MÉXICO
GOBIERNO DE LA REPÚBLICA

DIRECCIÓN JURÍDICA
ÓRGANO INTERNO DE CONTROL EN EL IMSS
DIVISIÓN DE ADMINISTRACIÓN DE DOCUMENTOS

IMSS

OFICIO No. 0952174000/ 276

OFICIO No. 00641/30.1/ 254 /2018

OFICIO No. 09B5446119C4/2018000243

Ciudad de México, a 02 de agosto de 2018

C.C. SECRETARIO GENERAL, DIRECTORAS
Y DIRECTORES NORMATIVOS
Presentes

En cumplimiento a lo establecido en el artículo 30, fracciones I y II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que establece entre las acciones que deberán realizar los responsables del tratamiento de datos personales para cumplir con el principio de responsabilidad, se encuentra la elaboración de las Políticas y Programas de Protección de Datos Personales, obligatorias y exigibles al interior de este Instituto Mexicano del Seguro Social.

Al respecto, con las aportaciones de las Direcciones Normativas y sus correspondientes Enlaces en Transparencia, el Comité de Transparencia elaboró el Programa de Protección de Datos Personales 2018 para el Instituto Mexicano del Seguro Social, el cual regula los deberes que nos asisten como Sujeto Obligado, responsable del tratamiento de datos personales.

El presente Programa es de observancia obligatoria para todas las Unidades Administrativas de Nivel Central y Delegacionales, así como para las Unidades Médicas de 1°, 2° y 3er Nivel de atención, en los procesos en los que se manejen datos personales, incluyendo los Fideicomisos que son administrados por el Instituto.

Como una de las primeras tareas que establece el Programa es el inventario de Datos Personales, a través del cual deberán identificar los tratamientos de datos personales que realicen, precisando la información que obtienen y el ciclo de vida de ésta, dicha actividad permitirá cumplir de manera puntual con las obligaciones subsecuentes que en el mismo se establece.

Programa de Protección de Datos Personales 2018

Instituto Mexicano del Seguro Social

CONTENIDO

GLOSARIO DE TÉRMINOS COMUNES

Activo: La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para el Instituto;

Áreas: Instancias del IMSS cuyas facultades se encuentran establecidas en los respectivos reglamentos interiores, manuales de organización y demás instrumentos normativos, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

Aviso de privacidad: Documento a disposición del titular de la información de forma física, electrónica o en cualquier formato generado por el IMSS y sus áreas, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

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;

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;

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

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;

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;

Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable;

Instituto: Instituto Mexicano del Seguro Social (IMSS).

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Medidas compensatorias: Cuando sea imposible para el responsable dar a conocer a los titulares el aviso de privacidad simplificado de manera directa, o ello exija esfuerzos desproporcionados, se podrán instrumentar mecanismos alternos de conformidad con lo previsto en los "*Criterios Generales para la Instrumentación de Medidas Compensatorias en el Sector Público del Orden Federal, Estatal y Municipal*", emitidos por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, para su difusión por medios masivos de comunicación u otros de amplio alcance.

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;

Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública;

Responsable: Entiéndase al IMSS, las áreas que lo conforman, así como los fideicomisos y fondos administrados por el Instituto, éstos últimos a través de la Coordinación Normativa responsable de coordinar su operación.

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

Titular: La persona física a quien corresponden los datos personales;

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, y

Unidad de Transparencia: Instancia dentro del Instituto a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

PRESENTACIÓN

De manera general, podemos entender a la Seguridad Social como la más amplia expresión de solidaridad humana entre los trabajadores; institucionalizada con el propósito de proteger su salud, su vida y su nivel de ingreso y el de sus familias, frente a los riesgos inherentes de la vida misma: la incapacidad, la enfermedad y la muerte[1]. Esta concepción de la seguridad social ha convertido al Instituto Mexicano del Seguro Social (IMSS), en la institución con mayor presencia en la atención a la salud y en la protección social de los mexicanos desde su fundación el 19 de enero de 1943, e inicio de operación el 01 de enero de 1944, protegiendo desde entonces a los trabajadores formales y otros sujetos de aseguramiento, para ello, combina la investigación y la práctica médica, con la administración de los recursos para el retiro de sus asegurados, con el fin de brindar tranquilidad y estabilidad a los trabajadores y sus familias, ante cualquiera de los riesgos especificados en la Ley del Seguro Social.

La seguridad social, como ha quedado de manifiesto, tiene por finalidad garantizar el derecho a la salud, la asistencia médica, la protección de los medios de subsistencia y los servicios sociales necesarios para el bienestar individual y colectivo, así como el otorgamiento de una pensión que, en su caso y previo cumplimiento de los requisitos legales, será garantizada por el Estado[2]; motivos suficientes por los cuales hoy en día, más de la mitad de la población mexicana, tiene relación con el IMSS; lo anterior es así, toda vez que al cierre del año 2016, el número de adscripciones al Instituto ascendió a 54 millones de derechohabientes. Por su parte, IMSS-PROSPERA brindó cobertura en salud a 12.3 millones de personas sin acceso a seguridad social.
Ahora bien, acorde con las atribuciones conferidas al IMSS, la mayor parte de la información que recaba, es de carácter personal, ya que una gran parte de los individuos que se encuentran inscritos en el Instituto, han realizado algún trámite o utilizado algún servicio otorgado por éste y han tenido que proporcionar sus datos.

---

[1] Ricardo García Sainz (2008)"A diez años de la reforma. Principios básicos de la seguridad social": Diez años de reformas a la seguridad social en México. Balance, perspectivas y propuestas. Rosario Ortiz Magallon (coordinadora) (pp 31-44) Centro de Producción Editorial. Consultado en https://archivos.juridicas.unam.mx/www/bjv/libros/7/3485/14.pdf
[2] Artículo 2 de la Ley del Seguro Social.

En este orden de ideas, considerando que la protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental, nuestra Constitución ha incorporado el **derecho de protección de datos personales**, primero en posesión de particulares y recientemente en posesión de sujetos obligados; cuyo bien jurídico tutelado son la privacidad y la intimidad.

Con el fin de equilibrar los mencionados bienes jurídicos de privacidad e intimidad, entre toda persona y aquellas instituciones públicas o entes privados que por sus actividades o funciones recaban o colectan datos personales, surgió el concepto de autodeterminación informativa o la protección de los datos personales. Bajo este supuesto, el titular o dueño de dichos datos tiene el derecho y la libertad de elegir qué desea comunicar, cuándo, a quién, y sobre todo, puede mantener el control sobre su información personal.[3]

Con la aprobación de las reformas a los artículos 6, 16 y 73 Constitucionales, se reconoce y regula el derecho a la protección de datos personales, plasmando los **derechos de acceso, rectificación, cancelación y oposición, denominados por su acrónimo derechos ARCO**.

En consecuencia a dichas reformas, el 26 de enero de 2017, se publicó en el Diario Oficial de la Federación la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)** cuyo objeto es 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, aplicable a cualquier tratamiento de datos personales que obre en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Por lo anterior, el IMSS al ser Sujeto Obligado de la LGPDPPSO, debe implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la propia Ley, así como rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y

[3] Myrna Elia García Barrera (2010), "La nueva Ley Federal de Protección de Datos Personales en Posesión de los particulares; pros y contras": Memorias XIV Congreso Iberoamericano de Derecho e Informática, Tomo 2. Dr. José Luis Prado Maillard (Director Facultad de Derecho y Criminología) (pp 830 a 848) Universidad Autónoma de Nuevo León.

organismos garantes, según corresponda, observando en todo momento la Constitución Política de los Estados Unidos Mexicanos y los Tratados Internacionales en los que el Estado Mexicano sea parte.

El artículo 30 de la LGPDPPSO, establece entre las acciones que deberán realizar los responsables del tratamiento de datos personales para cumplir con el principio de responsabilidad, las siguientes:

- Elaboración de **políticas y programas de protección de datos personales**, obligatorios y exigibles al interior de la organización del responsable, y destinar recursos necesarios para la implementación de dichos programas y políticas.

- Poner en práctica un **programa de capacitación y actualización del personal** sobre las obligaciones y demás deberes en materia de protección de datos personales;

- **Revisar periódicamente las políticas y programas de seguridad de datos personales** para determinar las modificaciones que se requieran;

- 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;

- 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.

Esto implica el desarrollo de un **Programa de Protección de Datos Personales Institucional**, mismo que deberá construirse con base en un **sistema de gestión para la protección de los datos personales**, entendido como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y

seguridad de los datos personales, de conformidad con lo previsto en la LGPDPPSO y las demás disposiciones que le resulten aplicables en la materia.

Por tanto, el presente documento responde a la necesidad de dar cumplimiento a las disposiciones previstas en la referida LGPDPPSO y regular los deberes que asisten al IMSS como responsable del tratamiento de datos personales.

1. OBJETIVOS DEL PROGRAMA

Para el desarrollo de este **Programa de Protección de Datos Personales del IMSS**, se enlistan los siguientes objetivos:

1. Proveer de los elementos y actividades de dirección, operación y control de los procesos del Instituto, que permitan proteger de manera sistemática y continua los datos personales que estén en su posesión.

2. Establecer los mecanismos para cumplir con las obligaciones que establece la LGPDPPSO, así como la normatividad que deriva de la misma.

3. Elaborar y coordinar diversos programas de capacitación y actualización del personal del Instituto sobre las obligaciones y demás deberes en materia de protección de datos personales.

4. Promover la adopción de mejores prácticas en la protección de datos personales, una vez que el programa haya alcanzado un nivel de madurez adecuado, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

5. Implementar un sistema de gestión de seguridad de los datos personales, el cual permita planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales.

2. RESPONSABILIDADES

Con fundamento en lo dispuesto por los artículos 83 y 84, fracción I de la LGPDPPSO, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

1. Elaborar el Programa en conjunto con los Enlaces Normativos en materia de Transparencia;

2. Proponer cambios y mejoras a partir de la experiencia de su implementación;

3. Dar a conocer el Programa al interior;

4. Coordinar la implementación del Programa;

5. Asesorar a las unidades administrativas respecto de su implementación, cuando así lo soliciten;

6. Las demás que de manera expresa se señalen en el presente Programa.

La implementación del Programa será de observancia obligatoria de todos los servidores públicos del IMSS, incluyendo los fideicomisos y fondos que son administrados por éste y que de acuerdo con el Padrón de Sujetos Obligados 2018, son considerados como Sujetos Obligados sin estructura, los cuales cumplen con sus obligaciones en materia de transparencia a través de la Dependencia o Entidad a la que pertenecen.

Las Direcciones Normativas, serán responsables de coordinar la operación del Programa y tendrán presente, en todo momento, que **los datos personales son propiedad de las personas a las que se refieren y que sólo ellas pueden decidir sobre los mismos**. En este sentido, harán uso de ellos sólo para aquellas finalidades para las que se encuentran debidamente facultados, respetando en todo momento los principios que establece la LGPDPPSO sobre protección de datos personales.

3. ALCANCES DEL PROGRAMA

El Programa de Protección de Datos Personales del IMSS, tiene como alcance la protección de los datos personales y su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Por lo cual el análisis de riesgo y las medidas de seguridad implementadas, se deberá enfocar en la protección de datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, así como en evitar las vulneraciones descritas en el artículo 38 de la LGPDPPSO.

El presente programa aplicará a todas las unidades administrativas del Instituto Mexicano del Seguro Social y a todos los tratamientos de datos personales que éstas realicen en ejercicio de sus atribuciones.

Asimismo, en virtud de que uno de los objetivos del Programa es cumplir con las obligaciones establecidas en la LGPDPPSO, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento.

Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren la Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública.

Las unidades administrativas que forman parte del IMSS, que deberán observar el Programa son las siguientes:

1. Dirección General
2. Dirección de Administración
3. Dirección de Finanzas
4. Director de Incorporación y Recaudación
5. Dirección de Innovación y Desarrollo Tecnológico
6. Dirección de Prestaciones Económicas y Sociales

7. Dirección de Prestaciones Médicas
8. Dirección de Vinculación Institucional y Evaluación de Delegaciones
9. Dirección de Planeación Estratégica Institucional
10. Dirección Jurídica
11. Secretaría General
12. Delegaciones Estatales y Regionales
13. Fideicomiso de Administración de Teatros y Salas de Espectáculos
14. Fideicomiso de Beneficios Sociales
15. Fideicomiso de Investigación en Salud
16. Fideicomiso Irrevocable de Administración e Inversión Niña del Milenio
17. Fideicomiso para el Desarrollo del Deporte No. 4611-1
18. Fondo de Fomento a la Educación
19. Fideicomiso para Ayudas Extraordinarias con motivo del incendio de la Guardería ABC

El listado comprende a las Direcciones Normativas, así como a los Fondos y Fideicomisos que son administrados por el IMSS, en el entendido de que estos son los responsables de coordinar la operación del Programa al interior de sus áreas y en sus representaciones delegacionales.

El presente Programa se desarrolla con base en el sistema de gestión para la protección de los datos personales Institucional, encuentra su fundamento legal en la normatividad siguiente:

- Fracciones II y III del apartado A del artículo 6; Segundo párrafo del artículo 16, así como la fracción XXIX-S del artículo 73, todos de la Constitución Política de los Estados Unidos Mexicanos.

- Artículo 30 y fracciones I, IV, V y VII del artículo 84 de Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

- Artículos 46 y 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

- Artículo 22 de la Ley del Seguro Social.

4. PRINCIPIOS DE PROTECCIÓN DE LOS DATOS PERSONALES

Licitud. Todo responsable, en el ámbito de su competencia, debe llevar a cabo el tratamiento de datos personales de forma lícita, esto es, respetando la legislación aplicable y los derechos y libertades de las personas. En ese sentido, el responsable sólo podrá hacer con los datos personales aquello que esté legalmente permitido.

Finalidad. El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades concretas, explícitas, lícitas y legítimas del responsable del tratamiento. La finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

Lealtad. La obtención y el tratamiento de datos personales no debe valerse del engaño o fraude, de forma tal que la persona no pueda conocer con propiedad los términos y condiciones vinculados a ese tratamiento. Es decir, la obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos, lo que implica que:

- No se recaben datos personales con dolo, mala fe o negligencia;
- Se deberá privilegiar la protección de los intereses del titular;
- No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado; y
- Se informen todas las finalidades del tratamiento en el aviso de privacidad.

Consentimiento. Como regla general, los datos personales sólo podrán ser tratados con el consentimiento de su titular. La manifestación de la voluntad del titular debe ser libre, informada y específica. La solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.

Calidad. Los datos personales deben ser exactos, completos, pertinentes, actualizados y correctos para el cumplimiento de las finalidades para las que sean tratados, asimismo, deben ser suprimidos una vez que se cumplan o agoten las finalidades para las cuales fueron recabados.

- Los datos personales son **exactos** cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles. Por ejemplo, un dato no sería exacto si se registra en la base de datos que una persona cuenta con Doctorado en Derecho, si el título que en realidad tiene es una Maestría en Derecho.

- Los datos personales están **completos** cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular. Por ejemplo, los datos de salud del titular están completos cuando el expediente médico contiene todos los documentos clínicos e información que debe estar integrada al mismo.

- Los datos personales son **pertinentes** cuando corresponden efectivamente al titular. Por ejemplo, los datos del adeudo son pertinentes cuando corresponden al deudor y no a una homonimia.

- Los datos están **actualizados** cuando están al día y corresponden a la situación real del titular. Por ejemplo, el número telefónico que se tiene registrado en la base de datos está actualizado cuando, efectivamente, corresponde al titular con el que está vinculado.

- Los datos personales son **correctos** cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

Proporcionalidad. El tratamiento de datos personales debe circunscribirse a aquéllos que resulten adecuados, relevantes y no excesivos con relación a las finalidades que justificaron su obtención.

El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron, las cuales, como se señaló anteriormente, deben estar previstas en el aviso de privacidad.

Información. Toda utilización de datos personales debe ser informada al titular, de tal manera que comprenda los términos generales y particulares de los usos a que será sometida su información.

Por virtud de este principio, los responsables se encuentran obligados a informar a los titulares de los datos personales, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del Aviso de privacidad. En ese sentido, todo responsable que trate datos personales, sin importar la actividad que realice, requiere elaborar y poner a disposición los avisos de privacidad que correspondan a los tratamientos que lleven a cabo.

Es importante tomar en cuenta que con independencia de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el Aviso de privacidad.

Asimismo, resulta pertinente aclarar que los responsables deben tener el número de Avisos de privacidad que resulten necesarios de acuerdo con los tipos de tratamientos que realicen. La puesta a disposición del Aviso de privacidad implica hacer del conocimiento del titular dicho documento.

Cuando sea imposible dar a conocer a los titulares el Aviso de privacidad simplificado de manera directa, o ello exija esfuerzos desproporcionados, se podrá recurrir a medidas compensatorias para darlo a conocer a través de su difusión en medios masivos de comunicación u otros mecanismos de amplio alcance, observando en todo momento lo dispuesto en los "*Criterios Generales para la Instrumentación de Medidas Compensatorias en el Sector Público del Orden Federal, Estatal y Municipal*", emitidos por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Responsabilidad. El responsable deberá adoptar políticas y está obligado a implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y obligaciones establecidas en la LGPDPPSO, así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares, como ante la autoridad garante.

El principio de responsabilidad cierra el círculo con relación a los principios que regulan la protección de los datos personales. A este principio se le conoce también como el principio de *"rendición de cuentas"*, ya que establece la obligación de los Responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante los titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales.

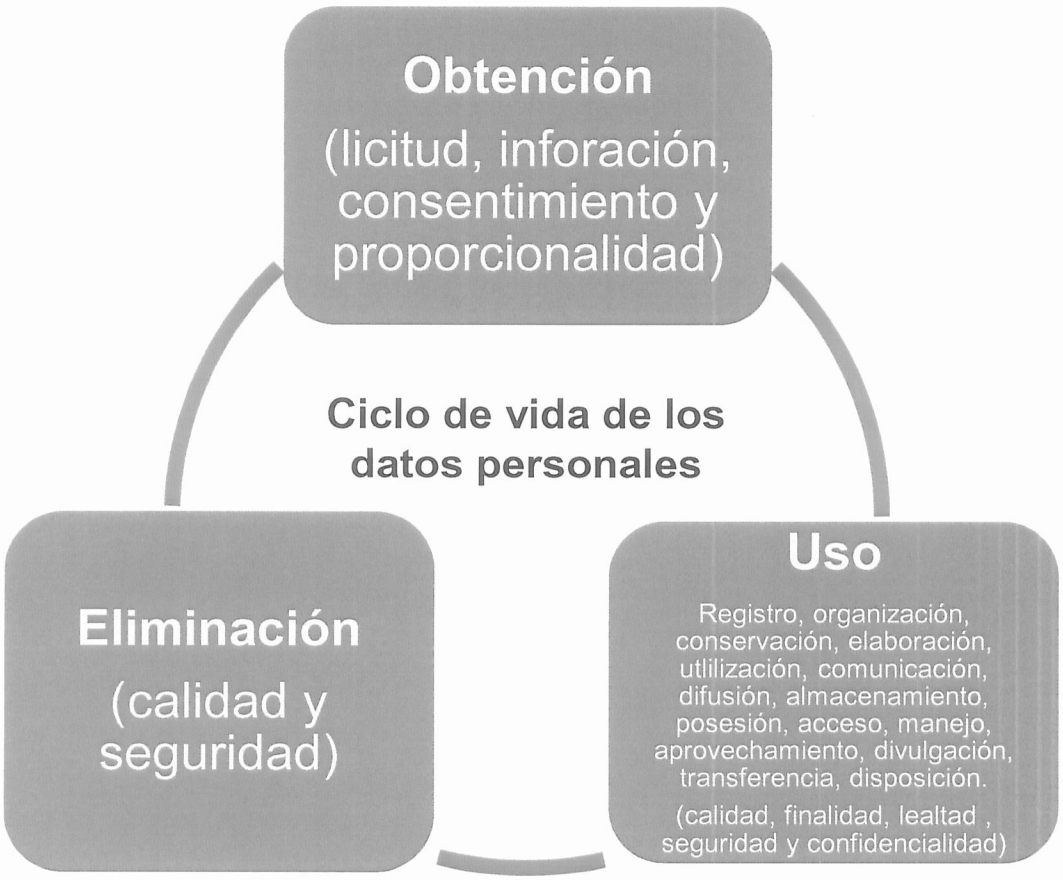
Bajo este principio, los responsables del tratamiento están obligados a velar por la protección de los datos personales aun y cuando los datos estén siendo tratados por encargados. Asimismo, este principio supone que el Responsable tome las medidas suficientes para que los términos establecidos en el aviso de privacidad sean respetados por aquéllos con los que mantenga una relación jurídica.

5. POLÍTICA DE GESTIÓN DE LOS DATOS PERSONALES

El tratamiento de datos personales que realicen las unidades administrativas deberá cumplir con los principios, deberes y obligaciones que establece la LGPDPPSO, para lo cual este programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

Asimismo, el IMSS procurará la adopción de mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan y según el nivel de madurez que exista.

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la LGPDPPSO, y según el ciclo de vida de los datos personales:



5.1 Inventario de tratamientos del IMSS

Para que sea posible el debido cumplimiento de las obligaciones que se establecen en el Programa de Protección de Datos Personales del IMSS, es necesario que cada una de las unidades administrativas realicen un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario de los tratamientos de datos personales que se realizan en el IMSS.

Por "inventario de tratamientos" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas del IMSS, realizado con orden y precisión.

El inventario de tratamientos incluirá el inventario de datos personales al que hace referencia la LGPDPPSO en los artículos 33, fracción III y 35, fracción I, e identificará los siguientes elementos relevantes:

1. ¿Qué tratamientos de datos personales realiza la unidad administrativa? Hay que identificar cada uno de los procesos en los que la unidad administrativa trata datos personales.

2. ¿Qué unidad administrativa está a cargo de estos procesos y que por tanto sea la administradora de las bases de datos o archivos que se generen con motivo de dichos tratamientos? Hay que identificar o definir si la unidad administrativa está a cargo del proceso en donde se tratan los datos personales, según las atribuciones o facultades normativas.

Podría ocurrir que una unidad administrativa trate datos personales recabados en el marco de un proceso del cual no es responsable. Por ejemplo, con motivo de una consulta, la unidad administrativa "X" podría tener acceso a datos de contacto del particular que realizó la consulta, sin embargo, la unidad administrativa que está a cargo del procedimiento de atención a consultas, y quien administra la base de datos de las consultas que recibe la institución es la unidad administrativa "Y".

Asimismo, podría darse el caso en que dos o más unidades administrativas estén a cargo de un proceso mediante el cual se recaban los datos personales y que administren las bases de datos correspondientes de manera conjunta.

En ese sentido, para definir quién está a cargo del proceso mediante el cual se recaban los datos personales y que, por tanto, administre las bases de datos o archivos correspondientes, es necesario analizar la función que realiza cada unidad administrativa dentro del proceso, y las atribuciones o facultades normativas que resulten aplicables.

3. Una vez que hayan sido identificados los tratamientos de los cuales está a cargo la unidad administrativa, será necesario identificar lo siguiente, de acuerdo con el ciclo de vida de los datos personales:

a. ¿Cómo se obtienen los datos personales?

- Directamente del titular
    - De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso.
    - Vía telefónica
    - Por correo electrónico
    - Por Internet o sistema informático
    - Por escrito presentado directamente en [nombre de la institución]
    - Por escrito enviado por mensajería
- Mediante una transferencia
    - Quién transfiere los datos personales y para qué fines
    - Medios por los que se realiza la transferencia
- De una fuente de acceso público

b. ¿Qué tipo de datos personales se tratan? ¿Son sensibles?

c. ¿Dónde se almacenan los datos personales?

- Sección, serie y subserie de archivos
- Formato en que se encuentra la base de datos: físico y/o electrónico
- Ubicación de la base de datos

d. ¿Para qué finalidades se utilizan los datos personales? Las finalidades son acciones más específicas de los procesos de los que derivan los tratamientos de datos personales. Por ejemplo, el procedimiento podría ser "recursos de revisión" y las finalidades "emitir los acuerdos y notificaciones correspondientes, y entrar en contacto con el recurrente con fines de orientación".

Será necesario identificar si se requiere el consentimiento o no de los titulares y el tipo de consentimiento (tácito o expreso y por escrito), y en caso de que no se requiera, definir qué supuestos (fracciones) del artículo 22 se actualizan.

Asimismo, se deberá señalar el marco jurídico que habilita para el tratamiento de datos personales (disposición normativa, artículo, fracción, inciso, párrafo).

e. ¿Quién tiene acceso a la base de datos o archivos y a quién se comunican los datos personales al interior del IMSS? Se deberá identificar el catálogo de servidores públicos al interior del IMSS que tienen acceso a los datos personales y para qué fin.

f. ¿Intervienen encargados en el tratamiento de los datos personales? Es necesario identificar el nombre del encargado y el número de contrato, pedido o convenio correspondiente.

g. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad? Hay que identificar las autoridades o terceros externos a [nombre de la institución] a quienes se comunican los datos personales y los fines de las transferencias.

Asimismo, es necesario señalar si se requiere el consentimiento para la transferencia, el tipo de consentimiento que se requiere en su caso (tácito o expreso y por escrito), y en caso de que no se

requiera el consentimiento, se deberá definir qué supuestos (fracciones) de los artículos 22, 66 o 70 se actualizan.

h. ¿Se difunden los datos personales? Hay que señalar si los datos personales se difunden y el fundamento jurídico para ello.

i. ¿Cuál es el plazo de conservación de los datos personales? Este plazo tendría que estar definido en los instrumentos de clasificación archivística, por lo que es necesario identificar a qué serie documental pertenecen los archivos o bases de datos en los que están contenidos los datos personales.

El diagnóstico se deberá realizar en la matriz correspondiente al Anexo 1 de este programa (Inventario de Tratamientos), y se deberá realizar por proceso.

Una vez que se haya realizado este diagnóstico inicial, estaremos preparados para cumplir de mejor manera con las obligaciones previstas en la LGPDPPSO.

5.2 Cumplimiento de obligaciones

Los datos personales que posee el IMSS, son indispensables para la prestación de servicios, trámites y procedimientos que se realizan a diario, por lo tanto, deben ser debidamente protegidos de una amplia gama de amenazas, a fin de garantizar la continuidad de las operaciones, minimizar el daño a la misma y ayudar a la toma de decisiones para aprovechar las oportunidades.

La información referente a datos personales existe y es transmitida en diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes o expuesta en una conversación. Cualquiera que sea la forma que adquiera la información o los medios por los cuales se distribuye o almacena, siempre debe estar protegida adecuadamente.

El tratamiento de datos personales implica realizar diversas operaciones, ya sean manuales o automatizadas, lo que permite recabar datos personales, registrarlos en una base de datos, modificarlos, consultarlos, utilizarlos, comunicarlos, bloquearlos o, incluso, destruirlos; por lo que para el tratamiento de dichos datos deberán cumplirse en todo momento las disposiciones sobre protección de estos.

Por lo tanto, para el tratamiento de datos personales, podemos identificar los siguientes momentos:

1. **Obtención**: Momento en el cual se recaban los datos del titular, ya sea que él mismo los proporcione, o a través de un tercero, mediante el uso de diversos medios (físicos o electrónicos).

2. **Uso**: Momento en el que los datos personales recabados se someten a diversos procedimientos, automatizados o no, de manera que son registrados en una base de datos, modificados, consultados o utilizados en cualquier forma.

Este momento supone la utilización de los datos personales, que puede ser interna o externa.

La utilización interna es cuando los datos personales son tratados por el responsable para cumplir con el propósito para el cual fueron recabados.

Hablamos de utilización externa en aquellos casos en los que los datos son compartidos con un tercero, es decir, se difunden o distribuyen a otra entidad. En este momento podemos distinguir entre la comunicación de datos o la dación de estos para la prestación de un servicio determinado al propio responsable.

3. **Eliminación, bloqueo y destrucción de los datos personales**: Momento en el cual los datos personales han dejado de ser necesarios para el cumplimiento de las finalidades previstas en el Aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, por lo que deberán ser Suprimidos, previo Bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Inventario de tratamiento de datos personales del IMSS

Un sistema de datos personales es el conjunto ordenado de éstos, a los que se puede acceder con base en un criterio determinado. Sobre este sistema se tendrán que cumplir las obligaciones que son exigidas por la normatividad vigente, tales como la adopción de medidas de seguridad.

En este orden de ideas, el criterio que determina la existencia de un sistema de datos personales **es el propósito con el que se tratan**, cumpliendo en todo momento los principios y obligaciones establecidas en la Ley, de manera que se garantice la privacidad del individuo cuyos datos personales son objeto de tratamiento.

Asimismo, con la finalidad de cumplir con lo establecido en el artículo 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el inventario de tratamiento de datos personales, deberá contener los siguientes elementos:

I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales.

II. La finalidad de cada tratamiento de datos personales.

III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;

IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.

V. La lista de Servidores Públicos que tienen acceso a los sistemas de tratamiento.

VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable.

VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifica éstas.

Motivo por el cual, se vuelve indispensable el apoyo de las diferentes áreas normativas, de operación administrativa desconcentrada y médicas del Instituto, con el fin de actualizar de manera permanente los datos que constituyen el inventario de tratamiento de datos personales.

Aunado a lo anterior, el referido inventario deberá considerar el ciclo de vida de los datos personales conforme a los siguientes aspectos:

- ✓ La obtención de los datos personales.

- ✓ El almacenamiento de los datos personales.

- ✓ El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin.

- ✓ La divulgación de los datos personales considerando las remisiones y transferencias que se efectúen.

- ✓ El bloqueo de los datos personales en su caso.

- ✓ La cancelación, supresión o destrucción de los datos personales.

Se deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal o cualquier otro recurso humano o material que resulte pertinente considerar.

Cumplimiento de obligaciones (entre ellos, obtención, uso y eliminación de datos personales)

La misión del IMSS es ser el instrumento básico de la seguridad social, establecido como un servicio público de carácter nacional, para todos los trabajadores, trabajadoras y sus familias.

Tal como se ha mencionado, la mayor parte de la información que se recaba **es de carácter personal,** datos que deben ser protegidos y que resultan indispensables para el cumplimiento de las funciones Institucionales.

El tratamiento de datos personales implica cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados, informáticos, manuales, mecánicos, digitales o electrónicos, aplicados a los sistemas de datos personales, relacionados con la obtención,

registro, organización, conservación, elaboración, utilización, cesión, difusión, cotejo o interconexión o cualquier otra forma que permita obtener información de los mismos y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos, así como su bloqueo, supresión o destrucción;

Por lo tanto, para el cumplimiento de las obligaciones establecidas en la Ley de la materia, se deberá observar lo siguiente:

- Obtención de datos personales:

  - Los datos personales podrán ser recabados de forma enunciativa, más no limitativa, por los siguientes medios:

    - Presentación de un escrito
    - Visita de instalaciones
    - Llenado de formatos
    - Formularios de internet
    - Trámites en ventanilla

  - Los medios a través de los cuáles se obtengan y traten los datos personales, deberán ser lícitos, privilegiando en todo momento la protección de los intereses del titular y la expectativa razonable de privacidad; evitando utilizar medios engañosos o fraudulentos.

  - Previo al tratamiento de datos personales, se deberá obtener el consentimiento del titular, de manera libre, específica e informada.

- El consentimiento se considera tácito, cuando habiéndose puesto a disposición del titular el Aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

- Tratándose de datos personales sensibles, se deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de firma autógrafa, electrónica o cualquier mecanismo de autenticación que al efecto se establezca. Para la obtención de dicho consentimiento, se facilitará al titular de los datos un medio sencillo y gratuito a través del cual pueda manifestar su voluntad, el cual le permita acreditar de manera indubitable y, en su caso, documentar que el titular otorgó su consentimiento.

o Se podrá obtener el consentimiento del titular para el tratamiento de sus datos personales, **de manera previa**, cuando sean recabados de manera directa de éste, y en su caso, sea requerido conforme al artículo 20 de la LGPDPPSO.

o Cuando se recaben datos indirectamente del titular y se requiera de su consentimiento para el uso de los mismos, no se podrán tratar los datos personales hasta contar con la manifestación de la voluntad libre, específica e informada del titular, mediante la cual autoriza el tratamiento de los mismos, ya sea de manera tácita o expresa.

➢ <u>Uso y almacenamiento de datos personales.</u>

o El responsable deberá adoptar las medidas necesarias para mantener exactos, pertinentes, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

o El tratamiento de datos personales que lleven a cabo las distintas áreas normativas, de operación administrativa y médicas que conforman a este Instituto, deberá sujetarse a las facultades o atribuciones que la normatividad aplicable les confiera, por lo que todo tratamiento de datos personales que se efectúe deberá estar justificado por finalidades:

- **Concretas**: el tratamiento de los datos personales deberá atender a los fines específicos o determinados, sin que admita errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.

- **Lícitas**: las finalidades que justifiquen el tratamiento de los datos personales deben ser acordes con las atribuciones o facultades del responsable, conforme a los ordenamientos jurídicos y normativos aplicables.

- **Explícitas**: las finalidades del tratamiento de los datos, deben ser expresas y darse a conocer de manera clara en el Aviso de privacidad.

- **Legítimas**: las finalidades que motivan el tratamiento de los datos personales, deberán estar habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

o En el tratamiento de datos personales, se deberán mantener mecanismos efectivos de seguridad de carácter administrativo, físico y técnico para la protección de los mismos, con el objeto de impedir, que se contravenga las disposiciones de la normatividad en la materia. Dichos mecanismos deberán permitir:

- Mantener identificada, clasificada y controlada la información que es propiedad del Instituto a fin de garantizar su confidencialidad, integridad y disponibilidad.

- Establecer normas y controles internos durante la recolección, procesamiento, almacenamiento, acceso y disposición de la información.

- Identificar, evaluar y tomar medidas que disminuyan riesgos en la administración de la información y garantizar la continuidad en los procesos.

- Implantar y mantener un modelo de seguridad de la información, eficiente, tolerante a fallas y fácil de monitorear, que involucren a todo el Instituto.

- Proteger al Instituto de posibles responsabilidades legales derivadas del uso indebido de los activos de información.

- Implantar y mantener un modelo de seguridad para conservar la confidencialidad e integridad de la información que se genere en el Instituto y se transmita a través de medios electrónicos o redes ya sean internas o externas.

- Implantar mecanismos necesarios que permitan conservar la integridad de los documentos y transacciones generados y entregados en el Instituto o fuera a terceras personas.

- Implantar mecanismos para almacenamiento y recuperación de la información en casos de desastre.

- Implantar mecanismos para prevención y corrección contra ataques de virus informáticos, códigos maliciosos y demás variantes.

- Recomendar y/o sugerir cambios o mejoras en el establecimiento de seguridad física dentro de las instalaciones del Instituto.

- Implantar y mantener mecanismos necesarios para determinar los accesos a los recursos del Instituto, como lo son impresoras, equipos, etc.

Estas políticas generales de seguridad de la información son el marco de referencia del cual se derivan estándares y procedimientos que rigen las operaciones y la

administración de la seguridad de la información del IMSS y, en consecuencia, de los datos personales que resguarda el Instituto.

- El Responsable deberá informar a los titulares, a través del Aviso de privacidad, la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

  El número de Avisos de privacidad que se debe tener, depende de las características y finalidad de los tratamientos que se lleven a cabo en las distintas actividades que realice el Instituto. **Por lo que debe elaborarse uno por cada tratamiento de datos que se efectué.**

- Se considera como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

  - La pérdida o destrucción no autorizada;
  - El robo, extravío o copia no autorizada;
  - El uso, acceso o tratamiento no autorizado, o
  - El daño, la alteración o modificación no autorizada.

- El Responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

- El Responsable deberá informar en un plazo máximo de setenta y dos horas al titular, al Comité de Transparencia y al Órgano Garante, las vulneraciones que afecten de forma significativa los **derechos patrimoniales** (de manera enunciativa, más no limitativa relacionado con sus bienes muebles e inmuebles, información

fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, AFORES, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular) **o morales** (de manera enunciativa, más no limitativa, relacionados con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, menoscabo ilegalmente de la libertad o integridad), en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados, puedan tomar las medidas para la defensa de sus derechos.

- La notificación de vulneración de seguridad al Comité de Transparencia, deberá contener los siguientes elementos:

  - Hora y fecha de identificación de la vulneración.
  - Hora y fecha del inicio de la investigación sobre vulneración.
  - La naturaleza del incidente o vulneración ocurrida.
  - La descripción detallada de las circunstancias en torno a la vulneración ocurrida.
  - Las categorías y número aproximado de titulares afectados.
  - Los sistemas de tratamiento y datos personales comprometidos.
  - Las acciones correctivas realizadas de forma inmediata.
  - Descripción de las posibles consecuencias de la de la vulneración de seguridad ocurrida.
  - Las recomendaciones dirigidas al titular.

- El medio puesto a disposición del titular para que pueda obtener mayor información al respecto.

- Nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar mayor información al Comité, en caso de requerirse.

- Cualquier otra información y documentación que considere conveniente hacer del conocimiento al Instituto.

➢ Eliminación de datos personales.

o Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el Aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser Suprimidos, previo Bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

o Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

o Se deberán establecer métodos y técnicas (trabajo en conjunto) para la supresión definitiva de los datos personales, de tal manera que la posibilidad de recuperarlos o reutilizarlos sea nula; para lo cual se deberán considerar los medios de almacenamiento físicos y/o electrónicos en los que se encuentren los datos personales, así como los siguientes atributos:

- **Irreversibilidad:** que el proceso utilizado no permita recuperar los datos personales.

- **Seguridad y confidencialidad:** en la eliminación definitiva de los datos personales, se deberán observar los deberes de confidencialidad y seguridad establecidos en la Ley de la materia.

- **Favorable al medio ambiente:** que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten al medio ambiente.

*Verificar el Anexo 5.2 Cumplimiento de Obligaciones.

6. REVISIONES Y AUDITORÍAS (SUPERVISIÓN), ASÍ COMO OTROS PROCEDIMIENTOS QUE SE DESARROLLEN EN EL MARCO DE ESTE

Con la finalidad de establecer y mantener las medidas de seguridad para los datos personales, el Comité de Transparencia evaluará y medirá los resultados de las políticas, planes, proceso y procedimientos implementados en materia de seguridad y tratamiento de los datos, de manera aleatoria y cuando así lo estime pertinente, a fin de verificar el cumplimiento de los objetivos planteados; por lo tanto, se deberá monitorear continuamente los siguientes aspectos:

- Los nuevos activos que se incluyan en la gestión de riesgos.
- Las modificaciones necesarias a los activos.
- Las nuevas amenazas que podrían estar activas dentro y fuera del Instituto y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
- Los incidentes y vulneraciones ocurridos.

Asimismo, se deberá implementar un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

7. MEJORA CONTINUA Y SANCIONES

El Comité de Transparencia del Instituto, podrá supervisar en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones en materia de protección de datos personales; así como la aplicación de las medidas de seguridad establecidas, sugiriendo en su caso, las acciones pertinentes a cada situación detectada (medidas preventivas y correctivas), atendiendo en todo momento, las posibilidades de su aplicación, lo anterior con la finalidad de mantener siempre actualizado el Programa de Protección de Datos Personales, y por lo tanto el sistema de gestión para la protección de éstos.

Ahora bien, de conformidad con lo establecido en la fracción VIII del artículo 84 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, entre las funciones del Comité de Transparencia, se encuentran la de dar vista al Órgano Interno de Control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales.

En este orden de ideas, serán causas de sanción por incumplimiento a las obligaciones establecidas, las siguientes:

I. Actuar con negligencia, dolo o mala fe en el tratamiento de los datos personales.

II. Incumplir con los plazos de atención previstos en la normatividad de la materia.

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.

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere la Ley General de Protección de Datos Personales en Posesión de Sujetos

Obligados, 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.

VII. Incumplir el deber de confidencialidad.

VIII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad.

IX. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley.

X. Obstruir los actos de supervisión del Comité de Transparencia.

XI. Crear bases de datos personales en contravención a lo dispuesto por la normatividad vigente.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, IX y XI, así como la reincidencia en las conductas previstas en el resto de las fracciones aludidas, serán consideradas como graves para efectos de su sanción administrativa.

Para las conductas referidas, se dará vista a la autoridad competente para que imponga o ejecute la sanción. Por lo tanto, las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a las disposiciones señaladas, son independientes de del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

8. ANÁLISIS DE RIESGO

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que se encuentran expuestos los datos personales; es decir, mediante el análisis de riesgo es posible identificar amenazas, evaluar vulnerabilidades, probabilidades de ocurrencia y estimar el impacto potencial.

Por lo tanto, la evaluación de riesgo es una consideración sistemática de los siguientes puntos:

- Impacto potencial de una falta de seguridad en las operaciones, teniendo en cuenta las potenciales consecuencias por una pérdida de confidencialidad, integridad o disponibilidad de los datos personales.

- Probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas y vulnerabilidades predominantes, y controles actualmente implementados.

Para estar en posibilidad de definir un plan de riesgo a tratar y posteriormente implementar controles de seguridad, de deben considerar diferentes criterios de evaluación que permitan delimitar el nivel de riesgo aceptable para los datos personales. Estos criterios de evaluación de riesgo de la seguridad de los datos personales deben considerar los factores que pueden incidir en el nivel de riesgo, tales como:

A. Los diferentes requerimientos normativos, inclusive los códigos de conducta o mejores prácticas de un sector específico.

B. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida.

C. El valor y exposición de los activos involucrados en el tratamiento de los datos personales.

D. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.

E. Los supuestos previstos en el artículo 32 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Las **vulnerabilidades** son debilidades en la seguridad de los activos y pueden ser identificadas en los siguientes ámbitos:

- Organizacionales
- De procesos y procedimientos
- De personal
- Del ambiente físico
- De la configuración de sistemas de información
- Del hardware, software o equipo de comunicación
- De la relación con prestadores de servicios
- De la relación con terceros

La presencia de vulnerabilidades no causa daño por sí misma, se requiere de una amenaza que la explote. Una vulnerabilidad que no se encuentre expuesta a una amenaza identificada posiblemente no requiera la implementación de un control, pero debe ser reconocida y monitoreada constantemente por el responsable, o bien, cuando surja algún cambio. Por ejemplo, un equipo de cómputo o un archivero con información personal es vulnerable a inundaciones si se encuentra instalado en un sótano por el que pasan las tuberías del servicio de suministro de agua. De manera inversa, la amenaza de inundación se descarta si el equipo de cómputo o el archivero

con datos personales se localiza en la parte más alta del edificio, lejos de tuberías de agua y de amenazas ambientales relacionadas.

Los controles usados incorrectamente o con una mala implementación son una causa de vulnerabilidades. Un control puede ser entonces efectivo o no efectivo dependiendo del contexto en el cual opera.

El análisis de riesgo deberá arrojar como resultado un valor de riesgo para cada uno de los activos identificados con respecto a cada una de las vulneraciones detectadas, de forma que se identifiquen los escenarios que podrían llevar a cada uno de los activos a las posibles vulneraciones y se seleccionen los controles y medidas de seguridad que permitan tratar dichos riesgos.

Con los conocimientos de los activos de información y de los controles existentes se puede realizar una ponderación de los escenarios de riesgo más importante, considerando que el riesgo es **la combinación de los factores: amenaza, vulnerabilidad e impacto (daño).**

Una vez identificados los activos y procesos relacionados a los datos personales, así como las amenazas, vulnerabilidades y escenarios de incidentes relacionados, se puede proceder al **análisis de brecha** de las medidas de seguridad.

El análisis de brecha, consiste en identificar:

- Las medidas de seguridad existente y efectiva
- Las medidas de seguridad faltantes
- La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Es importante detectar los controles que ya están funcionando de manera efectiva, con su respectivo nivel de madurez, así como las medidas identificadas como faltantes, para construir un programa de trabajo que refleje los recursos designados, los responsables, y las fechas compromiso para su implementación.

Asimismo, el responsable deberá **elaborar un plan de trabajo** que defina las acciones a implementar **de acuerdo con los resultados obtenidos del análisis de riesgo y del análisis de brecha**, priorizando las medidas de seguridad más relevantes e inmediatas a establecer. Esto considerando los recursos designados, el personal interno y externo del IMSS y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

9. PROGRAMAS DE CAPACITACIÓN

El Comité de Transparencia, será el responsable de diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en el IMSS, considerando los roles y responsabilidades asignados a cada uno para el tratamiento y seguridad de los datos personales y el perfil de sus puestos, lo anterior en colaboración del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

10. DOCUMENTO DE SEGURIDAD

La implementación del Programa de Protección de Datos Personales, requiere de la actualización del documento de seguridad, es decir, del instrumento que establece las medidas y procedimientos administrativos, físicos y técnicos de seguridad aplicables a los sistemas de datos personales necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas.

Por lo tanto, el responsable deberá elaborar un documento de seguridad que contenga los siguientes rubros:

1. El inventario de datos personales y de los sistemas de tratamiento.
2. Las funciones y obligaciones de las personas que traten datos personales.
3. El análisis de riesgo.
4. El análisis de brecha.
5. El plan de trabajo.
6. Los mecanismos de monitoreo y revisión de las medidas de seguridad.
7. El programa general de capacitación.

El presente Programa de Protección de Datos Personales del Instituto Mexicano del Seguro Social, fue autorizado por los miembros del Comité de Transparencia en su 4ª Sesión Ordinaria de Trabajo 2018, celebrada el 27 de junio de 2018.

Mtro. Ulises Moreno Munguía
Titular de la Dirección Jurídica y
Presidente del Comité de Transparencia

Lic. Marco Antonio Andrade Silva
Titular del OIC y Miembro del Comité de Transparencia

C.P. Rubén López Lazcano
Miembro del Comité de Transparencia y Titular de la División de Administración de Documentos Información