Salud
Secretaría de Salud

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN SALVADOR ZUBIRÁN

POLÍTICAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

INSTITUTO NACIONAL DE CIENCIAS MÉDICAS Y NUTRICIÓN "SALVADOR ZUBIRAN"

NOVIEMBRE 2024

CONTENIDO

I. INTRODUCCIÓN

El Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, es un Organismo Público Descentralizado de la Administración Pública Federal, agrupado en el Sector Salud, con personalidad jurídica y patrimonio propio, que tiene por objeto principal, la investigación científica y la prestación de servicios de atención médica de alta especialidad en el campo de las ciencias médicas y nutrición.

En esa tesitura, conforme a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General) el Instituto, es un sujeto obligado, responsable del tratamiento y protección de los datos personales que posee.

De acuerdo a lo establecido en dicha Ley, se deben establecer las medidas de seguridad de carácter administrativo, físico y técnico para proteger los datos personales observando en todo momento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los mismos.

En cumplimiento al principio de responsabilidad, con fundamento en lo dispuesto por los artículos 30, fracción II de la LGPDPPSO y 47 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos), se presentan las siguientes políticas en materia de protección de datos personales.

Cabe precisar, que el presente documento podrá ser sometido a su revisión, ajuste o actualización por parte del Comité de Transparencia, cuando se produzcan modificaciones sustanciales a las obligaciones previstas en las leyes aplicables a la materia.

Su fin es establecer un marco para dar un debido acceso, uso y tratamiento, así como prever los mecanismos y acciones en caso de pérdida, daño, alteración, destrucción o, su uso, acceso o tratamiento no autorizado.

II. FUNDAMENTO JURÍDICO

Constitución Política de los Estados Unidos Mexicanos

D.O.F. 05-II-1917 y sus reformas

Ley General de Transparencia y Acceso a la Información Pública

D.O.F. 04-V-2015 y sus reformas

Ley Federal de Transparencia y Acceso a la Información Pública

D.O.F. 09-V-2016 y sus reformas

Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligado

D.O.F. 26-I-2017 y sus reformas

Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público

D.O.F. 26-I-2018 y sus reformas

Acuerdo mediante el cual se aprueban los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

D.O.F. 26-XI-2021 y sus reformas

Es importante destacar que se incorporan las disposiciones vigentes al momento de elaboración del presente documento, con independencia de aquellas que pueden ser abrogadas, derogadas y/o publicadas de manera posterior y que sean aplicables en materia de protección de datos personales

III. OBJETIVOS

El objeto principal del presente, es dar cumplimiento al principio de responsabilidad establecido en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, estableciendo los parámetros a observar al interior de este Instituto en materia de protección de datos personales.

Entre los objetivos a lograr, están:

1. Cumplir con las obligaciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, así como la normatividad aplicable a este Instituto.
2. Establecer un marco de referencia y trabajo necesario para la protección de los datos personales en posesión de las Unidades Administrativas de este Instituto
3. Promover la adopción de mejores prácticas en materia de protección de datos personales
4. Implementar las presentes políticas de manera integral en este Instituto.

IV. ÁMBITO DE APLICACIÓN

Es de observancia general y obligatoria para todas las Unidades Administrativas de este Instituto, así como para todas las personas servidoras públicas que, de acuerdo a sus facultades, atribuciones, competencias y responsabilidades, realicen un tratamiento de datos personales al interior de esta Institución.

V. GLOSARIO

Para efectos de interpretar y entender las presentes políticas en materia de protección de datos personales, se presentan las siguientes definiciones retomadas, en su mayoría del artículo 3 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados:

Aviso de Privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

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

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

Comité de Transparencia: Órgano colegiado e integrado por la persona responsable del área coordinadora de archivos o equivalente; la persona titular de la Unidad de Transparencia, y El titular del Órgano Interno de Control o su equivalente en este Instituto.

III. El titular del Órgano Interno de Control de cada dependencia o entidad.

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

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

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

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

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

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

Instituto: Se refiere al Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán

Ley General: A la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados

Lineamientos Generales: A los 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

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización,
d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a. a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
b. b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.
c. c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
d. d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Órgano Garante: Al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Responsable: El Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán

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

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

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

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

Unidades Administrativas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.

Unidad de Transparencia: Es la oficina administrativa, al interior de este Instituto, encargada dar trámite a las solicitudes de acceso a la información y derechos ARCO, publicar, recabar, difundir la información generada en materia de transparencia, así como en el ejercicio de sus competencias, así como las demás que se desprendan de la normatividad aplicable.

VI. DISPOSICIONES GENERALES

1. Las presentes políticas son de observancia general para todas las personas servidoras públicas de este Instituto que, entre sus actividades, involucren el tratamiento de datos personales.

2. El Comité de Transparencia, con fundamento en lo dispuesto por el artículo 83 de los Ley General, es la autoridad máxima en materia de protección de datos personales al interior de este Instituto. En ese sentido, tiene como función aprobar, coordinar y supervisar las presentes políticas, así como realizar los ajustes y/o modificaciones pertinentes conforme las situaciones lo ameriten.

3. El Comité de Transparencia podrá sugerir y/o exhortar a las Unidades Administrativas a que realicen o eviten ciertas acciones, a efecto de prevenir algún incumplimiento de las disposiciones normativas aplicables a la materia de protección de datos personales. Asimismo, en caso de que advierta un hecho que pudiera constituir una probable falta administrativa en la materia, dará vista a la Instancia competente de acuerdo a la normatividad aplicable.

4. El Comité de Transparencia, podrá auxiliarse de la Unidad de Transparencia para el ejercicio de sus funciones previstas en las presentes políticas.

5. La Unidad de Transparencia, para el cumplimiento de las presentes políticas, tiene como función asesorar en materia de protección de datos personales a las Unidades Administrativas del Instituto, acorde a los principios, deberes y obligaciones establecidas en las disposiciones normativas aplicables.

6. Las personas Titulares de las Unidades Administrativas de este Instituto, deberán establecer comunicación efectiva y directa con la Unidad de Transparencia, a fin de cumplir con las presentes políticas.

7. Las personas Titulares de las Unidades Administrativas de este Instituto, son responsables del tratamiento de los datos personales que realicen, en el ámbito de sus atribuciones, facultades y competencias, debiendo observar en todo momento los principios, deberes y obligaciones establecidas en las disposiciones normativas aplicables.

VII. PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

Los principios de protección de datos personales, son directrices a seguir para garantizar una efectiva protección de los datos personales, lo cuales se deben observar por parte del responsable en el tratamiento de los datos personales, siendo los siguientes:

1. Principio de Licitud

Se refiere a que, el tratamiento el tratamiento de datos personales deberá de sujetarse a las facultades y atribuciones que tengan las Unidades Administrativas, de acuerdo a lo dispuesto por las normas aplicables, así como en estricto apego y cumplimiento a lo establecido por las disposiciones jurídicas aplicables a la protección de datos personales.

2. Principio de Proporcionalidad

El tratamiento de datos personales que efectúen las Unidades Administrativas, deberá de estar justificado por finalidades concretas, licitas, explicitas y legitimas, así como relacionadas con las atribuciones que las normas aplicables les confiere.

Se entenderá por:

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.

Explícitas: Cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.

Licitas: 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.

Legítimas: Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento de la persona titular, salvo que se actualice alguna de las causales de excepción previstas la normativa aplicable.

Las finalidades deben de ser determinadas, emitiéndose como tal, que las personas servidoras públicas deben especificar el objeto para el cual se trataran los datos personales, de una manera clara.

3. Principio de Lealtad

Las personas servidoras públicas de este Instituto, no deberán de obtener y tratar datos personales, de manera engañosa o fraudulenta, anteponiendo en todo momento el derecho a la privacidad, así como privilegiando la protección de los intereses del titular.

Dicho principio implica evitar utilizar prácticas que lleven a la obtención de datos de manera dolosa, de mala fe o con negligencia.

Los datos personales recabados, deberán tratarse conforme a los acordado e informado a la persona titular de los mismos.

4. Principio de Consentimiento

Por regla general, las personas servidoras públicas de este Instituto, previo al tratamiento de los datos personales, deben de obtener el consentimiento (tácito o expreso) del titular de manera libre, especifica e informada, definiéndose como:

Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.

Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento.

Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

El consentimiento no será requerido cuando se actualice alguna de las causales previstas por la normatividad aplicable.

5. Principio de Calidad

Se deben adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos en posesión de las Unidades Administrativas, con la finalidad de que no se altere la veracidad de estos.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme

a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

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

6. Principio de Proporcionalidad

Las Unidades Administrativas sólo deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifique su tratamiento. Se entenderá que 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 al responsable por la normatividad que le resulte aplicable.

7. Principio de Información

Cada Unidad Administrativa es responsable de informar a los titulares a través del aviso de privacidad, la existencia y las características principales del tratamiento al que serán sometidos sus datos personales.

Por ello, deben contar y poner a la vista o a disposición de las personas, los avisos de privacidad simplificado, o en su caso, integrales, que correspondan al tratamiento que lleven a cabo, en los términos de la normatividad aplicable.

8. Principio de Responsabilidad

Se refiere a la obligación de velar por el cumplimiento del resto de los principios, mediante la observancia y aplicación de los mecanismos para adoptar medidas necesarias como estándares y mejores prácticas para su aplicación y demostrar ante las personas titulares y al Órgano Garante que cumple con sus obligaciones en torno a la protección de datos personales.

VIII. DEBERES PARA LA PROTECCIÓN DE DATOS PERSONALES

Las Unidades Administrativas del Instituto, deben de establecer medidas de seguridad 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.

Bajo esa tesitura, al interior de este Instituto deben observarse dos deberes:

1. Seguridad
2. Confidencialidad

1. Deber de Seguridad

Independientemente del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, existe la obligación de establecer medidas de carácter de administrativo, físico, técnico u otras que estimen necesarias para brindar una mayor garantía en la protección de datos personales en su posesión.

Las obligaciones vinculadas con el cumplimiento del deber de seguridad por parte de las de las Unidades Administrativas que traten datos personales en este Instituto serán:

I. Implementar políticas de gestión, en las cuales se considere el tipo de datos personales recabados, el tratamiento que se les dará y el ciclo de vida, es decir, su obtención, uso y posterior supresión.
II. Designar a las personas servidoras públicas que podrán intervenir en el tratamiento de los datos personales y definir las funciones y obligaciones que tendrán.
III. Realizar un análisis de riesgo de los datos personales tratados, así como de los sistemas físicos y/o electrónicos en los cuales se desarrolle dicho tratamiento.
IV. Realizar un análisis de brecha y desarrollar acciones de prevención y mitigación de amenazas o vulneraciones de datos personales.
V. Monitorear y revisar las medidas de seguridad adoptadas para garantizar la protección de datos.
VI. Incentivar la capacitación de las personas servidoras públicas involucradas en el tratamiento de datos personales, conforme al nivel de responsabilidad que tengan asignado.

VII. Para acreditar el cumplimiento de este deber por parte de las personas titulares de las Unidades Administrativas de este Instituto, se deberá realizar lo siguiente:

a. Contar con un inventario de las bases de datos personales.
b. Describir los roles y las responsabilidades específicas de las personas servidoras públicas relacionadas con el tratamiento de datos personales.
c. Implementar mecanismos y/o políticas para la protección de datos y guardar evidencia de ello.
d. Llevar una bitácora en la cual se asiente cualquier amenaza o vulneración de datos personales suscitada, así como de las acciones realizadas para su mitigación.
e. Instrumentar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recabados, así como las acciones de monitoreo, análisis y revisión a implementar; a fin de mantenerlas actualizadas y, en su caso, detectar áreas de oportunidad para su desarrollo y ejecución.
f. Tener la evidencia documental de los cursos, talleres, seminarios o similares en los que haya participado el personal adscrito a la Unidad Administrativa y se encuentren relacionados con la materia de protección de datos personales.

2. Deber de Confidencialidad

Las Unidades Administrativas deberán establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Para su cumplimiento, es importante:

a) Prever controles mediante los cuales se garantice la confidencialidad de los datos personales que son tratados.
b) Establecer cláusulas en los contratos para que, los sujetos obligados del ámbito público o privado a los cuales les sean transferidos o remitidos los datos personales ,se obliguen a la confidencialidad de éstos durante y posterior a la vigencia del instrumento jurídico.
c) Todos los servidores públicos que traten datos personales, deberán de firmar la carta de confidencialidad aprobada por el Comité de Transparencia.

IX. DOCUMENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES

De acuerdo a la normatividad aplicable a la materia, se debe contar con los siguientes documentos, para garantizar protección al tratamiento de los datos personales en posesión de este Instituto:

1. Documento de Seguridad: Documento elaborado con información provista por cada una de las Unidades Administrativas de este Instituto, cuyo propósito es establecer las medidas administrativas, físicas y técnicas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

2. Aviso de Privacidad: Documento generado por las Unidades Administrativas de este Instituto que realicen cualquier tipo de tratamiento de datos personales, para dar a conocer a las personas titulares de los mismos, las finalidades de su tratamiento.

3. Programa de Capacitación: Documento en el cual se prevén actividades de capacitación y actualización en materia de datos personales, para todas las personas servidoras públicas adscritas a este Instituto, considerando sus roles y responsabilidades asignadas para el tratamiento de datos personales.

Dichos documentos, son un parámetro y marco dentro de este Instituto, implementadas con el objeto de asegurar una mejor protección los datos personales que están en posesión del mismo. Además, forman parte de los mecanismos implementados para asegurar el cumplimiento del deber de seguridad, dando cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas, para la protección de datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

La actualización de los mismos, se dará cuando se actualice alguno de los siguientes supuestos:

a. Se produzcan modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo.
b. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con el que se cuente.
c. Derivado de un proceso de mejora para mitigar el impacto de vulneración a la seguridad ocurrida.
d. Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad

GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES

X. ROLES Y RESPONSABILIDADES

Cada Unidad Administrativa deberá 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, conforme a sus atribuciones y competencias.

Cada persona servidora pública debe actuar bajos los principios y deberes descritos en estas políticas, en las actividades que desarrollen e impliquen un tratamiento de datos personales, teniendo conocimiento que una mala práctica en el manejo de los datos personales que posean, puede traer como consecuencia una sanción administrativa por la autoridad competente.

XI. CICLO DE VIDA DE LOS DATOS PERSONALES

El ciclo de vida de los Datos Personales se compone de seis etapas:

1. La obtención de los datos personales.
2. El almacenamiento de los datos personales.
3. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin.
4. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen.
5. El bloqueo de los datos personales, en su caso.
6. La cancelación, supresión o destrucción de los datos personales.

XII. EL PROCESO GENERAL DE ATENCIÓN DE LOS DERECHOS ARCO

Toda persona, respecto a sus datos personales, tiene reconocidos los Derechos ARCO, los cuales son:

Acceso: A sus datos personales, así como a conocer la información relacionada con las condiciones y generalidades de su tratamiento.

Rectificación: La persona titular tiene el derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.

Cancelación: La persona titular tiene derecho a solicitar la cancelación de sus datos personales que se encuentren en los archivos, registros, expedientes y sistemas del responsable, con la finalidad de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Oposición: La persona titular puede oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:

I. Aun siendo lícito el tratamiento, el mismo debe terminar para evitar que su persistencia cause un posible daño o perjuicio al titular.
II. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento

Para ejercer alguno de estos Derechos, la persona titular de los datos personales deberá presentarse en la Unidad de Transparencia, la cual, turnará la solicitud a la Unidad Administrativa que, conforme a sus atribuciones, competencias o funciones cuente, pueda contar; dar tratamiento y/o ser responsable o encargada de los datos personales.

Para ello, es requisito indispensable acreditar su identidad como titular de los datos personales mediante alguna identificación oficial vigente o en su caso, acreditar la identidad y personalidad con la que actue el representante.

La Unidad de Transparencia deberá observar el procedimiento, así como los plazos establecidos por la Ley General y demás normatividad aplicable a la materia.

Portabilidad de datos personales

Consiste en otorgar al titular de los datos personales el control para tranferir su información personal de una Institución a otra.

Tiene por objeto que el titular solicite:

1. Una copia de sus datos personales que hubiere facilitado directamente al Instituto, en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a otra Institución para su reutilización y aprovechamiento en un nuevo tratamiento.
2. La transmisión de sus datos personales a una Institución receptora, siempre que sea técnicamente posible, cuando el titular hubiere facilitado directamente sus datos personales este Instituto como transmisor, y cuando el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.
3. Para realizar la portabilidad de datos personales, este Instituto observará y se sujetará a lo dispuesto por las disposiciones normativas y legales que sean aplicables.

XIII. SUPERVISIÓN Y VIGILANCIA

Para el debido cumplimiento de los principios, deberes y obligaciones que establecen la Ley General, los Lineamientos Generales y la normativa aplicable en materia de protección de datos personales, el Comité de Transparencia podrá supervisar a las Unidades Administrativas para garantizar el derecho a la protección de datos personales en el Instituto.

La supervisión se sustanciará mediante requerimientos de información sobre el tratamiento de datos personales, así como de sugerencias a las Unidades Administrativas para prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales.

XIV. LAS SANCIONES EN CASO DE INCUMPLIMIENTO

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguno de los principios, deberes u obligaciones previstas en las presentes políticas, deberá realizar a la Unidad Administrativa correspondiente un exhorto para que lleve a cabo las acciones y diligencias que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

Asimismo, es importante mencionar que de acuerdo al artículo 163 de la Ley General, son causas de sanción por incumplimiento de las obligaciones establecidas en la materia, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.
II. Incumplir los plazos de atención previstos en la Ley General para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión de los servidos públicos de este Instituto.
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes mencionados en las presentes políticas
V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos por las disposiciones que resulten aplicables en la materia.
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa,

que haya quedado firme, respecto del criterio de clasificación de los datos personales.

VII. Incumplir el deber de confidencialidad.

VIII. No establecer las medidas de seguridad en los términos la normatividad aplicable.

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad conforme a la normatividad aplicable.

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto por las disposiciones normativas aplicables.

XI. Obstruir los actos de verificación de la autoridad competente.

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de Ley General

XIII. No acatar las resoluciones emitidas el Organismo Garante.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, así como la reincidencia en las conductas previstas en el resto los numerales, serán consideradas como graves para efectos de su sanción administrativa.

Adicional a lo anterior, conforme al artículo 105 de los Lineamientos Generales, cuando alguna Unidad Administrativa se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista al órgano interno de control, contraloría o instancia equivalente y, en su caso, dé inicio al procedimiento de responsabilidad administrativo respectivo.

No obstante, las responsabilidades que resulten de los procedimientos administrativos correspondientes son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.