por otro lado, la normatividad es muy específica para los casos de contratación de servicios de cómputo en la nube, definido como un "*modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente*"[209], pues para estos casos, solamente se podrá contratar o adherirse al servicio sí: (i) El proveedor garantiza el cumplimiento a los principios y deberes indicados anteriormente, y (ii) Cumpla con los siguientes requisitos y mecanismos, los cuales antes de una contratación deben cuestionarse al proveedor y solicitar evidencia de dicho cumplimiento.

Figura 11 Cómputo en la Nube



Fuente: Elaboración propia con propuesta de intervención.

Para finalizar sobre la remisión de datos personales, es importante señalar que la contravención de lo acordado entre el responsable y el encargado trae aparejado consigo que el encargado sea considerado como responsable del tratamiento, lo cual implica responder ante el titular sobre el tratamiento de sus datos.

[209] Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en *https://home.inai.org.mx/wp-content/uploads/_GuiaPrincipiosDeberes.pdf*, última fecha de consulta el 20 de agosto de 2019.

Por su parte, la **transferencia** de datos personales, es la comunicación de datos personales que se realiza a una persona física o moral, privada o pública, nacional o internacional, siendo dicha persona quien decide sobre el tratamiento de los datos personales. Por regla general, la transferencia de datos personales debe ser informada al titular de los datos personales, toda vez que, para efectuarse, se requiere de su consentimiento, sin embargo, las transferencias no requieren del consentimiento del titular si se configura alguno de los siguientes supuestos, lo que es necesario documentar para tener sustento de dicha comunicación:

Excepciones de consentimiento para transferencias. Artículos. 22, 66 y 70 LGPDPPSO.

1. No hay obligación para obtener consentimiento para el tratamiento de datos personales. Vea principio de consentimiento.
2. La transferencia sea nacional y la transferencia se realiza en virtud del cumplimiento de una disposición normativa.
3. La transferencia sea internacional y esté prevista en un instrumento adoptado por México, o bien, la trasferencia se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.
4. La transferencia esté prevista en una disposición normativa.

5. La transferencia se realice entre responsables y se ejerzan facultades compatibles, análogas o propias con la finalidad que motivó el tratamiento por el primer responsable.
6. La transferencia es exigible para investigación o persecución de delitos, o para la procuración y administración de justicia.
7. La transferencia sea requiera para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de dicha autoridad.
8. La transferencia es necesaria para prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.
9. La transferencia se requiera para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.
10. La transferencia se hace necesaria en virtud del cumplimiento de un contrato en interés del titular.
11. La transferencia es necesaria por razones de seguridad nacional.

Excepciones de consentimiento para transferencias. Artículos. 22, 66 y 70 LGPDPPSO.

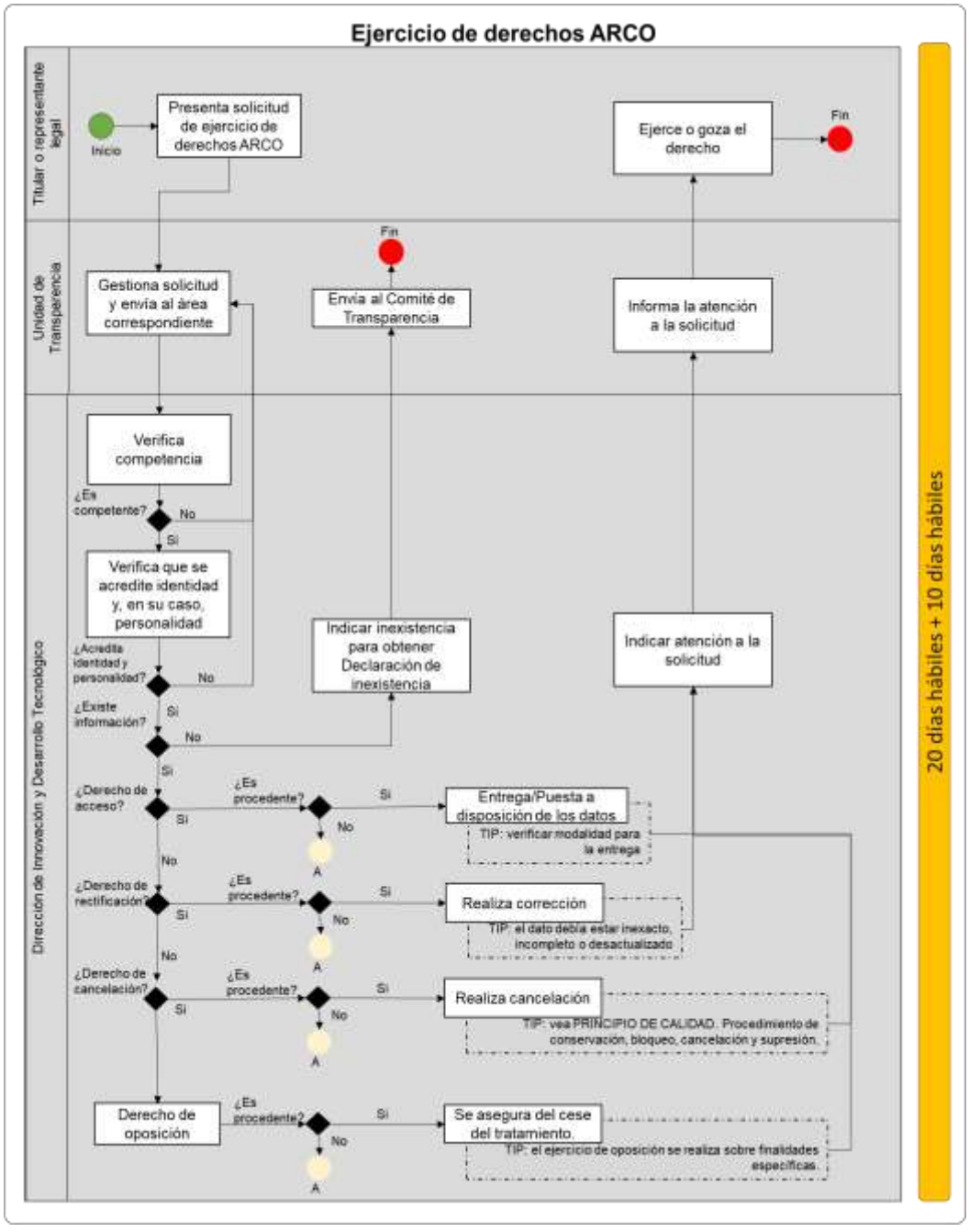
Al igual que la remisión de datos personales, para la transferencia también se hace necesario un instrumento jurídico que permita demostrar alcance de la transferencia.

Es importante distinguir que el IMSS puede comunicar datos personales en su carácter de responsable del tratamiento, o bien, puede recibir datos personales para su tratamiento derivado de una remisión adquiriendo el carácter de encargado del tratamiento, una subcontratación adquiriendo el carácter de subencargado, o bien, de una transferencia adquiriendo el carácter de nuevo encargado.

3.1.8 De los derechos ARCO

Los titulares de los datos personales, por su propio derecho o a través de un representante legal, tienen derecho en todo momento, previa entrega la solicitud correspondiente, al acceso, rectificación, cancelación u oposición de sus datos personales, esto es, el ejercicio de los denominados derechos ARCO.

Figura 1 Ejercicio de Derechos Arco



Fuente: Elaboración propia con datos de propuesta de intervención.

Derechos ARCO: Artículos 3 fracción XI, y 43 a 56 de la LGPDPPSO.

De conformidad con lo dispuesto en la LGPDPPSO la Unidad de Transparencia del Instituto es la encargada de gestionar las solicitudes para el ejercicio de derechos ARCO, sin embargo, al igual que las solicitudes de acceso a la información pública, para proporcionar la correspondiente respuesta, es necesario que la Unidad de Transparencia se auxilie de las diversas áreas administrativas del IMSS.

En razón de lo anterior, es importante conocer los aspectos normativos que deben ser observados para la tramitación de la solicitud y el ejercicio del derecho que corresponda, pues de configurarse alguna de las siguientes premisas, el derecho de que trate la solicitud correspondiente, no puede ser ejercido, situación que debe informarse fundada, motivada y oportunamente a la Unidad de Transparencia.

1. Verificar la competencia de la Dirección de Innovación y Desarrollo Tecnológico para la atención de la solicitud.
2. Verificar que el titular acredite su personalidad, y en su caso, su representante legal acredite su personalidad y la representación con la que actúa.
3. Verificar la existencia de los datos personales del titular que realiza la solicitud.
4. Verificar que no existan impedimentos legales que nieguen el ejercicio del derecho.
5. Verificar que con el ejercicio del derecho de que se trate, no se lesionen derechos de terceros, ni se obstaculice alguna actuación judicial o administrativa, o que los datos no son necesarios proteger los intereses del titular o para cumplimiento de obligados adquiridas por el mismo.
6. Verificar que no exista una resolución de autoridad competente que restrinja el ejercicio de alguno derecho ARCO.
7. Verificar que los datos de que se trate no sean necesarios para mantener integridad, estabilidad y permanencia del Estado mexicano.
8. Verificar que los datos personales no sean parte de la información que las entidades sujetas a la regulación y

Improcedencia para el ejercicio de derechos ARCO: Artículo 55 de la LGPDPPSO.

supervisión financiera del IMSS.

Si de conformidad con lo anterior, la solicitud resulta ser procedente, y se trata de una solicitud de acceso, los datos personales de que se trate deberán ser entregados o puestos a disposición del solicitante, de conformidad con la modalidad de entrega que el mismo hubiere indicado.

Si se tratare de una solicitud de rectificación, es porque los datos personales con los que se cuenta son inexactos, incompletos o desactualizados, por lo tanto, ante tal solicitud deberá realizarse la corrección en cada uno de los registros en los que los datos rectificados se encuentren.

Respecto a las solicitudes de cancelación, resultará procedente la ejecución del procedimiento de conservación, bloqueo, cancelación y supresión de datos personales a que se hizo referencia en el principio de calidad. La cancelación del dato personal supone el cese del tratamiento del mismo.

Finalmente, por cuanto hace a las solicitudes de oposición, el mismo se ejerce para que los datos no sean tratados sobre ciertas finalidades, en razón de lo anterior, se deberá tener extremo cuidado de la ejecución de finalidades solamente se realice sobre datos personales que no hubieren sido opuestos a su tratamiento.

Recuérdese que el IMSS cuenta con 20 días hábiles para atender las solicitudes para el ejercicio de derechos ARCO, sin embargo, la Unidad de Transparencia determina plazos menores para que la atención le sea otorgada.

3.1.9 De la portabilidad de los datos personales

Además de lo indicado en el numeral anterior para el ejercicio de derecho de acceso, es dable destacar que, para los datos personales contenidos en medios electrónicos en formatos estructurados y comúnmente utilizados, el titular de los datos, podrá obtener una copia en tal formato, esto es, tiene derecho a la portabilidad de sus datos personales.

Portabilidad: Artículo 57 de la LGPDPPSO.

Por otro lado, también la portabilidad de los datos personales, se refiere a la transmisión de los datos personales a un responsable receptor.

En razón de lo anterior, el 12 de febrero de 2018, Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, emitió el Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de los datos personales (en adelante “Lineamientos de portabilidad”), los cuales establecen las condiciones para el ejercicio de la portabilidad de los datos personales.

En primer lugar, para el ejercicio de la portabilidad de los datos personales, los mismos deben contenerse en un formato estructurado y comúnmente utilizado, esto es:

1. Se trate de un formato electrónico y accesible por medios automatizado.
2. Se permita la reutilización y/o aprovechamiento de datos personales.
3. El formato sea interoperable con otros sistemas, esto es, que entre el responsable transmisor y el receptor se permita la conexión de sus sistemas.

Por otro lado, es importante que se identifique aquéllos casos sobre los que no es procedente la portabilidad de los datos: (i) Cuando derivan de un análisis o tratamiento efectuado; (ii) Cuando se trata de pseudónimos, salvo que estén claramente vinculados al titular, y (iii) Cuando se trata de datos sometidos a proceso de disociación. Por su parte para que sea procedente la portabilidad: (i) El tratamiento debe realizarse en medios automatizados; (ii) Los datos deben encontrarse en posesión del IMSS o de un encargado; (iii) Los datos deben ser

del titular o de quien tenga legalmente derecho; (iv) El titular debió proporcionar sus datos personales, y (v) La portabilidad no debe afectar derechos o libertades de terceros.

Todos los datos susceptibles de ser portables deben ser protegidos al amparo de todos y cada uno de los principios den materia de protección de datos personales, sin embargo, sobre el principio de información, es importante destacar que, en el respectivo aviso integral de privacidad, debe indicarse al titular:

1. Posibilidad que tiene el titular de solicitar la portabilidad de sus datos;
2. Tipos o categorías de datos portables;
3. Tipo de formato estructurado y comúnmente utilizado, y
4. Los mecanismos, medios y procedimientos disponibles para solicitar la portabilidad.

Figura 2 Portabilidad de datos Personales

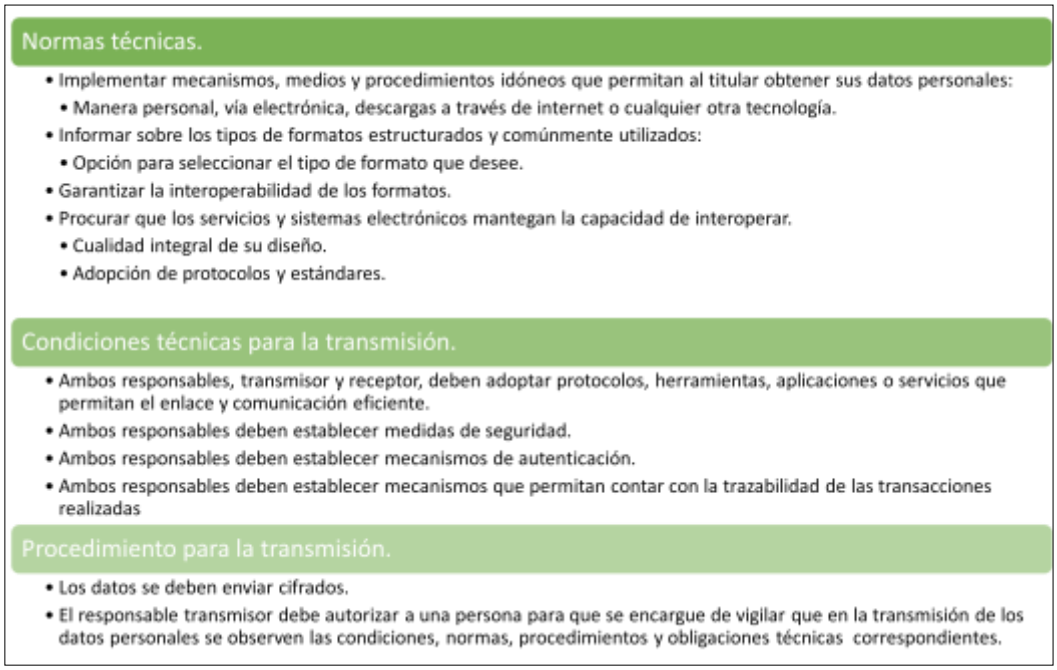
Fuente: Elaboración propia con datos de propuesta de intervención.

La solicitud de portabilidad de los datos debe cumplir con los requisitos de una solicitud de derecho de acceso, sin embargo, además deberá: (i) Contener la petición de la copia de los datos o la transmisión de los mismos; (ii) Si se trata de

transmisión, deberá indicar la denominación del responsable receptor y el documento que acredite su relación con dicho receptor, o bien, la disposición legal que ampare dicha transmisión, y (iii) Si se tratara de un caso de emergencia la explicación de tal situación. El último requisito es sumamente importante, pues por regla general se cuenta con 20 días hábiles para hacer efectiva la portabilidad, sin embargo, en caso de emergencias, el plazo se reduce a 6 días hábiles; plazos dentro de los cuales, o se deberá entregar al titular la copia de sus datos, o bien, notificarle que la transmisión solicitada ha sido realizada.

Para que la transmisión a un responsable receptor pueda efectuarse, debe garantizarse el cumplimiento de las siguientes normas técnicas y procedimientos para la transmisión de datos personales siguientes:

Figura 3 Normas Técnicas y Procedimientos para la Transmisión



Fuente: Elaboración propia con datos de propuesta de intervención.

3.1.10 De la Evaluación de impacto

Dadas las funciones y atribuciones de la Dirección de Innovación y Desarrollo Tecnológico, es importante tener en cuenta que para los casos en los que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología debe realizarse una **Evaluación de impacto en la protección de datos personales.**

Figura 4 Definición de Evaluación de Impacto

> *"Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique* ***el tratamiento intensivo o relevante*** *de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable."*

Fuente: Fracción XVI de la LGPDPPSO.

La evaluación de impacto debe presentarse ante el INAI, el cual podrá emitir recomendaciones de carácter no vinculantes especializadas en materia de protección de datos personales.

De este modo, el 23 de enero de 2018, Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, emitió el Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales (en adelante "Disposiciones Administrativas sobre la Evaluaciones de impacto"), el cual contiene las reglas que deben observarse para la elaboración, presentación y revisión de dicho documento.

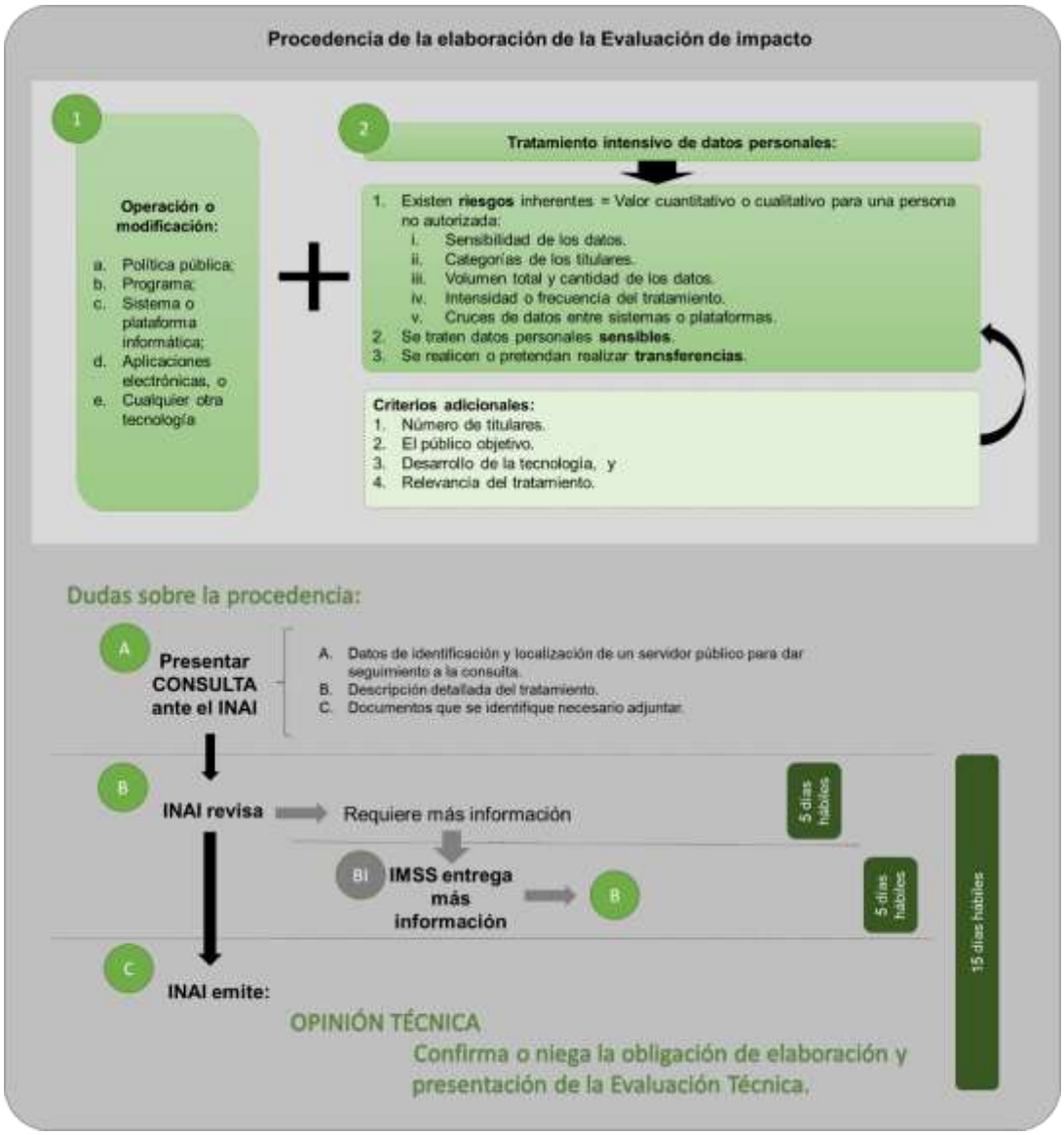
Evaluación de impacto: Artículos 3 fracción XVI y 74 a 79 de la LGPDPPSO.

Para determinar si debe o no realizarse un documento de Evaluación de impacto, es necesario, primero identificar que se cumplan dos requisitos:

PRIMERO: Encontrarnos frente a la puesta en operación o modificación de: (i) Políticas públicas; (ii) Programas; (iii) Sistemas o plataforma informáticas; (iv) Aplicaciones electrónicas, o (v) Cualquier otra tecnología, y

SEGUNDO: Que dicha puesta en operación o modificación implique un tratamiento intensivo o relevante de datos personales.

Figura 5 Procedencia de la Elaboración de la Evaluación de Impacto



Fuente: Elaboración propia con datos de propuesta de intervención.

Nos encontramos frente al tratamiento intensivo de datos relevantes al cumplir con lo indicado en la figura anterior, sin embargo, las Disposiciones

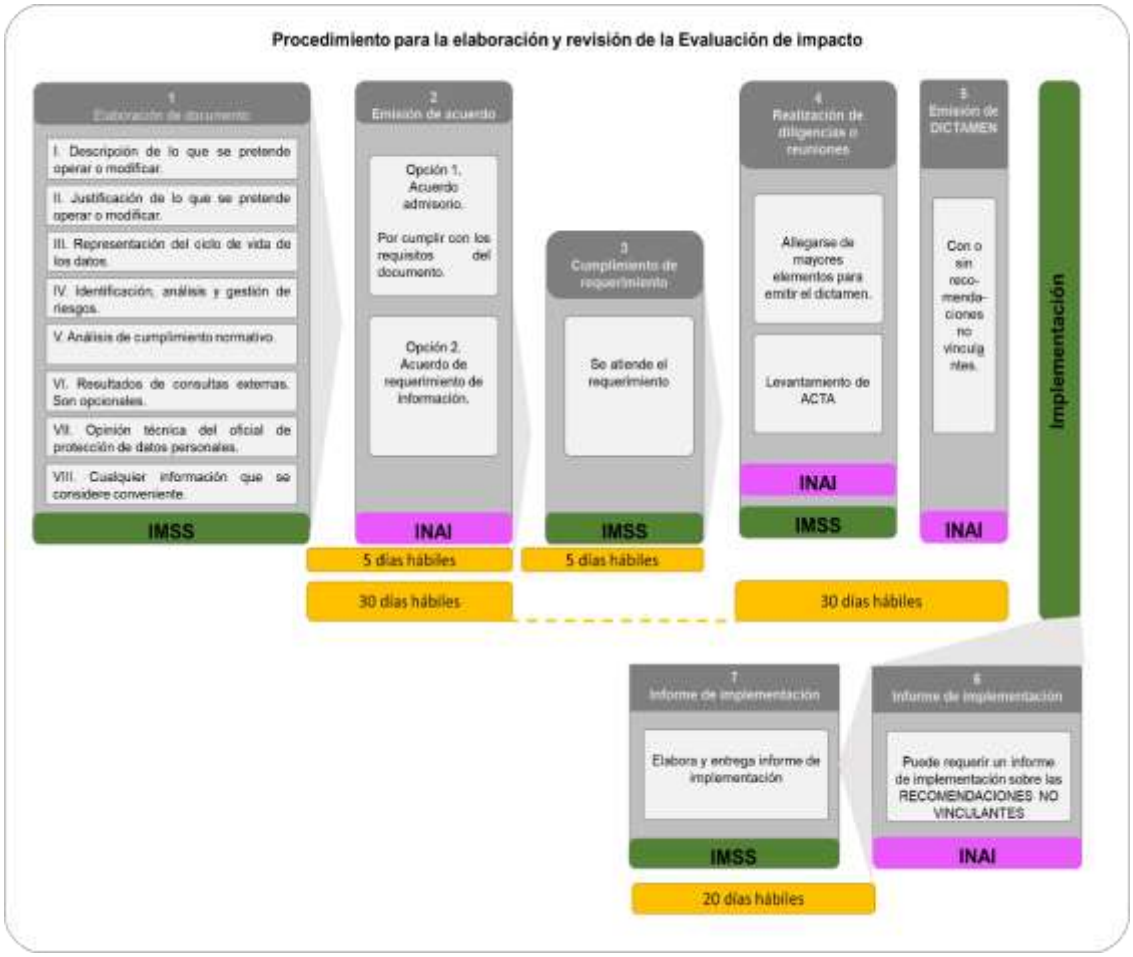
Administrativas sobre Evaluaciones de impacto, añade en su artículo 9o., los siguientes criterios que deben ser tomados en cuenta:

1. Cambio de finalidades de origen del tratamiento. Las nuevas resultan ser más intrusivas.
2. Evaluación, monitoreo, predicción, descripción o clasificación de conductas.
3. Datos personales de grupos vulnerables.
4. Bases de un número elevado de titulares.
5. Incluir o agregar nuevas categorías de datos y que existir una vulneración a la seguridad derive en una afectación en la esfera personal.
6. Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; minería de datos; biometría; Internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala.
7. Acceso a terceros.
8. Transferencias internacionales cuya normatividad no es equiparable a la mexicana.
9. Revierta la disociación de datos personales.
10. Datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos.
11. Elaboración de perfiles.
12. Tratamiento de datos personales relativos a condenas o infracciones penales.
13. Observación sistemática de una zona de acceso público.

Es de relevante importancia que, **ante la duda sobre la elaboración y posterior presentación de la evaluación de impacto,** es mejor activar el procedimiento de consulta ante el INAI, pues en éste supuesto, dicho Instituto tendrá que emitir una **opinión técnica sobre la procedencia o no** de la Evaluación de impacto. La solicitud debe presentarse por escrito ante el INAI y deberá cumplir con los requisitos indicados en la anterior figura; el INAI revisará la solicitud y de estimarse necesario podrá requerir al IMSS de mayor información,

la cual deberá ser entregada dentro de los 5 días hábiles siguientes, por lo tanto, desde la presentación de la solicitud o el cumplimiento del requerimiento de información, el INAI contará con 15 días hábiles para la emisión de la opinión técnica correspondiente, **por lo que en el cronograma de la implementación del sistema o plataforma de que se trate, para su puesta a disposición, deberán tomarse en consideración los 25 días hábiles que podría tomar el procedimiento de consulta para la elaboración del documento de Evaluación de impacto.**

Figura 6 Procedimiento para la Elaboración y Revisión de la Evaluación de Impacto



Fuente: Elaboración propia con datos de propuesta de intervención.

De resultar procedente la elaboración y presentación de la evaluación de impacto, la misma deberá atender al procedimiento esquematizado en la anterior figura, de lo que, a primera vista, es importante considerar **en el cronograma de la implementación del sistema o plataforma de que se trate, para su puesta**

a disposición, además de los 25 días hábiles de la consulta, considerar adicionalmente otros 35 días hábiles para la emisión del dictamen que recaiga a la evaluación de impacto correspondiente.

Para la elaboración de documento de evaluación de impacto deben indicarse los ocho requisitos indicados en el paso 1 de la figura anterior, de los que algunos de ellos tienen requerimientos especiales que se contendrán en la SECCIÓN SEGUNDA de esta guía. Una vez que se cuente con el documento de evaluación de impacto, el mismo se debe presentar ante el INAI, hoy en día mediante oficio escrito en el domicilio de ese Instituto.

Posteriormente, el INAI revisará el documento de evaluación de impacto; si cumple con los respectivos requisitos, dentro de los 5 días hábiles posteriores a la recepción del documento emitirá un acuerdo admisorio, sin embargo, de no cumplir con los requisitos antes referidos, dentro de los 5 días hábiles posteriores a la recepción del documento, emitirá un acuerdo preventivo, en el que indicarán los requisitos en los que el IMSS ha sido omiso o incompleto, caso en el que éste último, tendrá 5 días hábiles para subsanar o completar la información de que se trate.

Posterior a la emisión del acuerdo admisorio, o bien, del cumplimiento al requerimiento de información, el INAI podrá llevar a cabo las diligencias o reuniones que estime necesarias, de las cuales deberá emitir el acta respectiva. Dichas diligencias o reuniones se celebrarán con el objeto de contar con mayores elementos para emitir el dictamen correspondiente, el cual tiene como plazo el de 30 días hábiles contados a partir de la presentación del documento, siendo dicho plazo interrumpido durante los días en los que el IMSS, en su caso, atienda el correspondiente acuerdo de requerimiento de información.

El dictamen que emita el INAI indicará si se emiten o no recomendaciones no vinculantes, con lo cual el IMSS podrá o no poner a disposición las políticas públicas o los programas o los sistemas o plataformas informáticas o las aplicaciones electrónicas, o cualquier otra tecnología, según se trate.

Para el caso de que el dictamen contenga recomendaciones no vinculantes, el INAI puede requerir un Informe de implementación, el cual deberá ser entregado dentro de los 20 días hábiles siguientes posteriores a la recepción

del requerimiento de informe, por lo que, en este caso, es necesario documentar desde la implementación la atención a cada recomendación recibida.

Finalmente, es importante destacar que para aquéllos casos en lo que se estime que la implementación de que se trate pueda comprometer sus efectos, o bien, se encuentre frente a una situación de emergencia o urgencia, no será necesario realizar la evaluación de impacto, la que se sustituye con un Informe de exención, el cual deberá ser presentado durante los siguientes 30 días a la puesta en operación correspondiente, el cual debe cumplir con ciertos requisitos legales. De igual manera que en la evaluación de impacto, el INAI podrá realizar requerimientos de información, y en un plazo máximo de quince días, deberá emitir la respuesta correspondiente, la que puede reconocer la situación que supuestamente dio origen al Informe de exención, o bien, ordenando que dentro de los 10 días siguientes se presente el documento de evaluación de impacto, dado que no se actualizó ningún supuesto que motive la exención.

SECCIÓN SEGUNDA. INSTRUMENTOS QUE LE PERMITIRÁN DAR CUMPLIMIENTO A LO ESTABLECIDO EN LA NOMATIVIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

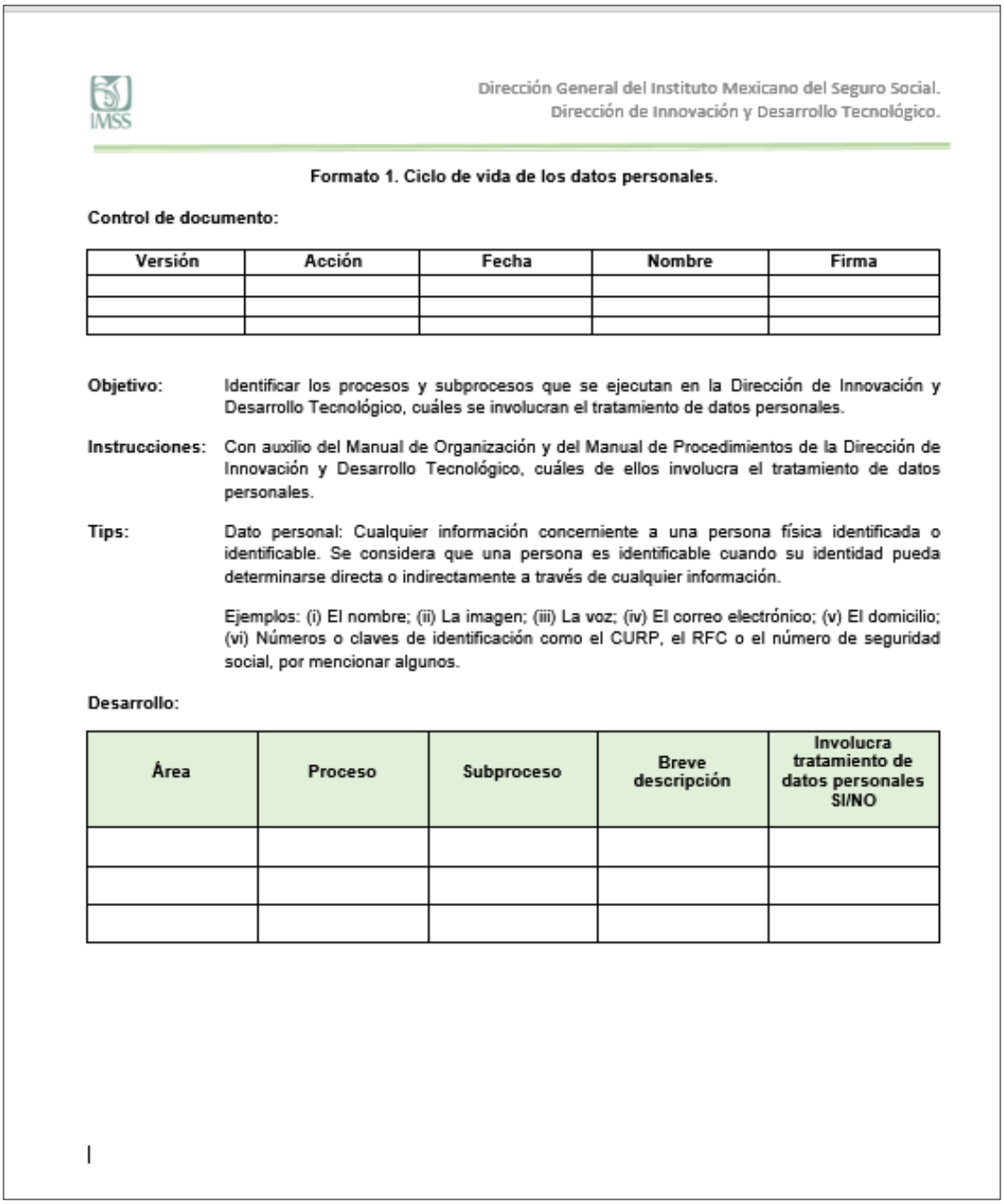
De la SECCIÓN PRIMERA de esta guía se desprende que la normatividad en materia de protección de datos personales se compone de principios, deberes y obligaciones, por lo que, en este apartado se proporcionarán instrumentos que deberán ser adoptados por la Dirección de Innovación y Desarrollo Tecnológico con los que preventivamente se ejecutarán las acciones conducentes para que el tratamiento de datos se realice con total apego a la normatividad en materia de protección de datos personales.

3.1.11 De la arquitectura de procesos de la Dirección de Innovación y Desarrollo Tecnológico

Antes de cualquier otro paso, lo primero es identificar los procesos con base en los cuales la Dirección de Innovación y Desarrollo Tecnológico desarrolla sus funciones y atribuciones, a efecto de que, con base en el mismo, se identifiquen a su vez, en cuáles de ellos se realiza el tratamiento de datos personales.

Para realizar el anterior levantamiento, se sugiere tomar como base los Manuales de organización y procedimientos de la Dirección y documentar el siguiente formato:

Documento 1. Arquitectura de Procesos



Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Formato 1. Ciclo de vida de los datos personales.

Control de documento:

Versión	Acción	Fecha	Nombre	Firma

Objetivo: Identificar los procesos y subprocesos que se ejecutan en la Dirección de Innovación y Desarrollo Tecnológico, cuáles se involucran el tratamiento de datos personales.

Instrucciones: Con auxilio del Manual de Organización y del Manual de Procedimientos de la Dirección de Innovación y Desarrollo Tecnológico, cuáles de ellos involucra el tratamiento de datos personales.

Tips: Dato personal: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Ejemplos: (i) El nombre; (ii) La imagen; (iii) La voz; (iv) El correo electrónico; (v) El domicilio; (vi) Números o claves de identificación como el CURP, el RFC o el número de seguridad social, por mencionar algunos.

Desarrollo:

Área	Proceso	Subproceso	Breve descripción	Involucra tratamiento de datos personales SI/NO

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

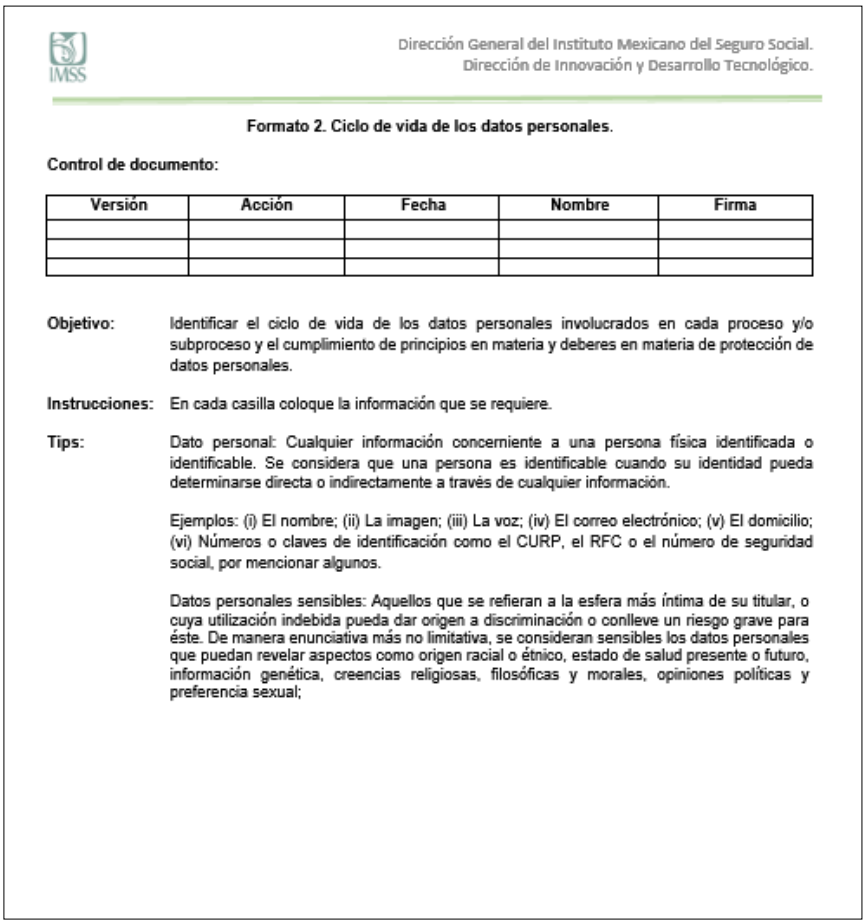
3.2.2 De la documentación de cada proceso, y en su caso, subproceso en el que se involucre el tratamiento de datos personales

Ahora bien, por cada uno de los procesos y subprocesos en los que se identifique que se realiza tratamiento de datos personales, es necesario documentar las acciones adoptadas para el cumplimiento de principios y deberes y obligaciones relacionadas con la comunicación de dichos datos personales.

Asimismo, si para los nuevos desarrollos de programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, también es necesario realizar dicha documentación, pues la misma será el análisis que, en su caso le permitirá presentar la Evaluación de Impacto correspondiente ante el INAI.

Para lo anterior, se sugiere la adopción del siguiente formato:

Documento 2. Formato 1. Ciclo de vida de los datos personales, página 1



Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Formato 2. Ciclo de vida de los datos personales.

Control de documento:

Versión	Acción	Fecha	Nombre	Firma

Objetivo: Identificar el ciclo de vida de los datos personales involucrados en cada proceso y/o subproceso y el cumplimiento de principios en materia y deberes en materia de protección de datos personales.

Instrucciones: En cada casilla coloque la información que se requiere.

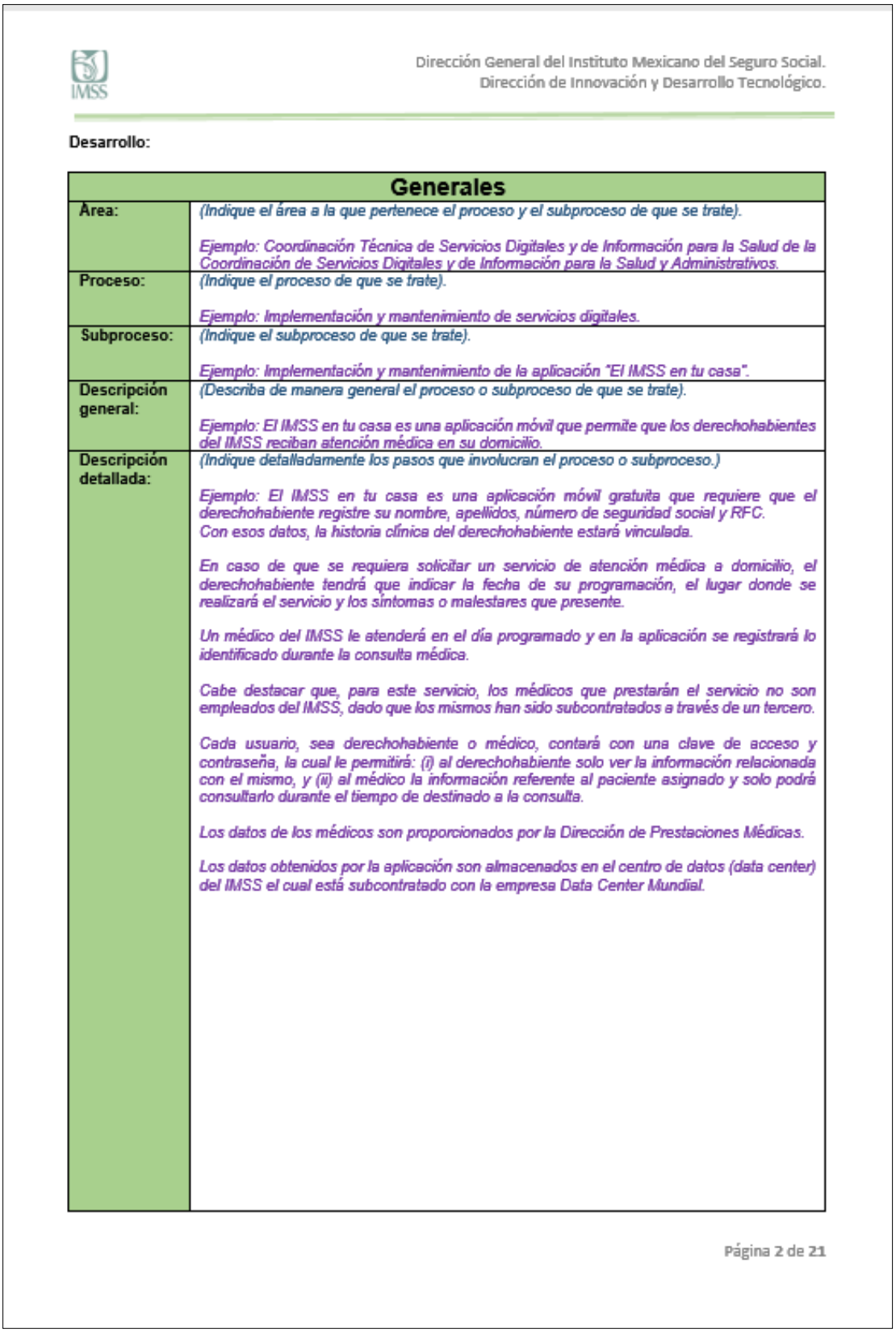
Tips: Dato personal: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Ejemplos: (i) El nombre; (ii) La imagen; (iii) La voz; (iv) El correo electrónico; (v) El domicilio; (vi) Números o claves de identificación como el CURP, el RFC o el número de seguridad social, por mencionar algunos.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 3. Formato 2 Ciclo de vida de los datos personales, página 2



Desarrollo:

Generales	
Área:	*(Indique el área a la que pertenece el proceso y el subproceso de que se trate).* *Ejemplo: Coordinación Técnica de Servicios Digitales y de Información para la Salud de la Coordinación de Servicios Digitales y de Información para la Salud y Administrativos.*
Proceso:	*(Indique el proceso de que se trate).* *Ejemplo: Implementación y mantenimiento de servicios digitales.*
Subproceso:	*(Indique el subproceso de que se trate).* *Ejemplo: Implementación y mantenimiento de la aplicación "El IMSS en tu casa".*
Descripción general:	*(Describa de manera general el proceso o subproceso de que se trate).* *Ejemplo: El IMSS en tu casa es una aplicación móvil que permite que los derechohabientes del IMSS reciban atención médica en su domicilio.*
Descripción detallada:	*(Indique detalladamente los pasos que involucran el proceso o subproceso.)* *Ejemplo: El IMSS en tu casa es una aplicación móvil gratuita que requiere que el derechohabiente registre su nombre, apellidos, número de seguridad social y RFC.* *Con esos datos, la historia clínica del derechohabiente estará vinculada.* *En caso de que se requiera solicitar un servicio de atención médica a domicilio, el derechohabiente tendrá que indicar la fecha de su programación, el lugar donde se realizará el servicio y los síntomas o malestares que presente.* *Un médico del IMSS le atenderá en el día programado y en la aplicación se registrará lo identificado durante la consulta médica.* *Cabe destacar que, para este servicio, los médicos que prestarán el servicio no son empleados del IMSS, dado que los mismos han sido subcontratados a través de un tercero.* *Cada usuario, sea derechohabiente o médico, contará con una clave de acceso y contraseña, la cual le permitirá: (i) al derechohabiente solo ver la información relacionada con el mismo, y (ii) al médico la información referente al paciente asignado y solo podrá consultarlo durante el tiempo de destinado a la consulta.* *Los datos de los médicos son proporcionados por la Dirección de Prestaciones Médicas.* *Los datos obtenidos por la aplicación son almacenados en el centro de datos (data center) del IMSS el cual está subcontratado con la empresa Data Center Mundial.*

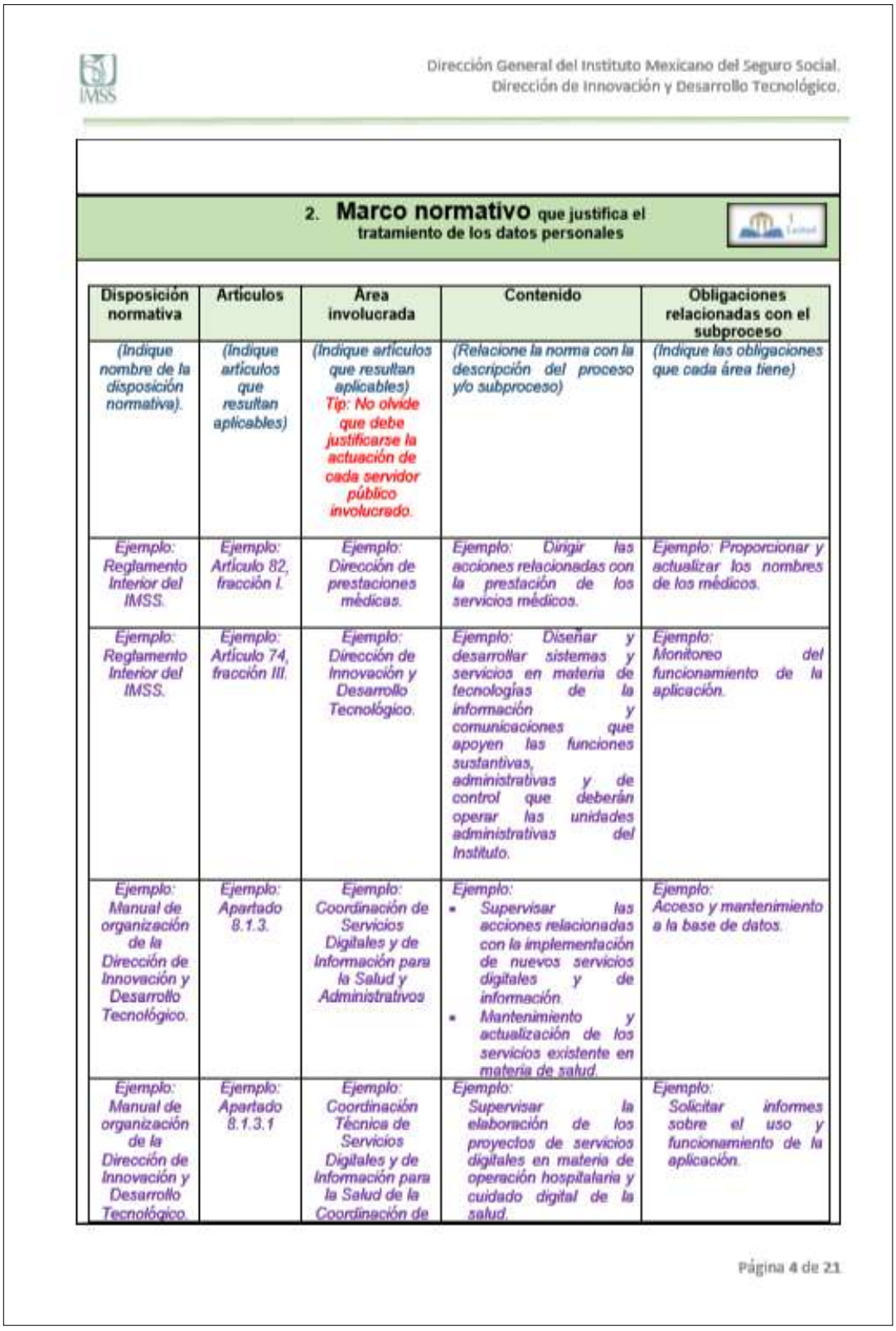
Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 4. Ciclo de vida de los datos personales, página 3

1. Identificación de datos personales involucrados

Dato o categoría de dato	Titular al que pertenecen	Medio de obtención	Dato sensible SI/NO
(Indique los datos o categorías de datos).	*(Indique el titular al que pertenecen)*	*(Indique el medio de obtención)*	*(Indique si el dato es sensible)*
Ejemplo: Datos de identificación: Nombre	*Ejemplo: Derechohabiente*	*Ejemplo: Electrónicamente del titular, con mecanismo de identificación.*	*Ejemplo: No.*
Ejemplo: Datos de salud.	*Ejemplo: Derechohabiente*	*Ejemplo: Electrónicamente del titular, con mecanismo de identificación.*	*Ejemplo: Si.*
Ejemplo: Datos de identificación: Nombre	*Ejemplo: Médicos*	*Ejemplo: Por otra unidad administrativa.*	*Ejemplo: No.*

Documento 5. Formato 2 Ciclo de vida de los datos personales, página 4



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

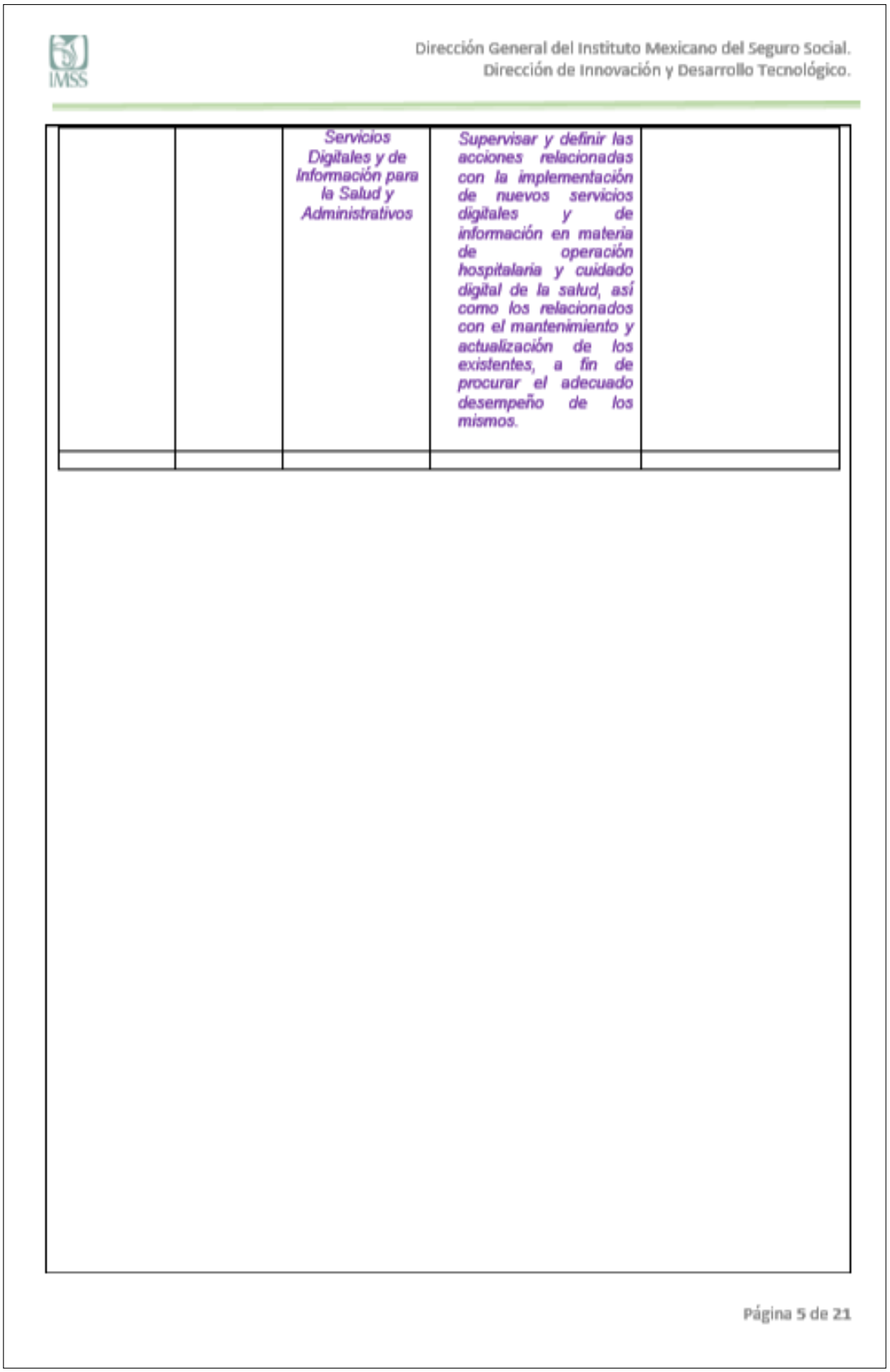
2. Marco normativo que justifica el tratamiento de los datos personales

Disposición normativa	Artículos	Área involucrada	Contenido	Obligaciones relacionadas con el subproceso
(Indique nombre de la disposición normativa).	*(Indique artículos que resultan aplicables)*	*(Indique artículos que resultan aplicables)* Tip: No olvide que debe justificarse la actuación de cada servidor público involucrado.	*(Relacione la norma con la descripción del proceso y/o subproceso)*	*(Indique las obligaciones que cada área tiene)*
Ejemplo: Reglamento Interior del IMSS.	*Ejemplo: Artículo 82, fracción I.*	*Ejemplo: Dirección de prestaciones médicas.*	*Ejemplo: Dirigir las acciones relacionadas con la prestación de los servicios médicos.*	*Ejemplo: Proporcionar y actualizar los nombres de los médicos.*
Ejemplo: Reglamento Interior del IMSS.	*Ejemplo: Artículo 74, fracción III.*	*Ejemplo: Dirección de Innovación y Desarrollo Tecnológico.*	*Ejemplo: Diseñar y desarrollar sistemas y servicios en materia de tecnologías de la información y comunicaciones que apoyen las funciones sustantivas, administrativas y de control que deberán operar las unidades administrativas del Instituto.*	*Ejemplo: Monitoreo del funcionamiento de la aplicación.*
Ejemplo: Manual de organización de la Dirección de Innovación y Desarrollo Tecnológico.	*Ejemplo: Apartado 8.1.3.*	*Ejemplo: Coordinación de Servicios Digitales y de Información para la Salud y Administrativos*	*Ejemplo:* • *Supervisar las acciones relacionadas con la implementación de nuevos servicios digitales y de información.* • *Mantenimiento y actualización de los servicios existente en materia de salud.*	*Ejemplo: Acceso y mantenimiento a la base de datos.*
Ejemplo: Manual de organización de la Dirección de Innovación y Desarrollo Tecnológico.	*Ejemplo: Apartado 8.1.3.1*	*Ejemplo: Coordinación Técnica de Servicios Digitales y de Información para la Salud de la Coordinación de*	*Ejemplo: Supervisar la elaboración de los proyectos de servicios digitales en materia de operación hospitalaria y cuidado digital de la salud.*	*Ejemplo: Solicitar informes sobre el uso y funcionamiento de la aplicación.*

Página 4 de 21

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 6. Formato 2 Ciclo de vida de los datos personales, página 5



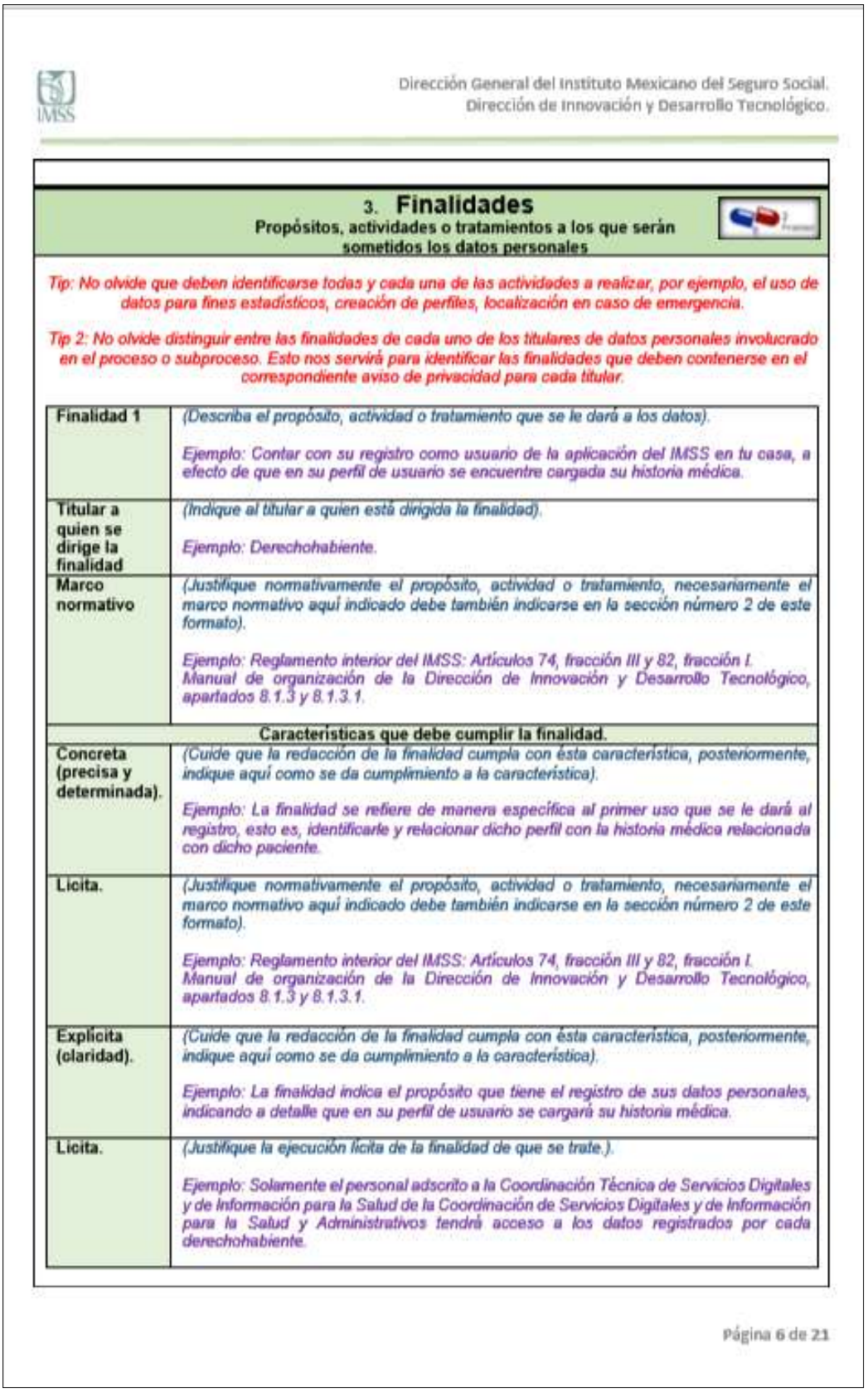
Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

		Servicios Digitales y de Información para la Salud y Administrativos	*Supervisar y definir las acciones relacionadas con la implementación de nuevos servicios digitales y de información en materia de operación hospitalaria y cuidado digital de la salud, así como los relacionados con el mantenimiento y actualización de los existentes, a fin de procurar el adecuado desempeño de los mismos.*	

Página 5 de 21

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 7. Formato 2 Ciclo de vida de los datos personales, página 6



3. Finalidades

Propósitos, actividades o tratamientos a los que serán sometidos los datos personales

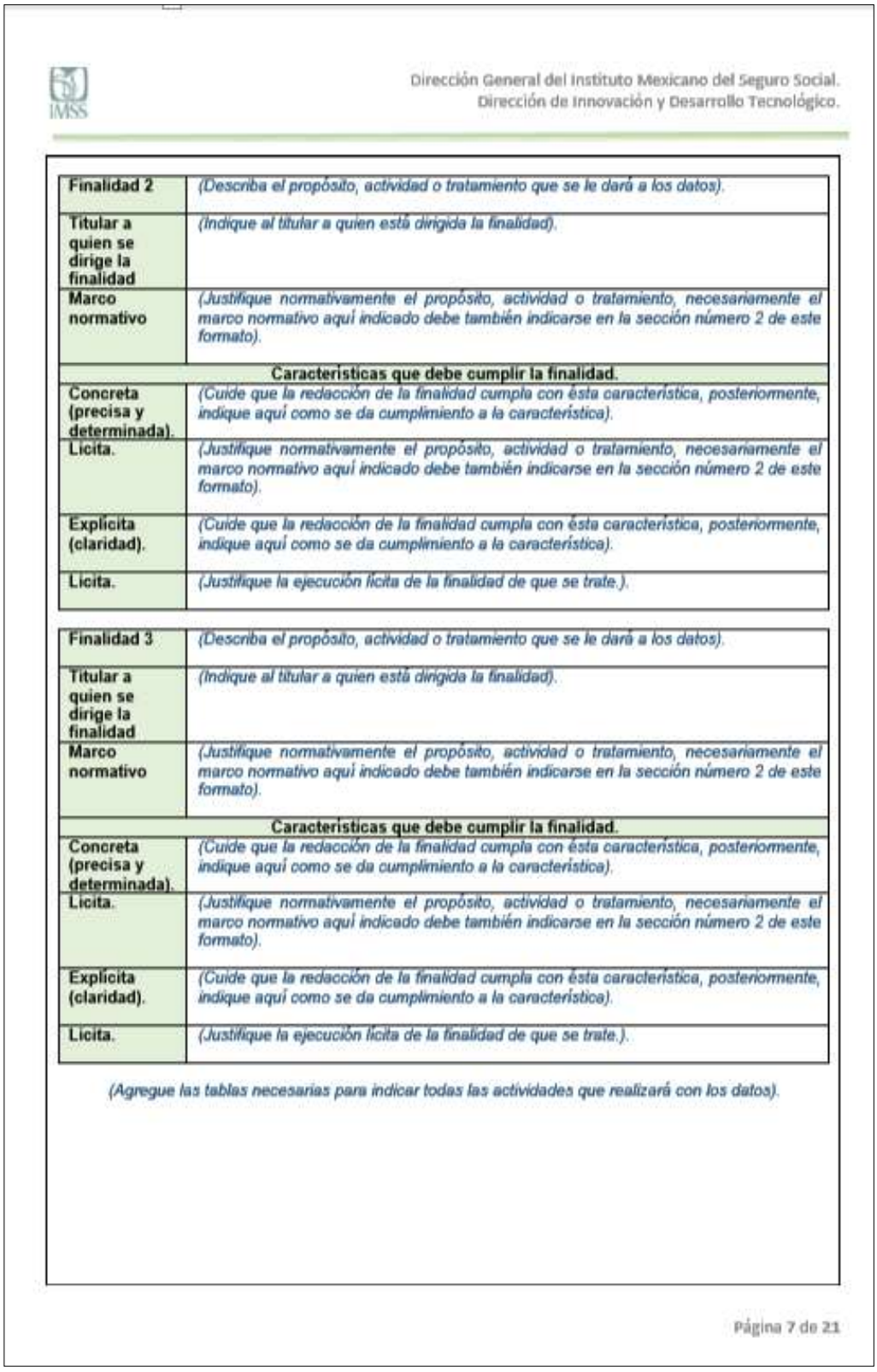
Tip: No olvide que deben identificarse todas y cada una de las actividades a realizar, por ejemplo, el uso de datos para fines estadísticos, creación de perfiles, localización en caso de emergencia.

Tip 2: No olvide distinguir entre las finalidades de cada uno de los titulares de datos personales involucrado en el proceso o subproceso. Esto nos servirá para identificar las finalidades que deben contenerse en el correspondiente aviso de privacidad para cada titular.

Finalidad 1	*(Describa el propósito, actividad o tratamiento que se le dará a los datos).* *Ejemplo: Contar con su registro como usuario de la aplicación del IMSS en tu casa, a efecto de que en su perfil de usuario se encuentre cargada su historia médica.*
Titular a quien se dirige la finalidad	*(Indique al titular a quien está dirigida la finalidad).* *Ejemplo: Derechohabiente.*
Marco normativo	*(Justifique normativamente el propósito, actividad o tratamiento, necesariamente el marco normativo aquí indicado debe también indicarse en la sección número 2 de este formato).* *Ejemplo: Reglamento interior del IMSS: Artículos 74, fracción III y 82, fracción I. Manual de organización de la Dirección de Innovación y Desarrollo Tecnológico, apartados 8.1.3 y 8.1.3.1.*
Características que debe cumplir la finalidad.	
Concreta (precisa y determinada).	*(Cuide que la redacción de la finalidad cumpla con ésta característica, posteriormente, indique aquí como se da cumplimiento a la característica).* *Ejemplo: La finalidad se refiere de manera específica al primer uso que se le dará al registro, esto es, identificarle y relacionar dicho perfil con la historia médica relacionada con dicho paciente.*
Licita.	*(Justifique normativamente el propósito, actividad o tratamiento, necesariamente el marco normativo aquí indicado debe también indicarse en la sección número 2 de este formato).* *Ejemplo: Reglamento interior del IMSS: Artículos 74, fracción III y 82, fracción I. Manual de organización de la Dirección de Innovación y Desarrollo Tecnológico, apartados 8.1.3 y 8.1.3.1.*
Explícita (claridad).	*(Cuide que la redacción de la finalidad cumpla con ésta característica, posteriormente, indique aquí como se da cumplimiento a la característica).* *Ejemplo: La finalidad indica el propósito que tiene el registro de sus datos personales, indicando a detalle que en su perfil de usuario se cargará su historia médica.*
Licita.	*(Justifique la ejecución lícita de la finalidad de que se trate.).* *Ejemplo: Solamente el personal adscrito a la Coordinación Técnica de Servicios Digitales y de Información para la Salud de la Coordinación de Servicios Digitales y de Información para la Salud y Administrativos tendrá acceso a los datos registrados por cada derechohabiente.*

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 8. Formato 2 Ciclo de vida de los datos personales, página 7



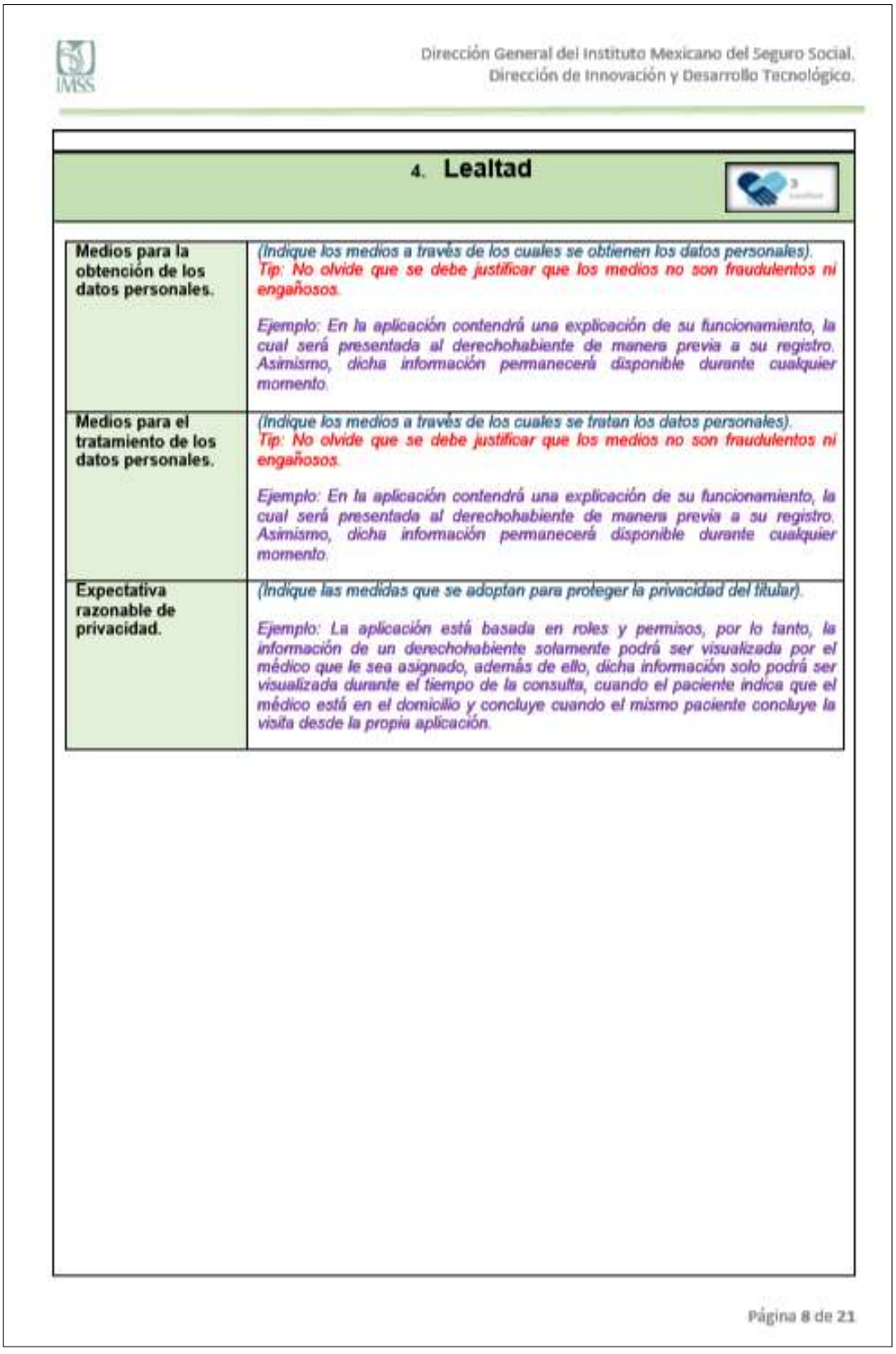
Finalidad 2	*(Describa el propósito, actividad o tratamiento que se le dará a los datos).*
Titular a quien se dirige la finalidad	*(Indique al titular a quien está dirigida la finalidad).*
Marco normativo	*(Justifique normativamente el propósito, actividad o tratamiento, necesariamente el marco normativo aquí indicado debe también indicarse en la sección número 2 de este formato).*
Características que debe cumplir la finalidad.	
Concreta (precisa y determinada).	*(Cuide que la redacción de la finalidad cumpla con ésta característica, posteriormente, indique aquí como se da cumplimiento a la característica).*
Licita.	*(Justifique normativamente el propósito, actividad o tratamiento, necesariamente el marco normativo aquí indicado debe también indicarse en la sección número 2 de este formato).*
Explicita (claridad).	*(Cuide que la redacción de la finalidad cumpla con ésta característica, posteriormente, indique aquí como se da cumplimiento a la característica).*
Licita.	*(Justifique la ejecución lícita de la finalidad de que se trate.).*

Finalidad 3	*(Describa el propósito, actividad o tratamiento que se le dará a los datos).*
Titular a quien se dirige la finalidad	*(Indique al titular a quien está dirigida la finalidad).*
Marco normativo	*(Justifique normativamente el propósito, actividad o tratamiento, necesariamente el marco normativo aquí indicado debe también indicarse en la sección número 2 de este formato).*
Características que debe cumplir la finalidad.	
Concreta (precisa y determinada).	*(Cuide que la redacción de la finalidad cumpla con ésta característica, posteriormente, indique aquí como se da cumplimiento a la característica).*
Licita.	*(Justifique normativamente el propósito, actividad o tratamiento, necesariamente el marco normativo aquí indicado debe también indicarse en la sección número 2 de este formato).*
Explicita (claridad).	*(Cuide que la redacción de la finalidad cumpla con ésta característica, posteriormente, indique aquí como se da cumplimiento a la característica).*
Licita.	*(Justifique la ejecución lícita de la finalidad de que se trate.).*

(Agregue las tablas necesarias para indicar todas las actividades que realizará con los datos).

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 9. Formato 2 Ciclo de vida de los datos personales, página 8



Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

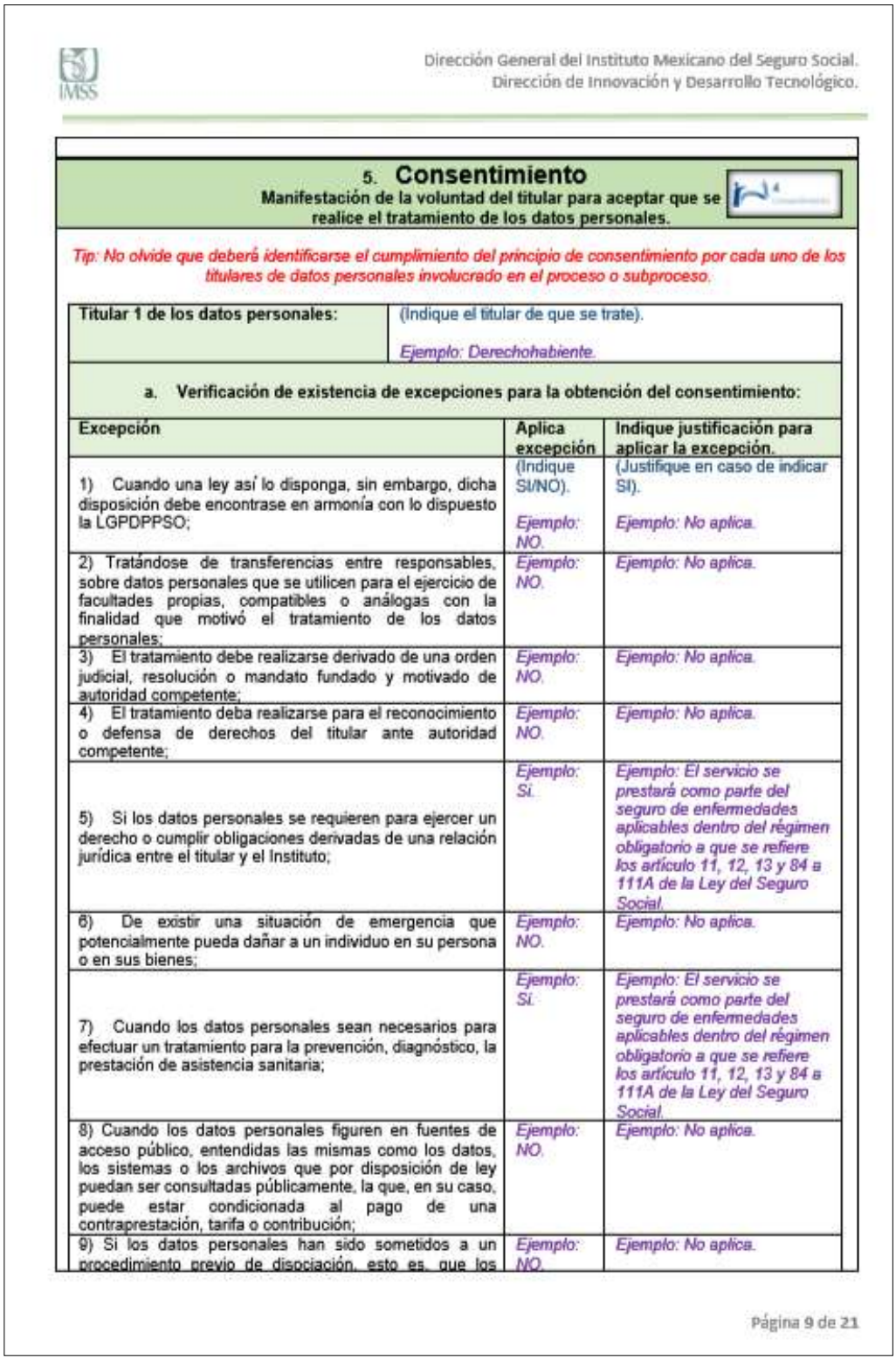
4. Lealtad

Medios para la obtención de los datos personales.	*(Indique los medios a través de los cuales se obtienen los datos personales).* *Tip: No olvide que se debe justificar que los medios no son fraudulentos ni engañosos.* *Ejemplo: En la aplicación contendrá una explicación de su funcionamiento, la cual será presentada al derechohabiente de manera previa a su registro. Asimismo, dicha información permanecerá disponible durante cualquier momento.*
Medios para el tratamiento de los datos personales.	*(Indique los medios a través de los cuales se tratan los datos personales).* *Tip: No olvide que se debe justificar que los medios no son fraudulentos ni engañosos.* *Ejemplo: En la aplicación contendrá una explicación de su funcionamiento, la cual será presentada al derechohabiente de manera previa a su registro. Asimismo, dicha información permanecerá disponible durante cualquier momento.*
Expectativa razonable de privacidad.	*(Indique las medidas que se adoptan para proteger la privacidad del titular).* *Ejemplo: La aplicación está basada en roles y permisos, por lo tanto, la información de un derechohabiente solamente podrá ser visualizada por el médico que le sea asignado, además de ello, dicha información solo podrá ser visualizada durante el tiempo de la consulta, cuando el paciente indica que el médico está en el domicilio y concluye cuando el mismo paciente concluye la visita desde la propia aplicación.*

Página 8 de 21

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 10. Formato 2 Ciclo de vida de los datos personales, página 9



5. Consentimiento

Manifestación de la voluntad del titular para aceptar que se realice el tratamiento de los datos personales.

Tip: No olvide que deberá identificarse el cumplimiento del principio de consentimiento por cada uno de los titulares de datos personales involucrado en el proceso o subproceso.

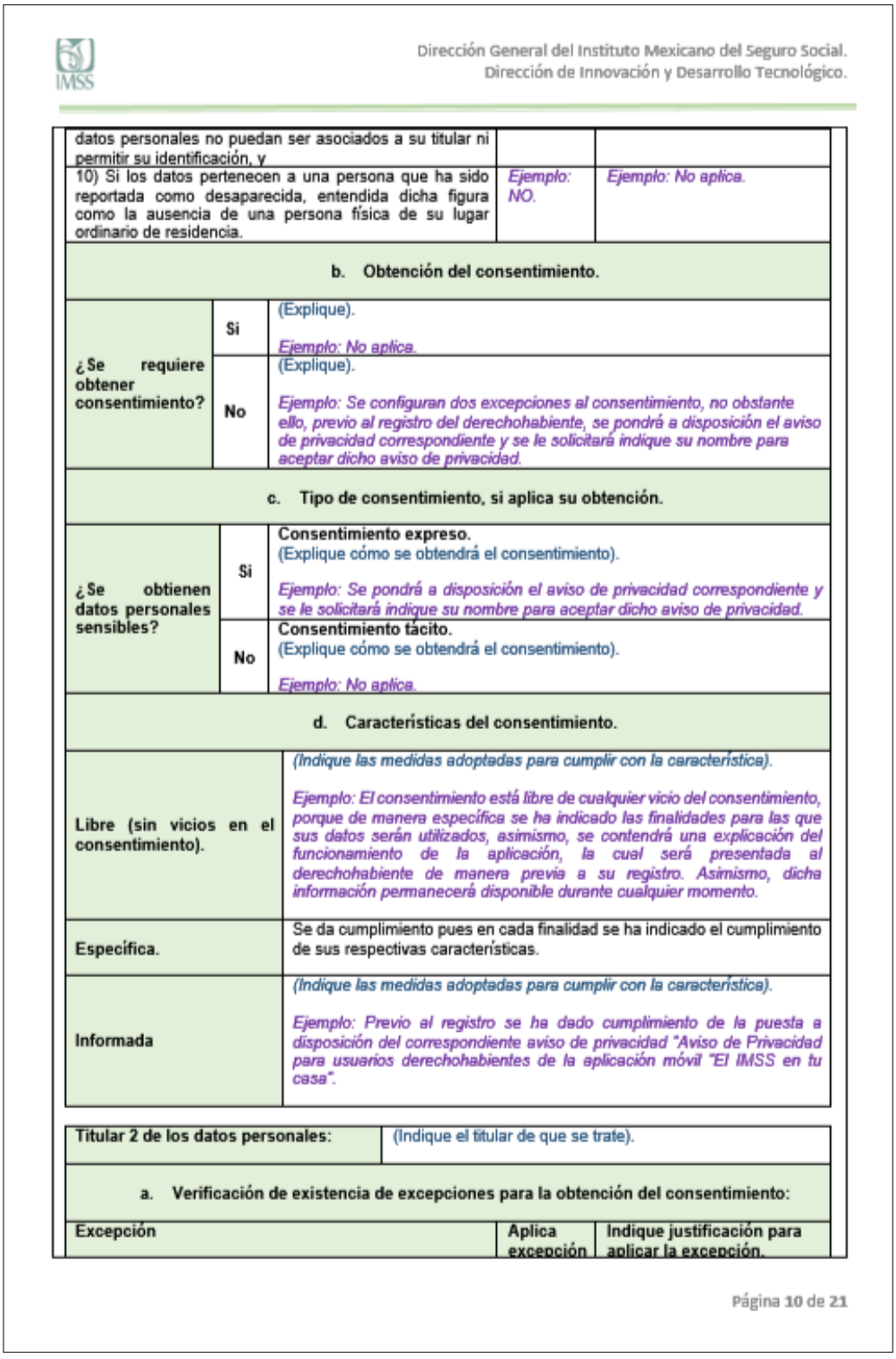
Titular 1 de los datos personales:	(Indique el titular de que se trate). *Ejemplo: Derechohabiente.*

a. Verificación de existencia de excepciones para la obtención del consentimiento:

Excepción	**Aplica excepción**	**Indique justificación para aplicar la excepción.**
1) Cuando una ley así lo disponga, sin embargo, dicha disposición debe encontrase en armonía con lo dispuesto la LGPDPPSO;	(Indique SI/NO). *Ejemplo: NO.*	(Justifique en caso de indicar SI). *Ejemplo: No aplica.*
2) Tratándose de transferencias entre responsables, sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;	*Ejemplo: NO.*	*Ejemplo: No aplica.*
3) El tratamiento debe realizarse derivado de una orden judicial, resolución o mandato fundado y motivado de autoridad competente;	*Ejemplo: NO.*	*Ejemplo: No aplica.*
4) El tratamiento deba realizarse para el reconocimiento o defensa de derechos del titular ante autoridad competente;	*Ejemplo: NO.*	*Ejemplo: No aplica.*
5) Si los datos personales se requieren para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el Instituto;	*Ejemplo: Si.*	*Ejemplo: El servicio se prestará como parte del seguro de enfermedades aplicables dentro del régimen obligatorio a que se refiere los artículo 11, 12, 13 y 84 a 111A de la Ley del Seguro Social.*
6) De existir una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;	*Ejemplo: NO.*	*Ejemplo: No aplica.*
7) Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;	*Ejemplo: Si.*	*Ejemplo: El servicio se prestará como parte del seguro de enfermedades aplicables dentro del régimen obligatorio a que se refiere los artículo 11, 12, 13 y 84 a 111A de la Ley del Seguro Social.*
8) Cuando los datos personales figuren en fuentes de acceso público, entendidas las mismas como los datos, los sistemas o los archivos que por disposición de ley puedan ser consultadas públicamente, la que, en su caso, puede estar condicionada al pago de una contraprestación, tarifa o contribución;	*Ejemplo: NO.*	*Ejemplo: No aplica.*
9) Si los datos personales han sido sometidos a un procedimiento previo de disociación, esto es, que los	*Ejemplo: NO.*	*Ejemplo: No aplica.*

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 11. Formato 2 Ciclo de vida de los datos personales, página 10



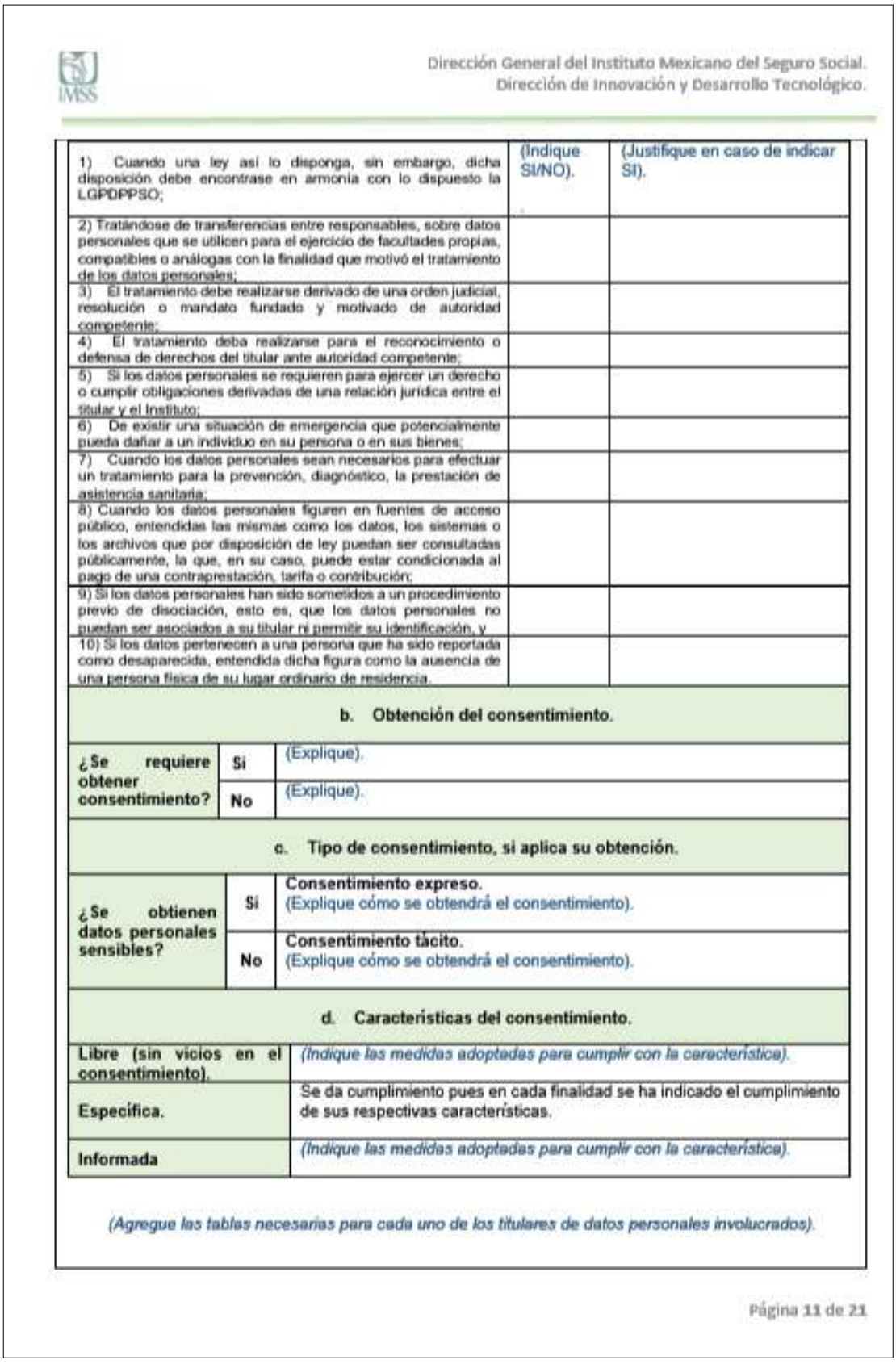
Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

datos personales no puedan ser asociados a su titular ni permitir su identificación, y			
10) Si los datos pertenecen a una persona que ha sido reportada como desaparecida, entendida dicha figura como la ausencia de una persona física de su lugar ordinario de residencia.		*Ejemplo: NO.*	*Ejemplo: No aplica.*
b. Obtención del consentimiento.			
¿Se requiere obtener consentimiento?	**Si**	(Explique). *Ejemplo: No aplica.*	
	No	(Explique). *Ejemplo: Se configuran dos excepciones al consentimiento, no obstante ello, previo al registro del derechohabiente, se pondrá a disposición el aviso de privacidad correspondiente y se le solicitará indique su nombre para aceptar dicho aviso de privacidad.*	
c. Tipo de consentimiento, si aplica su obtención.			
¿Se obtienen datos personales sensibles?	**Si**	**Consentimiento expreso.** (Explique cómo se obtendrá el consentimiento). *Ejemplo: Se pondrá a disposición el aviso de privacidad correspondiente y se le solicitará indique su nombre para aceptar dicho aviso de privacidad.*	
	No	**Consentimiento tácito.** (Explique cómo se obtendrá el consentimiento). *Ejemplo: No aplica.*	
d. Características del consentimiento.			
Libre (sin vicios en el consentimiento).		*(Indique las medidas adoptadas para cumplir con la característica).* *Ejemplo: El consentimiento está libre de cualquier vicio del consentimiento, porque de manera específica se ha indicado las finalidades para las que sus datos serán utilizados, asimismo, se contendrá una explicación del funcionamiento de la aplicación, la cual será presentada al derechohabiente de manera previa a su registro. Asimismo, dicha información permanecerá disponible durante cualquier momento.*	
Específica.		Se da cumplimiento pues en cada finalidad se ha indicado el cumplimiento de sus respectivas características.	
Informada		*(Indique las medidas adoptadas para cumplir con la característica).* *Ejemplo: Previo al registro se ha dado cumplimiento de la puesta a disposición del correspondiente aviso de privacidad "Aviso de Privacidad para usuarios derechohabientes de la aplicación móvil "El IMSS en tu casa".*	
Titular 2 de los datos personales:		(Indique el titular de que se trate).	
a. Verificación de existencia de excepciones para la obtención del consentimiento:			
Excepción		**Aplica excepción**	**Indique justificación para aplicar la excepción.**

Página 10 de 21

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 12 Formato 2 Ciclo de vida de los datos personales, página 11



1) Cuando una ley así lo disponga, sin embargo, dicha disposición debe encontrase en armonía con lo dispuesto la LGPDPPSO;	(Indique SI/NO).	(Justifique en caso de indicar SI).
2) Tratándose de transferencias entre responsables, sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;		
3) El tratamiento debe realizarse derivado de una orden judicial, resolución o mandato fundado y motivado de autoridad competente;		
4) El tratamiento deba realizarse para el reconocimiento o defensa de derechos del titular ante autoridad competente;		
5) Si los datos personales se requieren para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el Instituto;		
6) De existir una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;		
7) Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;		
8) Cuando los datos personales figuren en fuentes de acceso público, entendidas las mismas como los datos, los sistemas o los archivos que por disposición de ley puedan ser consultadas públicamente, la que, en su caso, puede estar condicionada al pago de una contraprestación, tarifa o contribución;		
9) Si los datos personales han sido sometidos a un procedimiento previo de disociación, esto es, que los datos personales no puedan ser asociados a su titular ni permitir su identificación, y		
10) Si los datos pertenecen a una persona que ha sido reportada como desaparecida, entendida dicha figura como la ausencia de una persona física de su lugar ordinario de residencia.		

b. Obtención del consentimiento.		
¿Se requiere obtener consentimiento?	**Si**	(Explique).
	No	(Explique).

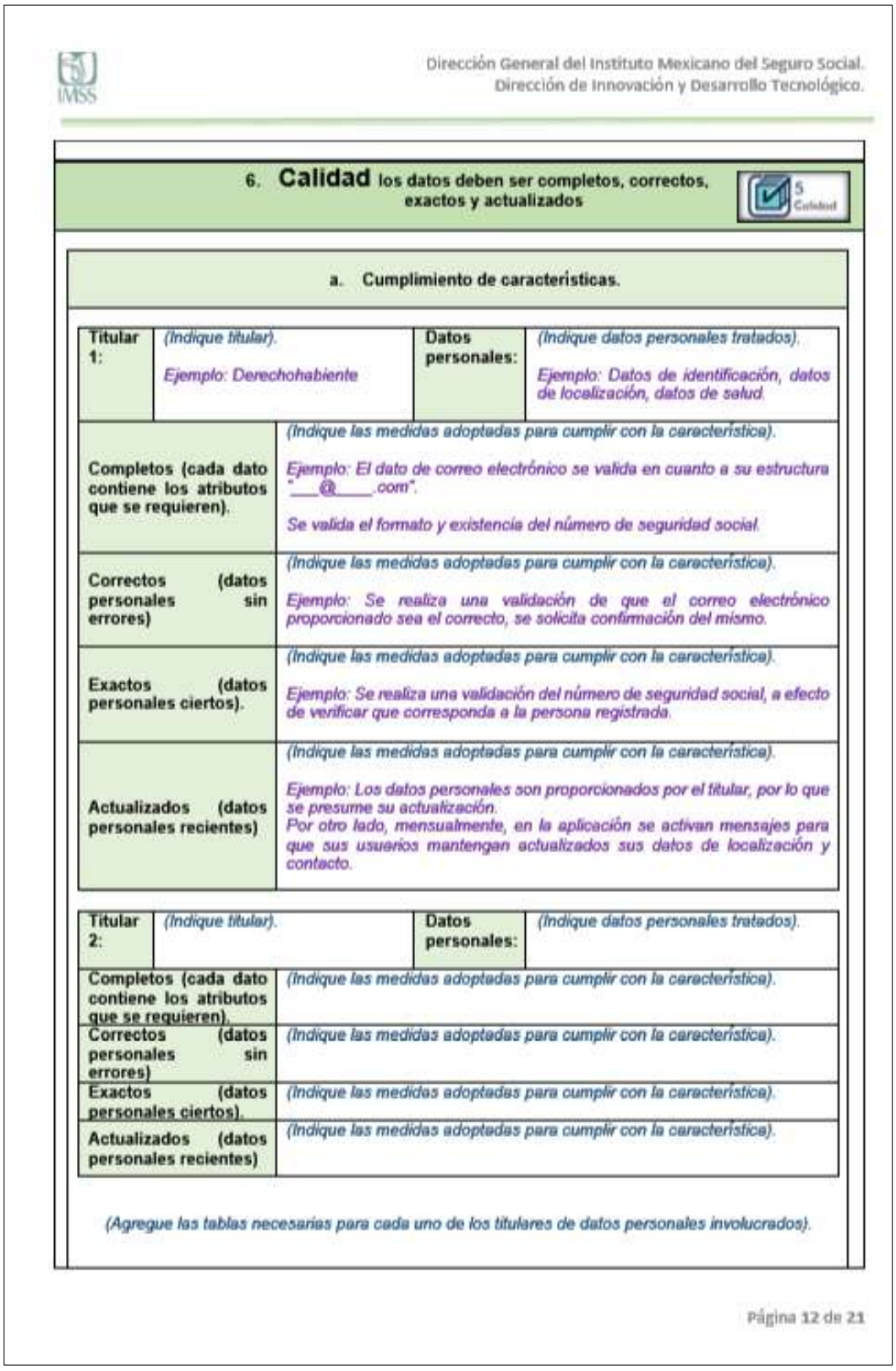
c. Tipo de consentimiento, si aplica su obtención.		
¿Se obtienen datos personales sensibles?	**Si**	**Consentimiento expreso.** (Explique cómo se obtendrá el consentimiento).
	No	**Consentimiento tácito.** (Explique cómo se obtendrá el consentimiento).

d. Características del consentimiento.	
Libre (sin vicios en el consentimiento).	*(Indique las medidas adoptadas para cumplir con la característica).*
Específica.	Se da cumplimiento pues en cada finalidad se ha indicado el cumplimiento de sus respectivas características.
Informada	*(Indique las medidas adoptadas para cumplir con la característica).*

(Agregue las tablas necesarias para cada uno de los titulares de datos personales involucrados).

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 13. Formato 2 Ciclo de vida de los datos personales, página 12



6. Calidad los datos deben ser completos, correctos, exactos y actualizados

a. Cumplimiento de características.

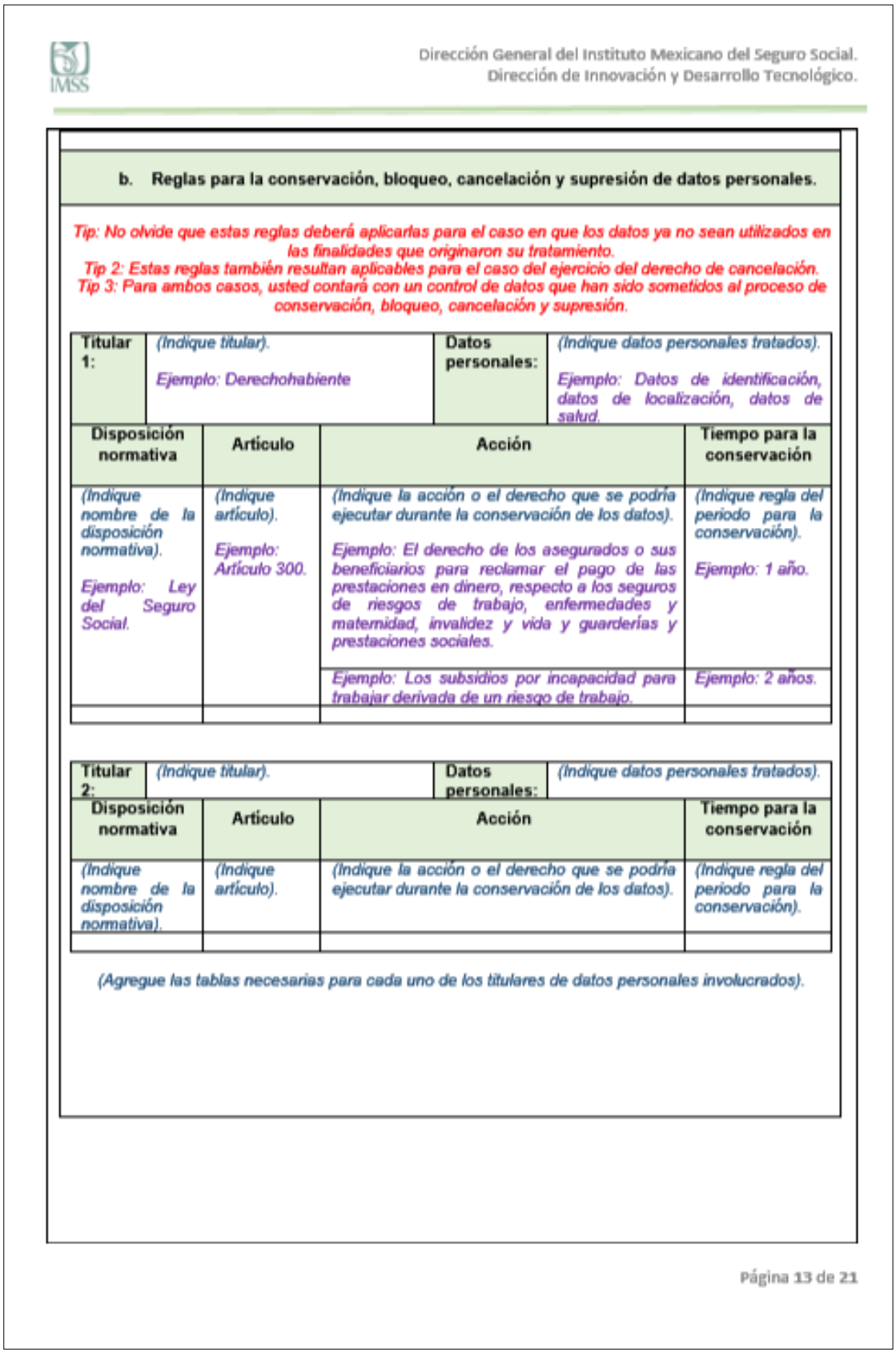
Titular 1:	*(Indique titular).* *Ejemplo: Derechohabiente*	**Datos personales:**	*(Indique datos personales tratados).* *Ejemplo: Datos de identificación, datos de localización, datos de salud.*
Completos (cada dato contiene los atributos que se requieren).	*(Indique las medidas adoptadas para cumplir con la característica).* *Ejemplo: El dato de correo electrónico se valida en cuanto a su estructura "___@____.com".* *Se valida el formato y existencia del número de seguridad social.*		
Correctos (datos personales sin errores)	*(Indique las medidas adoptadas para cumplir con la característica).* *Ejemplo: Se realiza una validación de que el correo electrónico proporcionado sea el correcto, se solicita confirmación del mismo.*		
Exactos (datos personales ciertos).	*(Indique las medidas adoptadas para cumplir con la característica).* *Ejemplo: Se realiza una validación del número de seguridad social, a efecto de verificar que corresponda a la persona registrada.*		
Actualizados (datos personales recientes)	*(Indique las medidas adoptadas para cumplir con la característica).* *Ejemplo: Los datos personales son proporcionados por el titular, por lo que se presume su actualización.* *Por otro lado, mensualmente, en la aplicación se activan mensajes para que sus usuarios mantengan actualizados sus datos de localización y contacto.*		

Titular 2:	*(Indique titular).*	**Datos personales:**	*(Indique datos personales tratados).*
Completos (cada dato contiene los atributos que se requieren).	*(Indique las medidas adoptadas para cumplir con la característica).*		
Correctos (datos personales sin errores)	*(Indique las medidas adoptadas para cumplir con la característica).*		
Exactos (datos personales ciertos).	*(Indique las medidas adoptadas para cumplir con la característica).*		
Actualizados (datos personales recientes)	*(Indique las medidas adoptadas para cumplir con la característica).*		

(Agregue las tablas necesarias para cada uno de los titulares de datos personales involucrados).

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 14. Formato 2 Ciclo de vida de los datos personales, página 13



b. Reglas para la conservación, bloqueo, cancelación y supresión de datos personales.

Tip: No olvide que estas reglas deberá aplicarlas para el caso en que los datos ya no sean utilizados en las finalidades que originaron su tratamiento.
Tip 2: Estas reglas también resultan aplicables para el caso del ejercicio del derecho de cancelación.
Tip 3: Para ambos casos, usted contará con un control de datos que han sido sometidos al proceso de conservación, bloqueo, cancelación y supresión.

Titular 1:	*(Indique titular).* *Ejemplo: Derechohabiente*	**Datos personales:**	*(Indique datos personales tratados).* *Ejemplo: Datos de identificación, datos de localización, datos de salud.*

Disposición normativa	Artículo	Acción	Tiempo para la conservación
(Indique nombre de la disposición normativa). *Ejemplo: Ley del Seguro Social.*	*(Indique artículo).* *Ejemplo: Artículo 300.*	*(Indique la acción o el derecho que se podría ejecutar durante la conservación de los datos).* *Ejemplo: El derecho de los asegurados o sus beneficiarios para reclamar el pago de las prestaciones en dinero, respecto a los seguros de riesgos de trabajo, enfermedades y maternidad, invalidez y vida y guarderías y prestaciones sociales.*	*(Indique regla del periodo para la conservación).* *Ejemplo: 1 año.*
		Ejemplo: Los subsidios por incapacidad para trabajar derivada de un riesgo de trabajo.	*Ejemplo: 2 años.*

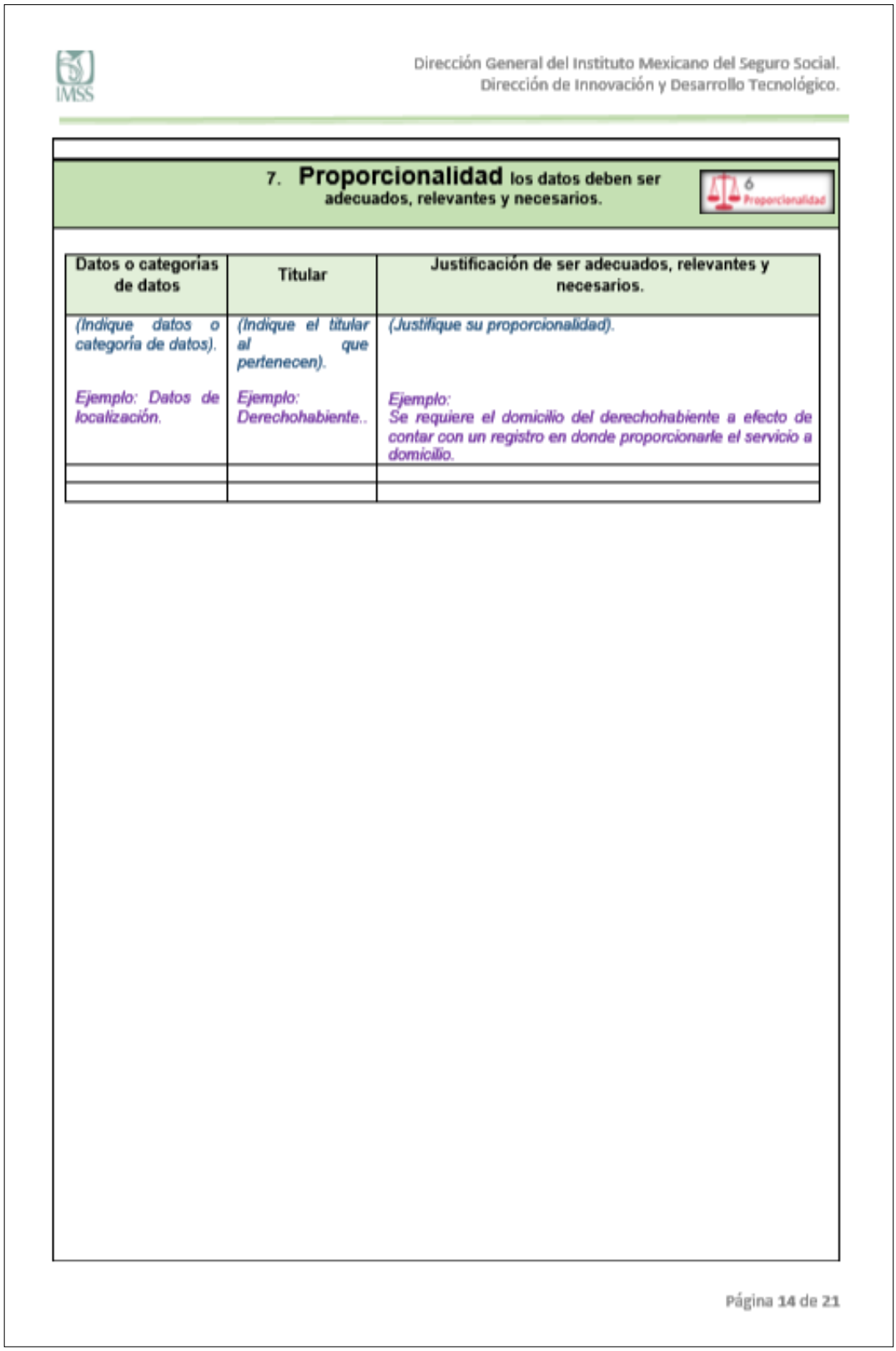
Titular 2:	*(Indique titular).*	**Datos personales:**	*(Indique datos personales tratados).*

Disposición normativa	Artículo	Acción	Tiempo para la conservación
(Indique nombre de la disposición normativa).	*(Indique artículo).*	*(Indique la acción o el derecho que se podría ejecutar durante la conservación de los datos).*	*(Indique regla del periodo para la conservación).*

(Agregue las tablas necesarias para cada uno de los titulares de datos personales involucrados).

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 15. Formato 2 Ciclo de vida de los datos personales, página 14



Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

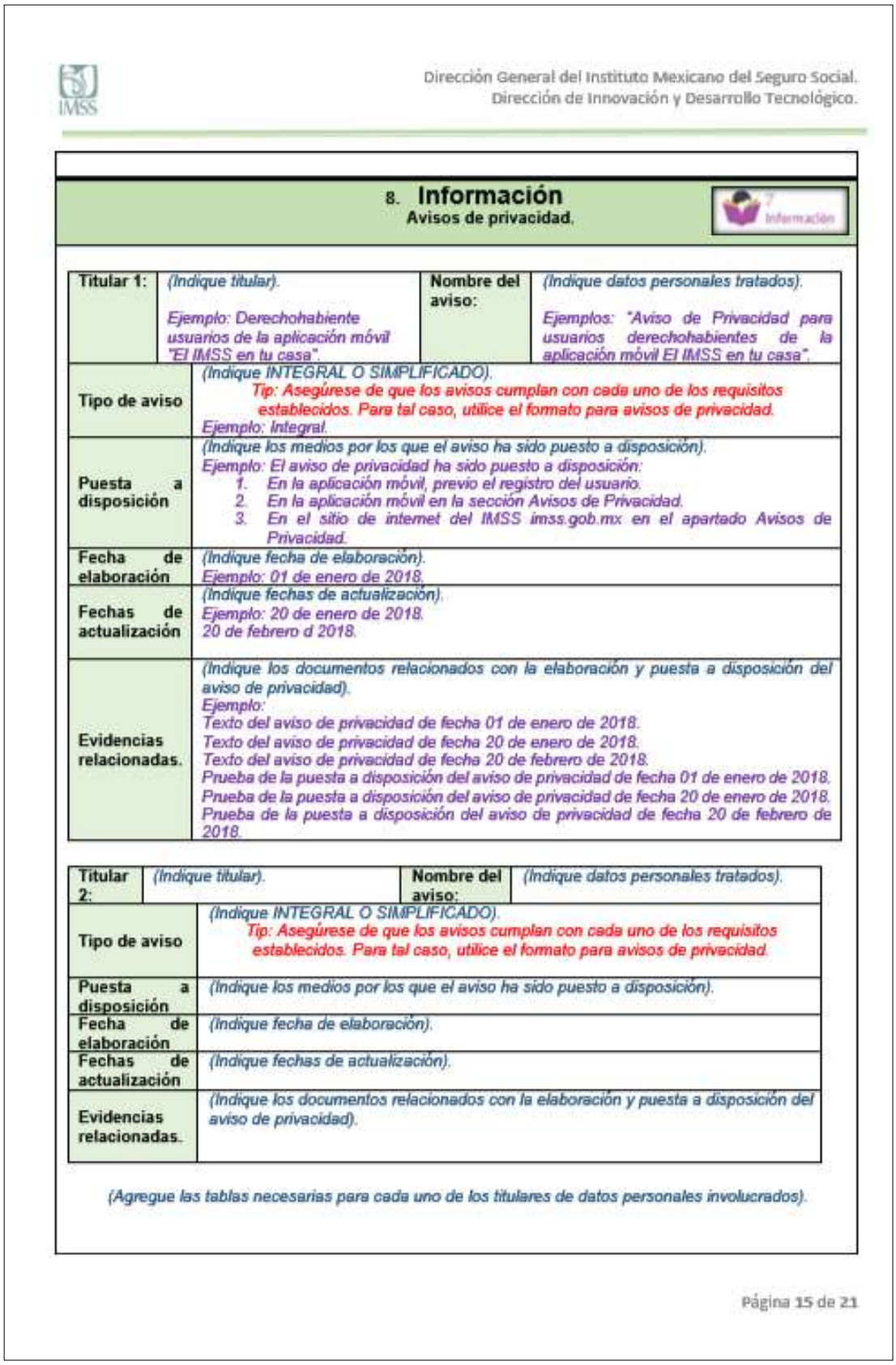
7. **Proporcionalidad** los datos deben ser adecuados, relevantes y necesarios.

Datos o categorías de datos	Titular	Justificación de ser adecuados, relevantes y necesarios.
(Indique datos o categoría de datos). *Ejemplo: Datos de localización.*	*(Indique el titular al que pertenecen).* *Ejemplo: Derechohabiente..*	*(Justifique su proporcionalidad).* *Ejemplo: Se requiere el domicilio del derechohabiente a efecto de contar con un registro en donde proporcionarle el servicio a domicilio.*

Página 14 de 21

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI

Documento 16. Formato 2 Ciclo de vida de los datos personales, página 15



Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

8. Información
Avisos de privacidad.

Titular 1:	*(Indique titular).* *Ejemplo: Derechohabiente usuarios de la aplicación móvil "El IMSS en tu casa".*	**Nombre del aviso:**	*(Indique datos personales tratados).* *Ejemplos: "Aviso de Privacidad para usuarios derechohabientes de la aplicación móvil El IMSS en tu casa".*
Tipo de aviso	*(Indique INTEGRAL O SIMPLIFICADO).* *Tip: Asegúrese de que los avisos cumplan con cada uno de los requisitos establecidos. Para tal caso, utilice el formato para avisos de privacidad.* *Ejemplo: Integral.*		
Puesta a disposición	*(Indique los medios por los que el aviso ha sido puesto a disposición).* *Ejemplo: El aviso de privacidad ha sido puesto a disposición:* *1. En la aplicación móvil, previo el registro del usuario.* *2. En la aplicación móvil en la sección Avisos de Privacidad.* *3. En el sitio de internet del IMSS imss.gob.mx en el apartado Avisos de Privacidad.*		
Fecha de elaboración	*(Indique fecha de elaboración).* *Ejemplo: 01 de enero de 2018.*		
Fechas de actualización	*(Indique fechas de actualización).* *Ejemplo: 20 de enero de 2018.* *20 de febrero d 2018.*		
Evidencias relacionadas.	*(Indique los documentos relacionados con la elaboración y puesta a disposición del aviso de privacidad).* *Ejemplo:* *Texto del aviso de privacidad de fecha 01 de enero de 2018.* *Texto del aviso de privacidad de fecha 20 de enero de 2018.* *Texto del aviso de privacidad de fecha 20 de febrero de 2018.* *Prueba de la puesta a disposición del aviso de privacidad de fecha 01 de enero de 2018.* *Prueba de la puesta a disposición del aviso de privacidad de fecha 20 de enero de 2018.* *Prueba de la puesta a disposición del aviso de privacidad de fecha 20 de febrero de 2018.*		

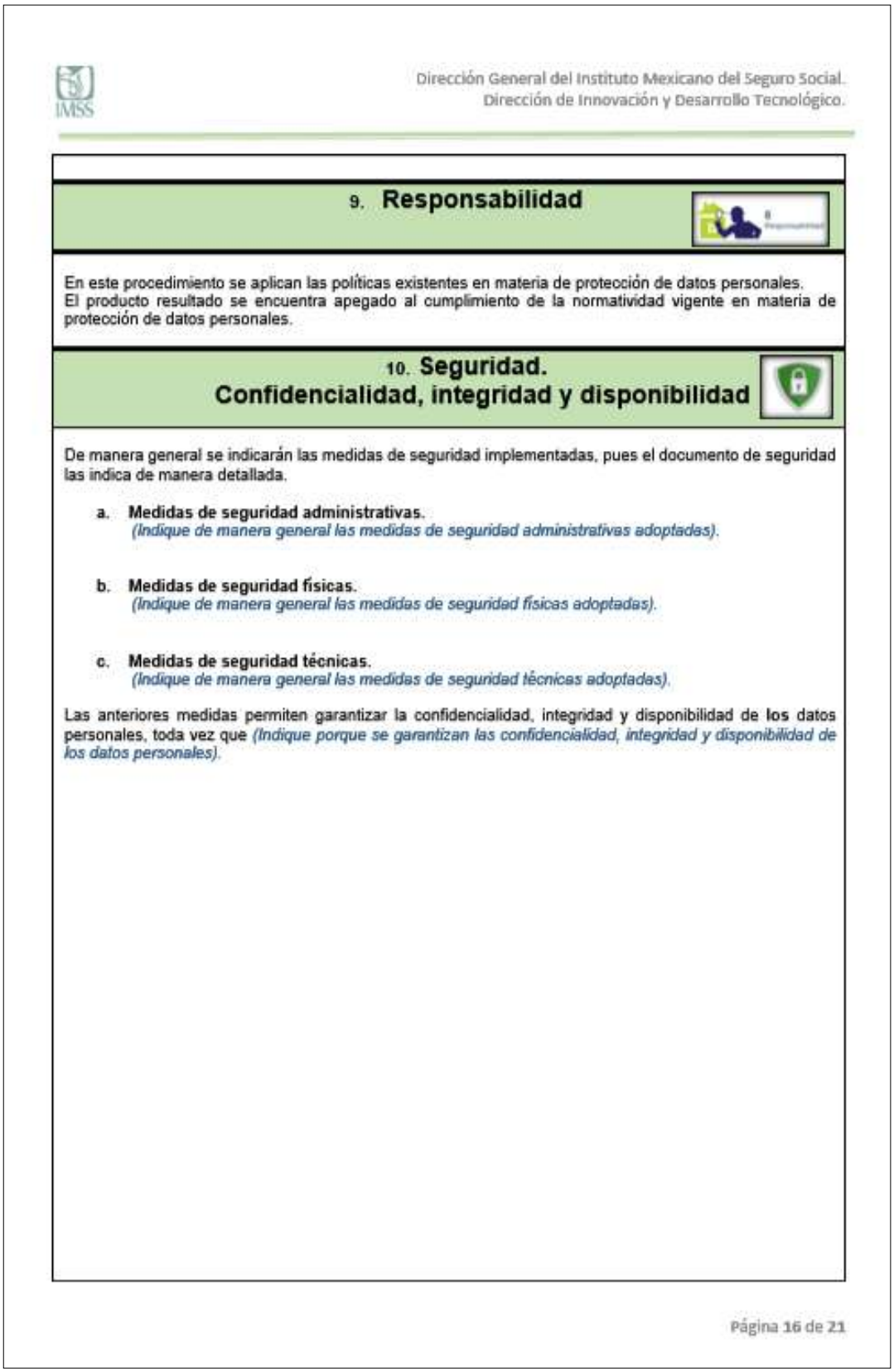
Titular 2:	*(Indique titular).*	**Nombre del aviso:**	*(Indique datos personales tratados).*
Tipo de aviso	*(Indique INTEGRAL O SIMPLIFICADO).* *Tip: Asegúrese de que los avisos cumplan con cada uno de los requisitos establecidos. Para tal caso, utilice el formato para avisos de privacidad.*		
Puesta a disposición	*(Indique los medios por los que el aviso ha sido puesto a disposición).*		
Fecha de elaboración	*(Indique fecha de elaboración).*		
Fechas de actualización	*(Indique fechas de actualización).*		
Evidencias relacionadas.	*(Indique los documentos relacionados con la elaboración y puesta a disposición del aviso de privacidad).*		

(Agregue las tablas necesarias para cada uno de los titulares de datos personales involucrados).

Página 15 de 21

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 17. Formato 2 Ciclo de vida de los datos personales, página 16



9. Responsabilidad

En este procedimiento se aplican las políticas existentes en materia de protección de datos personales.
El producto resultado se encuentra apegado al cumplimiento de la normatividad vigente en materia de protección de datos personales.

10. Seguridad.
Confidencialidad, integridad y disponibilidad

De manera general se indicarán las medidas de seguridad implementadas, pues el documento de seguridad las indica de manera detallada.

a. **Medidas de seguridad administrativas.**
(Indique de manera general las medidas de seguridad administrativas adoptadas).

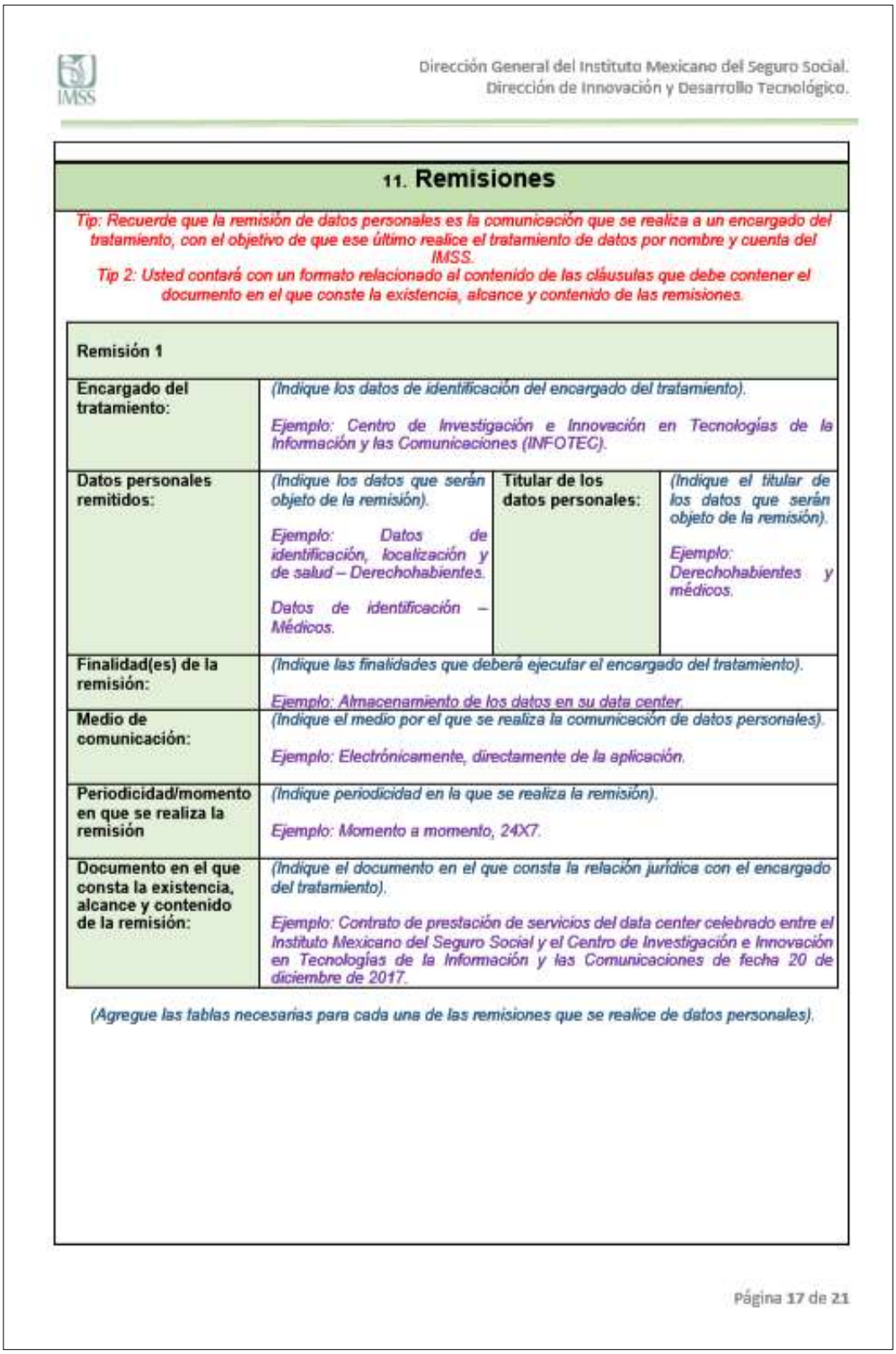
b. **Medidas de seguridad físicas.**
(Indique de manera general las medidas de seguridad físicas adoptadas).

c. **Medidas de seguridad técnicas.**
(Indique de manera general las medidas de seguridad técnicas adoptadas).

Las anteriores medidas permiten garantizar la confidencialidad, integridad y disponibilidad de los datos personales, toda vez que *(Indique porque se garantizan las confidencialidad, integridad y disponibilidad de los datos personales).*

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 18. Formato 2 Ciclo de vida de los datos personales, página 17



11. Remisiones

Tip: Recuerde que la remisión de datos personales es la comunicación que se realiza a un encargado del tratamiento, con el objetivo de que ese último realice el tratamiento de datos por nombre y cuenta del IMSS.

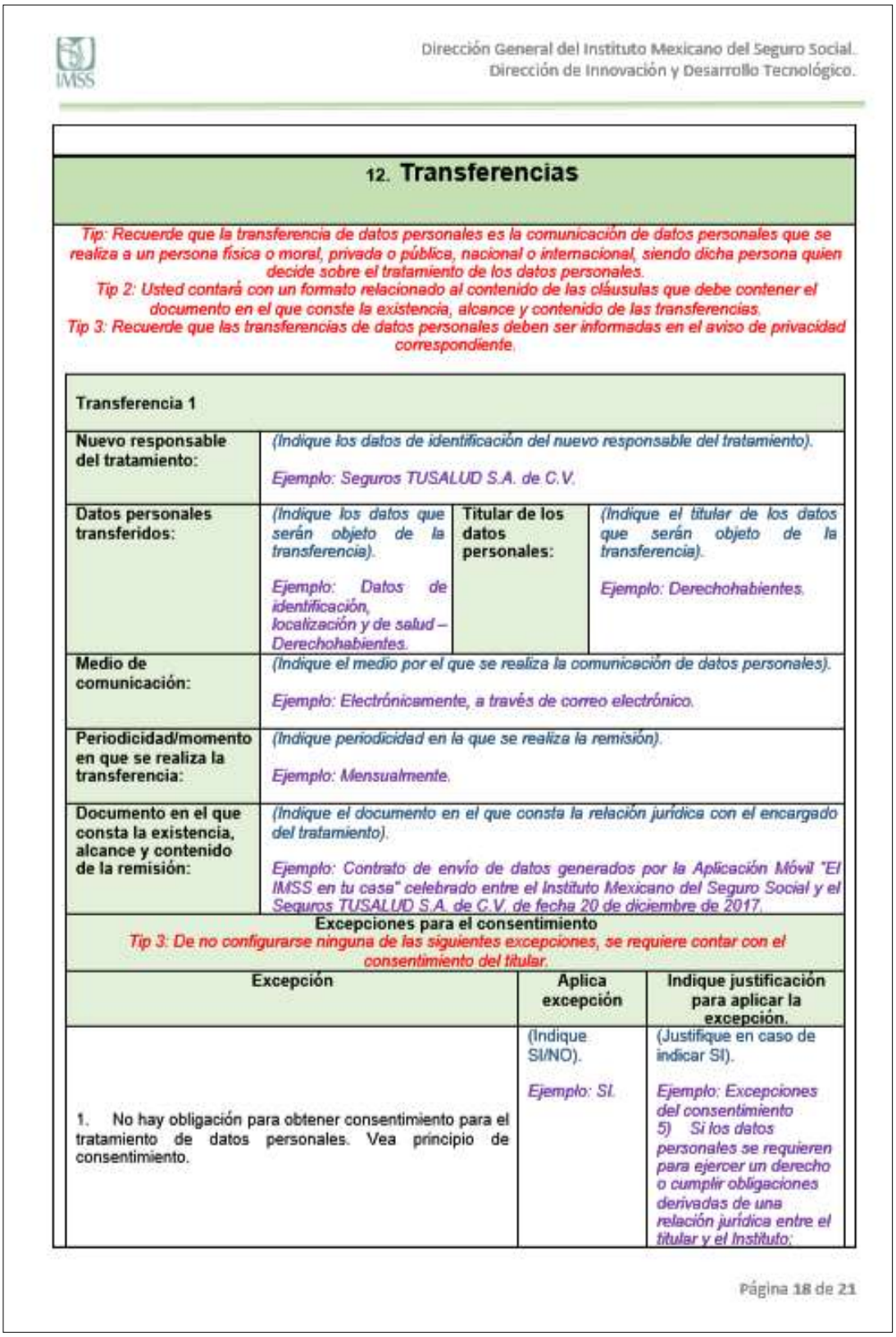
Tip 2: Usted contará con un formato relacionado al contenido de las cláusulas que debe contener el documento en el que conste la existencia, alcance y contenido de las remisiones.

Remisión 1			
Encargado del tratamiento:	*(Indique los datos de identificación del encargado del tratamiento).* *Ejemplo: Centro de Investigación e Innovación en Tecnologías de la Información y las Comunicaciones (INFOTEC).*		
Datos personales remitidos:	*(Indique los datos que serán objeto de la remisión).* *Ejemplo: Datos de identificación, localización y de salud – Derechohabientes.* *Datos de identificación – Médicos.*	**Titular de los datos personales:**	*(Indique el titular de los datos que serán objeto de la remisión).* *Ejemplo: Derechohabientes y médicos.*
Finalidad(es) de la remisión:	*(Indique las finalidades que deberá ejecutar el encargado del tratamiento).* *Ejemplo: Almacenamiento de los datos en su data center.*		
Medio de comunicación:	*(Indique el medio por el que se realiza la comunicación de datos personales).* *Ejemplo: Electrónicamente, directamente de la aplicación.*		
Periodicidad/momento en que se realiza la remisión	*(Indique periodicidad en la que se realiza la remisión).* *Ejemplo: Momento a momento, 24X7.*		
Documento en el que consta la existencia, alcance y contenido de la remisión:	*(Indique el documento en el que consta la relación jurídica con el encargado del tratamiento).* *Ejemplo: Contrato de prestación de servicios del data center celebrado entre el Instituto Mexicano del Seguro Social y el Centro de Investigación e Innovación en Tecnologías de la Información y las Comunicaciones de fecha 20 de diciembre de 2017.*		

(Agregue las tablas necesarias para cada una de las remisiones que se realice de datos personales).

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 19. Formato 2 Ciclo de vida de los datos personales, página 18



12. Transferencias

Tip: Recuerde que la transferencia de datos personales es la comunicación de datos personales que se realiza a un persona física o moral, privada o pública, nacional o internacional, siendo dicha persona quien decide sobre el tratamiento de los datos personales.
Tip 2: Usted contará con un formato relacionado al contenido de las cláusulas que debe contener el documento en el que conste la existencia, alcance y contenido de las transferencias.
Tip 3: Recuerde que las transferencias de datos personales deben ser informadas en el aviso de privacidad correspondiente.

Transferencia 1			
Nuevo responsable del tratamiento:	*(Indique los datos de identificación del nuevo responsable del tratamiento).* *Ejemplo: Seguros TUSALUD S.A. de C.V.*		
Datos personales transferidos:	*(Indique los datos que serán objeto de la transferencia).* *Ejemplo: Datos de identificación, localización y de salud – Derechohabientes.*	**Titular de los datos personales:**	*(Indique el titular de los datos que serán objeto de la transferencia).* *Ejemplo: Derechohabientes.*
Medio de comunicación:	*(Indique el medio por el que se realiza la comunicación de datos personales).* *Ejemplo: Electrónicamente, a través de correo electrónico.*		
Periodicidad/momento en que se realiza la transferencia:	*(Indique periodicidad en la que se realiza la remisión).* *Ejemplo: Mensualmente.*		
Documento en el que consta la existencia, alcance y contenido de la remisión:	*(Indique el documento en el que consta la relación jurídica con el encargado del tratamiento).* *Ejemplo: Contrato de envío de datos generados por la Aplicación Móvil "El IMSS en tu casa" celebrado entre el Instituto Mexicano del Seguro Social y el Seguros TUSALUD S.A. de C.V. de fecha 20 de diciembre de 2017.*		

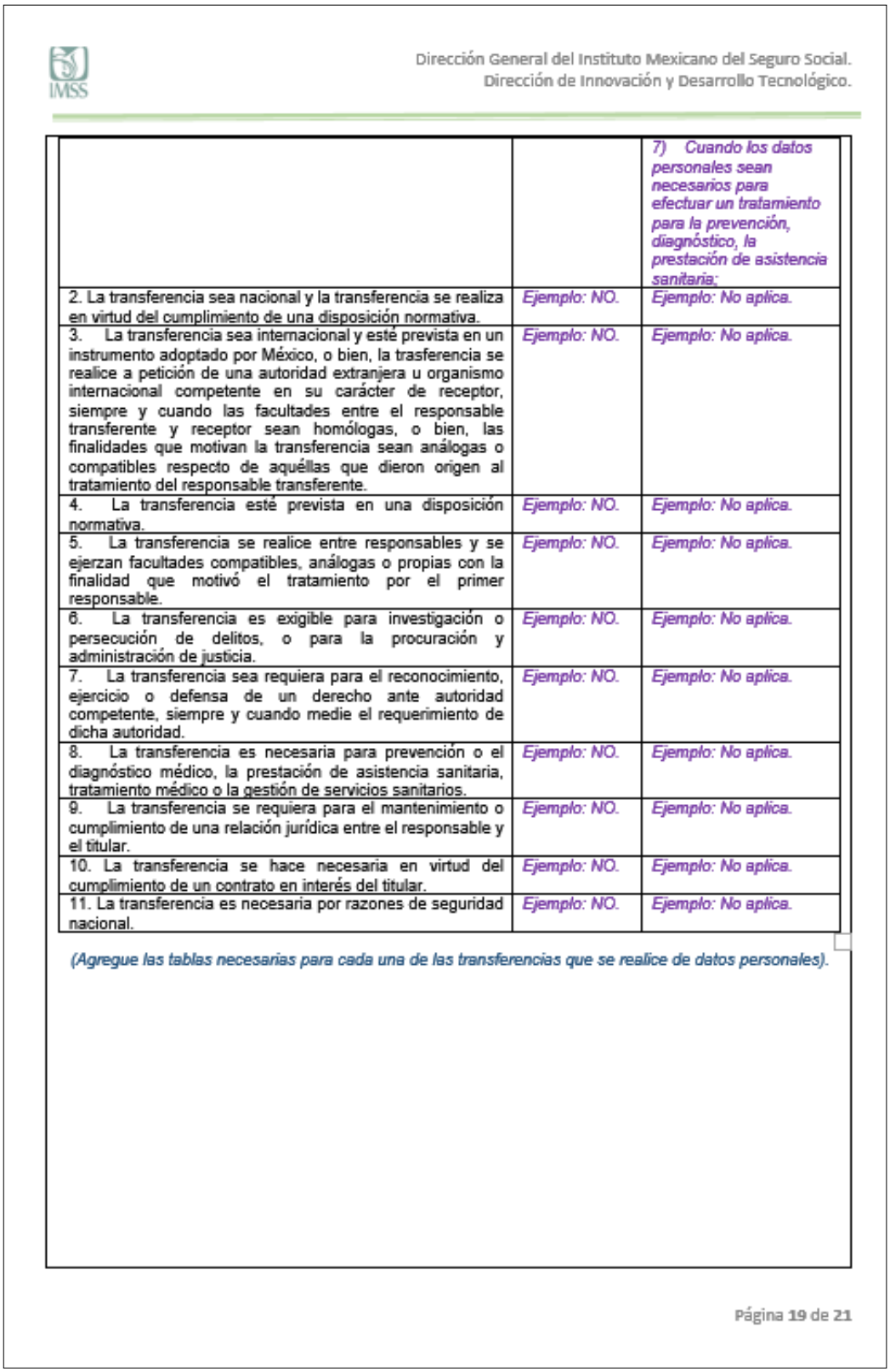
Excepciones para el consentimiento

Tip 3: De no configurarse ninguna de las siguientes excepciones, se requiere contar con el consentimiento del titular.

Excepción	**Aplica excepción**	**Indique justificación para aplicar la excepción.**
1. No hay obligación para obtener consentimiento para el tratamiento de datos personales. Vea principio de consentimiento.	(Indique SI/NO). *Ejemplo: SI.*	(Justifique en caso de indicar SI). *Ejemplo: Excepciones del consentimiento 5) Si los datos personales se requieren para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el Instituto;*

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 20. Formato 2 Ciclo de vida de los datos personales, página 19

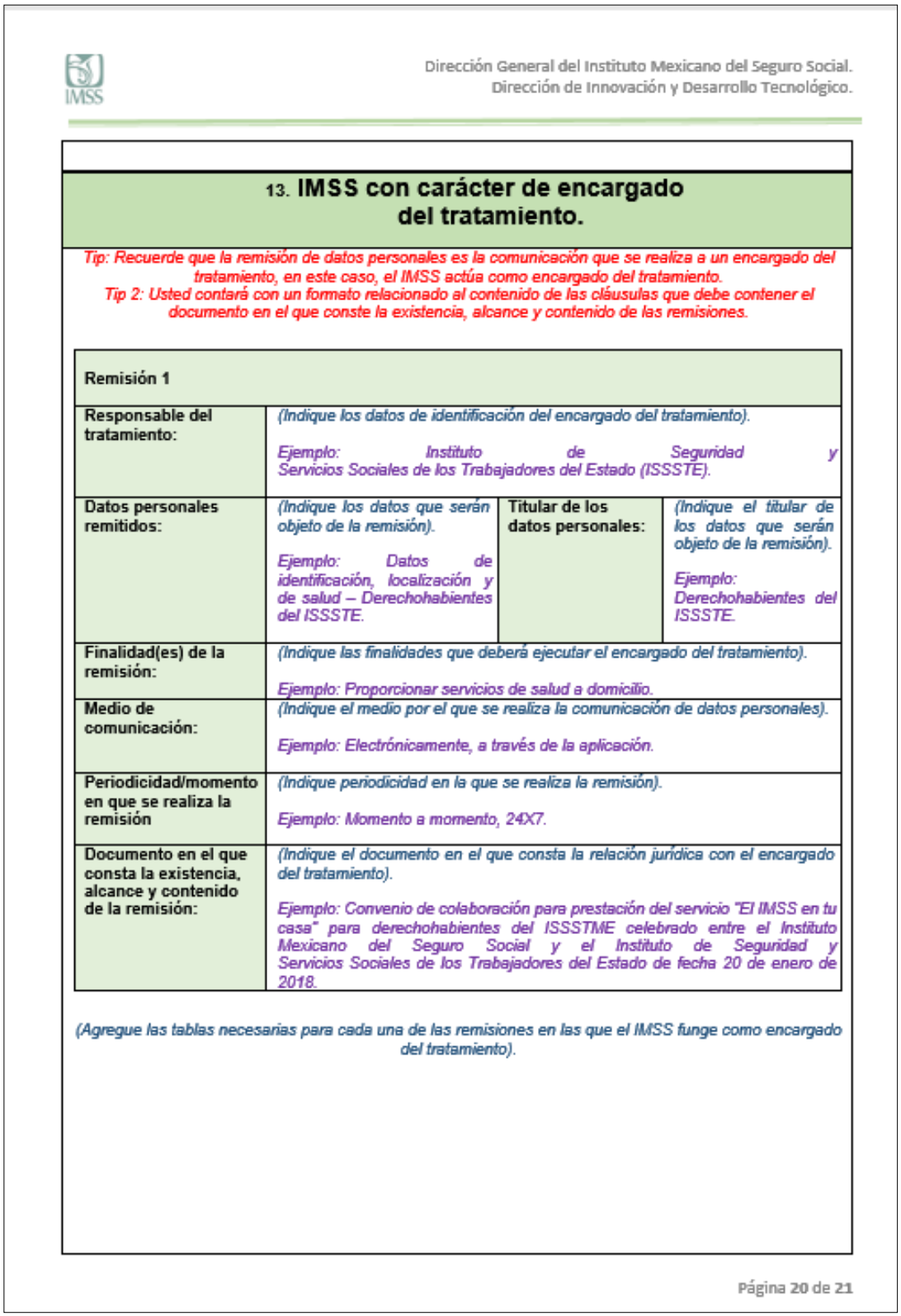


		7) Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
2. La transferencia sea nacional y la transferencia se realiza en virtud del cumplimiento de una disposición normativa.	*Ejemplo: NO.*	*Ejemplo: No aplica.*
3. La transferencia sea internacional y esté prevista en un instrumento adoptado por México, o bien, la trasferencia se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.	*Ejemplo: NO.*	*Ejemplo: No aplica.*
4. La transferencia esté prevista en una disposición normativa.	*Ejemplo: NO.*	*Ejemplo: No aplica.*
5. La transferencia se realice entre responsables y se ejerzan facultades compatibles, análogas o propias con la finalidad que motivó el tratamiento por el primer responsable.	*Ejemplo: NO.*	*Ejemplo: No aplica.*
6. La transferencia es exigible para investigación o persecución de delitos, o para la procuración y administración de justicia.	*Ejemplo: NO.*	*Ejemplo: No aplica.*
7. La transferencia sea requiera para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de dicha autoridad.	*Ejemplo: NO.*	*Ejemplo: No aplica.*
8. La transferencia es necesaria para prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.	*Ejemplo: NO.*	*Ejemplo: No aplica.*
9. La transferencia se requiera para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.	*Ejemplo: NO.*	*Ejemplo: No aplica.*
10. La transferencia se hace necesaria en virtud del cumplimiento de un contrato en interés del titular.	*Ejemplo: NO.*	*Ejemplo: No aplica.*
11. La transferencia es necesaria por razones de seguridad nacional.	*Ejemplo: NO.*	*Ejemplo: No aplica.*

(Agregue las tablas necesarias para cada una de las transferencias que se realice de datos personales).

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 21. Formato 2 Ciclo de vida de los datos personales, página 20



13. IMSS con carácter de encargado del tratamiento.

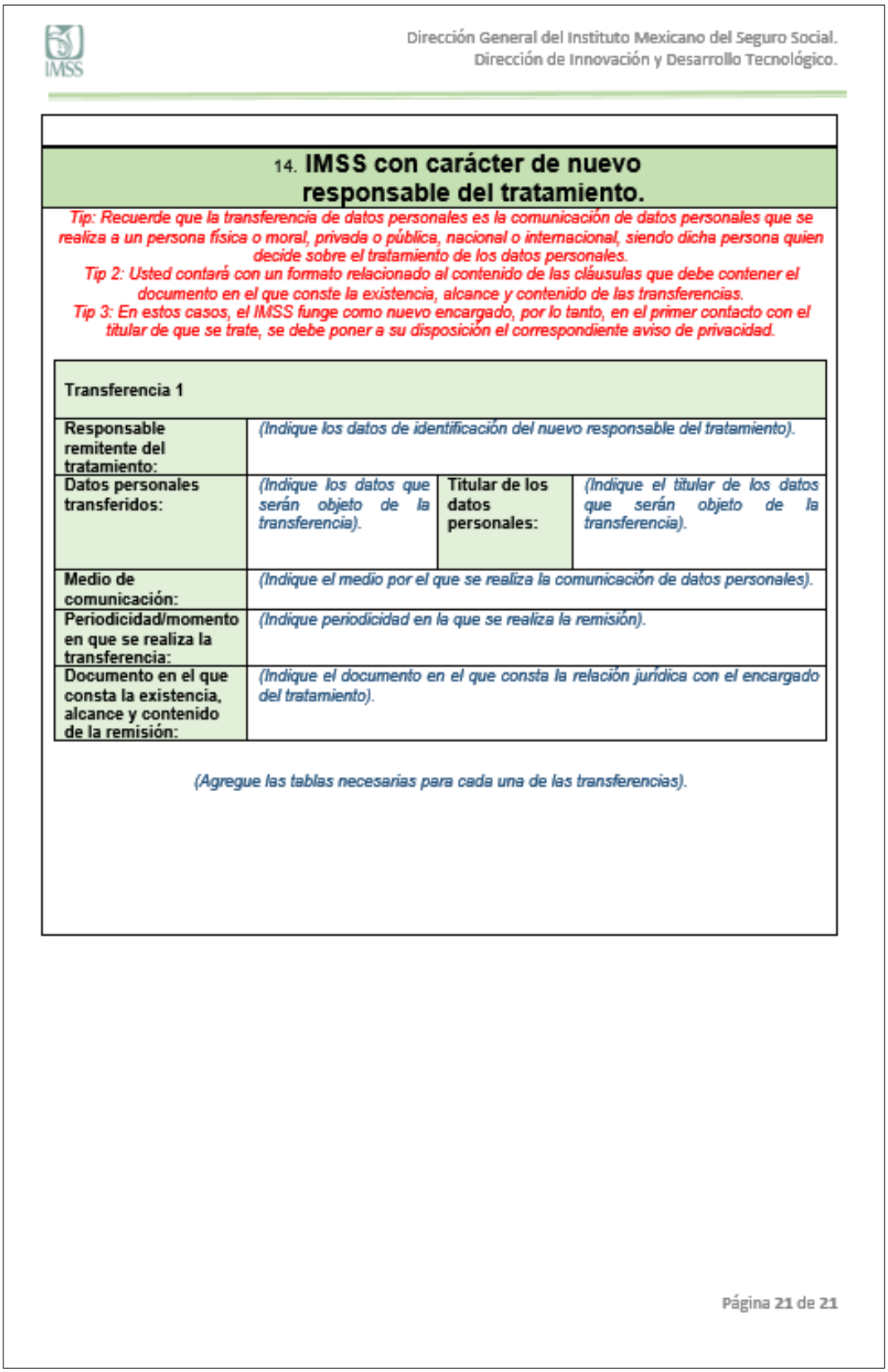
Tip: Recuerde que la remisión de datos personales es la comunicación que se realiza a un encargado del tratamiento, en este caso, el IMSS actúa como encargado del tratamiento.
Tip 2: Usted contará con un formato relacionado al contenido de las cláusulas que debe contener el documento en el que conste la existencia, alcance y contenido de las remisiones.

Remisión 1			
Responsable del tratamiento:	*(Indique los datos de identificación del encargado del tratamiento).* *Ejemplo: Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE).*		
Datos personales remitidos:	*(Indique los datos que serán objeto de la remisión).* *Ejemplo: Datos de identificación, localización y de salud – Derechohabientes del ISSSTE.*	**Titular de los datos personales:**	*(Indique el titular de los datos que serán objeto de la remisión).* *Ejemplo: Derechohabientes del ISSSTE.*
Finalidad(es) de la remisión:	*(Indique las finalidades que deberá ejecutar el encargado del tratamiento).* *Ejemplo: Proporcionar servicios de salud a domicilio.*		
Medio de comunicación:	*(Indique el medio por el que se realiza la comunicación de datos personales).* *Ejemplo: Electrónicamente, a través de la aplicación.*		
Periodicidad/momento en que se realiza la remisión	*(Indique periodicidad en la que se realiza la remisión).* *Ejemplo: Momento a momento, 24X7.*		
Documento en el que consta la existencia, alcance y contenido de la remisión:	*(Indique el documento en el que consta la relación jurídica con el encargado del tratamiento).* *Ejemplo: Convenio de colaboración para prestación del servicio "El IMSS en tu casa" para derechohabientes del ISSSTME celebrado entre el Instituto Mexicano del Seguro Social y el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado de fecha 20 de enero de 2018.*		

(Agregue las tablas necesarias para cada una de las remisiones en las que el IMSS funge como encargado del tratamiento).

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 22. Formato 2 Ciclo de vida de los datos personales, página 21



14. IMSS con carácter de nuevo responsable del tratamiento.

Tip: Recuerde que la transferencia de datos personales es la comunicación de datos personales que se realiza a un persona física o moral, privada o pública, nacional o internacional, siendo dicha persona quien decide sobre el tratamiento de los datos personales.
Tip 2: Usted contará con un formato relacionado al contenido de las cláusulas que debe contener el documento en el que conste la existencia, alcance y contenido de las transferencias.
Tip 3: En estos casos, el IMSS funge como nuevo encargado, por lo tanto, en el primer contacto con el titular de que se trate, se debe poner a su disposición el correspondiente aviso de privacidad.

Transferencia 1			
Responsable remitente del tratamiento:	*(Indique los datos de identificación del nuevo responsable del tratamiento).*		
Datos personales transferidos:	*(Indique los datos que serán objeto de la transferencia).*	**Titular de los datos personales:**	*(Indique el titular de los datos que serán objeto de la transferencia).*
Medio de comunicación:	*(Indique el medio por el que se realiza la comunicación de datos personales).*		
Periodicidad/momento en que se realiza la transferencia:	*(Indique periodicidad en la que se realiza la remisión).*		
Documento en el que consta la existencia, alcance y contenido de la remisión:	*(Indique el documento en el que consta la relación jurídica con el encargado del tratamiento).*		

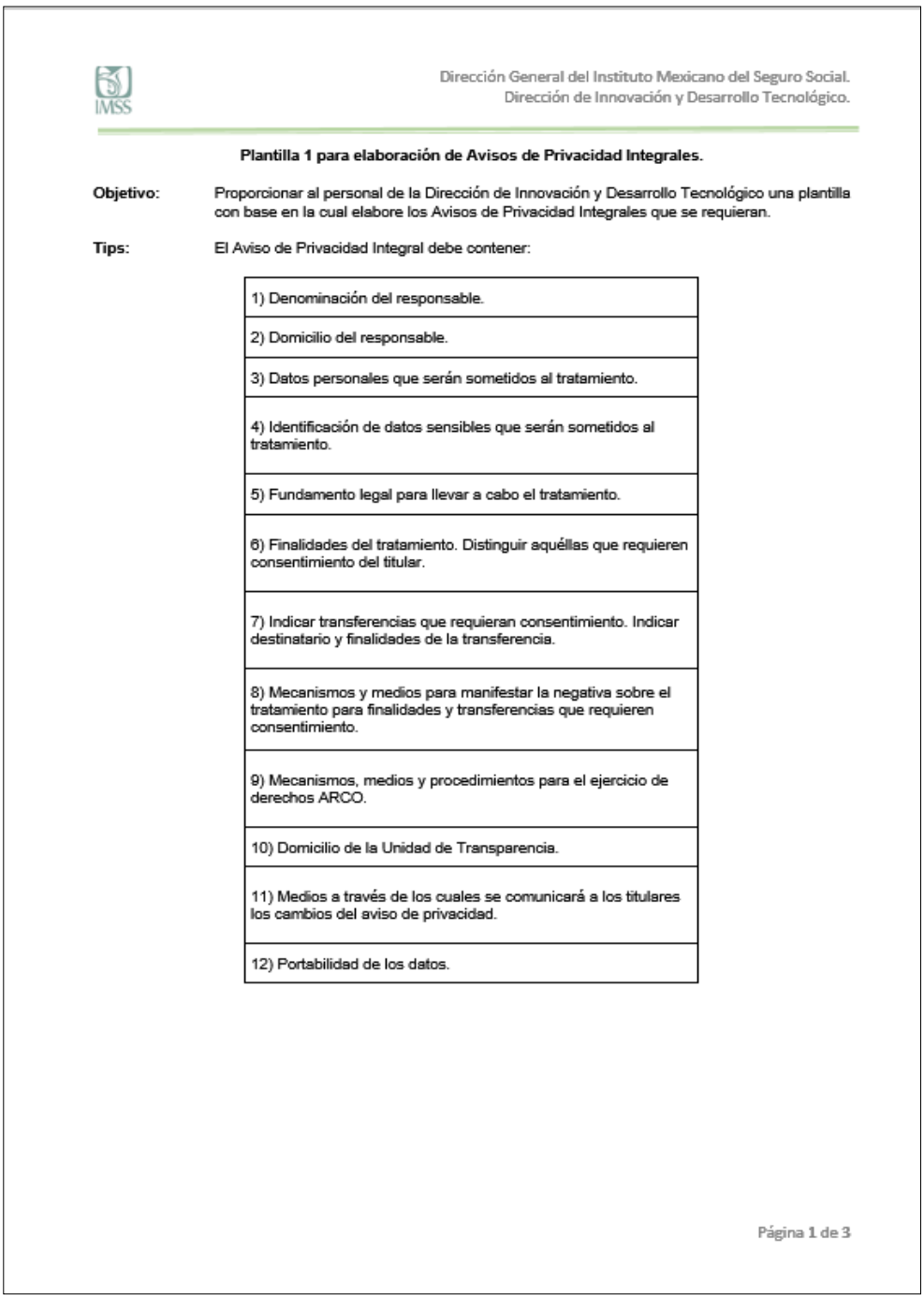
(Agregue las tablas necesarias para cada una de las transferencias).

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

3.2.3 De los avisos de privacidad

A efecto de que usted cuente con un instrumento para la elaboración de los avisos de privacidad que se requieran, a continuación, se proporciona un formato para avisos de privacidad integrales.

Documento 23. Plantilla 1 para la elaboración de Avisos de Privacidad Integrales, página 1



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Plantilla 1 para elaboración de Avisos de Privacidad Integrales.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico una plantilla con base en la cual elabore los Avisos de Privacidad Integrales que se requieran.

Tips: El Aviso de Privacidad Integral debe contener:

1) Denominación del responsable.
2) Domicilio del responsable.
3) Datos personales que serán sometidos al tratamiento.
4) Identificación de datos sensibles que serán sometidos al tratamiento.
5) Fundamento legal para llevar a cabo el tratamiento.
6) Finalidades del tratamiento. Distinguir aquéllas que requieren consentimiento del titular.
7) Indicar transferencias que requieran consentimiento. Indicar destinatario y finalidades de la transferencia.
8) Mecanismos y medios para manifestar la negativa sobre el tratamiento para finalidades y transferencias que requieren consentimiento.
9) Mecanismos, medios y procedimientos para el ejercicio de derechos ARCO.
10) Domicilio de la Unidad de Transparencia.
11) Medios a través de los cuales se comunicará a los titulares los cambios del aviso de privacidad.
12) Portabilidad de los datos.

Página 1 de 3

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 24. Plantilla 1 para la elaboración de Avisos de Privacidad Integrales, página 2

Plantilla:

Aviso de Privacidad Integral para *(colocar titular al que va dirigido – ejemplo: Usuarios de la Aplicación Móvil "El IMSS en tu casa")*.

1. Responsable del tratamiento de sus datos personales.

El Instituto Mexicano del Seguro Social (IMSS) con domicilio en *(colocar domicilio completo)*, es el sujeto obligado y responsable del tratamiento de los datos personales que se recaban a través de *(colocar medio – ejemplo: la Aplicación Móvil "El IMSS en tu casa")*, los cuales serán protegidos conforme a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás normatividad que resulte aplicable.

2. Datos personales que serán sometidos a tratamiento.

Los datos personales recabados a través de *(colocar medio – ejemplo: la Aplicación Móvil "El IMSS en tu casa")*, son: *(colocar categorías y datos – ejemplo: Datos de identificación como su nombre, número de seguridad social y RFC; datos de localización como su domicilio, correo electrónico y número telefónico, y datos de salud)*.

3. Identificación de datos sensibles que serán sometidos al tratamiento.

Se informa que *(indicar si se tratarán datos personales sensibles – ejemplo: por la naturaleza de la Aplicación Móvil de que se trata, y el servicio que se proporcionará a través de la misma, serán tratados datos de salud, los que son considerados como sensibles)*.

4. Fundamento legal para llevar a cabo el tratamiento.

El tratamiento de sus datos personales se realiza bajo el amparo de los dispuesto en *(indicar marco normativo *vea apartado 2 del formato 2* – ejemplo: el Reglamento interior del IMSS: Artículos 74, fracción III y 82, fracción I, así como en el Manual de organización de la Dirección de Innovación y Desarrollo Tecnológico, apartados 8.1.3 y 8.1.3.1)*.

5. Finalidades del tratamiento.

Sus datos personales serán tratados para realizar las siguientes finalidades:

- *(colocar finalidades *vea apartado 3 del formato 2* – ejemplo: Contar con su registro como usuario de la aplicación del IMSS en tu casa, a efecto de que en su perfil de usuario se encuentre cargada su historia médica)*.

6. Transferencias de sus datos personales.

Se le informa que sus datos personales *(indicar si se realizarán transferencias *vea apartado 12 del formato 2*, de indicar el destinatario y la finalidad de la transferencia)*.

Además, se realizarán las transferencias necesarias para atender requerimientos de

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 25. Plantilla 1 para la elaboración de Avisos de Privacidad Integrales, página 3

información de una autoridad competente, que esté debidamente fundados y motivados.

7. Mecanismos y medios para manifestar la negativa sobre el tratamiento para finalidades y transferencias que requieren consentimiento.

El titular de los datos personales podrá manifestar la negativa sobre el tratamiento para finalidades y transferencias que requieren consentimiento ***(indicar mecanismos y medios, este punto debe ser de acuerdo a lo establecido ya por la Unidad de Transparencia del IMSS)***.

8. Mecanismos y medios para y procedimientos para el ejercicio de derechos ARCO (acceso, rectificación, cancelación y oposición).

El titular de los datos personales podrá ejercer cualquiera de sus derechos ARCO ***(indicar mecanismos y medios, este punto debe ser de acuerdo a lo establecido ya por la Unidad de Transparencia del IMSS)***.

9. Portabilidad de los datos personales.

Se informa que se podrá ejercer el derecho de la portabilidad de los siguientes datos personales: ***(colocar categorías y datos – ejemplo: Datos de identificación como su nombre, número de seguridad social y RFC; datos de localización como su domicilio, correo electrónico y número telefónico, y datos de salud)***.

Dichos datos personales se encuentran ***(indicar tipo de formato estructurado y comúnmente utilizado).***

Usted podrá ejercer este derecho ***(indicar mecanismos y medios, este punto debe ser de acuerdo a lo establecido ya por la Unidad de Transparencia del IMSS)***.

10. Domicilio de la Unidad de Transparencia.

La Unidad de Transparencia del IMMS tiene su domicilio en ***(colocar domicilio completo)***.

11. Mecanismos a través de los cuales se comunicarán cambios a este aviso de privacidad.

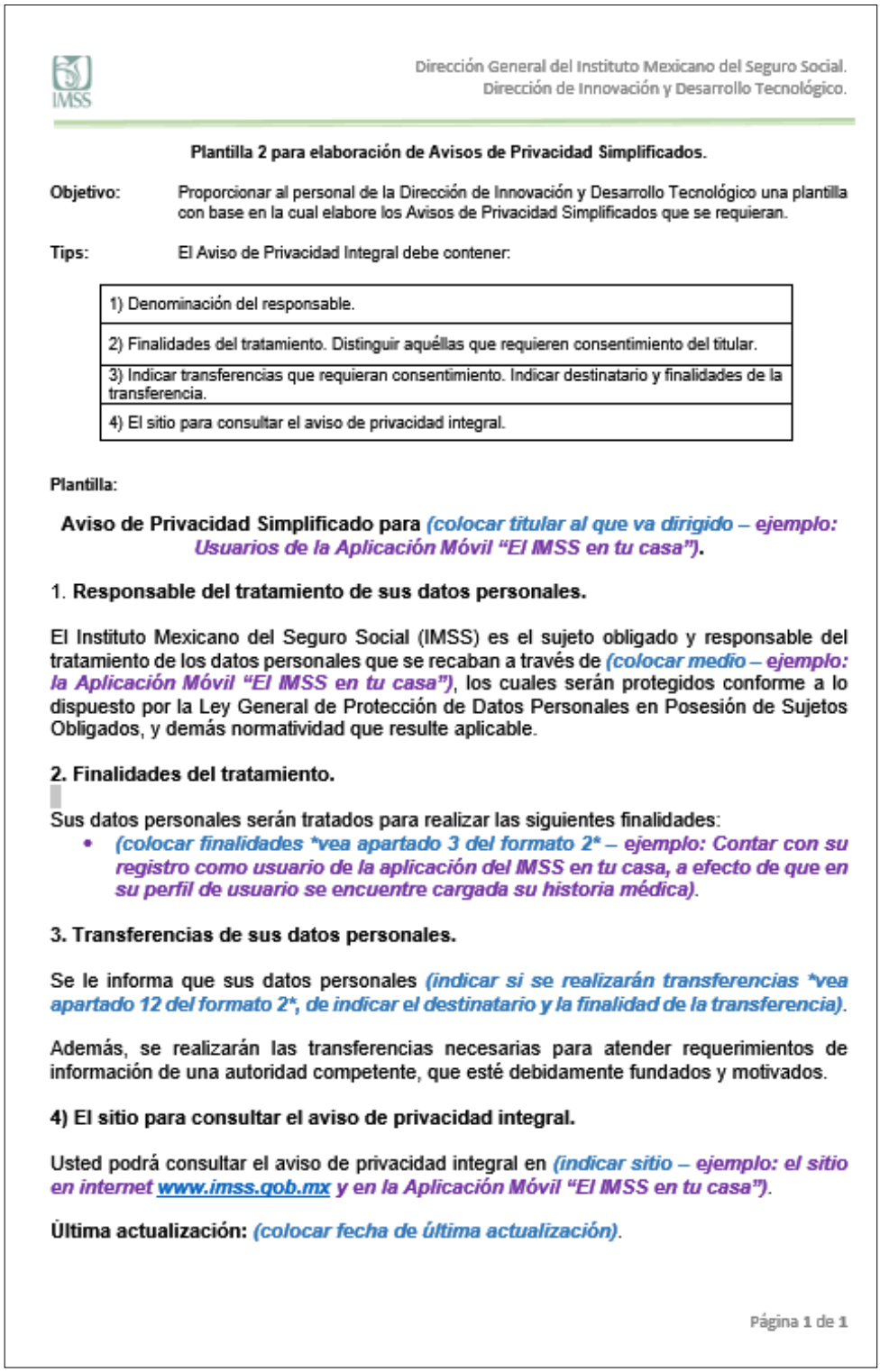
En caso de que exista un cambio de este aviso de privacidad, lo haremos de su conocimiento ***(indicar mecanismo – ejemplo: a través del sitio en internet www.imss.gob.mx y en la Aplicación Móvil "El IMSS en tu casa")***.

Última actualización: ***(colocar fecha de última actualización)***.

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Por su parte, para el aviso de privacidad simplificado, se presenta el siguiente formato:

Documento 26. Plantilla 2 para la elaboración de Avisos de Privacidad Simplificados



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Plantilla 2 para elaboración de Avisos de Privacidad Simplificados.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico una plantilla con base en la cual elabore los Avisos de Privacidad Simplificados que se requieran.

Tips: El Aviso de Privacidad Integral debe contener:

1) Denominación del responsable.
2) Finalidades del tratamiento. Distinguir aquéllas que requieren consentimiento del titular.
3) Indicar transferencias que requieran consentimiento. Indicar destinatario y finalidades de la transferencia.
4) El sitio para consultar el aviso de privacidad integral.

Plantilla:

Aviso de Privacidad Simplificado para *(colocar titular al que va dirigido – ejemplo: Usuarios de la Aplicación Móvil "El IMSS en tu casa")*.

1. **Responsable del tratamiento de sus datos personales.**

El Instituto Mexicano del Seguro Social (IMSS) es el sujeto obligado y responsable del tratamiento de los datos personales que se recaban a través de ***(colocar medio – ejemplo: la Aplicación Móvil "El IMSS en tu casa")***, los cuales serán protegidos conforme a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás normatividad que resulte aplicable.

2. Finalidades del tratamiento.

Sus datos personales serán tratados para realizar las siguientes finalidades:

- ***(colocar finalidades *vea apartado 3 del formato 2* – ejemplo: Contar con su registro como usuario de la aplicación del IMSS en tu casa, a efecto de que en su perfil de usuario se encuentre cargada su historia médica)***.

3. Transferencias de sus datos personales.

Se le informa que sus datos personales ***(indicar si se realizarán transferencias *vea apartado 12 del formato 2*, de indicar el destinatario y la finalidad de la transferencia)***.

Además, se realizarán las transferencias necesarias para atender requerimientos de información de una autoridad competente, que esté debidamente fundados y motivados.

4) El sitio para consultar el aviso de privacidad integral.

Usted podrá consultar el aviso de privacidad integral en ***(indicar sitio – ejemplo: el sitio en internet www.imss.gob.mx y en la Aplicación Móvil "El IMSS en tu casa")***.

Última actualización: ***(colocar fecha de última actualización)***.

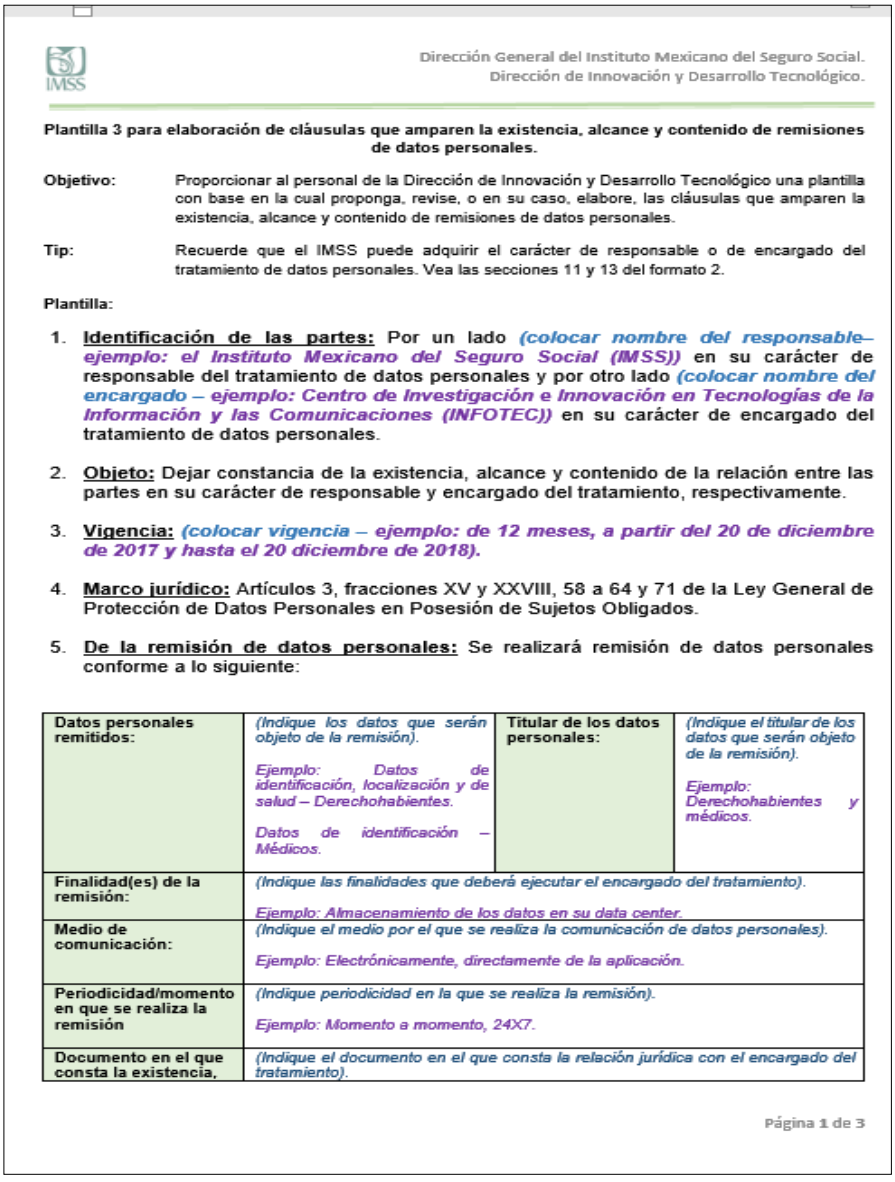
Página 1 de 1

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

3.2.4 De las comunicaciones de datos personales

Con el objetivo de asegurar que las remisiones de datos consten en instrumentos jurídicos con las cláusulas que se requieren para comprobar su existencia, alcance y contenido, a continuación, se presenta una plantilla con las cláusulas que para tal efecto pueden ser adoptadas. Es importante recordar que el IMSS puede adquirir el carácter de encargado del tratamiento o de encargado del tratamiento.

Documento 27. Plantilla 3 para la elaboración de cláusulas que amparen la existencia, alcance y contenido de remisiones de datos personales, página 1



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Plantilla 3 para elaboración de cláusulas que amparen la existencia, alcance y contenido de remisiones de datos personales.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico una plantilla con base en la cual proponga, revise, o en su caso, elabore, las cláusulas que amparen la existencia, alcance y contenido de remisiones de datos personales.

Tip: Recuerde que el IMSS puede adquirir el carácter de responsable o de encargado del tratamiento de datos personales. Vea las secciones 11 y 13 del formato 2.

Plantilla:

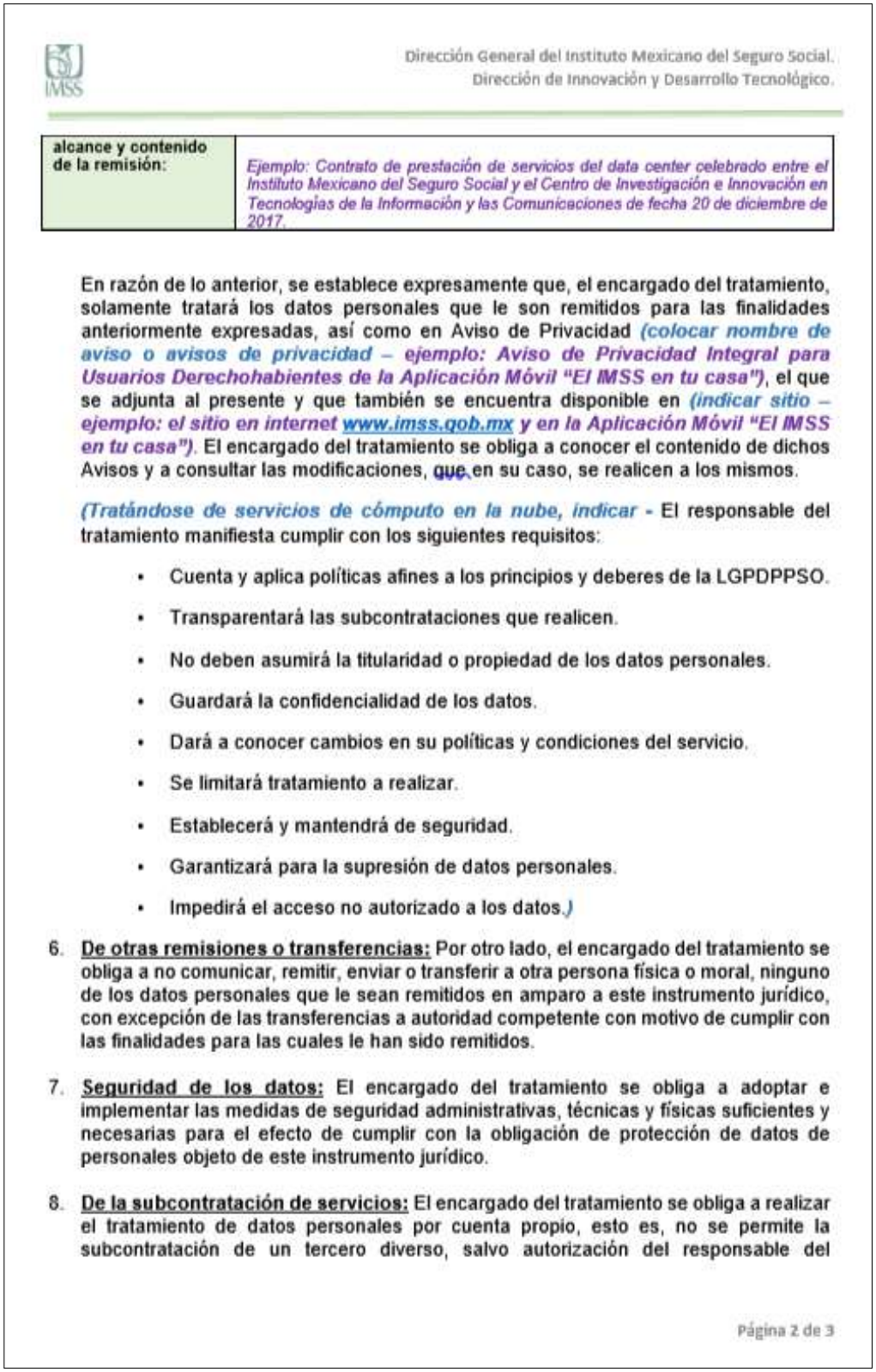
1. **Identificación de las partes:** Por un lado ***(colocar nombre del responsable– ejemplo: el Instituto Mexicano del Seguro Social (IMSS))*** en su carácter de responsable del tratamiento de datos personales y por otro lado ***(colocar nombre del encargado – ejemplo: Centro de Investigación e Innovación en Tecnologías de la Información y las Comunicaciones (INFOTEC))*** en su carácter de encargado del tratamiento de datos personales.
2. **Objeto:** Dejar constancia de la existencia, alcance y contenido de la relación entre las partes en su carácter de responsable y encargado del tratamiento, respectivamente.
3. **Vigencia:** ***(colocar vigencia – ejemplo: de 12 meses, a partir del 20 de diciembre de 2017 y hasta el 20 diciembre de 2018).***
4. **Marco jurídico:** Artículos 3, fracciones XV y XXVIII, 58 a 64 y 71 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
5. **De la remisión de datos personales:** Se realizará remisión de datos personales conforme a lo siguiente:

Datos personales remitidos:	*(Indique los datos que serán objeto de la remisión).* *Ejemplo: Datos de identificación, localización y de salud – Derechohabientes.* *Datos de identificación – Médicos.*	**Titular de los datos personales:**	*(Indique el titular de los datos que serán objeto de la remisión).* *Ejemplo: Derechohabientes y médicos.*
Finalidad(es) de la remisión:	*(Indique las finalidades que deberá ejecutar el encargado del tratamiento).* *Ejemplo: Almacenamiento de los datos en su data center.*		
Medio de comunicación:	*(Indique el medio por el que se realiza la comunicación de datos personales).* *Ejemplo: Electrónicamente, directamente de la aplicación.*		
Periodicidad/momento en que se realiza la remisión	*(Indique periodicidad en la que se realiza la remisión).* *Ejemplo: Momento a momento, 24X7.*		
Documento en el que consta la existencia,	*(Indique el documento en el que consta la relación jurídica con el encargado del tratamiento).*		

Página 1 de 3

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 28. Plantilla 3 para la elaboración de cláusulas que amparen la existencia, alcance y contenido de remisiones de datos personales, página 2



alcance y contenido de la remisión:	*Ejemplo: Contrato de prestación de servicios del data center celebrado entre el Instituto Mexicano del Seguro Social y el Centro de Investigación e Innovación en Tecnologías de la Información y las Comunicaciones de fecha 20 de diciembre de 2017.*

En razón de lo anterior, se establece expresamente que, el encargado del tratamiento, solamente tratará los datos personales que le son remitidos para las finalidades anteriormente expresadas, así como en Aviso de Privacidad ***(colocar nombre de aviso o avisos de privacidad – ejemplo: Aviso de Privacidad Integral para Usuarios Derechohabientes de la Aplicación Móvil "El IMSS en tu casa")***, el que se adjunta al presente y que también se encuentra disponible en ***(indicar sitio – ejemplo: el sitio en internet www.imss.gob.mx y en la Aplicación Móvil "El IMSS en tu casa")***. El encargado del tratamiento se obliga a conocer el contenido de dichos Avisos y a consultar las modificaciones, que en su caso, se realicen a los mismos.

(Tratándose de servicios de cómputo en la nube, indicar - El responsable del tratamiento manifiesta cumplir con los siguientes requisitos:

- Cuenta y aplica políticas afines a los principios y deberes de la LGPDPPSO.
- Transparentará las subcontrataciones que realicen.
- No deben asumirá la titularidad o propiedad de los datos personales.
- Guardará la confidencialidad de los datos.
- Dará a conocer cambios en su políticas y condiciones del servicio.
- Se limitará tratamiento a realizar.
- Establecerá y mantendrá de seguridad.
- Garantizará para la supresión de datos personales.
- Impedirá el acceso no autorizado a los datos.*)*

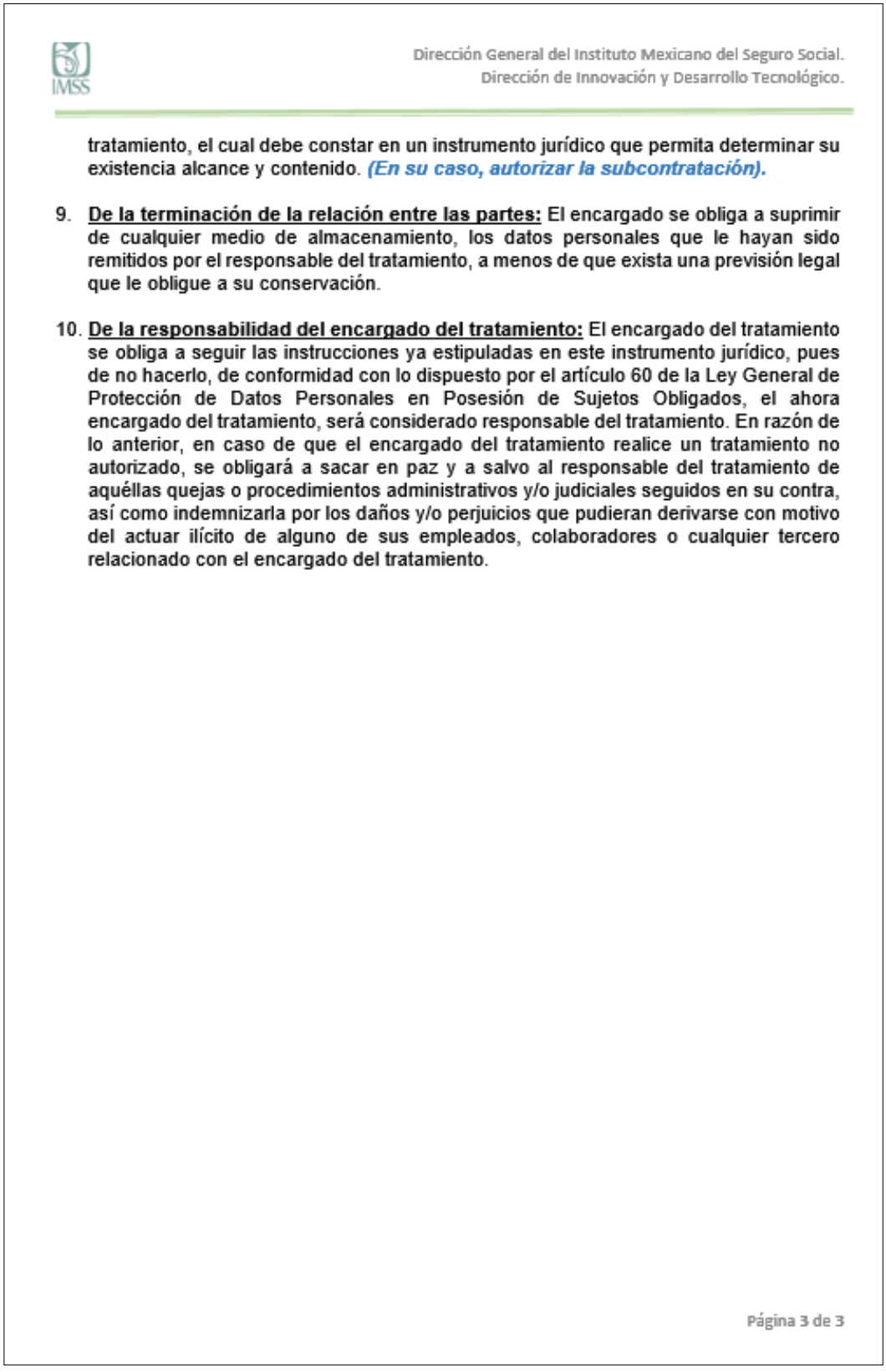
6. **De otras remisiones o transferencias:** Por otro lado, el encargado del tratamiento se obliga a no comunicar, remitir, enviar o transferir a otra persona física o moral, ninguno de los datos personales que le sean remitidos en amparo a este instrumento jurídico, con excepción de las transferencias a autoridad competente con motivo de cumplir con las finalidades para las cuales le han sido remitidos.

7. **Seguridad de los datos:** El encargado del tratamiento se obliga a adoptar e implementar las medidas de seguridad administrativas, técnicas y físicas suficientes y necesarias para el efecto de cumplir con la obligación de protección de datos de personales objeto de este instrumento jurídico.

8. **De la subcontratación de servicios:** El encargado del tratamiento se obliga a realizar el tratamiento de datos personales por cuenta propio, esto es, no se permite la subcontratación de un tercero diverso, salvo autorización del responsable del

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Documento 29. Plantilla 3 para la elaboración de cláusulas que amparen la existencia, alcance y contenido de remisiones de datos personales, página 3



tratamiento, el cual debe constar en un instrumento jurídico que permita determinar su existencia alcance y contenido. ***(En su caso, autorizar la subcontratación).***

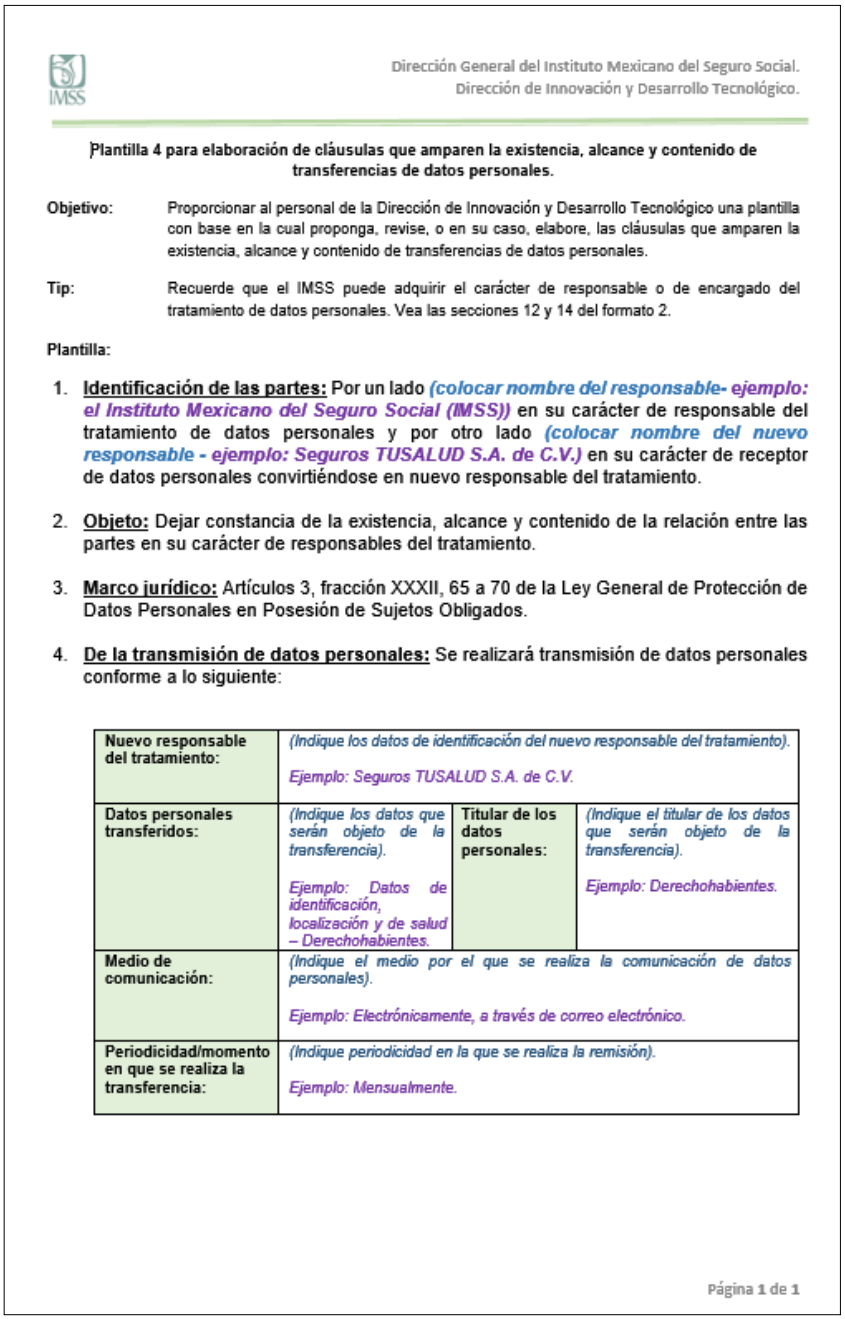
9. **De la terminación de la relación entre las partes:** El encargado se obliga a suprimir de cualquier medio de almacenamiento, los datos personales que le hayan sido remitidos por el responsable del tratamiento, a menos de que exista una previsión legal que le obligue a su conservación.

10. **De la responsabilidad del encargado del tratamiento:** El encargado del tratamiento se obliga a seguir las instrucciones ya estipuladas en este instrumento jurídico, pues de no hacerlo, de conformidad con lo dispuesto por el artículo 60 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el ahora encargado del tratamiento, será considerado responsable del tratamiento. En razón de lo anterior, en caso de que el encargado del tratamiento realice un tratamiento no autorizado, se obligará a sacar en paz y a salvo al responsable del tratamiento de aquéllas quejas o procedimientos administrativos y/o judiciales seguidos en su contra, así como indemnizarla por los daños y/o perjuicios que pudieran derivarse con motivo del actuar ilícito de alguno de sus empleados, colaboradores o cualquier tercero relacionado con el encargado del tratamiento.

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

Por su parte, para documentar la existencia, alcance y contenido sobre transferencias de datos personales, a continuación, se presenta una plantilla con las cláusulas que para tal efecto pueden ser adoptadas. Es importante recordar que el IMSS puede adquirir el carácter de responsable emisor o receptor.

Documento 30. Plantilla 4 para la elaboración de cláusulas que amparen la existencia, alcance y contenido de transferencias de datos personales



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Plantilla 4 para elaboración de cláusulas que amparen la existencia, alcance y contenido de transferencias de datos personales.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico una plantilla con base en la cual proponga, revise, o en su caso, elabore, las cláusulas que amparen la existencia, alcance y contenido de transferencias de datos personales.

Tip: Recuerde que el IMSS puede adquirir el carácter de responsable o de encargado del tratamiento de datos personales. Vea las secciones 12 y 14 del formato 2.

Plantilla:

1. **Identificación de las partes:** Por un lado ***(colocar nombre del responsable- ejemplo: el Instituto Mexicano del Seguro Social (IMSS))*** en su carácter de responsable del tratamiento de datos personales y por otro lado ***(colocar nombre del nuevo responsable - ejemplo: Seguros TUSALUD S.A. de C.V.)*** en su carácter de receptor de datos personales convirtiéndose en nuevo responsable del tratamiento.

2. **Objeto:** Dejar constancia de la existencia, alcance y contenido de la relación entre las partes en su carácter de responsables del tratamiento.

3. **Marco jurídico:** Artículos 3, fracción XXXII, 65 a 70 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

4. **De la transmisión de datos personales:** Se realizará transmisión de datos personales conforme a lo siguiente:

Nuevo responsable del tratamiento:	*(Indique los datos de identificación del nuevo responsable del tratamiento).* *Ejemplo: Seguros TUSALUD S.A. de C.V.*		
Datos personales transferidos:	*(Indique los datos que serán objeto de la transferencia).* *Ejemplo: Datos de identificación, localización y de salud – Derechohabientes.*	**Titular de los datos personales:**	*(Indique el titular de los datos que serán objeto de la transferencia).* *Ejemplo: Derechohabientes.*
Medio de comunicación:	*(Indique el medio por el que se realiza la comunicación de datos personales).* *Ejemplo: Electrónicamente, a través de correo electrónico.*		
Periodicidad/momento en que se realiza la transferencia:	*(Indique periodicidad en la que se realiza la remisión).* *Ejemplo: Mensualmente.*		

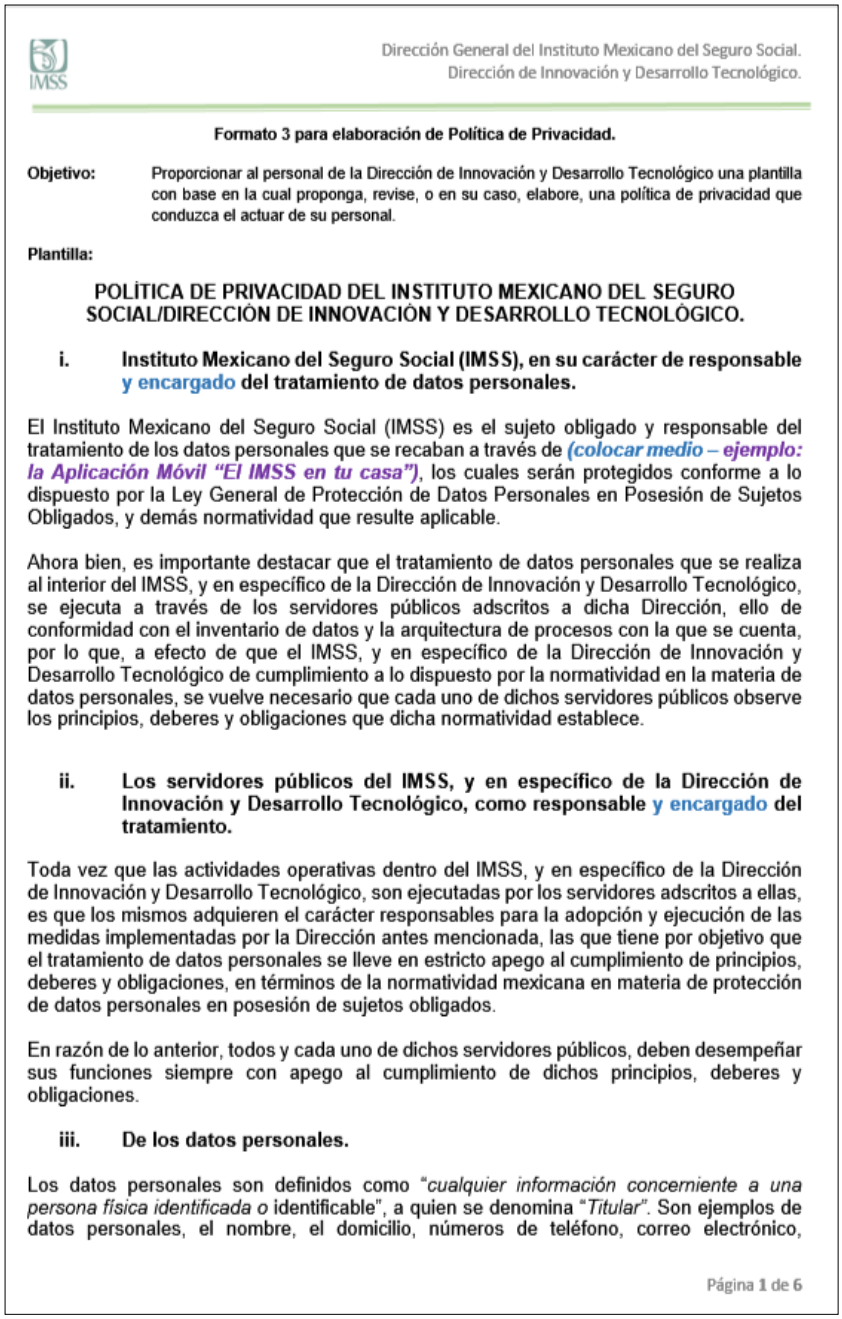
Página 1 de 1

Fuente: Elaboración propia con propuesta de intervención y formatos MAAGTICSI.

3.2.5 De las Política de privacidad.

Uno de los mecanismos para dar cumplimiento al principio de responsabilidad es la emisión y cumplimiento de políticas, en razón de ello, se sugiere el siguiente formato de política de privacidad para la Dirección de Innovación y Desarrollo Tecnológico.

Documento 31. Formato 3. Política de Privacidad, página 1



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Formato 3 para elaboración de Política de Privacidad.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico una plantilla con base en la cual proponga, revise, o en su caso, elabore, una política de privacidad que conduzca el actuar de su personal.

Plantilla:

POLÍTICA DE PRIVACIDAD DEL INSTITUTO MEXICANO DEL SEGURO SOCIAL/DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO.

i. Instituto Mexicano del Seguro Social (IMSS), en su carácter de responsable y encargado del tratamiento de datos personales.

El Instituto Mexicano del Seguro Social (IMSS) es el sujeto obligado y responsable del tratamiento de los datos personales que se recaban a través de ***(colocar medio – ejemplo: la Aplicación Móvil "El IMSS en tu casa")***, los cuales serán protegidos conforme a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás normatividad que resulte aplicable.

Ahora bien, es importante destacar que el tratamiento de datos personales que se realiza al interior del IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, se ejecuta a través de los servidores públicos adscritos a dicha Dirección, ello de conformidad con el inventario de datos y la arquitectura de procesos con la que se cuenta, por lo que, a efecto de que el IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico de cumplimiento a lo dispuesto por la normatividad en la materia de datos personales, se vuelve necesario que cada uno de dichos servidores públicos observe los principios, deberes y obligaciones que dicha normatividad establece.

ii. Los servidores públicos del IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, como responsable y encargado del tratamiento.

Toda vez que las actividades operativas dentro del IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, son ejecutadas por los servidores adscritos a ellas, es que los mismos adquieren el carácter responsables para la adopción y ejecución de las medidas implementadas por la Dirección antes mencionada, las que tiene por objetivo que el tratamiento de datos personales se lleve en estricto apego al cumplimiento de principios, deberes y obligaciones, en términos de la normatividad mexicana en materia de protección de datos personales en posesión de sujetos obligados.

En razón de lo anterior, todos y cada uno de dichos servidores públicos, deben desempeñar sus funciones siempre con apego al cumplimiento de dichos principios, deberes y obligaciones.

iii. De los datos personales.

Los datos personales son definidos como "*cualquier información concerniente a una persona física identificada o* identificable", a quien se denomina "*Titular*". Son ejemplos de datos personales, el nombre, el domicilio, números de teléfono, correo electrónico,

Página **1** de **6**

Fuente: Elaboración propia con propuesta de intervención.

Documento 32. Formato 3. Política de Privacidad, página 2

características físicas, informes médicos, fotografías, videos, voz, por mencionar algunos.

Asimismo, aquéllos datos que "*afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste*", son considerados como datos personales sensibles. Se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

iv. Del tratamiento de datos personales.

El tratamiento de los datos personales puede resumirse en cualquier actividad que sea realizada a los datos personales, esto es obtenerlos, usarlos, divulgarlos o guardarlos.

En consecuencia de lo anterior, cualquier particular que realice tratamiento de datos debe observar lo dispuesto en la normatividad en materia de protección de datos personales en posesión de sujetos obligados, que podemos agrupar en tres grandes secciones: principios, deberes y obligaciones.

Ahora bien, cuando dentro del tratamiento se realiza comunicación de datos personales, la misma puede efectuarse como una remisión o una transferencia. La primera, es la que se hace a un "encargado del tratamiento", quien deberá tratar los datos conforme a las instrucciones y por cuenta del responsable del tratamiento. Por otro lado, la transferencia de datos personales es la comunicación que se hace a "otro responsable del tratamiento", ello es, porque ese nuevo responsable será quien decida sobre el tratamiento de los datos personales.

v. De los principios en materia de protección de datos personales.

Los principios son enunciados normativos que rigen el deber actuar de quienes tratan datos personales y son ocho: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

El principio de ***lealtad***[1]**,** se materializa cuando el tratamiento de los datos personales se realiza con apego y cumplimiento a lo dispuesto en la normatividad que resulte aplicable, y (ii) el tratamiento debe realizarse conforme a las facultades y atribuciones de cada servidor público involucrado en dicho tratamiento.

El principio de ***consentimiento***[2], se traduce en la aceptación del titular para que el responsable trate sus datos, de conformidad con una o varias finalidades determinadas.

El consentimiento puede otorgarse de manera tácita, esto es, cuando no existe oposición y expresa, esto es, que se requiere de un mecanismo en el que se deje constancia de la aceptación, como puede ser verbal, escrita, a través de medios electrónicos, ópticos o cualquier otra tecnología o a través de signos inequívocos. Cuando se trata de datos

[1] Artículo 17 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).
[2] Artículo 20 a 22 de la LGPDPPSO.

Fuente: Elaboración propia con propuesta de intervención.

Documento 33. Formato 3. Política de Privacidad, página 3

personales sensibles, el consentimiento debe ser expreso.

El consentimiento debe otorgarse observando que su obtención sea:

- LIBRE. Que no debe exista error, mala fe, violencia o dolo.
- ESPECÍFICA. Se debe referir a una o varias finalidades determinadas que justifiquen el tratamiento.
- INFORMADA: Previo al tratamiento de los datos, el titular debe tener conocimiento del Aviso de Privacidad, al que nos referimos en breve. Asimismo, debe saber de las consecuencias que traerá el consentimiento otorgado.

El principio de ***información***[3] se traduce en el tan afamado Aviso de Privacidad, esto es, el documento a través del cual se da a conocer al titular la información relativa a la existencia y características principales del tratamiento al que sus datos personales serán sometidos. Existen dos modalidades de Avisos de Privacidad, el integral y el simplificado.

El principio de ***calidad***[4] se traduce en que los datos tratados sean completos, correctos, exactos y actualizados de conformidad con la finalidad para la cual son tratados. Asimismo, para cumplir con el principio es necesario observar las reglas de conservación de los mismos, esto es para atender los aspectos administrativos, contables, fiscales, jurídicos e históricos necesarios, por lo que posterior a dicho periodo deben entrar en un periodo de bloqueo, en el que solo podrían ser consultados para determinar posibles responsabilidades derivadas de su tratamiento y pasado dicho periodo, proceder a su posterior supresión.

Ahora bien, el principio de ***finalidad***[5] se refiere a los usos que les será dado a los datos. Las finalidades deben ser concretas, lícitas, explícitas y legítimas.

El principio de ***lealtad***[6] es que el tratamiento de los datos personales se realice privilegiando la protección a los intereses y su expectativa razonable de privacidad.

El principio de ***proporcionalidad***[7] se cumple cuando los datos sujetos a tratamiento resultan ser los necesarios, adecuados y relevantes de conformidad con las finalidades por las que fueron obtenidos.

Finalmente, el principio de ***responsabilidad***[8] es el que se refiere a la implementación de los mecanismos necesarios para acreditar el cumplimiento de principios, deberes y obligaciones en materia de protección de datos personales en posesión de sujetos obligados.

vi. De los deberes en materia de protección de datos personales.

Los deberes en materia de protección de datos personales son dos, el de seguridad que se traduce en la adopción de medidas físicas, administrativas y técnicas que protejan a los

[3] Artículos 3, fracción II y 26 a 28 de la LGPDPPSO.
[4] Artículos 23 y 24 de la LGPDPPSO.
[5] Artículo 18 de la LGPDPPSO.
[6] Artículo 19 de la LGPDPPSO.
[7] Artículo 25 de la LGPDPPSO.
[8] Artículo 29 y 30 de la LGPDPPSO.

Fuente: Elaboración propia con propuesta de intervención.

Documento 34. Formato 3. Política de Privacidad, página 4

datos personales de sufrir daños, pérdidas, alteraciones, destrucciones o usos, acceso o tratamientos no autorizados[9], las cuales deben garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

vii. **Protección de datos personales en el IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico.**

Son *(indicar cantidad de titulares identificados en el inventario de datos)* los titulares de quienes se trata información al interior del IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico: *(indicar titulares – Ejemplo: Usuarios derechohabientes de la Aplicación Móvil "El IMSS en tu casa". Médicos que prestan servicios con base en la Aplicación Móvil "El IMSS en tu casa")*. Es por ello que, ante dichos titulares, como institución, nos comprometemos, que a través de cada uno de los servidores públicos que colaboran en el IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, realizan el tratamiento de los datos personales con estricto a apego a la normatividad mexicana en materia de protección de datos personales en posesión de sujetos obligados, de conformidad con lo siguiente:

a. Cumplimiento de principios en materia de protección de datos personales.

El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, da cumplimiento a los principios en materia de protección de datos personales, de conformidad con lo siguiente:

1. *Principio de información*. El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico cuenta con los siguientes avisos de privacidad: *(indicar avisos de privacidad – Ejemplo: Aviso de Privacidad Integral para Usuarios derechohabientes de la Aplicación Móvil "El IMSS en tu casa")*.

   Dichos Avisos de Privacidad cumplen con los requisitos establecidos por las disposiciones normativas aplicables y han sido puestos a disposición de sus titulares conforme la norma lo indica.

2. *Principio de consentimiento*. El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, cuenta con inventario de datos personales relacionado con los procedimientos que se ejecutan al interior de la organización. Partiendo de dicho inventario, se han identificado aquéllos datos personales que requieren de un especial consentimiento.
3. *Principio de finalidad*. El tratamiento de los datos personales en El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, se encuentra limitado a las finalidades previstas en los Avisos de Privacidad con los que se cuenta.

   Asimismo, en dichos Avisos de Privacidad, se ha indicado el mecanismo que los titulares podrán ejecutar para manifestar la negativa sobre el tratamiento para finalidades y transferencias que requieren consentimiento.

4. *Principio de calidad*. El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, se asegura que los datos personales con los que cuenta

[9] Artículos 3 fracciones XVI y XX a XXIII y 31 a 42 de la LGPDPPSO.

Fuente: Elaboración propia con propuesta de intervención.

Documento 35. Formato 3. Política de Privacidad, página 5

sean los completos, correctos, exactos y actualizados, por ello, constantemente se verifica con los titulares de dichos datos que se cumpla con dichas características.

Por otro lado, al interior de El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, se cuenta con la Política de Calidad de Datos Personales, la cual establece el procedimiento que debe seguirse para la conservación, bloqueo y supresión de los datos personales.

5. *Principio de proporcionalidad.* El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, ha verificado que los datos personales que trata sean los necesarios, adecuados y relevantes en relación con las finalidades para las que son recabados.
6. *Principio de lealtad.* El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, siempre tratará los datos personales de los titulares de que se trate privilegiando sus intereses, así como su expectativa razonable de privacidad, esto es, la confianza que los mismos depositan en el IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico.
7. *Principio de responsabilidad.* El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, entre otros, ha implementado los siguientes mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones en materia de protección de datos personales en posesión de sujetos obligados.
    a. Cuenta con políticas de privacidad y políticas obligatorios al interior de la institución, y en específico de la Dirección de Innovación y Desarrollo Tecnológico.
    b. Cuenta con un sistema de supervisión y vigilancia interna que le permiten comprobar el cumplimiento de sus políticas de privacidad.
    c. Revisa periódicamente la vigencia de sus políticas y programas de privacidad.
    d. Establece medidas que permitan dar cumplimiento a los deberes en materia de protección de datos personales.
    e. Cuenta con mecanismos que permitan garantizar el cumplimiento de la ley para proteger los datos personales en remisiones y transferencias de datos personales.
    f. Para los casos en los que el IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, funge como encargado del tratamiento, ha instrumentado acciones para dar cumplimiento a cada una de las obligaciones contenidas en la ley en materia de protección de datos personales en posesión de particulares.
    g. Diseña, desarrolla e implementa sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la LGPDPDPSO.

Fuente: Elaboración propia con propuesta de intervención.

Documento 36. Formato 3. Política de Privacidad, página 6

h. Garantiza que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia.

8. *Principio de legalidad.* Con todos y cada uno de los procedimientos y acciones ejecutadas en el IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, para proteger los datos personales en su posesión, el tratamiento de datos personales se traduce en una práctica que se encuentra de un marco legal, ello de conformidad con lo establecido por la normatividad en materia de protección de datos personales en posesión de sujetos obligados.

b. Cumplimiento de deberes en materia de protección de datos personales.

El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, da cumplimiento a los deberes en materia de protección de datos personales, de conformidad con lo siguiente:

Deber de seguridad. El IMSS, y en específico de la Dirección de Innovación y Desarrollo Tecnológico, ejecuta medidas de seguridad físicas, administrativas y técnicas que permiten proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Con ello, garantiza la confidencialidad, integridad y disponibilidad de dichos datos.

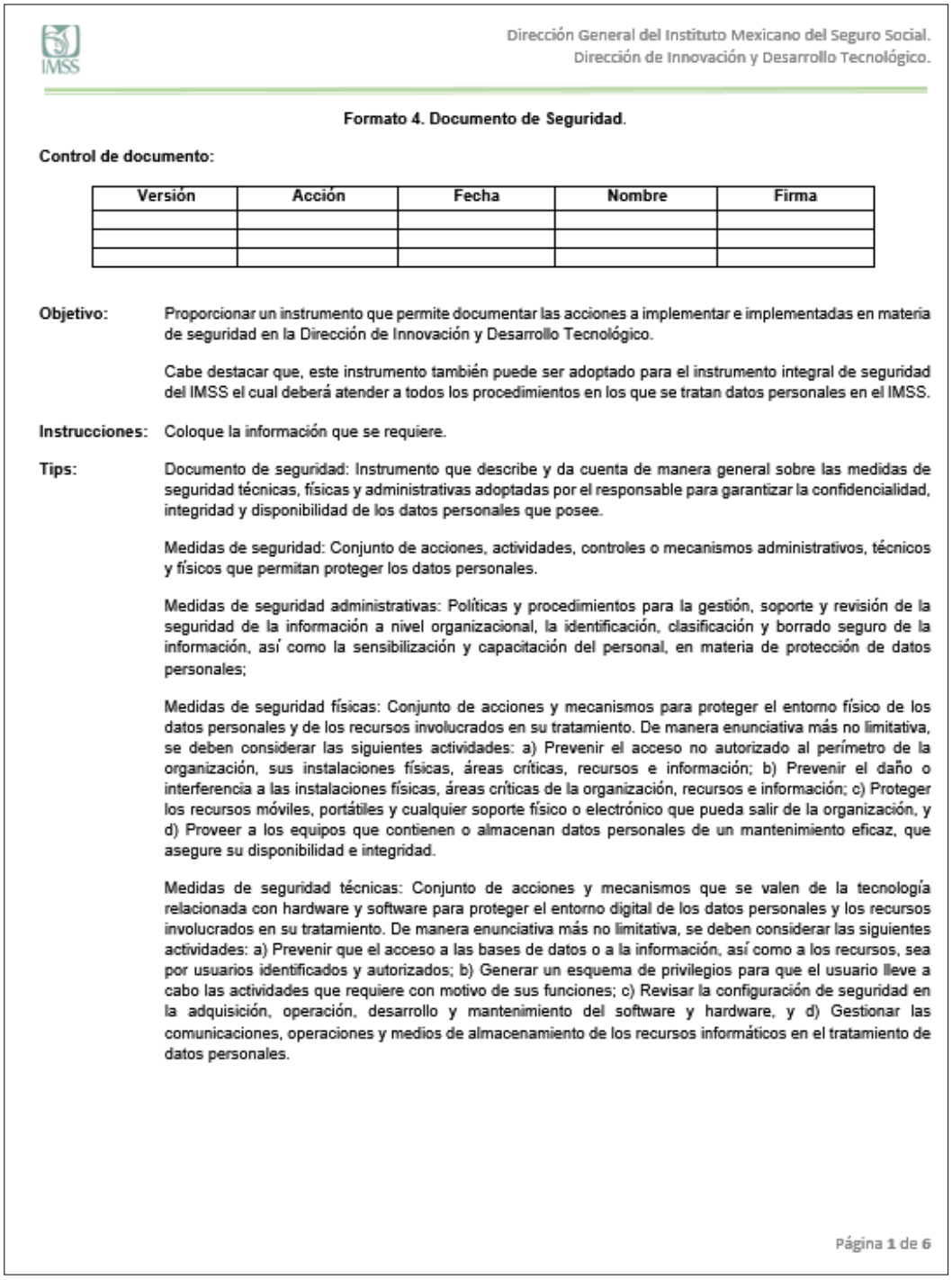
Última actualización: ***(colocar fecha de última actualización)***.

Fuente: Elaboración propia con propuesta de intervención.

3.2.6 Del deber de seguridad

Como una obligación general, la LGPDPPSO requiere la emisión de un instrumento referente a la seguridad adoptada por el responsable, por lo que a continuación se presenta el formato que para tal efecto se propone.

Documento 37. Formato 4. Documento de seguridad, página 1



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Formato 4. Documento de Seguridad.

Control de documento:

Versión	Acción	Fecha	Nombre	Firma

Objetivo: Proporcionar un instrumento que permite documentar las acciones a implementar e implementadas en materia de seguridad en la Dirección de Innovación y Desarrollo Tecnológico.

Cabe destacar que, este instrumento también puede ser adoptado para el instrumento integral de seguridad del IMSS el cual deberá atender a todos los procedimientos en los que se tratan datos personales en el IMSS.

Instrucciones: Coloque la información que se requiere.

Tips: Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información; c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Página 1 de 6

Fuente: Elaboración propia con propuesta de intervención.

Documento 38. Formato 4. Documento de seguridad, página 2

Desarrollo:

Documento de Seguridad sobre los datos personales tratados en la Dirección de Innovación y Desarrollo Tecnológico.

1. **Inventario de datos personales.**

Los datos personales que se son tratados en la Dirección de Innovación y Desarrollo Tecnológico son los siguientes *(vea los datos que registró en el formato 2, tendrá que hacer referencia a cada subproceso en el que se traten datos personales)*:

Área:	*(Indique el área a la que pertenece el proceso y el subproceso de que se trate).* *Ejemplo: Coordinación Técnica de Servicios Digitales y de Información para la Salud de la Coordinación de Servicios Digitales y de Información para la Salud y Administrativos.*
Proceso:	*(Indique el proceso de que se trate).* *Ejemplo: Implementación y mantenimiento de servicios digitales.*
Subproceso:	*(Indique el subproceso de que se trate).* *Ejemplo: Implementación y mantenimiento de la aplicación "El IMSS en tu casa".*

Dato o categoría de dato	Titular al que pertenecen	Medio de obtención	Dato sensible SI/NO
(Indique los datos o categorías de datos).	*(Indique el titular al que pertenecen)*	*(Indique el medio de obtención)*	*(Indique si el dato es sensible)*
Ejemplo: Datos de identificación: Nombre	*Ejemplo: Derechohabiente*	*Ejemplo: Electrónicamente del titular, con mecanismo de identificación.*	*Ejemplo: No.*
Ejemplo: Datos de salud.	*Ejemplo: Derechohabiente*	*Ejemplo: Electrónicamente del titular, con mecanismo de identificación.*	*Ejemplo: Si.*
Ejemplo: Datos de identificación: Nombre	*Ejemplo: Médicos*	*Ejemplo: Por otra unidad administrativa.*	*Ejemplo: No.*

Área:	*(Indique el área a la que pertenece el proceso y el subproceso de que se trate).*
Proceso:	*(Indique el proceso de que se trate).*
Subproceso:	*(Indique el subproceso de que se trate).*

Dato o categoría de dato	Titular al que pertenecen	Medio de obtención	Dato sensible SI/NO
(Indique los datos o categorías de datos).	*(Indique el titular al que pertenecen)*	*(Indique el medio de obtención)*	*(Indique si el dato es sensible)*

(Agregue las tablas que requiera).

Fuente: Elaboración propia con propuesta de intervención.

Documento 39. Formato 4. Documento de seguridad, página 3

2. Medidas de seguridad adoptadas.

A continuación, se hace referencia a las medidas de seguridad administrativas, físicas y técnicas que han sido adoptadas en la Dirección de Innovación y Desarrollo Tecnológico para proteger los datos personales que somete a tratamiento.

Tip: Recuerde que usted puede hacer referencia a la adopción de: (i) El proceso de Administración de la Seguridad de la Información (ASI), y (ii) El proceso de Operación y Controles de Seguridad de la Información y del ERISC (OPEC), ambos contenidos en el Manual Administrativo de Aplicación General aplicable en las materias de tecnologías de la información y las comunicaciones (MAAGTICSI).

A. Medidas de seguridad administrativas.

Las medidas de seguridad adoptadas de carácter administrativo, giran en torno a los documentos rectores que se deben seguirse al interior de la Dirección de Innovación y Desarrollo Tecnológico, la definición de los roles de cada uno de los servidores públicos adscritos a ella, así como la documentación de las acciones de capacitación y sensibilización que les es proporcionada.

a. **Políticas internas para la gestión y tratamiento de datos personales:** *(Indique las acciones adoptadas al respecto - Ejemplo: Al interior de la Dirección de Innovación y Desarrollo Tecnológico se cuenta con el instrumento denominado Política de Privacidad, el cual tiene por objeto que su personal conozca los ejes rectores en materia de protección de datos personales y el conjunto de medidas que debe adoptar para que los mismos sean siempre observados. También con cada servidor público involucrado en el tratamiento de datos personales, se han firmado convenios de confidencialidad).*

b. **Definición de funciones y obligaciones del personal:** *(Indique las acciones adoptadas al respecto, puede hacerse referencia al apartado 2 del formato 2, o bien, colocar aquí el contenido de dicho apartado como a continuación se indica).*

Área:	*Ejemplo: Coordinación Técnica de Servicios Digitales y de Información para la Salud de la Coordinación de Servicios Digitales y de Información para la Salud y Administrativos.*			
Proceso:	*Ejemplo: Implementación y mantenimiento de servicios digitales.*			
Subproceso:	*Ejemplo: Implementación y mantenimiento de la aplicación "El IMSS en tu casa".*			
Disposición normativa	**Artículos**	**Área involucrada**	**Contenido**	**Obligaciones relacionadas con el subproceso**
Ejemplo: Reglamento Interior del IMSS.	*Ejemplo: Artículo 82, fracción I.*	*Ejemplo: Dirección de prestaciones médicas.*	*Ejemplo: Dirigir las acciones relacionadas con la prestación de los servicios médicos.*	*Ejemplo: Proporcionar y actualizar los nombres de los médicos.*
Ejemplo: Reglamento Interior del IMSS.	*Ejemplo: Artículo 74, fracción III.*	*Ejemplo: Dirección de Innovación y Desarrollo Tecnológico.*	*Ejemplo: Diseñar y desarrollar sistemas y servicios en materia de tecnologías de la información y comunicaciones que apoyen las funciones sustantivas, administrativas y de control que deberán operar las unidades administrativas del Instituto.*	*Ejemplo: Monitoreo del funcionamiento de la aplicación.*
Ejemplo: Manual de organización de la Dirección de Innovación y Desarrollo Tecnológico.	*Ejemplo: Apartado 8.1.3.*	*Ejemplo: Coordinación de Servicios Digitales y de Información para la Salud y Administrativos*	*Ejemplo:* • *Supervisar las acciones relacionadas con la implementación de nuevos servicios digitales y de información.* • *Mantenimiento y actualización de los servicios existente en materia de salud.*	*Ejemplo: Acceso y mantenimiento a la base de datos.*

Fuente: Elaboración propia con propuesta de intervención.

Documento 40. Formato 4. Documento de seguridad, página 4

Ejemplo: Manual de organización de la Dirección de Innovación y Desarrollo Tecnológico.	*Ejemplo: Apartado 8.1.3.1*	*Ejemplo: Coordinación Técnica de Servicios Digitales y de Información para la Salud de la Coordinación de Servicios Digitales y de Información para la Salud y Administrativos*	*Ejemplo: Supervisar la elaboración de los proyectos de servicios digitales en materia de operación hospitalaria y cuidado digital de la salud. Supervisar y definir las acciones relacionadas con la implementación de nuevos servicios digitales y de información en materia de operación hospitalaria y cuidado digital de la salud, así como los relacionados con el mantenimiento y actualización de los existentes, a fin de procurar el adecuado desempeño de los mismos.*	*Ejemplo: Solicitar informes sobre el uso y funcionamiento de la aplicación.*

Área:	*(Indique el área a la que pertenece el proceso y el subproceso de que se trate).*			
Proceso:	*(Indique el proceso de que se trate).*			
Subproceso:	*(Indique el subproceso de que se trate).*			
Disposición normativa	**Artículos**	**Área involucrada**	**Contenido**	**Obligaciones relacionadas con el subproceso**
(Indique nombre de la disposición normativa).	*(Indique artículos que resultan aplicables)*	*(Indique artículos que resultan aplicables) Tip: No olvide que debe justificarse la actuación de cada servidor público involucrado.*	*(Relacione la norma con la descripción del proceso y/o subproceso)*	*(Indique las obligaciones que cada área tiene)*

c. **Acciones de capacitación y sensibilización:** *(Indique las acciones adoptadas al respecto, recuerde que las facultades en materia de capacitación las tiene el Comité y la Unidad de Transparencia, por lo que para este apartado tendrá que reportar las actividades realizadas por las mismas. No obstante, lo anterior, está guía también es un instrumento de sensibilización y capacitación, el cual puede ser reportado en este apartado).*

d. **Borrado seguro de información:** *(Indique las acciones adoptadas al respecto – Pueden emitirse Políticas para el borrado seguro de la información y reportarse los borrados seguros realizados).*

Fuente: Elaboración propia con propuesta de intervención.

Documento 41. Formato 4. Documento de seguridad, página 5

B. Medidas de seguridad técnicas.

Las medidas de seguridad adoptadas de carácter técnico, han sido separadas en dos grandes rubros, las que se refieren al software y al hardware:

a. **Mecanismos relacionados con el software:** *(Indique las acciones adoptadas al respecto. Tip. No olvide referirse a las acciones en materia de roles, permisos, control de accesos, configuración de seguridad, gestión de las comunicaciones y medios de almacenamiento).*

b. **Mecanismos relacionados con el hardware:** *(Indique las acciones adoptadas al respecto. Tip. No olvide referirse a las acciones en sobre la infraestructura que soporta el tratamiento de los datos personales, las cuales pueden referirse a roles, permisos, control de accesos, configuración de seguridad, sistemas de control, configuración de redes, seguridad de las comunicaciones, entre otros).*

C. Medidas de seguridad físicas.

Las medidas de seguridad físicas son clasificadas de acuerdo al medio en que los datos personales son tratados.

a. **Tratamiento de los datos personales en medios físicos:** *(Indique las acciones adoptadas al respecto. Tip. No olvide referirse a mecanismos para asegurarse que solo personas autorizadas tengan acceso a los datos, medidas para proteger los datos personales de casos fortuitos o fuerza mayor, políticas para el préstamo de medios físicos que contengan los datos, entre otros).*

b. **Tratamiento de los datos personales en medios electrónicos:** *(Indique las acciones adoptadas al respecto. Tip. No olvide referirse a mecanismos para asegurarse que solo personas autorizadas tengan acceso a los datos, medidas para proteger los datos personales de casos fortuitos o fuerza mayor, políticas para el uso de medios de almacenamiento portátiles, entre otros).*

Fuente: Elaboración propia con propuesta de intervención.

Documento 42. Formato 4. Documento de seguridad, página 6

3. **Garantía de la confidencialidad, integridad y disponibilidad de la información.**

Las medidas administrativas, técnicas y físicas mencionadas anteriormente, garantizan la confidencialidad, integridad y disponibilidad de la información, toda vez que *(Indique porque se garantizan las confidencialidad, integridad y disponibilidad de los datos personales. Vea apartado 10 del formato 2).*

4. **Análisis de riesgos.**

(Indique lo realizado, recuerde que la Política TIC y el MAAGTICSI en el proceso ASI prevén la elaboración de un análisis de riesgo).

5. **Acciones para el monitoreo y vigilancia.**

(Describa las acciones adoptadas para realizar monitoreo y vigilancia de las medidas de seguridad implementadas).

6. **Resultado de revisiones realizadas.**

(Indicar el resultado de las acciones de monitoreo y vigilancia).

7. **Análisis de brecha.**

Una vez realizado un estudio de las medidas que hoy en día han sido adoptadas en materia de seguridad de los datos personales, se identifica que deben ejecutarse las siguientes acciones para robustecer a las medidas ya implementadas:

A. **Medidas de seguridad administrativas:** *(Indique las acciones que deben adoptarse para su robustecimiento y justifique porque a la fecha de identificación de la necesidad, la misma no había sido implementada).*
B. **Medidas de seguridad técnicas:** *(Indique las acciones que deben adoptarse para su robustecimiento y justifique porque a la fecha de identificación de la necesidad, la misma no había sido implementada).*
C. **Medidas de seguridad físicas:** *(Indique las acciones que deben adoptarse para su robustecimiento y justifique porque a la fecha de identificación de la necesidad, la misma no había sido implementada).*

Para la implementación de dichas medidas que robustecerán el esquema de seguridad de los datos personales, se seguirá el siguiente PLAN DE TRABAJO *(colocar plan de trabajo).*

8. **Vulneraciones.**

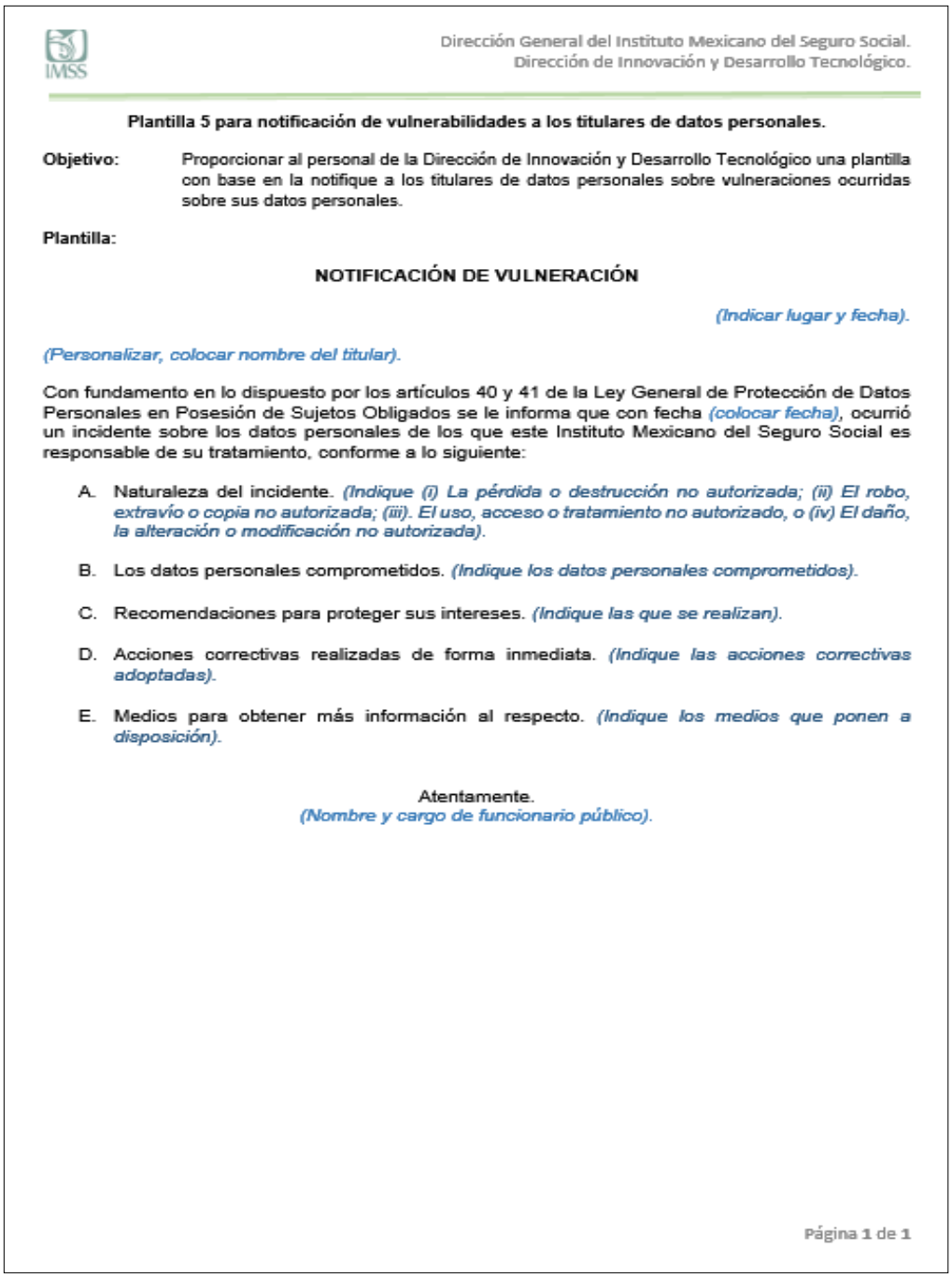
En esta sección se documentarán las vulneraciones ocurridas en materia de seguridad y las acciones ejecutadas en torno a ellas.

Vulneración 1	
Tipo de vulneración	*(Indique (i) La pérdida o destrucción no autorizada; (ii) El robo, extravío o copia no autorizada; (iii). El uso, acceso o tratamiento no autorizado, o (iv) El daño, la alteración o modificación no autorizada).*
Fecha de la vulnerabilidad	*(Fecha de la vulneración).*
Datos personales comprometidos y titular a quien corresponden.	*(Indique los datos personales comprometidos y los titulares de quien se relaciona).*
Descripción de la vulnerabilidad	*(Describa la vulneración).*
Motivo de la vulnerabilidad	*(Indique motivo de la vulneración).*
Recomendaciones al titular para proteger sus intereses.	*(Indique las que se realizan).*
Acciones correctivas	*(Indique las acciones correctivas adoptadas. Tip: Recuerde que dichas medidas deben adoptarse inmediatamente).*
Notificaciones realizadas	*(Indique las notificaciones realizadas, la fecha de las mismas y los documentos probatorios de tal notificación. Usted puede auxiliarse de la plantilla para la notificación de vulneración para realizar dicha notificación. Tip: Recuerde que, si se causa una afectación significativa a los derechos patrimoniales o morales del titular, debe notificarse al mismo y al INAI. En caso de no ameritar notificación, justifique aquí los motivos).*
Medios para obtener información	*(Indique los medios adoptados).*

Fuente: Elaboración propia con propuesta de intervención.

En caso de acontecer alguna vulneración en los datos personales, y se requiera efectuar la correspondiente notificación al titular afecto y al INAI, se presentan las siguientes plantillas.

Documento 43. Plantilla 5 para notificación de vulnerabilidades a los titulares de datos personales



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Plantilla 5 para notificación de vulnerabilidades a los titulares de datos personales.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico una plantilla con base en la notifique a los titulares de datos personales sobre vulneraciones ocurridas sobre sus datos personales.

Plantilla:

NOTIFICACIÓN DE VULNERACIÓN

(Indicar lugar y fecha).

(Personalizar, colocar nombre del titular).

Con fundamento en lo dispuesto por los artículos 40 y 41 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados se le informa que con fecha *(colocar fecha)*, ocurrió un incidente sobre los datos personales de los que este Instituto Mexicano del Seguro Social es responsable de su tratamiento, conforme a lo siguiente:

A. Naturaleza del incidente. *(Indique (i) La pérdida o destrucción no autorizada; (ii) El robo, extravío o copia no autorizada; (iii). El uso, acceso o tratamiento no autorizado, o (iv) El daño, la alteración o modificación no autorizada).*

B. Los datos personales comprometidos. *(Indique los datos personales comprometidos).*

C. Recomendaciones para proteger sus intereses. *(Indique las que se realizan).*

D. Acciones correctivas realizadas de forma inmediata. *(Indique las acciones correctivas adoptadas).*

E. Medios para obtener más información al respecto. *(Indique los medios que ponen a disposición).*

Atentamente.
(Nombre y cargo de funcionario público).

Página 1 de 1

Fuente: Elaboración propia con propuesta de intervención.

Documento 44. Plantilla 6 para notificación de vulnerabilidades al INAI

Plantilla 6 para notificación de vulnerabilidades al INAI.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico una plantilla con base en la notifique a los titulares de datos personales sobre vulneraciones ocurridas sobre sus datos personales.

Plantilla:

NOTIFICACIÓN DE VULNERACIÓN

(Indicar lugar y fecha).

Instituto Nacional de Transparencia y de Transparencia,
Acceso a la Información y Protección de Datos Personales.

Con fundamento en lo dispuesto por los artículos 40 y 41 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados se le informa que con fecha *(colocar fecha)*, ocurrió un incidente sobre los datos personales de los que este Instituto Mexicano del Seguro Social es responsable de su tratamiento, conforme a lo siguiente:

Tipo de vulneración	*(Indique (i) La pérdida o destrucción no autorizada; (ii) El robo, extravío o copia no autorizada; (iii). El uso, acceso o tratamiento no autorizado, o (iv) El daño, la alteración o modificación no autorizada).*
Fecha de la vulnerabilidad	*(Fecha de la vulneración).*
Datos personales comprometidos y titular a quien corresponden.	*(Indique los datos personales comprometidos y los titulares de quien se relaciona).*
Descripción de la vulnerabilidad	*(Describa la vulneración).*
Motivo de la vulnerabilidad	*(Indique motivo de la vulneración).*
Recomendaciones al titular para proteger sus intereses.	*(Indique las que se realizan).*
Acciones correctivas	*(Indique las acciones correctivas adoptadas. Tip: Recuerde que dichas medidas deben adoptarse inmediatamente).*
Notificaciones realizadas	*(Indique las notificaciones realizadas, la fecha de las mismas y los documentos probatorios de tal notificación. Usted puede auxiliarse de la plantilla para la notificación de vulneración para realizar dicha notificación. Tip: Recuerde que, si se causa una afectación significativa a los derechos patrimoniales o morales del titular, debe notificarse al mismo y al INAI. En caso de no ameritar notificación, justifique aquí los motivos).*
Medios para obtener información	*(Indique los medios adoptados).*

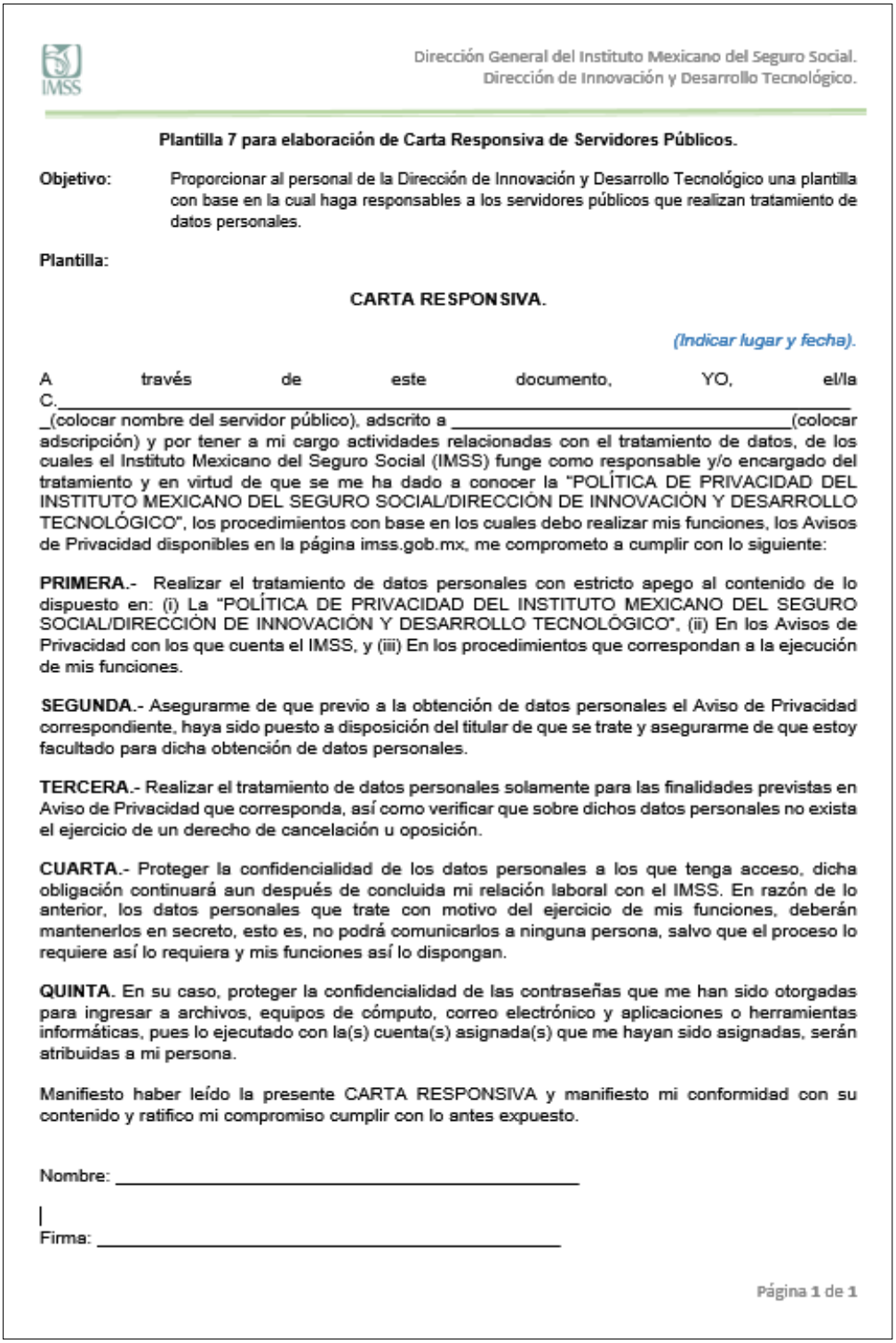
Lo anterior para los efecto conducentes.

Atentamente.
(Nombre y cargo de funcionario público).

Fuente: Elaboración propia con propuesta de intervención.

Por último, las medidas de seguridad implementadas deben garantizar, entre otras, la confidencialidad de los datos personales, por lo que como una de las medidas que se pueden adoptar es que los servidores públicos involucrados en el tratamiento de datos personales se comprometan a guardar la confidencialidad de los mismos y a observar cada una de las medidas implementadas por la Dirección de Innovación y Desarrollo Tecnológico. En razón de ello, a continuación, se presenta un formato de carta responsiva para que se documente que cada servidor público conoce de las acciones que debe seguir en materia de protección de datos personales.

Documento 45. Plantilla 7 para la elaboración de Carta Responsiva de Servidores Públicos



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Plantilla 7 para elaboración de Carta Responsiva de Servidores Públicos.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico una plantilla con base en la cual haga responsables a los servidores públicos que realizan tratamiento de datos personales.

Plantilla:

CARTA RESPONSIVA.

(Indicar lugar y fecha).

A través de este documento, YO, el/la C._____
_(colocar nombre del servidor público), adscrito a _____(colocar adscripción) y por tener a mi cargo actividades relacionadas con el tratamiento de datos, de los cuales el Instituto Mexicano del Seguro Social (IMSS) funge como responsable y/o encargado del tratamiento y en virtud de que se me ha dado a conocer la "POLÍTICA DE PRIVACIDAD DEL INSTITUTO MEXICANO DEL SEGURO SOCIAL/DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO", los procedimientos con base en los cuales debo realizar mis funciones, los Avisos de Privacidad disponibles en la página imss.gob.mx, me comprometo a cumplir con lo siguiente:

PRIMERA.- Realizar el tratamiento de datos personales con estricto apego al contenido de lo dispuesto en: (i) La "POLÍTICA DE PRIVACIDAD DEL INSTITUTO MEXICANO DEL SEGURO SOCIAL/DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO", (ii) En los Avisos de Privacidad con los que cuenta el IMSS, y (iii) En los procedimientos que correspondan a la ejecución de mis funciones.

SEGUNDA.- Asegurarme de que previo a la obtención de datos personales el Aviso de Privacidad correspondiente, haya sido puesto a disposición del titular de que se trate y asegurarme de que estoy facultado para dicha obtención de datos personales.

TERCERA.- Realizar el tratamiento de datos personales solamente para las finalidades previstas en Aviso de Privacidad que corresponda, así como verificar que sobre dichos datos personales no exista el ejercicio de un derecho de cancelación u oposición.

CUARTA.- Proteger la confidencialidad de los datos personales a los que tenga acceso, dicha obligación continuará aun después de concluida mi relación laboral con el IMSS. En razón de lo anterior, los datos personales que trate con motivo del ejercicio de mis funciones, deberán mantenerlos en secreto, esto es, no podrá comunicarlos a ninguna persona, salvo que el proceso lo requiere así lo requiera y mis funciones así lo dispongan.

QUINTA. En su caso, proteger la confidencialidad de las contraseñas que me han sido otorgadas para ingresar a archivos, equipos de cómputo, correo electrónico y aplicaciones o herramientas informáticas, pues lo ejecutado con la(s) cuenta(s) asignada(s) que me hayan sido asignadas, serán atribuidas a mi persona.

Manifiesto haber leído la presente CARTA RESPONSIVA y manifiesto mi conformidad con su contenido y ratifico mi compromiso cumplir con lo antes expuesto.

Nombre: _____

Firma: _____

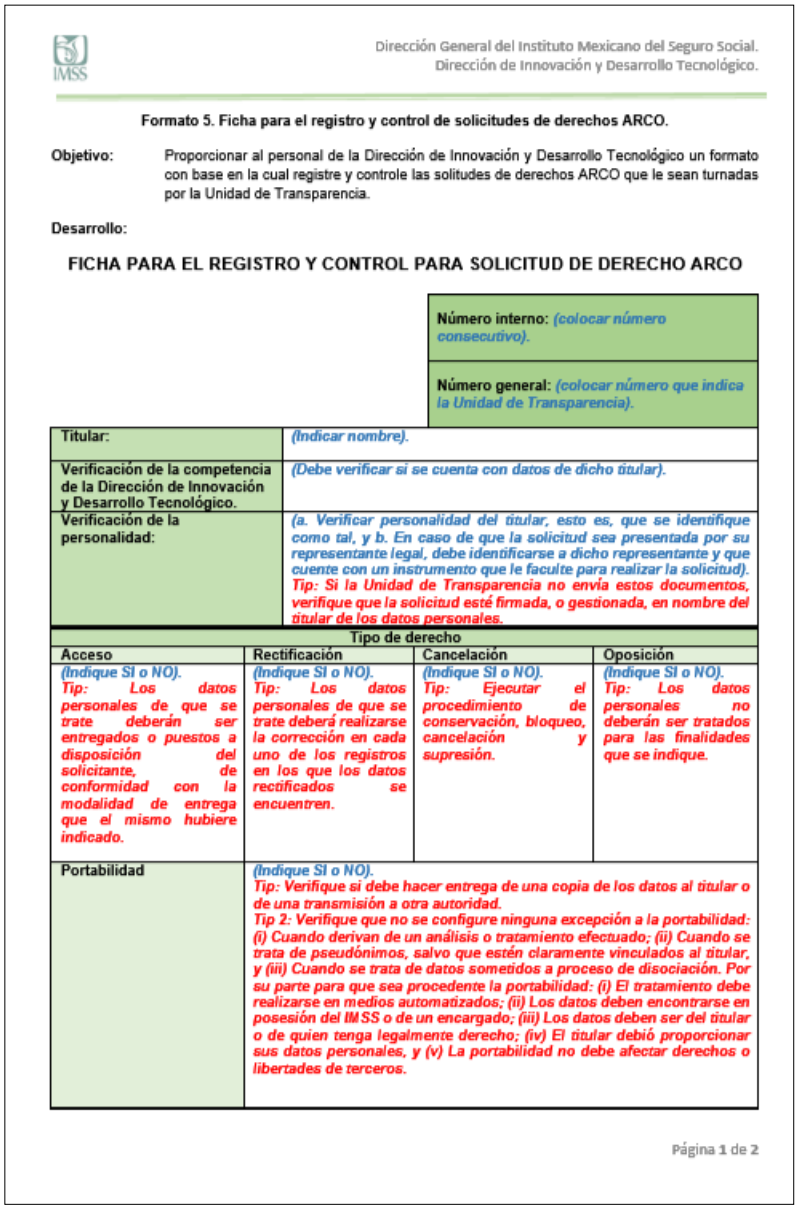
Página **1** de **1**

Fuente: Elaboración propia con propuesta de intervención.

3.2.6 Del ejercicio de derecho ARCO

La Unidad de Transparencia es la encargada de la gestión de las solicitudes ARCO, sin embargo, de aquéllos datos que sean tratados en la Dirección de Innovación y Desarrollo Tecnológico, dicha Unidad podrá realizarnos requerimientos de información, por ello, se presenta el siguiente formato que será auxiliar para el registro y control de cada solicitud que nos sea turnada.

Documento 46. Formato 5. Ficha para el registro y control de solicitudes de derechos ARCO, página 1



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Formato 5. Ficha para el registro y control de solicitudes de derechos ARCO.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico un formato con base en la cual registre y controle las solitudes de derechos ARCO que le sean turnadas por la Unidad de Transparencia.

Desarrollo:

FICHA PARA EL REGISTRO Y CONTROL PARA SOLICITUD DE DERECHO ARCO

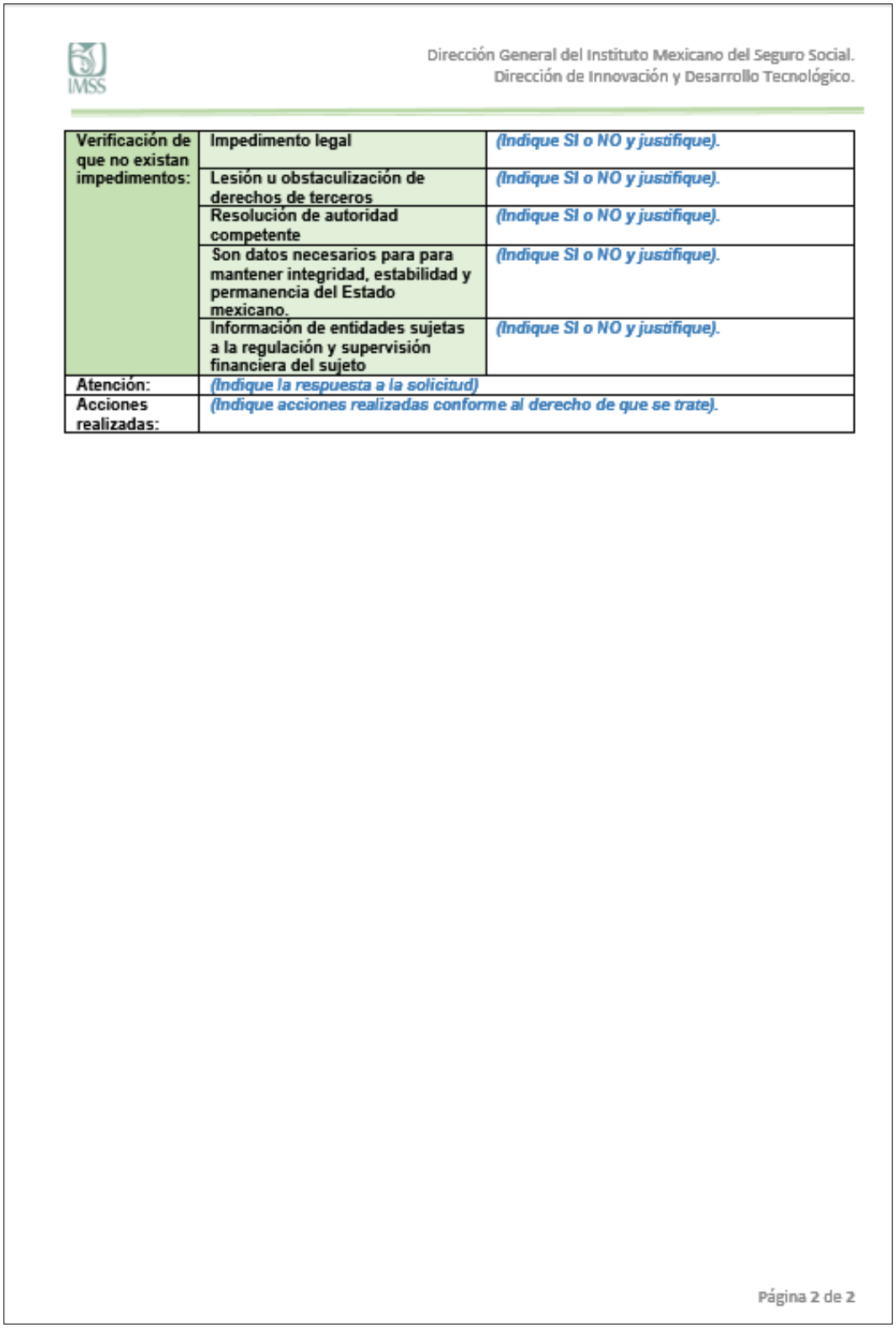
	Número interno: *(colocar número consecutivo).*
	Número general: *(colocar número que indica la Unidad de Transparencia).*
Titular:	*(Indicar nombre).*
Verificación de la competencia de la Dirección de Innovación y Desarrollo Tecnológico.	*(Debe verificar si se cuenta con datos de dicho titular).*
Verificación de la personalidad:	*(a. Verificar personalidad del titular, esto es, que se identifique como tal, y b. En caso de que la solicitud sea presentada por su representante legal, debe identificarse a dicho representante y que cuente con un instrumento que le faculte para realizar la solicitud). Tip: Si la Unidad de Transparencia no envía estos documentos, verifique que la solicitud esté firmada, o gestionada, en nombre del titular de los datos personales.*

Tipo de derecho			
Acceso	**Rectificación**	**Cancelación**	**Oposición**
(Indique SI o NO). Tip: Los datos personales de que se trate deberán ser entregados o puestos a disposición del solicitante, de conformidad con la modalidad de entrega que el mismo hubiere indicado.	*(Indique SI o NO). Tip: Los datos personales de que se trate deberá realizarse la corrección en cada uno de los registros en los que los datos rectificados se encuentren.*	*(Indique SI o NO). Tip: Ejecutar el procedimiento de conservación, bloqueo, cancelación y supresión.*	*(Indique SI o NO). Tip: Los datos personales no deberán ser tratados para las finalidades que se indique.*
Portabilidad	*(Indique SI o NO). Tip: Verifique si debe hacer entrega de una copia de los datos al titular o de una transmisión a otra autoridad. Tip 2: Verifique que no se configure ninguna excepción a la portabilidad: (i) Cuando derivan de un análisis o tratamiento efectuado; (ii) Cuando se trata de pseudónimos, salvo que estén claramente vinculados al titular, y (iii) Cuando se trata de datos sometidos a proceso de disociación. Por su parte para que sea procedente la portabilidad: (i) El tratamiento debe realizarse en medios automatizados; (ii) Los datos deben encontrarse en posesión del IMSS o de un encargado; (iii) Los datos deben ser del titular o de quien tenga legalmente derecho; (iv) El titular debió proporcionar sus datos personales, y (v) La portabilidad no debe afectar derechos o libertades de terceros.*		

Página 1 de 2

Fuente: Elaboración propia con propuesta de intervención.

Documento 47. Formato 5. Ficha para el registro y control de solicitudes de derechos ARCO, página



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

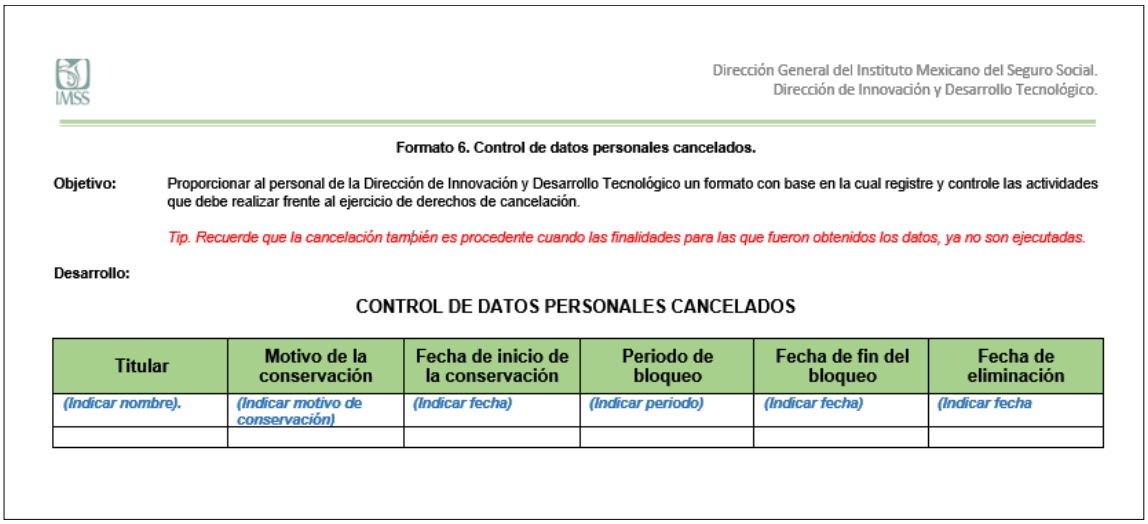
Verificación de que no existan impedimentos:	**Impedimento legal**	***(Indique SI o NO y justifique).***
	Lesión u obstaculización de derechos de terceros	***(Indique SI o NO y justifique).***
	Resolución de autoridad competente	***(Indique SI o NO y justifique).***
	Son datos necesarios para para mantener integridad, estabilidad y permanencia del Estado mexicano.	***(Indique SI o NO y justifique).***
	Información de entidades sujetas a la regulación y supervisión financiera del sujeto	***(Indique SI o NO y justifique).***
Atención:	***(Indique la respuesta a la solicitud)***	
Acciones realizadas:	***(Indique acciones realizadas conforme al derecho de que se trate).***	

Página 2 de 2

Fuente: Elaboración propia con propuesta de intervención.

Ahora bien, en caso de la procedencia de un derecho de cancelación activa el procedimiento de conservación, bloqueo, cancelación y supresión, por lo que debe tenerse un control estricto de los datos sometidos a dicho procedimiento, pues los datos personales ya no pueden ser tratados. En razón de ello se propone el siguiente formato.

Documento 48. Formato 6. Control de datos personales cancelados



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Formato 6. Control de datos personales cancelados.

Objetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico un formato con base en la cual registre y controle las actividades que debe realizar frente al ejercicio de derechos de cancelación.

Tip. Recuerde que la cancelación también es procedente cuando las finalidades para las que fueron obtenidos los datos, ya no son ejecutadas.

Desarrollo:

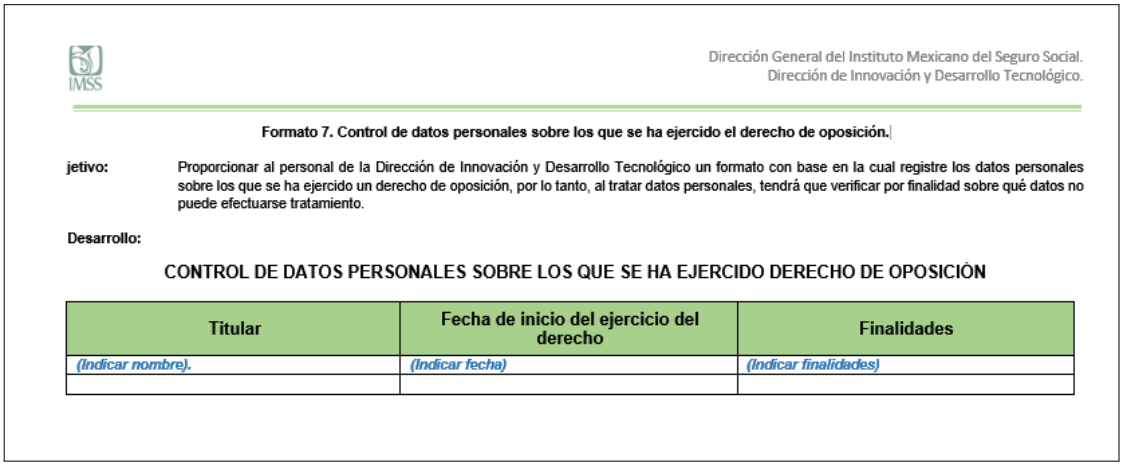
CONTROL DE DATOS PERSONALES CANCELADOS

Titular	Motivo de la conservación	Fecha de inicio de la conservación	Periodo de bloqueo	Fecha de fin del bloqueo	Fecha de eliminación
(Indicar nombre).	*(Indicar motivo de conservación)*	*(Indicar fecha)*	*(Indicar periodo)*	*(Indicar fecha)*	*(Indicar fecha*

Fuente: Elaboración propia con propuesta de intervención.

Por cuanto hace al derecho de oposición, también debe tenerse especial cuidado pues los datos no podrán ser tratados para las finalidades indicadas. Para controlar los datos personales sobre los que se ejercido el derecho de oposición, se propone el siguiente formato.

Documento 49. Control de datos sobre los que se ha ejercido el derecho de oposición



IMSS

Dirección General del Instituto Mexicano del Seguro Social.
Dirección de Innovación y Desarrollo Tecnológico.

Formato 7. Control de datos personales sobre los que se ha ejercido el derecho de oposición.

jetivo: Proporcionar al personal de la Dirección de Innovación y Desarrollo Tecnológico un formato con base en la cual registre los datos personales sobre los que se ha ejercido un derecho de oposición, por lo tanto, al tratar datos personales, tendrá que verificar por finalidad sobre qué datos no puede efectuarse tratamiento.

Desarrollo:

CONTROL DE DATOS PERSONALES SOBRE LOS QUE SE HA EJERCIDO DERECHO DE OPOSICIÓN

Titular	Fecha de inicio del ejercicio del derecho	Finalidades
(Indicar nombre).	*(Indicar fecha)*	*(Indicar finalidades)*

Fuente: Elaboración propia con propuesta de intervención.

Conclusiones

Conclusiones

1. El derecho a la protección a la vida privada de las personas es un derecho relativamente joven, el que a nivel internacional se encuentra en proceso de maduración. Dicho proceso ha sido acelerado en gran medida, gracias al Reglamento General de Protección de Datos de la Unión Europea, pues las relaciones con países a quienes les resulta aplicable y donde se encuentra involucrado el tratamiento de datos personales, han adoptado estándares que exigen a otros países, como es el caso de México, a adoptar medidas que demuestren que el tratamiento de datos personales se realiza conforme a dicho Reglamento.

2. México no es la excepción al proceso de madurez del derecho de la protección a la vida privada, el que si bien nación en el sector público, el que se garantizaba en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, también es cierto que fue la Ley Federal de Protección de Datos Personales en Posesión de Particulares, el instrumento normativo que impulsó la adopción de medidas por el sector privado, siendo está la base para la creación de la Ley General de Protección de Datos Personales.

3. Para garantizar la protección de los datos personales en el sector público, es necesario que cada sujeto obligado adopte una serie de medidas que den cumplimiento a principios, deberes y obligaciones que se encuentran establecidos en la normatividad aplicable en materia de protección de datos personales en posesión de sujetos obligados.

4. El INAI ha emitido un Programa Nacional de Protección de Datos Personales, el que contiene un plan de acción a efecto de que la protección de datos personales se garantice en el sector privado. Si bien es cierto que dichas acciones coadyuvan en la madurez de la protección de los datos personales, también es cierto que la normatividad es vigente, por lo tanto, hoy en día existe la posibilidad de que el tratamiento de datos personales se realice violando lo estipulado en la norma.

5. El instrumento propuesto en esta intervención se convertirá en un instrumento de apoyo para los sujetos obligados, los que si bien deben apegarse a lo que el

Programa indica, también pueden adoptar instrumentos que de inicio sean tendientes a garantizar la protección de datos personales en el sector público.

6. El instrumento aquí presentado, además de fungir como coadyuvante en que los sujetos obligados garanticen la protección de los datos personales que tienen que tratar en su calidad de responsables y/o encargados del tratamiento, también es coadyuvante en la labor de los servidores públicos que operan en el día a día con el tratamiento de datos personales.

Dicho apoyo se traduce en optimización de los procesos hoy ya implementados y que los mismos se apeguen a la norma de protección de datos personales, pero además les brindará tranquilidad de que si el tratamiento de datos personales se realiza conforme a lo indica la ley, no se configurarán las consecuencias de violación a la misma, las que como ya vimos, pueden costar hasta la inhabilitación del ejercicio en el servicio público.

Bibliografía

- Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, disponible en *http://www.dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018.*
- Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, disponible en *http://dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018.*
- Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias, disponible en *https://www.dof.gob.mx/nota_detalle.php?codigo=5532585&fecha=23/07/2018.*
- BASTERRA, Marcela I., *Protección de Datos Personales,* Buenos Aires, UNAM-EDIAR, 2008.
- CABALLERO GEA, José Alfredo, *Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen. Derecho de Rectificación. Calumnia e Injuria,* España, Dykinson, 2007.
- CABEZUELO ARENAS, Ana Laura, *Derecho a la Intimidad*, España, Tirant lo Blanch, 1998.
- CAMPUZANO TOME, Herminia, *Vida Privada y Datos Personales*, España, Tecnos, 2000.
- Código Civil Federal, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/2_090318.pdf.*
- Código Fiscal de la Federación, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/8_241218.pdf.*

- Código Penal Federal, disponible en *www.ordenjuridico.gob.mx/Documentos/Federal/wo83048.doc.*
- Convención Americana de Derechos Humanos, disponible en *http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D1BIS.pdf.*
- Convención Europea de Derechos Humanos, disponible en *https://www.echr.coe.int/Documents/Convention_SPA.pdf.*
- Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, disponible en *https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Convenio108-19811.pdf.*
- Declaración Universal de Derechos Humanos, disponible en *https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf.*
- Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, disponible en *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_185_30abr09.pdf.*
- Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, disponible en *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf.*
- Decreto por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente, disponible en *http://www.dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018.*
- Dictamen de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, a través del documento

disponible en *http://legislacion.scjn.gob.mx/Buscador/Paginas/wfProcesoLegislativoCompleto.aspx?q=EI+gQjK83C7L/d/8KCB3tZtIjA0olo1k5kA5s0Az0/3mRsTKKxvwltTA+JdhcERhEgjwsdDRf54DN/Pn+oG4IQ.*

- Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, consultada el 31 de octubre de 2014, disponible en *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML.*
- Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales (23 de septiembre de 1980), disponibles en *https://www.oecd.org/sti/ieconomy/15590267.pdf.*
- ESCALANTE GONZALBO, Fernando, *El Derecho a la Privacidad*, México, IFAI, 2004.
- Exposición de motivos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, a través del documento disponible en *http://legislacion.scjn.gob.mx/Buscador/Paginas/wfProcesoLegislativoCompleto.aspx?q=EI+gQjK83C7L/d/8KCB3tZtIjA0olo1k5kA5s0Az0/3mRsTKKxvwltTA+JdhcERhRMt8zhqTkHuyE1MiNvj8vg.*
- GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la era del Big Data y la computación ubicua,* España, Dykinson., 2016, disponible en *https://books.google.com.mx/books?id=qxkJDAAAQBAJ&pg=PA75&lpg=PA75&dq=derecho+a+estar+s%C3%B3lo+cooley&source=bl&ots=kbIJe9DxxT&sig=ACfU3U1H-aUDFrJNQBpi-ZdEzJkvj1Jc5A&hl=es-419&sa=X&ved=2ahUKEwiF-efai8nhAhVPtZ4KHb7JB2UQ6AEwAnoECAkQAQ#v=onepage&q=derecho%20a%20estar%20s%C3%B3lo%20cooley&f=false.*
- GARRIGA DOMÍNGUEZ, Ana, *Tratamiento de Datos Personales*, 21. ed., España, Dykinson, 2008.
- Iniciativa que reforma el artículo 6 de la Constitución Política de los

Estados Unidos Mexicanos, disponible en *https://www.ctainl.org.mx/descargas/IniciativaGacetaParlamentaria[1].pdf.*

- LAJE, Agustín, *Derecho a la Intimidad*, Buenos Aires-Bogotá, Astrea, 2014.
- Ley de Información Estadística y Geográfica, disponible en *http://www.diputados.gob.mx/LeyesBiblio/abro/lieg/LIEG_abro.pdf.*
- Ley del Seguro Social, disponible en *http://www.imss.gob.mx/sites/all/statics/pdf/leyes/LSS.pdf.*
- Ley Federal de Protección al Consumidor, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/113_120419.pdf.*
- Ley Federal de Protección de Datos Personales en Posesión de Particulares, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.*
- Ley Federal de Telecomunicaciones, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_020419.pdf.*
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, a través del documento disponible en *https://www.dof.gob.mx/nota_detalle.php?codigo=727870&fecha=11/06/2002.*
- Ley General de Salud, disponible en *http://www.salud.gob.mx/cnts/pdfs/LEY_GENERAL_DE_SALUD.pdf.*
- Ley General de Transparencia y Acceso a la Información Pública, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf.*
- Ley Orgánica de la Administración Pública Federal, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/153_120419.pdf.*
- Lineamientos de Protección de Datos Personales, a través del documento disponible en *http://dof.gob.mx/nota_detalle.php?codigo=2093669&fecha=30/09/2005.*
- Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicación en el Diario Oficial de la Federación en

http://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018.

- Lineamientos Generales de Protección de Datos Personales para el Sector Público, disponibles en *https://colaboracion.uv.mx/rept/files/2018/08/066/LinamientosGeneralesDatosPersonales.pdf.*
- Lineamientos para la elaboración, ejecución y evaluación del Programa Nacional de Protección de Datos Personales, disponibles en *http://dof.gob.mx/nota_detalle.php?codigo=5436058&fecha=04/05/2016.*
- Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de los datos personales, disponibles en *http://www.dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018.*
- LÓPEZ MARTÍN, Gemma Ana y Chichón Álvarez, Javier, *Nuevos retos y amenazas a ala protección de los derechos humanos en la era de la globalización*, España, Tirant lo Blanch, 2016.
- LÓPEZ-VIDRIERO TEJEDOR, Iciar y Santos Pascual, Efrén, *Protección de Datos Personales. Manual práctico para empresas*, España, FC Editorial e ICEF Consultores, 2000.
- Marco de Privacidad de la APEC, disponible en *https://sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf.*
- Marco de Privacidad de la OCDE, disponible en *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.*
- MEJÁN, Luis Miguel, *El Derecho a la Intimidad y la Informática*, México, Porrúa, 1994.
- MICHEL, James, *Privacy and Human Rights*, Gran Bretaña, UNESCO, 1994.
- MURILLO DE LA CUEVA, Pablo, *El Derecho a la Autodeterminación Informativa,* España, Tecnos, 1990.

- Pacto Internacional de Derechos Civiles y Políticos, disponible en *www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D47.pdf.*
- PENDÁS, Benigno y BASELGA, Pilar, *Samuel Warren y Luis Brandeis. El derecho a la intimidad,* España, Civitas, 1995.
- Plan Nacional de Desarrollo 2007-2012, a través del documento disponible en *http://pnd.calderon.presidencia.gob.mx/pdf/PND_2007-2012.pdf.*
- Proceso legislativo de reforma al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, a través del documento disponible en *https://www.sitios.scjn.gob.mx/constitucion1917-2017/sites/default/files/CPEUM_1917_CC/procLeg/185%20-%2030%20ABR%202009.pdf.*
- Programa Nacional de Protección de Datos Personales, disponible en *http://www.dof.gob.mx/nota_detalle.php?codigo=5511542&fecha=26/01/2018.*
- Protocolo adicional de Convenio No. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos, disponible en *http://transparencia.udg.mx/sites/default/files/Protocolo%20adicional%20del%20convenio%20No.%20108.pdf.*
- REBOLLO DELGADO, Lucrecio, *El Derecho Fundamental a la Intimidad*, España, Dykinson, 2000.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, disponible en *http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf.*
- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, a través del documento disponible en *http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf.*
- Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, disponible en *https://europass.cedefop.europa.eu/sites/default/files/regulation-es.pdf.*

- SALDAÑA, María, “Derecho a la Privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales”, *Revista UNED. Teoría y Realidad Constitucional*, España, núm. 28, 2011, disponible en *https://dialnet.unirioja.es/descarga/articulo/3883001.pdf* y *http:///revistas.uned.es/index.php/TRC/article/view/6960.*
- TENORIO CUETO, Gillermo, Coordinador, *Los Datos Personales en México,* México, Porrúa y Universidad Panamericana, 2012.
- VILLANUEVA, Ernesto y Nucci, Hilda, *Comentarios a la Ley Federal de Protección de Daatos Personales en Posesión de los Particulares*, México, Novum, 2012.
- WACKS, Raymond, *Privacy. A very short introduction*, 3a. ed., Gran Bretaña, Oxford, 2015.