POLÍTICA INTERNA PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DE LA SECRETARÍA DE SALUD

ÍNDICE

PRESENTACIÓN

La Secretaría de Salud como dependencia de la Administración Pública Centralizada[1] y Sujeto Obligado según la actualización del Padrón de Sujetos obligados en el ámbito Federal aprobado por el Sistema Nacional de Transparencia mediante ACUERDO ACT-PUB/20/03/2024.08[2], con la finalidad de dar cumplimiento a lo dispuesto en los artículo 30, fracción II y 33 fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se elaboró la presente Política Interna para la Gestión y Tratamiento de Datos Personales de la Secretaría de Salud (Política), la cual se define como mecanismo para cumplir con el principio de responsabilidad, así como el lineamiento 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el cual prevé la elaboración e implementación de políticas de protección de datos personales para dirigir, operar y controlar los procesos que impliquen tratamiento de datos personales en el ejercicio de funciones y atribuciones.

Su contenido, se encuentra alineado al marco normativo aplicable en la materia, entre los instrumentos que destacan se cita la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales),.

Esta Política se implementa para dar cumplimiento a los principios, deberes y obligaciones en materia de protección de datos personales, a fin de que las “Áreas” (unidades administrativas, órganos desconcentrados, así como el Consejo de Salubridad General), que se encuentren previstos en Reglamento Interior de la Secretaría de Salud, estatutos orgánicos, que no cuentan con Comité de Transparencia y lleven a cabo tratamiento de datos personales observen la misma a fin de garantizar la adecuada protección y ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición.

[1] Artículos 2, 26 y 39 Ley Orgánica de la Administración Pública Federal https://www.diputados.gob.mx/LeyesBiblio/pdf/LOAPF.pdf
[2] https://home.inai.org.mx/wp-content/documentos/Micrositios/Padron_Sujetos_Obligados.pdf

MARCO NORMATIVO.

- Constitución Política de los Estados Unidos Mexicanos, artículo 6°, Base A y segundo párrafo del artículo 16. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

- Reglamento Interior de la Secretaría de Salud. Disponible en: http://www.oag.salud.gob.mx/descargas/LV/RISSA_DOF-7-02-2018.pdf

- Lineamientos Generales de Protección de Datos Personales para el Sector Público. Disponible en: https://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf

- Lineamientos que establecen los parámetros, modalidades y procesamiento para la portabilidad de datos personales publicados el 23 de enero de 2018. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018#gsc.tab=0

Tabla: Referencias normativas

Principios y Obligaciones en Materia de Protección de Datos Personales. **(Definiciones Claves).**	**Correlativos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.** **(LGPDPPSO y LGPSPSP)**
Inventario de Datos	Artículos 33, fracción III, 35 , Fracción I, LGPDPPSO y 58 de los Lineamientos Generales.

Ciclo de Vida de los Datos Personales	Artículo 33, fracción I, de la LGPDPPSO.
Aviso de Privacidad	Artículo 3 Fracción II, 26, 27 y 28 LGPDPPSO y artículos 27,28,29,30,1,32,33,34,35,36,37,38 y 39 de los Lineamientos Generales.
Consentimiento	Artículo 1 Fracción VIII , 22 de la LGPDPPSO y Artículos 12.13,14,15,16, 18,19 y 20 LGPSPSP
Confidencialidad	Articulo 42 LGPDPPSO y 71 de los Lineamientos Generales.
Información	Artículo 26 LGPDPPSO y 26 de Lineamientos Generales.
Licitud	Artículo 17 de la LGPDPPSO y 8 de los Lineamientos Generales.
Lealtad	Artículo 19 de la LGPDPPSO y 11 de los Lineamientos Generales.
Finalidad	Artículo 18 de la LGPDPPSO y 9 de los Lineamientos Generales
Proporcionalidad	Artículo 25 de la LGPDPPSO y 24 de los Lineamientos Generales.
Responsabilidad	Artículos 29 y 30 de la LGPDPPSO y 46 de los Lineamientos Generales.
Mecanismos para acreditar y el cumplimiento de los principios deberes y obligaciones de la Ley General.	Artículo 30 de la LGPDPPSO.

Gestión de Seguridad de Datos Personales.	Artículo 34 de la LGPDPPSO.
Documento de Seguridad	Artículos 3, fracción XIV Artículo 35 de la LGPDPPSO.
Funciones y Obligaciones de las personas que tratan datos personales.	33, fracción II y 35, fracción II de la LGPDPPSO; Artículo 57 de los Lineamientos Generales.
Análisis de Riesgo	33, fracción IV y 35, fracción III de la LGPDPPSO y 60 de los Lineamientos Generales.
Análisis de Brecha	33, fracción V y 35, fracción IV de la LGPDPPSO y 61 de los Lineamientos Generales.
Plan de Trabajo	33, fracción VI y 35, fracción V de la LGPDPPSO y 62 de los Lineamientos Generales.
Programa General de Capacitación	33, fracción VIII y 35, fracción VII de la LGPDPPSO 64 de los Lineamientos Generales.
Actualización del Documento de Seguridad.	Artículo 36 de la LGPDPPSO.
Políticas Internas	Artículos 30 y 33 LGPDPPSO; Artículo 56 de los Lineamientos Generales.
Cambios en las Políticas Internas	Artículo 49 de los Lineamientos Generales.
Trazabilidad de tratamiento	Definición obtenida de la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales. Documento emitido por el INAI en el año 2015.
Transferencias	Artículo 65,66,67,68,69 y 70 LGPDPPSO y Artículos 113,114,115.116 y 118 de los Lineamientos Generales.
Vulneraciones	Artículo 37 de la LGPDPPSO.

GLOSARIO

Activo: En términos generales, un activo es cualquier elemento que representa un valor para la Secretaría de Salud en materia de protección de datos personales, definido como:

a) grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar
bienestar o deleite y

b) cualidad de las cosas, en virtud de la cual se da por poseerlas o equivalente.

Los activos pueden ser tangibles o intangibles. Los activos tangibles son objetos físicos que proporcionan una utilidad en las actividades del día a día, como la infraestructura tecnológica, el equipo de cómputo, de comunicaciones o cualquier dispositivo electrónico.

En otro sentido, los activos intangibles incluyen datos, información digital, aplicaciones, transacciones, planes, propiedad intelectual, conocimiento, imagen, principios, valores, entre otros.

Activo de Apoyo: Base de datos, programa de cómputo, bien informático físico, solución tecnológica, sistema o aplicativo, relacionados con el tratamiento de la misma, que contengan todo documento, ya sean expedientes, reporte, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus servidores públicos e integrantes, sin importar su fuente o

fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico, en los que se efectúen mediante procedimientos manuales o automatizados un tratamiento 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, que tengan valor para la Secretaría.

Amenaza: Causa potencial o incidente no deseado que puede resultar en daños a un sistema o a la información de la Secretaría, como la circunstancia o evento con la capacidad de causar daño a las cuales incluyen amenazas cibernéticas o ciberamenazas, la cuales son amenazas a la seguridad de la información o a la informática.

En el anexo B de la SGSDP del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) se establece una serie de amenazas a partir del origen, motivación/causa y posibles consecuencias. De ahí se desprende que las amenazas varían en el tiempo y las causas pueden ser clasificadas en internas y externas, de origen natural o humano, y ser accidentales o deliberadas. Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo.

Dentro de las primeras está una gestión deficiente, falta de formación, ausencia de políticas y procedimientos, así como ausencia de mecanismos de disuasión, los cuales habitualmente facilitan o desencadenan un incidente de fuga de información.

Las segundas tienen como actores a agentes externos a la propia red o sistema que consiguen acceder a información no autorizada y/o modificar o interferir el propio funcionamiento del sistema mediante el ataque por medios telemáticos de las vulnerabilidades del sistema.

Las amenazas, tanto internas como externas, por lo general, implican la ausencia o ineficiencia de algún tipo de control o medida de seguridad.

Áreas: Las "Áreas" centrales de la Secretaría de Salud; unidades administrativas, órganos desconcentrados, así como el Consejo de Salubridad General.

Aviso de Privacidad: Documento a disposición de la persona 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.

Base 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: Mecanismo o restricción administrativa, aplicable en un lapso de tiempo en el que se conservan los datos personales de una persona física una vez cumplida la finalidad para la cual fueron recabados, que impide cualquier tratamiento, antes de proceder a su cancelación, ya sea como consecuencia natural del agotamiento de las propias finalidades establecidas en el aviso de privacidad, o bien, a instancia del titular de los datos personales o de su representante mediante el ejercicio de su derecho de cancelación conforme al artículo 46 de la LGPDPPSO.

Ciclo de vida del dato: Tratamiento que se efectúa considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada, en función de la finalidad con la que fue recabado.

Comité de Transparencia: Autoridad máxima en materia de protección de datos personales al interior de la Secretaría de Salud.

Consentimiento: Manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de los mismos, existen dos tipos de consentimiento: **Tácito y Expreso**.

a) Tácito: Tiene lugar cuando habiéndose puesto a disposición de la persona titular el aviso de privacidad, ésta no manifiesta su voluntad en sentido contrario. Es decir, se actualiza cuando, a pesar de que el sujeto obligado pone a disposición el aviso de privacidad de manera previa a realizar el tratamiento, la persona titular no realiza un pronunciamiento en sentido contrario, o manifiesta su negativa para evitarlo, para todas o algunas de las finalidades señaladas en el aviso de privacidad. Por regla general, es válido el consentimiento tácito, salvo que la Ley General o alguna otra disposición aplicable en la materia exija que la voluntad de la persona titular se manifieste expresamente.

b) Expreso: Tiene lugar cuando la voluntad de la persona titular se manifiesta de manera verbal, por escrito, por algún medio electrónico, óptico, signo inequívoco o por cualquier otra tecnología, siempre y cuando se permita de manera indubitable acreditar que la persona titular otorgó su consentimiento. Es decir, es aquél que otorga la persona titular sin dejar lugar a dudas de que efectivamente lo ha proporcionado.

Custodios: Son aquéllos con responsabilidad funcional sobre los activos, como: los responsables del departamento de datos, administradores de sistemas o responsables de un proceso o de un proyecto en específico, entre otros.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o de cualquier otro tipo. Una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente, mediante cualquier información que no implique plazos, medios o actividades desproporcionadas.

Derechos Arco: Los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.

Disociación: Procedimiento mediante el cual los datos personales no pueden asociarse a la persona 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/a: 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

Enlace Responsable: Persona servidora pública de nivel mando y técnico operativo (apoyo), para fungir al interior de ésta, así como ante la Unidad de Transparencia y el Comité de Transparencia.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Interés Jurídico: Aquél que tiene una persona física que, con motivo del fallecimiento del titular, mismo que pretende ejercer los derechos ARCO de éste, para el reconocimiento de derechos, atendiendo a la relación de parentesco por consanguinidad o afinidad que haya tenido con el titular, el cual se acreditará en términos de las disposiciones legales aplicables.

Inventario: Inventario de datos personales al que se refieren los artículos 33, fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

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

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público

Medidas de Seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Política: Política Interna para la Gestión y Tratamiento de Datos Personales de la Secretaría de Salud

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y el/la encargado/a, dentro o fuera del territorio mexicano.

Responsable: Los sujetos obligados a que se refiere el artículo 1 de la Ley General que deciden sobre el tratamiento de datos personales (Secretaría de Salud).

SSA: Secretaría de Salud.

Persona 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 de la persona titular, del responsable o del/de la encargado/a.

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.

Unidad de Transparencia: Entidad administrativa de la Oficina del Abogado General que tiene la función de ser el vínculo entre la Secretaría, los solicitantes de información y el INAI, así como la recibir, dar trámite a las solicitudes de información y notificar las correspondientes respuestas.**Vulneraciones:** Debilidad o ausencia de seguridad en un activo o grupo de activos.

OBJETIVO

El objetivo de esta Política es establecer las reglas generales para asegurar el cumplimiento de los principios y deberes en materia de protección de datos personales, relacionados con los tratamientos de datos personales que las personas servidoras públicas llevan a cabo en los procesos en los que la Secretaría de Salud realice algún tratamiento de los mismos, así como los deberes de seguridad y confidencialidad que obliga a todo sujeto que realice el tratamiento de los datos a prever medidas de seguridad físicas, técnicas y administrativas para garantizar la seguridad y confidencialidad de los datos personales.

Además, orientar a las personas servidoras públicas, encargados, custodios, y prestadores de servicios relacionados con el tratamiento de los datos personales para que lleven un correcto tratamiento de datos personales velados por los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley General, los Lineamientos Generales y demás normativa aplicable en la materia.

Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

ÁMBITO DE APLICACIÓN

Esta Política es de observancia general y obligatoria para todo el personal de la Secretaría de Salud que se involucre en el tratamiento de datos personales. Su aplicación corresponde a todas las “Áreas” que en el ámbito de sus competencias y facultades traten datos personales, conforme lo previsto en la Ley General, los Lineamientos Generales y demás disposiciones aplicables en materia de protección de datos personales.

Asimismo, las personas servidoras públicas involucradas en el tratamiento de datos personales, deberán adoptar las medidas de seguridad de carácter administrativo, físico

y técnico necesarias para la protección de datos personales, acordes con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en dicho tratamiento y los deberes de seguridad y confidencialidad, a fin de evitar su alteración, daño, destrucción, acceso a tratamiento no autorizado, pérdida y transmisión.

ALCANCE

La presente Política se concentra en las medidas encaminadas a la protección de datos personales, su observancia permitirá proteger los activos de información contra daños, pérdidas, alteraciones, destrucciones o usos y accesos o tratamientos no autorizados, de ahí la importancia de desarrollar medidas de seguridad, administrativas, físicas y técnicas en el tratamiento de los datos personales que se lleven a cabo todas las "Áreas" en ejercicio de sus funciones y atribuciones, las cuales deberán observar el presente instrumento, con el objeto de que, todas las personas servidoras públicas que lleven a cabo un tratamiento de datos personales la implementen en su actuar.

En este contexto, el alcance de la Política radica en que todas las "Áreas" que participan en el tratamiento de datos, o bien, que participan en algún momento del ciclo de vida de los datos; identifiquen los activos, es decir, los datos personales que se recaban deberán en todo momento observar los principios, deberes y demás obligaciones establecidas en la normativa aplicable en la materia, como el conjunto de reglas, procedimientos y controles para asegurar la confidencialidad, integridad y su disponibilidad, características conocidas como la triada de la información.

Asegurar la confidencialidad de la información significa que no será expuesta o accedida por entes no autorizadas, en tanto, la integridad significa que solo las entidades autorizadas podrán realizar alguna modificación o eliminación y dicha información estará lista para acceder a ella en el momento que se necesite y en la forma requerida

La presente Política, es el reflejo de los principios rectores de esta Secretaría; alineados a su misión y visión, la cual establece en forma clara, las acciones a realizar para no poner en riesgo la información, bajo un marco normativo que contenga una estructura

de gobierno y un procedimiento de gestión de ciclo de vida que asegure su correcta creación, autorización, difusión, cumplimiento y actualización.

Los procedimientos para garantizar la seguridad de la información son actividades que, en su conjunto, conforman un proceso sistemático de gestión de seguridad de la información que se implementan para mitigar los riesgos que pueden ser administrativos, de procedimiento o tecnológicos.

Cuando la información a proteger se trata de datos personales, entonces el deber de seguridad refiere a la obligación de implementar y mantener mecanismos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos personales, conforme al artículo 47 de los Lineamientos Generales.

CAPÍTULO I. DE LA IMPLEMENTACIÓN Y ACREDITACIÓN DE LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DE LA SECRETARÍA DE SALUD

I.1. DE LA IMPLEMENTACIÓN

La presente Política será de observancia obligatoria para todas las "Áreas" que realicen tratamiento de datos personales en ejercicio de sus funciones y atribuciones, su objetivo radica en implementar las medidas de seguridad administrativas, físicas y técnicas en el tratamiento de Datos Personales, en cumplimiento a lo previsto en el artículo 33 de la Ley General, resulta de trascendencia describir que el tratamiento de datos personales consiste en cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a 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.

Las "Áreas" deberán considerar, de manera enunciativa más no limitativa, el desarrollo tecnológico y las técnicas existentes, la naturaleza, contexto, alcance y finalidades del tratamiento de los datos personales, conforme las atribuciones, facultades y demás cuestiones que considere convenientes conforme su ámbito de competencia.

Una vez identificado el tratamiento de datos personales, estos deberán contenerse en un Inventario de Datos Personales, con el objeto de realizar un análisis que permita confrontar las medidas de seguridad existentes con las que cuentan las "Áreas", los roles, privilegios de aquellos servidores públicos que trataran los datos personales y las vulneraciones que pudieran o no sobrevenir.

Las "Áreas" al realizar dicha actividad, mejor conocida como Análisis de Brecha de Seguridad, estarán en posibilidad de identificar nuevas Medidas de Seguridad y Protección de Datos Personales a implementar en un Plan de Trabajo; mismas que

permitirán desarrollar planes de acción y ejecutar procedimientos específicos ante vulneraciones subsecuentes.

En este contexto, la implementación de la presente Política, se concentra en las medidas encaminadas a la protección de datos personales, su observancia permitirá proteger los activos de información contra daños, pérdidas, alteraciones, destrucciones o usos y accesos o tratamientos no autorizados.

I.2. DESIGNACIÓN DEL ENLACE RESPONSABLE

Cada Área designará a una persona servidora pública de nivel mando y técnico operativo (apoyo), para fungir al interior de ésta, así como ante la Unidad de Transparencia y el Comité de Transparencia, como enlace responsable de las actividades de protección de datos personales, con el fin de garantizar y evidenciar el cumplimiento de esta Política ante la persona titular de los datos y la Secretaría de Salud.

La persona servidora pública designada como enlace responsable, que en el ejercicio de sus atribuciones traten datos personales, deberán garantizar su confidencialidad, integridad y disponibilidad dando cumplimiento a las obligaciones siguientes:

I. Observar y dar cumplimiento a los principios de licitud finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

II. Implementar y observar en su Área, el cumplimiento de los principios y deberes de acuerdo con las directrices señaladas por esta Política y el Comité de Transparencia.

III. Tratar los datos personales para finalidades concretas, lícitas, explícitas y legítimas en ejercicio a las facultades o atribuciones que la normatividad aplicable les confiera.

IV. Evitar la obtención y tratamiento de datos personales a través de medios engañosos o fraudulentos.

V. Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión a fin de que no se altere la veracidad de éstos.

VI. Mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

VI. Participar en la integración y actualización de los documentos normativos exigidos por la Ley General y demás disposiciones aplicables.

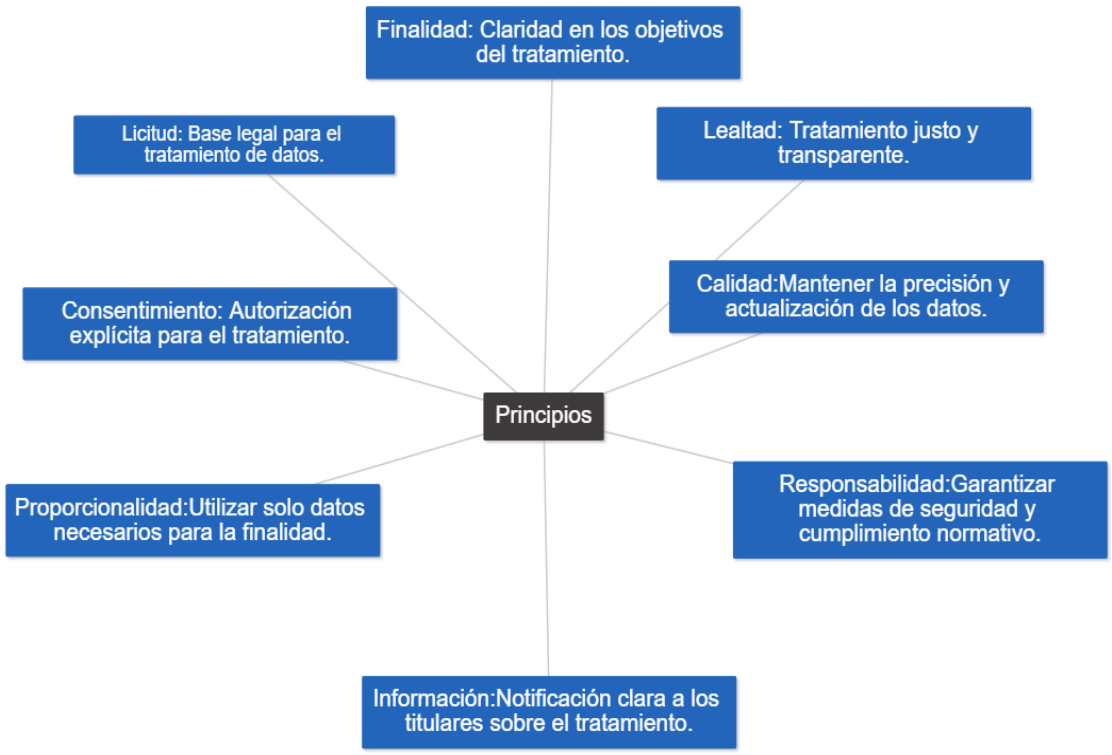
VII. Gestionar al interior de su Área, la debida atención de solicitudes relativas al ejercicio de los derechos ARCO que sean presentadas ante la Unidad de Transparencia.

VIII. Las demás disposiciones normativas que determine el INAI o aquéllas que deriven de las resoluciones emitidas por el Comité de Transparencia.

Dentro de esta Secretaría de Salud, se establecen diversos tratamientos de datos personales mismos que constantemente son analizados a partir de la valoración de los activos utilizados a la par de la calidad de los datos recabados.

En ese orden de ideas cada una de las “Áreas” responsables del tratamiento cuentan con la obligación ficta de someterse a diversas dinámicas de cotejo llevadas a cabo por parte de la Dirección de Apoyo Técnico Normativo, adscrita a la Oficina del Abogado General; con la única finalidad de precisar los principios finalidad, lealtad, calidad, responsabilidad, proporcionalidad, consentimiento y licitud.

CAPÍTULO II. DE LOS PRINCIPIOS



II.1. PRINCIPIOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES EN LA SECRETARÍA DE SALUD

Las "Áreas" responsables del tratamiento de datos personales deben observar los principios rectores siguientes:

I. Licitud;

II. Finalidad;

III. Lealtad;

IV. Consentimiento;

V. Calidad;

VI. Proporcionalidad;

VII Información, y

VIII. Responsabilidad.

II.2. PRINCIPIO DE LICITUD

Este principio consiste en tratar los datos personales que posea conforme las atribuciones o facultades que la normatividad aplicable le confiera a cada una de las Áreas, así como con estricto apego y cumplimiento de lo dispuesto en la Ley General, los Lineamientos Generales, la presente Política y demás disposiciones normativas que resulten aplicables.

II.2.1. Actividades vinculadas al Principio de Licitud.

Es responsabilidad de las personas servidoras públicas de las Áreas identificar el marco normativo que regula el tratamiento de datos personales dentro del ámbito de su competencia. Esto incluye la identificación del tipo de datos que se manejan y las finalidades para las cuales son utilizados.

II.2.2. Mecanismos para acreditar el cumplimiento del Principio de Licitud.

Con el fin de asegurar el cumplimiento del principio de licitud, las unidades administrativas deben incorporar en el Aviso de Privacidad Integral, y en caso de ser necesario, en el inventario, la base legal que les otorga la facultad de tratar datos personales.

II.3. PRINCIPIO DE FINALIDAD

Todo tratamiento de datos personales realizado por las "Áreas" debe estar justificado por finalidades específicas, legales, claras y legítimas. Estas finalidades se definen como:

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 en la persona 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 personales 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.

IV. **Legítimas:** Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran autorizadas por el consentimiento del/de la titular, salvo que se actualice alguna de las causales de excepción a que se refiere la Ley General y la presente Política.

II.3.1. Actividades relacionadas con el Principio de Finalidad

Como parte del principio de finalidad, las Áreas que manejen datos personales deben:

I. Detallar en el aviso de privacidad todas las finalidades para las cuales se tratan los datos personales, en concordancia con las facultades y responsabilidades que les han sido otorgadas.

II. Tratar los datos personales conforme a las finalidades específicas, legales, claras y legítimas establecidas en el aviso de privacidad.

III. Obtener el consentimiento de las personas titulares de los datos cuando sea necesario, excepto en los casos previstos en la Ley General y esta Política.

V. Informar a las personas titulares sobre cualquier tratamiento adicional de sus datos personales que no esté contemplado en el aviso de privacidad, siempre y cuando se cuente con las facultades o responsabilidades correspondientes y se obtenga su consentimiento, a excepción de lo establecido en la Ley General.

VI. Considerar la expectativa razonable de privacidad de la persona titular, la naturaleza de los datos personales y las posibles consecuencias del tratamiento de los mismos.

II.2. Mecanismos para dar cumplimiento al Principio de Finalidad.

Para garantizar el cumplimiento del principio de finalidad, las unidades administrativas deben:

I. Verificar que las finalidades de cada tratamiento sean específicas y estén alineadas con las atribuciones y responsabilidades de la Secretaría de Salud y su área correspondiente.

II. Supervisar que el personal solo manipule datos personales de acuerdo con las finalidades establecidas en el aviso de privacidad respectivo.

III. Verificar que los avisos de privacidad informen claramente todas las finalidades del tratamiento de datos personales, evitando la utilización de lenguaje que pueda generar confusión.

IV. Informar a las personas titulares de los datos personales sobre cualquier tratamiento adicional de sus datos personales para diferentes finalidades.

VII. Obtener el consentimiento de las personas titulares de los datos personales cuando sea necesario.

II.4. PRINCIPIO DE LEALTAD.

Este principio consiste en abstenerse de obtener y tratar datos personales a través de medios engañosos o fraudulentos. Para cumplir con este principio, las "Áreas" se comprometen a obtener y manejar datos personales de manera íntegra y transparente, garantizando la protección de los derechos e intereses de las personas titulares y su legítima expectativa de privacidad.

II.4.1. Actividades relacionadas con el Principio de Lealtad

En concordancia con el principio de lealtad, las Áreas encargadas del manejo de datos personales deben:

I. Manejar y tratar los datos personales de forma honesta, sin involucrar engaño, medios fraudulentos, dolo, mala fe o negligencia.

II. Priorizar o privilegiar los intereses de las personas titulares de los datos y evitar cualquier forma de discriminación, injusticia o arbitrariedad en relación con sus datos.

III. Respetar la legítima expectativa de privacidad de las personas titulares de los datos personales en todo momento, es decir, la confianza que el titular ha depositado en el responsable respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la Ley General y los presentes Lineamientos generales.

II.4.2. Mecanismos para dar cumplimiento al Principio de Lealtad

Para dar cumplimiento al principio de lealtad, las Áreas deben:

I. Garantizar la elaboración de avisos de privacidad conforme a lo establecido en la Ley General, Lineamientos Generales y las disposiciones internas de esta Política.

II. Establecer mecanismos de supervisión que aseguren que los tratamientos de datos no generen discriminación, trato injusto o arbitrario hacia los titulares.

III. Verificar que el manejo de datos personales se realice exclusivamente para los propósitos informados en el aviso de privacidad correspondiente.

Este principio se reconoce en el artículo 15 de la LGPDPPSO y obliga al responsable a tratar los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos, la mayoría de estos mecanismos se encuentran públicamente disponibles en el portal de la Secretaría de Salud; a través de los avisos de privacidad desarrollados por las diversas áreas de este Sujeto Obligado para cada tratamiento de datos personales.

II.5. PRINCIPIO DE CONSENTIMIENTO

Consiste en obtener el consentimiento del titular previo al tratamiento de sus datos personales, las “Áreas”, deben obtener el consentimiento (tácito, expreso, escrito o verbal, según proceda) de la persona la titular de los datos personales, de manera libre, específica e informada, en términos de lo dispuesto en la Ley General, salvo que se actualice alguna de las causales de excepción siguientes:

I. Cuando una ley así lo disponga, en cuyo caso, los supuestos de excepción deben ser acordes con las bases, principios y disposiciones establecidos en la Ley General que, en ningún caso, puede contravenirla.

II. Cuando las transferencias que se realicen entre la Secretaría de Salud y otro sujeto responsable sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o acordes con la finalidad que motivó el tratamiento de los datos personales.

III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.

IV. Para el reconocimiento o defensa de derechos del/de la titular ante autoridad competente.

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre la persona titular de los datos y la Secretaría de Salud.

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.

VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria.

VIII. Cuando los datos personales figuren en fuentes de acceso público.

IX. Cuando los datos personales se sometan a un procedimiento previo de disociación.

X. Cuando la persona titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

La actualización de alguno de los supuestos no exime a las “Áreas” y a las personas servidoras públicas responsables del tratamiento de datos personales del cumplimiento de las demás obligaciones establecidas en la Ley General, los Lineamientos Generales y la presente Política.

i)Consentimiento tácito. - Cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario en términos de lo señalado en el artículo 21, segundo párrafo de la Ley General.

ii) Consentimiento expreso. - Será cuando la voluntad del titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología, de acuerdo con lo dispuesto en el artículo 21, primer párrafo de la Ley General.

iii) Consentimiento escrito y verbal. - De manera verbal cuando lo externe oralmente de manera presencial o mediante el uso de cualquier otra tecnología que permita la interlocución oral, en ambos casos, ante la persona que represente al responsable, y el titular otorga su consentimiento por escrito cuando manifieste su voluntad en un documento, físico o electrónico, a través de cierta declaración en sentido afirmativo, firma autógrafa, huella dactilar, firma electrónica o cualquier mecanismo o procedimiento equivalente autorizado por la normatividad aplicable.

II.5.I Actividades relacionadas con el Principio de Consentimiento

En atención al Principio de Consentimiento, las Áreas de la Secretaría de Salud deben:

I. Obtener el consentimiento de la persona titular de los datos personales, previo al tratamiento, salvo que se actualice alguno de los supuestos de excepción descritos en el artículo anterior.

II. Recabar el consentimiento expreso y, en su caso, por escrito, a través de formatos claros y sencillos, cuando así proceda, debiendo ser acorde con el perfil de la persona titular de los datos personales, en los cuales se distingan los datos y finalidades del tratamiento que requieren de la manifestación de su voluntad.

III. Implementar medios sencillos y gratuitos para la obtención del consentimiento, independientemente de la modalidad en que este se requiera, cuando así proceda.

IV. Se podrá solicitar de nuevo el consentimiento cuando se realicen cambios a las finalidades; cuando requiera recabar datos personales sensibles adicionales a aquéllos informados en el aviso de privacidad original, los cuales no se obtengan de manera directa de la persona titular y se requiera de su consentimiento para el tratamiento de éstos, el responsable cambie su identidad; o se modifiquen las condiciones de las transferencias de datos personales o se pretendan realizar transferencias no previstas inicialmente y el consentimiento de la persona titular sea necesario.

V. En los supuestos en los que se requiera realizar el tratamiento de datos de personas menores de edad, el consentimiento deberá obtenerse a través de aquélla que ejerza la patria potestad o tutela, al ser la legítima representante de las y los que están bajo de

ella. Tratándose de personas con incapacidad legal o en estado de interdicción, se sugiere obtenerlo a través de la persona que ejerce la tutela.

VI. En su caso, habilitar en el aviso de privacidad casillas y/o espacios para que la persona titular exprese su consentimiento, respecto de cada una de las finalidades para las cuales son tratados sus datos personales.

VII. Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de la LGPDPPSO, en el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología, en tal caso, el consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario. Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de la LGPDPPSO.

II.5.2 Mecanismos para acreditar el cumplimiento del Principio de Consentimiento.

Para acreditar el Principio de Consentimiento, las “Áreas” deben:

I. Identificar en el aviso de privacidad, aquellos datos y finalidades que requieren del consentimiento de la persona titular de los datos personales, para su tratamiento.

II. Mantener bajo su resguardo una copia del documento en el cual se haya manifestado el consentimiento de la persona titular de los datos personales para el tratamiento de los mismos, cuando este proceda.

III. Documentar que se pone a disposición de la persona titular de los datos personales el aviso de privacidad, en aquellos casos en los cuales sea válido el consentimiento tácito.

II.6. PRINCIPIO DE CALIDAD

Este principio consiste en que las Áreas deberán tomar las medidas necesarias para mantener los datos personales precisos, correctos, completos y actualizados, asegurando así la veracidad de los mismos.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por la persona titular y hasta que éste no manifieste y acredite lo contrario.

Se considera que los datos personales son:

I. Precisos y correctos: Cuando no contienen errores que puedan afectar su veracidad.

II. Completos: Cuando su integridad permite cumplir con las finalidades para las cuales fueron obtenidos y las atribuciones del responsable.

III. Actualizados: Cuando reflejan fielmente la situación actual del titular.

Cuando los datos personales se obtienen indirectamente del titular, las “Áreas” deben garantizar que cumplan con el principio de calidad, considerando la categoría de datos y las condiciones del tratamiento.

Ante la identificación de datos personales que ya no son necesarios para cumplir con las finalidades establecidas en el aviso de privacidad, estos deben ser eliminados después de un período de conservación adecuado.

El periodo de bloqueo supone un plazo adicional y posterior a aquél que es necesario para

el cumplimiento de las finalidades que motivaron el tratamiento de los datos personales.

Su duración, entonces, debe considerar los plazos legales y contractuales que resulten aplicables para demostrar posibles responsabilidades, todo lo cual depende, a su vez, de la
materia de la que se trate.

Asimismo, debe considerarse que en ocasiones existen disposiciones jurídicas que establecen plazos específicos de conservación de datos personales, por ejemplo, en materia, administrativa o histórica, mismos que deberán tomarse en consideración antes de proceder a la supresión de la información.

II.6.1. Actividades vinculadas al Principio de Calidad

Para cumplir con el principio de calidad, las "Áreas" deben:

I. Implementar medidas para que las actualizaciones se reflejen de inmediato en todas las bases de datos que contengan información de la persona titular.

II. Establecer plazos de conservación de la información de acuerdo con las disposiciones legales pertinentes.

III. Desarrollar procedimientos para la conservación, bloqueo y eliminación de datos personales.

II.6.2. Mecanismos para acreditar el cumplimiento del Principio de Calidad

Para demostrar el cumplimiento del principio de calidad, las "Áreas" deben realizar lo siguiente:

I. Elaborar un registro de todas las bases de datos y el tipo de información personal que contienen, facilitando su vinculación cuando sea necesario.

II. Documentar las actualizaciones y supresiones realizadas.

III. Tener procedimientos establecidos para la conservación, bloqueo y supresión de datos personales.

II.7 PRINCIPIO DE PROPORCIONALIDAD

Este principio consiste en tratar solo aquellos datos personales que resulten adecuados, relevantes y necesarios en relación con las finalidades para las cuales se obtuvieron. Se entiende que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas.

II.7.1. Actividades relacionadas con el principio de proporcionalidad

Para garantizar el cumplimiento del principio de proporcionalidad, las "Áreas" encargadas del tratamiento de datos personales deben:

I. Recabar únicamente los datos personales necesarios, apropiados y pertinentes para las finalidades para las que fueron obtenidos.

II. Realizar esfuerzos razonables para tratar al mínimo necesario los datos personales recabados, teniendo en cuenta las finalidades que justifican su procesamiento.

III. Reducir al mínimo necesario el período de procesamiento de datos personales.

II.7.2. Métodos para demostrar el cumplimiento del principio de proporcionalidad

Con el fin de demostrar el cumplimiento del principio de proporcionalidad, las Áreas deben llevar a cabo, como mínimo, las siguientes acciones:

I. Revisar cuidadosamente que en su área solo se soliciten los datos personales indispensables para cumplir con las finalidades pertinentes.

II. Fomentar en su área la solicitud del mínimo necesario de datos personales para alcanzar los objetivos previstos.

III. Apoyar prácticas que reduzcan la obtención y el período de tratamiento de datos personales, y documentarlas

Al respecto, para el cumplimiento al principio de proporcionalidad se advierte que la finalidad del tratamiento se da a conocer al titular de los datos personales, el aviso de privacidad, el cual contendrá los fines para los cuales serán tratados sus datos.

Así pues, dentro del aviso de privacidad se informa que los datos requeridos son exactos y proporcionales para las finalidades delimitadas de manera exacta y precisa mismos que son presentados por las áreas pertenecientes a este Sujeto Obligado siempre que realicen tratamientos de datos personales; dichos documentos de ponen a disposición la persona 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 informar los propósitos del tratamiento, así como los medios de recolección de los datos requeridos.

II.8. PRINCIPIO DE INFORMACIÓN

Independientemente de que se requiera o no el consentimiento de la persona titular de los datos personales para su tratamiento, las Áreas deben informar a los titulares a través del aviso de privacidad de forma clara sobre la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

Las Áreas que traten datos personales, sin importar la función con la que se vincule, deben elaborar y poner a disposición los avisos de privacidad simplificados e integrales que correspondan a los tratamientos llevados a cabo, en los términos establecidos por la Ley General, los Lineamientos Generales, así como en la presente Política, para un debido cumplimiento.

En cualquier momento, la persona titular de datos personales puede revocar el consentimiento que hubiese otorgado para el tratamiento, sin que se le atribuyan efectos retroactivos a la revocación, a través del ejercicio de los derechos de cancelación

y oposición de conformidad con lo dispuesto en la Ley General y los Lineamientos Generales.

II.8.1. Actividades relacionadas con el Principio de Información

Para cumplir con el principio de información, las unidades de transparencia que manejen datos personales deben:

I. Elaborar las versiones de los avisos de privacidad, integral y simplificado necesarios según los tratamientos realizados.

II. Asegurarse de que los avisos de privacidad contengan todos los elementos informativos y normativos aplicables, presentados de manera clara y comprensible, con un diseño y estructura que faciliten su entendimiento, y garantizando su accesibilidad para personas con discapacidad.

III. Publicar el aviso de privacidad en medios electrónicos y físicos siempre que sea posible, dado que el principio de información se materializa a través de la puesta a disposición del aviso de privacidad al titular de los datos personales que serán sujetos a tratamiento.

De este punto reviste el rol protagónico que tiene el aviso de privacidad en la normatividad de datos personales en México, ya que la única manera que se puede cumplir con el principio de información es mediante el aviso de privacidad, mismo que garantiza la salvaguarda del derecho de autodeterminación informativa reconocido en las normatividades de protección de datos personales, además de ser puesto a disposición de la persona titular, por medio de diversos formatos como físicos, electrónicos, ópticos, sonoros visuales o a través de cualquier tecnología que permita su comunicación eficaz.

IV. Colocar el aviso de privacidad en un lugar visible y de fácil acceso para su consulta, sin importar el medio utilizado para su difusión o reproducción.

VI. Fomentar la redacción de los avisos de privacidad buscando que este se encuentre siempre en un lenguaje sencillo, utilizando únicamente la información necesaria para su correcta interpretación de acuerdo con lo establecido en la Ley General y los Lineamientos Generales.

VII. Comunicar el aviso de privacidad a las personas a quienes se transfieran datos personales.

VIII. Considerar y continuar con la implementación de medidas alternativas, de acuerdo con lo establecido en la Ley General y otras disposiciones aplicables, para dar a conocer los avisos de privacidad a través de medios de difusión masiva (como periódicos oficiales, sitios web, carteles u otros similares) en casos donde sea imposible hacerlo de manera directa al titular o esto requiera esfuerzos excesivos.

II.8.2. Actividades para acreditar el cumplimiento del principio de información

Con el propósito de demostrar el respeto al principio de información, las Áreas deben llevar a cabo las siguientes acciones:

I. Contar con los avisos de privacidad integral y simplificado por cada proceso de tratamiento de datos personales que lleven a cabo.

II. Gestionar la publicación de los avisos de privacidad, tanto en su forma simplificada como integral, en la página web oficial, en una sección designada para este fin, para su difusión electrónica.

III. Registrar los lugares y medios donde se divulgan y colocan los avisos de privacidad para un mejor seguimiento y evidencia.

IV. Documentar la comunicación del aviso de privacidad a terceros a quienes se transfieran los datos personales.

II.8.3. AVISOS DE PRIVACIDAD

Documento a disposición de la persona 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 cumpliendo de esta manera con, la obligación de informar al titular de los datos personales, entre otras cosas, quién es el responsable del tratamiento, para qué fines se utilizarán, con quién se compartirán y cómo ejercer

A. la identidad del responsable del tratamiento;

B. las finalidades, primarias y secundarias;

C. los terceros a quienes se transferirán los datos personales (si éste fuera el caso);

D. los mecanismos para que el titular pueda ejercer los derechos vinculados a la protección de datos personales;

E. un procedimiento para comunicar los cambios en los avisos de privacidad;

F. el posible tratamiento de datos personales sensibles, entre otras cuestiones.

Algunos de los requisitos de información específicos que se exigen en la regulación aplicable para el sector público son los siguientes:

A. fecha de elaboración o de última actualización del aviso de privacidad;

B. el fundamento legal que faculta al responsable para llevar a cabo el tratamiento, con independencia de que se requiera o no el consentimiento (incluir artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente que lo faculta o le confiera atribuciones para realizar el tratamiento de datos personales que informa en el aviso de privacidad, precisando su fecha de publicación o, en su caso, la fecha de la última reforma o modificación);

C. el domicilio de la unidad de transparencia (calle, número, colonia, ciudad, municipio o delegación, código postal y entidad federativa, así como su número y extensión telefónica

II.8.3. Avisos de privacidad para cada proceso de tratamiento de datos personales

La Secretaría de Salud, debe disponer de un aviso de privacidad integral y su versión simplificada para cada proceso de tratamiento de datos personales, en concordancia con el principio de información. En casos excepcionales, cuando varios procesos tengan la misma finalidad o función, se puede emplear un único aviso de privacidad, siempre y cuando se especifiquen claramente las finalidades del tratamiento y las unidades administrativas involucradas, evitando ambigüedades para los propietarios de los datos.

II.8.3. Formatos para la elaboración o actualización de avisos de privacidad

Los formatos para crear los avisos de privacidad deben cumplir con los requisitos establecidos por la Ley General y los Lineamientos Generales. Además, se deben estructurar de manera que sean comprensibles para las personas titulares de los datos.

La Unidad de Transparencia puede proporcionar orientación para mantener la coherencia en la presentación de los avisos.

II.8.4. Redacción de los avisos de privacidad

Es fundamental que la redacción de los avisos de privacidad sea clara, sencilla y comprensible para los titulares de los datos. Se deben evitar frases inexactas o ambiguas, así como cualquier intento de influir en las decisiones de los titulares. Además, se debe evitar referenciar a documentos no disponibles para los titulares.

Los enlaces responsables o de apoyo técnico operativo pueden solicitar asesoría técnica a la Unidad de Transparencia en todo momento para la elaboración o actualización de los avisos de privacidad.

II.6.5. Casos en los que se requiere un nuevo aviso de privacidad

Se deberá elaborar un nuevo aviso de privacidad en casos como el cambio de área o denominación, la necesidad de recabar datos sensibles no informados previamente, cambios en las finalidades o condiciones de transferencia de datos, que no estaban contempladas inicialmente, mismo que se actualizara cuando los datos personales

sensibles se obtengan de manera indirecta y se requiera de su consentimiento para realizar el tratamiento.

Asimismo, se requerirá un nuevo aviso de privacidad cuando se modifiquen las condiciones de las transferencias de datos personales o bien se pretendan realizar transferencias no previstas inicialmente, misma que requerirán el consentimiento de la persona titular del dato.

Es propio mencionar que a la fecha de actualización de las presentes políticas no se realizan transferencias a terceros por parte de ningún área adscrita a la Secretaría de Salud.

II.9. PRINCIPIO DE RESPONSABILIDAD

Las Áreas deben garantizar el cumplimiento de todos los principios mencionados anteriormente, promover la adopción de medidas necesarias para su aplicación y demostrar a las personas titulares de los datos y al organismo encargado que se cumplen con las obligaciones de protección de datos personales.

II.9.1. Actividades relacionadas con el principio de responsabilidad

Para cumplir con el principio de responsabilidad, las Áreas deben:

I. Establecer entre el personal la obligatoriedad de cumplir con el programa de protección de datos personales aprobado por el Comité de Transparencia.

II. Establecer actividades de operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continua.

III. Participar en los programas de capacitación y actualización en materia de protección de datos

V. Revisar periódicamente el programa de protección de datos y el Documento de Seguridad para determinar modificaciones necesarias.

V. Establecer procedimientos para recibir y responder a dudas y quejas de los titulares.

II.9.2. Métodos para el cumplimiento del principio de responsabilidad

Para demostrar el cumplimiento del principio de responsabilidad, las Áreas deben:

I. Contar con registros de capacitación del personal en temas relacionados con la protección de datos personales.

II. Mantener un registro de las inquietudes y quejas de los titulares de los datos.

III. Documentar la comunicación interna de la presente Política y del programa de protección de datos aprobado.

IV. Conservar evidencia del cumplimiento de la presente Política.

CAPÍTULO III. Obligaciones

III.1. Obligaciones para la protección de datos personales en la Secretaría de Salud

Aunado a lo anterior las "Áreas" deberán cumplir con:

I. El deber de confidencialidad, y

II. El deber de seguridad

III.2. Deber de confidencialidad

Las Áreas deben establecer controles o mecanismos de cumplimiento obligatorio para las personas que participen en cualquier fase del tratamiento de datos, con el fin de garantizar la confidencialidad de los datos personales, obligación que persistirá incluso después de terminar su relación laboral con la Secretaría de Salud.

Constituye una de las piedras angulares junto con la integridad y la disponibilidad de lo que es la seguridad de la información, características conocidas como la triada de la seguridad, siendo el deber de confidencialidad la obligación que tiene una entidad de resguardar la información que tiene bajo responsabilidad o custodia, considerándola un principio ético al mismo tiempo que funge como obligación para el sujeto obligado, ya que de darse a conocer esta información, podría afectar directamente la esfera jurídica así como la integridad física del titular de la información.

Por otro lado, para poder cumplir con el deber de confidencialidad, es necesario adoptar mecanismos de seguridad de carácter técnico que implican el uso de infraestructura tecnológica en los datos personales en cualquier etapa del ciclo de vida de su tratamiento.

En forma general, los mecanismos de seguridad técnicos para garantizar la confidencialidad se clasifican en:

a) mecanismos de cifrado
b) mecanismos de control de acceso
c) mecanismos de prevención de fuga de datos

La confidencialidad es la propiedad que posee la información manipulada por esta Secretaría misma que no deberá ser divulgada o expuesta a entidades no autorizadas.

Por otro lado, el deber de confidencialidad es la obligación que tiene la Secretaría de resguardar la confidencialidad de lo que tiene bajo responsabilidad o custodia.

Incumplir el deber de confidencialidad establecido en el artículo 21 de la LGPDDPSO.

El artículo 21 confiere la obligación de preservar la confidencialidad de los datos personales a toda persona que realice algún tratamiento a los datos personales durante su ciclo de vida, esta obligación estará vigente aun después de terminar la relación con el titular de los datos, y, por lo tanto, finalice cualquier actividad que tenga que ver con el tratamiento de los mismos.

Mientras que el artículo 63 establece que es una infracción a la Ley no cumplir con el deber de confidencialidad y, por lo tanto, dicho incumplimiento será sancionado.

III.2.1. Actividades relacionadas con el deber de confidencialidad

Para cumplir con el deber de confidencialidad, las Áreas deben:

I. Implementar controles para garantizar la confidencialidad de los datos personales tratados.

II. Establecer cláusulas en los contratos para que los receptores de los datos, tanto del ámbito público como privado, se comprometan a tratar los datos para los fines acordados durante y después de la vigencia del contrato.

III. Realizar campañas de concientización para el personal sobre la importancia de la confidencialidad y el tratamiento adecuado de los datos personales obtenidos en el ejercicio de sus funciones.

IV. Proponer la implementación de mejores prácticas al interior de la Secretaría para garantizar la secrecía de los datos personales, cuando así proceda.

Para acreditar el cumplimiento del deber de confidencialidad, las Áreas llevarán a cabo, como mínimo, las siguientes acciones:

I. Incluir en el Documento de Seguridad los controles y medidas de seguridad aplicadas para garantizar la confidencialidad de los datos personales.

II. Generar evidencia de los controles implementados para asegurar la confidencialidad de los datos.

III. Establecer cláusulas de confidencialidad de datos personales en los contratos cuando sea pertinente, en relación con transferencias o remisiones.

IV. Mantener evidencia documental de la participación del personal en cursos, talleres, seminarios u otras actividades relacionadas con el tratamiento de datos personales, según los roles y niveles de control pertinentes.

V. Documentar la implementación de buenas prácticas que garanticen la confidencialidad de los datos tratados.

VI. Identificar dentro de los flujos de datos personales las funciones y obligaciones de las personas que los tratan.

VII. Identificar los datos personales, así como el personal que tiene acceso a ellos, será una medida fundamental ya que es la base para combatir la amenaza de divulgación de datos personales por personal interno de la Organización.

VIII. establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización.

IX. Ejecutar medios de verificación y auditoria interna que permita determinar que el área tratante de los datos cuenta con las medidas o mecanismos suficientes para cumplir con el deber de confidencialidad.

X. De observarse durante la verificación que la vulneración Atribuible al área responsable del tratamiento de los datos, será necesario la notificación al Instituto Nacional de Transparencia, así como a la persona titular de los datos.

Apostrofe a lo anterior, el propio Instituto podría dar vista al Órgano Interno de Control a fin de que inicie las acciones conducentes, de estimarlo pertinente.

III.3. Deber de seguridad

Las Áreas de la Secretaría de Salud adoptarán e implementarán medidas de seguridad físicas, técnicas y administrativas para asegurar la protección de los datos personales tratados, con el objetivo de prevenir cualquier tipo de afectación a estos datos y a sus propietarios.

III.3.1. Actividades relacionadas con el deber de seguridad

Para cumplir con el deber de seguridad, las Áreas llevarán a cabo, al menos, las siguientes acciones:

I. Desarrollar e implementar políticas de gestión que consideren el tipo de datos personales recopilados, su tratamiento y ciclo de vida.

II. Identificar al personal autorizado en cada una de las Áreas de la Secretaría de Salud para intervenir en el tratamiento de datos personales, así como definir sus funciones y responsabilidades correspondientes.

III. Realizar actividades de cooperación institucional para realizar análisis de riesgos de los datos personales tratados y de los sistemas utilizados para su tratamiento.

IV. Implementar acciones de cooperación institucional para prevenir y mitigar amenazas o vulneraciones de los datos personales en posesión.

V. Supervisar y revisar regularmente las medidas de seguridad adoptadas para garantizar la protección de los datos personales bajo custodia.

VI. Fomentar la capacitación del personal involucrado en el tratamiento de datos personales de acuerdo con sus niveles de responsabilidad.

Una de los deberes es garantizar la integridad de la información de tal modo, que su creación, modificación o eliminación la podrán realizar solo entidades autorizadas.

En el caso de la disponibilidad, implica que la información estará lista para para acceder a ella en el momento que se necesite y en la forma requerida.

Los procedimientos para garantizar la seguridad de la información son actividades que, en su conjunto, conforman un proceso sistemático de gestión de seguridad de la información, deben ser creados bajo un marco normativo que contenga una estructura de gobierno y un procedimiento de gestión de ciclo de vida de las políticas que asegure su correcta creación, autorización, difusión, cumplimiento y actualización.

III.3.2. Métodos para demostrar el cumplimiento del deber de seguridad

Para demostrar el cumplimiento del deber de seguridad, las Áreas deberán llevar a cabo, como mínimo, las siguientes acciones:

I. Elaborar un inventario de datos y sistemas de tratamiento de datos personales.

II. Comunicar al personal las políticas de protección de datos implementadas y conservar evidencia de esta comunicación.

III. Mantener un registro de amenazas o vulneraciones de datos personales, así como de las medidas tomadas para mitigarlas.

IV. Implementar y documentar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recopilados, así como las acciones de monitoreo, análisis y revisión necesarias para mantenerlas actualizadas y mejorarlas.

VI. Conservar evidencia documental de la participación del personal en actividades de capacitación relacionadas con la protección de datos personales.

CAPÍTULO IV. PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES

IV.1. Propósito y Alcance del Programa de Protección de Datos Personales

Se implementará un programa de protección de datos personales, sujeto a la consideración y aprobación, de ser necesario, por parte del Comité de Transparencia. Este programa tiene como objetivo establecer las directrices generales para mantener el cumplimiento de los principios y obligaciones, así como garantizar el derecho a la protección de datos personales dentro de la institución.

IV.2. Actualización del Programa de Protección de Datos Personales

El programa de protección de datos personales deberá estar actualizado a fin de asegurar un desarrollo continuo de las actividades, el cual podrá ser sometido a su revisión y actualización al Comité de Transparencia de la Secretaría de Salud conforme a lo estipulado por la normativa aplicable, con el fin de lograr mejoras continuas.

IV.3. Contenido Esencial del Programa de Protección de Datos Personales

El Programa de Protección de Datos Personales de la Secretaría de Salud deberá contemplar como mínimo:

I. Marco de trabajo necesario para la protección de datos personales en posesión de la Secretaría.

II. Un análisis de los problemas, necesidades o áreas de oportunidad identificadas para el cumplimiento de los principios y obligaciones en materia de protección de datos personales dentro de la institución.

III. Las actividades propuestas para cumplir con las obligaciones en la materia, incluyendo su viabilidad, objetivos y su vinculación con las necesidades detectadas.

IV. Una propuesta de medición para cuantificar el avance y cumplimiento de las actividades propuestas.

IV.4. Supervisión del Programa de Protección de Datos Personales

Se deberá dar seguimiento de las actividades del programa de protección de datos personales e informará al Comité de Transparencia sobre su ejecución.

CAPÍTULO V. DOCUMENTO DE SEGURIDAD

V.1. Propósito y Alcance del Documento de Seguridad

Este Sujeto Obligado, a través de sus Áreas deberá contar con el Documento de Seguridad correspondiente, como parte de sus mecanismos para garantizar el cumplimiento del deber de seguridad en materia de datos personales. Este documento tiene como objetivo establecer de manera general las medidas de seguridad técnicas, físicas y administrativas para asegurar la confidencialidad, integridad y disponibilidad de los datos personales tratados.

El Documento de Seguridad deberá incluir al menos:

I. Un inventario de datos personales y sistemas de tratamiento.

II. Las funciones y responsabilidades de las personas que manejan datos personales.

III. Un análisis de riesgos.

IV. Un análisis de brechas.

V. Un plan de trabajo.

VI. Mecanismos de monitoreo y revisión de las medidas de seguridad.

VII. Un programa general de capacitación.

V.2. Actualizaciones al Documento de Seguridad

Las actualizaciones al Documento de Seguridad requerirán la participación de todas las Áreas correspondientes, a través de las personas asignadas a nivel de mando y técnico operativo, estas personas deberán adherirse en todo momento a los principios y obligaciones establecidos por la Ley General, los Lineamientos Generales y otras disposiciones legales aplicables. De acuerdo con lo estipulado en la Ley General, se actualizará el Documento de Seguridad en los siguientes casos:

I. Cuando haya cambios sustanciales en el tratamiento de los datos personales que resulten en un cambio en el nivel de riesgo.

II. Como parte de un proceso de mejora continua derivado de la revisión y monitoreo del sistema de gestión, o para mitigar el impacto de una violación de seguridad.

III. En respuesta a la implementación de acciones correctivas y preventivas frente a una violación de seguridad.

Independientemente de los casos mencionados, el Documento de Seguridad podrá ser actualizado cuando resulte necesario.

Cuando algún Área se encuentre en los casos mencionados, el enlace designado como responsable deberá solicitar por escrito al Comité de Transparencia de la Secretaría de Salud las actualizaciones necesarias, y este resolverá en consecuencia. Los enlaces designados y el enlace técnico operativo pueden buscar orientación de la Unidad de Transparencia de la Secretaría de Salud para la elaboración o cualquier acción relacionada con el Documento de Seguridad.

V.3. Violaciones a la Seguridad de los Datos

Se considerarán violaciones a la seguridad de los datos personales, de acuerdo con lo establecido en la Ley General, los siguientes eventos:

I. Pérdida o destrucción no autorizada.

II. Robo, extravío o copia no autorizada.

III. Uso, acceso o tratamiento no autorizado.

IV.-. Daño, alteración o modificación no autorizada.

V.4. Acciones ejecutadas en caso de vulneraciones a datos personales.

En situaciones donde las violaciones afecten de manera significativa los derechos a la privacidad de las personas titulares de los datos personales y datos sensibles, como puede ser; datos relacionados con el estado de salud, las unidades administrativas pertinentes deben elaborar un informe detallado que incluya, al menos, los siguientes aspectos:

I. Descripción del incidente.

II. Identificación de los datos personales comprometidos.

III. Informar a la persona titular del dato el tipo de vulneración acontecida.

IV. Notificar al Instituto Nacional de Transparencia, mismo que podría dar vista al Órgano Interno de Control a fin de que inicie las acciones conducentes, de estimarlo pertinente.

V. Recomendaciones para el titular de los datos afectado respecto a las medidas que puede tomar para proteger sus intereses.

VI. Acciones correctivas implementadas para mitigar la violación.

VII. Datos de contacto del enlace responsable y técnico operativo de apoyo de la unidad administrativa correspondiente, a quien el titular de los datos afectado puede dirigirse para obtener más información.

Este informe deberá ser enviado a la Unidad de Transparencia en un plazo máximo de dos días hábiles posteriores a la confirmación de la violación, para su divulgación entre los titulares de datos involucrados y el Comité de Transparencia de la Secretaría de Salud.

Además, las unidades administrativas deben incluir en el informe a notificar al INAI a través de la Unidad de Transparencia los siguientes puntos:

Fecha y hora de identificación de la violación.

Fecha y hora de inicio de la investigación sobre la violación.

Descripción detallada de la violación.

Circunstancias en torno a la violación.

Categorías y número aproximado de titulares afectados.

Sistemas de tratamiento y datos comprometidos.

Posibles consecuencias de la violación.

Cualquier otra información relevante.

Que el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos señala que 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 al uso de su información personal, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos personales, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros, siendo así que cualquier interés, individual o colectivo, cualificado, actual, real y jurídicamente relevante, que puede poner en riesgo la esfera jurídica más íntima de la persona titular

del dato en sentido amplio, que puede ser de índole económica, profesional, de salud, o de cualquier otra, debe ser notificada y dado sea el caso; resarcida en medida de lo posible.

En casos donde no sea viable notificar directamente a los propietarios de los datos personales, las unidades administrativas deben implementar medidas alternativas de comunicación, como publicación en medios oficiales, sitios web, carteles, u otros medios similares.

CAPÍTULO VI. PROGRAMA DE CAPACITACIÓN Y ACTUALIZACIÓN

Se implementará un Programa de Capacitación y Actualización en protección de datos personales, adaptado a los diferentes roles y responsabilidades del personal que maneja información personal.

VI.1. Elaboración y aprobación del programa de capacitación y actualización

El Comité de Transparencia de la Secretaría de Salud aprobará el Programa de Capacitación y Actualización propuesto por la Unidad de Transparencia, el cual analiza las necesidades de capacitación de las “Áreas” y la oferta disponible, incluyendo aquella proporcionada por el INAI.

CAPÍTULO VII. EJERCICIO DE LOS DERECHOS ARCO

VII.1. Conceptos de los derechos ARCO.

Para los propósitos de este procedimiento, se definen los derechos ARCO de la siguiente manera:

I. Acceso: Es el derecho de la persona titular de los datos para solicitar a la Secretaría de Salud el acceso a sus datos personales en posesión de la misma, así como obtener información sobre cómo se manejan y tratan dichos datos.

II. Rectificación: Consiste en el derecho que tiene la persona titular de los datos para requerir a la Secretaría de Salud la corrección de cualquier dato personal que sea inexacto, incompleto o esté desactualizado.

III. Cancelación: Este derecho permite a la persona titular solicitar a la Secretaría de Salud que sus datos personales sean bloqueados y eliminados de los archivos, registros y sistemas institucionales, para que dejen de ser tratados y no estén más en posesión de la Secretaría.

IV Oposición: Es el derecho de la persona titular para solicitar a la Secretaría de Salud que se abstenga de utilizar sus datos personales para ciertos fines o que se detenga su uso, con el fin de prevenir algún daño o perjuicio a su persona.

VII.2. Medios disponibles para la recepción de solicitudes de ejercicio de los derechos ARCO.

Para presentar solicitudes de derechos ARCO, se pueden utilizar los siguientes medios de recepción:

I. Dirigiéndose a la Unidad de Transparencia, ubicada en avenida Marina Nacional, número. 60, Planta Baja, Colonia Tacuba, Demarcación Territorial Miguel Hidalgo, Ciudad de México, código postal 11410.

II. Enviando un correo electrónico a: unidadenlace@salud.gob.mx;

III. Utilizando el servicio postal o de mensajería, con dirección al domicilio mencionado anteriormente;

IV. Accediendo a la Plataforma Nacional de Transparencia (PNT) a través del siguiente enlace: http://www.plataformadetransparencia.org.mx/ ; y

V. Llamando al teléfono del INAI: 800 835 4324.

VI Llamando al teléfono de la Unidad de Transparencia de la Secretaría de Salud, 55 5062 1600, extensión 42011

VI.3. Relación entre la Secretaría de Salud y el/la encargado.

Se entiende por remisión toda comunicación de datos personales realizada entre la Secretaría de Salud y el/la encargado/a, ya sea dentro o fuera del territorio mexicano.

El Responsable puede encomendar el tratamiento de datos personales a terceros, ya sean personas físicas o jurídicas, únicamente cuando exista un acuerdo formalizado mediante un instrumento jurídico suscrito por funcionarios autorizados para tal fin.

a) Tratar los datos por cuenta de un responsable: El encargado solo debe tratar los datos objeto del encargo para cumplir los fines del tratamiento que decida e instruya el responsable, no los suyos propios. Es decir, la condición de encargado se refiere y se mantiene únicamente en los tratamientos que se realicen por cuenta de uno o varios responsables siguiendo sus instrucciones.

b) El encargado no tiene poder de decisión acerca de los tratamientos: Las decisiones sobre el uso, destino y finalidad del tratamiento corresponden al responsable, siendo el encargado el que ejecuta sus instrucciones respecto al tratamiento.

c) Es ajeno a la organización del responsable: No debe confundirse al encargado del tratamiento con el empleado o empleados que realizan algún tratamiento dentro de la organización del responsable. El encargado pertenece a una entidad diferente, es decir, otra empresa, un profesional independiente o un prestador de servicios, por señalar algunos ejemplos.

No debe pasar por inadvertido que el encargado se limita a actuar en virtud de las instrucciones conferidas por el responsable del tratamiento, y por eso la definición señala que éste ejecutará sus acciones “por cuenta del responsable”. Por lo anterior, la condición de responsable o encargado del tratamiento viene determinada en virtud de la capacidad de decisión sobre los fines y medios del tratamiento, siendo el encargado un sujeto que no cuenta con dicha facultad exclusiva.

VI.4. Obligaciones generales del/la encargado/a

El/la encargado/a debe procesar los datos personales en nombre y por cuenta de la Secretaría de Salud (responsable), limitando sus acciones al alcance y condiciones estipuladas por esta última, sin tener autoridad para decidir sobre la naturaleza del tratamiento.

VI.5. Formalización del acuerdo según el aviso de privacidad

Cualquier acuerdo formalizado entre el Responsable y el/la encargado/a debe ajustarse a lo establecido en la Ley General, los Lineamientos Generales y la presente política, así como a las condiciones previamente informadas en el aviso de privacidad, que se ha puesto a disposición de los titulares de los datos personales.

Así, la LGPDPPSO en su artículo 66 establece que las transferencias deberán formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

La obligación de formalización de las transferencias no será aplicable cuando: La transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos.

La transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, 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 área responsable.

De la misma forma, debe notarse que, en el caso de las transferencias nacionales, la Secretaría de Salud, a través del Área responsable, así como el receptor de los datos personales queda sujeto al cumplimiento de las obligaciones de confidencialidad y respeto al principio de finalidad.

Finalmente, para que la transferencia de datos personales sea lícita, será necesario que el tercero receptor de los datos se obligue a proteger y dar tratamiento a los datos conforme a las condiciones de la LGPDPPSO así como a los términos convenidos en el aviso de privacidad.

VI.6. Obligaciones específicas del/la encargado/a en el contrato

El contrato entre el Responsable y el/la encargado/a deberá contener, al menos, las siguientes obligaciones para este último:

I. Tratar los datos personales siguiendo las instrucciones de Responsable.

II. No utilizar los datos personales para fines distintos a los indicados por el Responsable.

III. Implementar las medidas de seguridad requeridas por la normativa.

IV. Informar al Responsable en caso de una violación de datos.

V. Mantener la confidencialidad de los datos tratados.

VI. Eliminar o devolver los datos al finalizar la relación contractual.

VII. No transferir los datos sin autorización expresa de Responsable.

VIII. Permitir inspecciones por parte del INAI o la Secretaría de Salud.

IX. Colaborar con investigaciones del INAI, proporcionando la información necesaria.

X. Mantener documentación que acredite el cumplimiento de estas obligaciones.

VI. 7 Ciclo de vida de datos personales

Los datos personales como cualquier tipo de información están sometidos a un ciclo de vida conformado por diversas fases, constituyendo el ciclo de vida de la información, las cuales son:

I. **Planear:** Consiste en el entendimiento de cómo la información será utilizada en los procesos de la organización, determinar el valor del activo, realizar su clasificación, identificar sus objetivos y definir la arquitectura tecnológica para su procesamiento.

II. **Diseñar**: Se detallan aspectos de la información como su representación, operación de los sistemas informáticos, desarrollo de estándares y definiciones para los procesos de tratamiento de datos.

III. **Construir:** La fase de construcción y adquisición de datos es donde la información es creada, adquirida o alimentada de fuentes externas.

IV. **Operar**: La fase de uso y operación corresponde a la etapa más importante del ciclo de vida de la información.

> *"En esta fase se realizan actividades de almacenamiento en forma electrónica o en papel (inclusive en la memoria humana), actividades de compartición mediante mecanismos de distribución como pudiera ser un sistema de mensajería o una base de datos y propiamente actividades de uso de consulta o procesamiento para completar las tareas importantes de la organización"*

V. **Monitorear**: En la fase de monitoreo se garantiza que las fuentes de información continúen operando correctamente y que la información se mantenga actualizada y de calidad.

VI. **Eliminar**: La fase de eliminación implica que la información ya no es de utilidad en la operación del día a día de la organización, por lo que se debe aislar y retener o en su defecto destruir.

Apéndice a lo anterior, las “Áreas” responsables en coordinación con sus respectivas “Áreas” de archivos tienen el deber de identificar el plazo de conservación, en razón de que cada dato personal tiene un tiempo de vida útil, según sea el tratamiento, posterior a su periodo de conservación archivística.

De esta manera, cuando se haya cumplido la finalidad para la cual haya sido recabado, debe desvincularse del propio sistema de tratamiento para ser bloqueado y posteriormente suprimido, de conformidad con o establecido en la Ley General de Archivo.

VI.8. Subcontratación de servicios que impliquen el tratamiento de datos personales

El Responsable, en caso de requerirlo podrá subcontratar servicios que impliquen el tratamiento de datos personales previamente remitidos, siempre y cuando el contrato entre el Responsable y el subcontratista lo permita. Este contrato debe formalizarse mediante un instrumento jurídico que detalle la relación y las obligaciones del subcontratista.

VI.9. Proveedores/as de servicios de cómputo en la nube y otras materias

El Responsable puede utilizar servicios de cómputo en la nube y otros servicios relacionados, siempre que el proveedor garantice el cumplimiento de las normativas vigentes. Para ello, se debe solicitar un dictamen técnico y firmar un contrato que establezca las cláusulas necesarias para la protección de los datos personales.

CAPÍTULO VII. DE LAS TRANSFERENCIAS DE DATOS PERSONALES

VII.1. Transferencias a terceros

El Responsable puede transferir datos personales a terceros, tanto nacional como internacionalmente, de acuerdo con lo establecido en la normativa vigente.

VII.2. Condiciones generales de las transferencias

Toda transferencia de datos personales debe contar con el consentimiento del titular, a menos que existan excepciones previstas en la ley. Las Áreas deben informar al titular sobre la finalidad y el destinatario de la transferencia, permitiendo que el titular manifieste su consentimiento.

X.3. Comunicación de avisos de privacidad a terceros receptores

En todas las transferencias de datos personales, el Responsable debe comunicar el aviso de privacidad correspondiente al receptor de los datos, documentando esta comunicación de manera detallada.

VII.4. Formalización de la transferencia

Toda transferencia de datos personales debe formalizarse mediante un instrumento jurídico que establezca las obligaciones y responsabilidades de las partes. Sin embargo, existen excepciones para ciertos tipos de transferencias nacionales o internacionales.

VII.5. Transferencias internacionales

Antes de realizar transferencias internacionales de datos personales, el Responsable debe asegurarse de que el receptor en el extranjero se comprometa a proteger los datos de acuerdo con las leyes mexicanas. En caso necesario, se puede solicitar la opinión del INAI respecto a estas transferencias internacionales.

ANEXO 1 “UNIDADES ADMINISTRATIVAS”

SECRETARÍA DE SALUD	
Consejo de Salubridad General	**CSG**
Oficina del C. Secretario	**SS**
Subsecretaría de Integración y Desarrollo del Sector Salud	**SIDSS**
Subsecretaría de Prevención y Promoción de la Salud	**SPPS**
Unidad de Administración y Finanzas	**UAF**
Oficina del Abogado General	**OAG**
Comisión Coordinadora de Institutos Nacionales de Salud y Hospitales de Alta Especialidad	**CCINSHAE**
Unidad Coordinadora de Vinculación y Participación Social	**UCVPS**
Unidad de Análisis Económico	**UAE**
Dirección General de Calidad y Educación en Salud	**DGCES**
Dirección General de Comunicación Social	**DGCS**
Dirección General de Coordinación de los Hospitales Federales de Referencia	**DGCHFR**
Dirección General de Coordinación de los Hospitales Regionales de Alta Especialidad	**DGCHRAE**
Dirección General de Coordinación de los Institutos Nacionales de Salud	**DGCINS**
Dirección General de Desarrollo de la Infraestructura Física	**DGDIF**
Dirección General de Evaluación del Desempeño	**DGED**
Dirección General de Información en Salud	**DGIS**
Dirección General de Planeación y Desarrollo en Salud	**DGPLADES**
Dirección General de Políticas de Investigación en Salud	**DGPIS**
Dirección General de Programación y Presupuesto	**DGPyP**
Dirección General de Promoción de la Salud	**DGPS**
Dirección General de Recursos Humanos y	**DGRHyO**

Organización	
Dirección General de Recursos Materiales y Servicios Generales	**DGRMySG**
Dirección General de Relaciones Internacionales	**DGRI**
Dirección General de Tecnologías de la Información	**DGTI**
Dirección General de Epidemiología	**DGEPI**
Secretariado Técnico del Consejo Nacional de Salud	**STCONASA**
Secretariado Técnico del Consejo Nacional para la Prevención de Accidentes	**STCONAPRA**
ÓRGANOS ADMINISTRATIVOS DESCONCENTRADOS	**SIGLAS**
Administración del Patrimonio de la Beneficencia Pública	**APBP**
Centro Nacional de Equidad de Género y Salud Reproductiva	**CNEGSR**
Centro Nacional de Excelencia Tecnológica en Salud	**CENETEC**
Centro Nacional de la Transfusión Sanguínea	**CNTS**
Centro Nacional de Trasplantes	**CENATRA**
Centro Nacional de Programas Preventivos y Control de Enfermedades	**CENAPRECE**
Comisión Nacional de Salud Mental y Adicciones	**CONASAMA**
Centro Nacional para la Prevención y el Control del VIH/SIDA	**CENSIDA**
Centro Nacional para la Salud de la Infancia y la Adolescencia	**CENSIA**
Comisión Nacional de Bioética	**CONBIOETICA**

ANEXO 2 REQUISITOS PARA LA RECEPCIÓN DE SOLICITUDES DE EJERCICIO DE LOS DERECHOS ARCO.

La solicitud debe presentar ante el responsable que posea los datos personales respecto de
los cuales requieras el acceso, rectificación, cancelación u oposición.

Los requisitos que debe tener la solicitud son:

- El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;

- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;

- De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;

- 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;

- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y

- La persona solicitante, podrá acompañar su solicitud, en caso de ser necesario, el medio magnético, electrónico o el mecanismo a través del cual requiere la reproducción de estos, el cual podrá entregarse una vez que la persona titular sea notificada sobre la procedencia del ejercicio del derecho solicitado.

- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Adicionalmente se informa que la Secretaría de Salud, a través del área responsable y por medio de la Unidad de Transparencia deberá atender la solicitud en la modalidad requerida por la persona titular salvo que exista una imposibilidad física o jurídica que lo

limite a reproducir los datos en dicha modalidad, ofreciendo en este caso otras modalidades de entrega; fundando y motivando dicha actuación.

De igual manera cuando la persona titular del dato no pueda cubrir los costos de reproducción o envió de sus datos personales en virtud de una situación socioeconómica, deberá de manifestar la circunstancia en la solicitud, a efecto de que la Unidad de Transparencia determine lo conducente conforme a lo previsto en el artículo 50 de la LGPDPPSO.

Con relación a los requisitos específicos, según el derecho que se quiera ejercer, están los siguientes:

Acceso: Debe indicar la modalidad en la que el titular prefiere que se reproduzcan los datos personales solicitados.

Rectificación: El titular debe especificar las modificaciones que se solicitan a los datos personales, así como aportar los documentos que sustenten la solicitud.

Cancelación: Deben señalar las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable.

Oposición: El titular debe manifestar las causas o la situación que llevan a solicitar que concluya el tratamiento de sus datos personales, así como el daño que le causaría que dicho tratamiento continúe. En el caso de que la solicitud se refiera a un tratamiento en lo particular, se deben indicar las finalidades específicas respecto de las cuales se solicita el ejercicio del derecho.

Función de la Unidad de Transparencia en el ejercicio de los Derechos ARCO

La Unidad de Transparencia deberá auxiliar al titular en la elaboración de las solicitudes para el ejercicio de derechos ARCO, así como informar sobre la obligación del titular de acreditar su identidad. Deberá atender a cada titular atendiendo su situación particular, facilitando la información que estos requieran.

Otra función de la unidad es cuando ya han recibido la solicitud y esta haya sido admitida deberá turnar la misma al área correspondiente que conforme a sus atribuciones, facultades, competencias o funciones puedan o deban poseer los datos.

Acreditación de la identidad del titular y en su caso del representante

Como se señaló anteriormente, un requisito fundamental para el ejercicio de derechos ARCO es que previamente se demuestre que quien desea ejercer el derecho, es el titular de los datos personales.

Para ello, es necesario que previo a que se ejerza el derecho de acceso, rectificación, cancelación u oposición se acredite la identidad del titular de los datos personales y de su representante, en caso de que la solicitud se realice por medio de este último, a través de la presentación de una identificación oficial.

Hay tres medios para acreditar la identidad:

➢ Identificación oficial

➢ Instrumentos electrónicos o mecanismos de autenticación, como la Firma Electrónica.

➢ Mecanismos establecidos por el responsable de manera previa, siempre y cuando permitan de forma inequívoca la acreditación de la identidad del titular.

Por su parte el representante deberá acreditar su personalidad mediante:

➢ Copia de identificación oficial del titular de los datos;

➢ Identificación del representante, y

➢ Instrumento notarial o Carta Poder (firmada por dos testigos y sus respectivas identificaciones)

Acreditación de la personalidad en supuestos de menores de edad, en estado de interdicción o fallecidas

Por su parte en el caso de las solicitudes de ejercicio de derechos ARCO de una persona menor de edad, en estado de interdicción o incapacidad legal, o fallecida. Cuando se pretenda ejercer los derechos ARCO con relación a datos personales de una persona menor de edad o en estado de interdicción o incapacidad legal se deberá de observar lo

dispuesto en las leyes civiles y la representación será conforme a las reglas que establezca dicha normatividad.

En cuanto a los datos personales de una persona fallecida, sólo la persona que acredite tener interés jurídico, conforme a las leyes aplicables, podrá ejercer los derechos ARCO, siempre que el titular de los datos personales hubiere expresado fehacientemente su voluntad o exista un mandato judicial al respecto, y se trate de una solicitud presentada ante un responsable del sector público.

En general, la representación de estas personas podrá acreditarse mediante los siguientes documentos:

Menores de edad

En el caso de que los padres tengan la patria potestad del menor y sean los que deseen ejercer los derechos ARCO, además de acreditar la identidad del menor deberán presentar los siguientes documentos:

➢ Acta de nacimiento del menor de edad;

➢ Documento de identificación oficial del padre o de la madre que pretenda ejercer el derecho, y

➢ Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o madre, según sea el caso, ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

En los casos en que la patria potestad la ejerce una persona distinta a los padres, y es ella quien desea ejercer los derechos ARCO, además de acreditar la identidad del menor deberá presentar los siguientes documentos:

➢ Acta de nacimiento del menor de edad;

➢ Documento legal que acredite el ejercicio de la patria potestad;

Acreditación de la personalidad en los artículos 78, 79 y 80 de la Ley General

➢ Documento de identificación oficial de quien ejerce la patria potestad y presenta la solicitud, y

➢ Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

Cuando quien desee ejercer los derechos ARCO sea el tutor del menor de edad, además de acreditar la identidad del menor, deberá presentar los siguientes documentos:

➢ Acta de nacimiento del menor de edad;

➢ Documento legal que acredite la tutela;

➢ Documento de identificación oficial del tutor, y

➢ Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

Personas en estado de interdicción o incapacidad legal:

➢ Instrumento legal de designación del tutor;

➢ Documento de identificación oficial del tutor, y

➢ Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

Personas fallecidas:

➢ Acta de defunción;

➢ Documento(s) que acrediten el interés jurídico de quien presenta la solicitud, y

➢ Documento de identificación oficial de quien presenta la solicitud.

Procedimiento y plazos a seguir en una solicitud de ejercicio de derechos ARCO

El procedimiento inicia cuando el titular o su representante presentan la solicitud de ejercicio de derechos ARCO respecto de los datos personales de los cuales se requiere el acceso, rectificación, cancelación u oposición.

A continuación, se describe el procedimiento y plazos para la presentación y atención de las
solicitudes de derechos ARCO:

Plazo para el titular:

Paso 1. Recepción de la solitud formulada por el titular o su representante.
* En cualquier momento.

La solicitud debe acusarse de recibida constando fecha de la misma.

Paso 2. Informará al titular si procede o no el ejercicio del derecho solicitado.
* 20 días hábiles.

Paso 3. En caso de que haya procedido el ejercicio del derecho, el responsable llevará a cabo
las acciones necesarias para hacerlo efectivo.

* 15 días hábiles.

El plazo antes señalado se puede ampliar por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

Ahora bien, si la solicitud no cuenta con la información suficiente en su solicitud para el ejercicio de los derechos ARCO, entre el paso 1 y 2, el responsable podrá solicitar al titular que proporcione la información faltante por medio de un escrito denominado “prevención”, el cual se deberá emitir en un plazo de máximo 5 días hábiles contados a

partir del día siguiente de la presentación de la solicitud. El titular contará con 10 días hábiles, después de recibir la prevención, para proporcionar la información requerida, pues de lo contrario se tendrá como no presentada su solicitud.

Recuerda que, aunque no proceda el ejercicio de los derechos ARCO, el responsable deberá responder la solicitud, explicando las causas de la improcedencia respectiva, en el plazo de 20 días hábiles señalado en el paso 2.

Por otra parte, toma en cuenta que cuando la normatividad aplicable a determinados tratamientos de datos personales establezca un trámite o procedimiento diferente para solicitar el ejercicio de derechos ARCO, procederá lo siguiente:

➢ El responsable deberá informar al titular sobre la existencia de dicho trámite o procedimiento en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud, a fin de que el titular decida si presentará su solicitud de ejercicio de derechos ARCO de acuerdo con el trámite específico o con base en el procedimiento establecido en la ley.

Gratuidad o en su costo del ejercicio de derechos ARCO

El ejercicio de los derechos ARCO es gratuito, y sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío de información, para ello hay determinadas reglas entre las que se encuentran las siguientes:

➢ Cuando el titular proporcione un medio magnético, electrónico o el mecanismo necesario para la reproducción de los datos personales, por ejemplo, un USB o un Disco Compacto, éstos deberán ser entregados sin costo.

➢ La información deberá ser entregada sin costo cuando implique la entrega de no más de 20 hojas simples.

Causas en las que será improcedente el ejercicio de derechos ARCO.

Conforme a lo establecido en el artículo 55 de la LGPDPPSO las causales en las que no será procedente el ejercicio de derechos ARCO son:

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;

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.

De conformidad con el artículo 104 de la LGPDPPSO, la persona titular del dato personal podrá interponer un recurso de revisión ante el Instituto o, en su caso, ante los Organismos garantes o la Unidad de Transparencia de la Secretaría que haya conocido de la solicitud para el ejercicio de los derechos ARCO, dentro de un plazo que no podrá exceder de quince días contados a partir del siguiente a la fecha de la notificación de la respuesta, mismo que procederá en los siguientes supuestos:

I. Se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;

II. Se declare la inexistencia de los datos personales;

III. Se declare la incompetencia por el responsable;

IV. Se entreguen datos personales incompletos;

V. Se entreguen datos personales que no correspondan con lo solicitado;

VI. Se niegue el acceso, rectificación, cancelación u oposición de datos personales;

VII. No se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia;

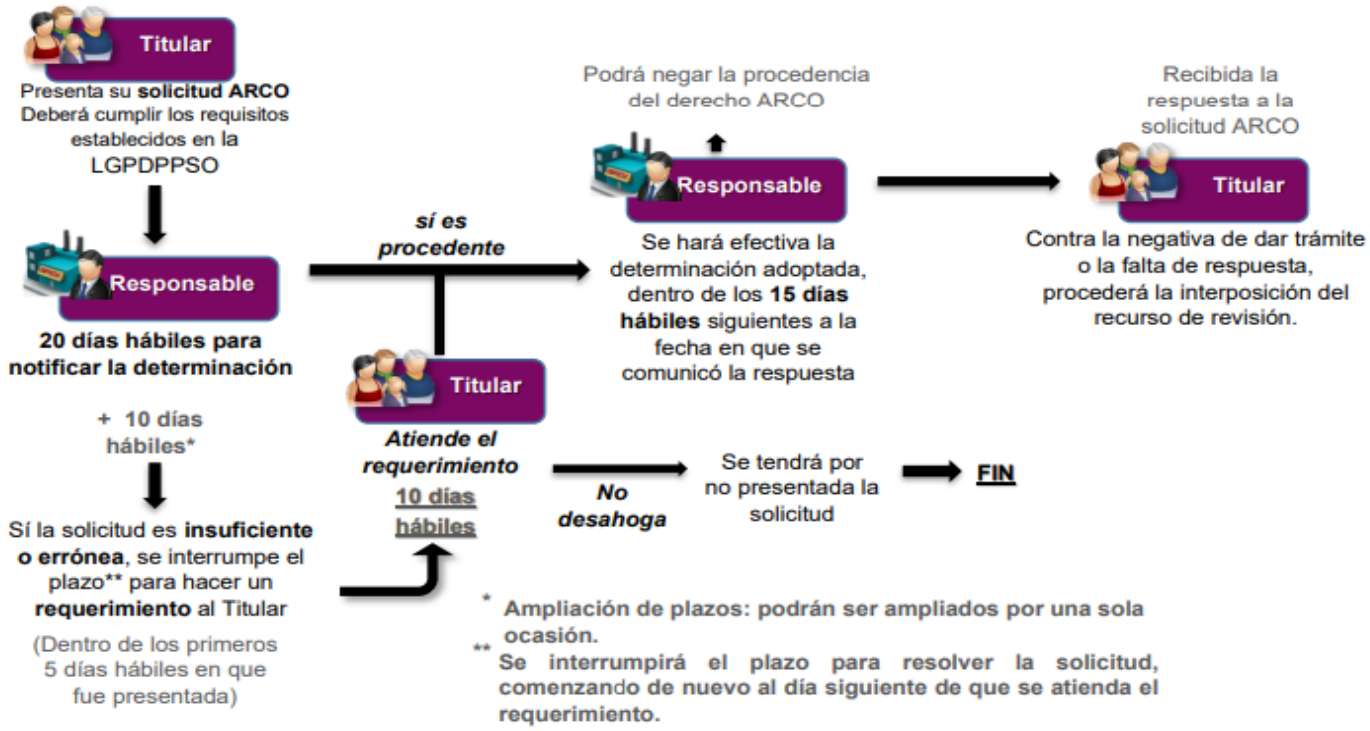
VIII. Se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;

IX. El titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales;

X. Se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos;

XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO, y

XI. En los demás casos que dispongan las leyes.



TRANSITORIOS

Artículo Primero: La presente Política entrará en vigor a partir de su aprobación por parte del Comité de Transparencia de la Secretaría de Salud y deberán difundirse al interior de la Secretaría de Salud, asimismo, publicarse en el apartado correspondiente a protección de datos personales.

Artículo Segundo: La persona servidora pública responsable del área de protección de datos personales llevará a cabo programas de capacitación y concientización sobre la nueva Política interna en materia de protección de datos personales.

Artículo Tercero: La Política interna en materia de protección de datos personales de la Secretaría de Salud, serán objeto de revisión periódica, con el fin de asegurar su actualización.

Artículo cuarto: La presente Política tendrá un carácter vinculante para todo el personal y "Áreas" de la institución, y su cumplimiento será obligatorio en todos los niveles jerárquicos.