POLÍTICA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES

Comité de Transparencia
abril2025

1. INTRODUCCIÓN

a. Naturaleza jurídica del PT con respecto a los datos personales

El Partido del Trabajo es una entidad de interés público cuya finalidad consiste en ser vehículo de la población general para el acceso a la función pública y fungir como promotor de la democracia, tal y como lo señala el artículo 41 constitucional. En ese carácter y por ser sujeto obligado por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, tiene como obligación primordial el proteger los datos personales, los cuales en sí son un derecho humano. Esto hace que, para efecto de la transparencia y los datos personales, el Partido del Trabajo sea equiparable a una autoridad y por ende, se encuentra obligada a respetar y garantizar derechos humanos en términos del artículo 1º de la Constitución Política de los Estados Unidos Mexicanos.

b. Objetivos del Partido del Trabajo con respecto a los datos personales

Las presentes Políticas tienen por objeto establecer los procedimientos administrativos internos del Partido del Trabajo que deberán llevar a cabo sus Órganos Internos Responsables en el tratamiento y protección de los datos personales. Este instituto político nacional tiene como meta el tratar los datos personales que se encuentren bajo su resguardo de conformidad con la Ley y a las mejores prácticas existentes, sabiendo que esta actividad protege los derechos humanos de datos personales y ARCOP, consagrados en el artículo 16 constitucional. Esto se logra tanto por los procedimientos, formatos y lineamientos que se establezcan, así como por la normativa interna que al efecto tiene el Partido del Trabajo para regirse en la materia.

c. Alcances de la política de gestión de datos personales en posesión del Partido del Trabajo

La política de gestión de datos del Partido del Trabajo se da en cumplimiento del mandato que realiza el artículo 27 de la Ley General de Datos Personales en Posesión de los Sujetos Obligados que al efecto dice:

> ***Artículo 27.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *I. Crear políticas internas para la gestión y tratamiento de los datos personales que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;*
> *(…)*

d. Marco Normativo

- Constitución Política de los Estados Unidos Mexicanos
- Ley General de Transparencia y Acceso a la Información Pública
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

- Lineamientos generales de protección de datos personales para el sector público
- Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales
- Reglamento del Instituto Nacional Electoral en materia de Transparencia y Acceso a la Información Pública
- Estatutos del Partido del Trabajo

2. DEFINICIONES[1]

Autoridad Garante o INE: El Instituto Nacional Electoral, por cuanto hace a la Transparencia, Acceso a la Información y Protección de Datos Personales para Partidos Políticos, a través de la Comisión de Transparencia de Acceso a la Información y Protección de Datos Personales y la Unidad Técnica de los Contencioso Electoral, encargada de la sustanciación y resolución de las denuncias por incumplimiento de las obligaciones de transparencia de los partidos políticos.

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.

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.

Colaborador administrativo custodio: La o las personas colaboradoras administrativas designados por Titulares de los Órganos Internos, responsables del tratamiento de datos personales.

Comité: Órgano colegiado creado por la Comisión Ejecutiva Nacional, es la autoridad máxima en materia de acceso a la información pública y la protección y ejercicio de derechos ARCOP de los datos personales de titulares, en posesión del Partido, que conoce de los asuntos más relevantes para este sujeto obligado, relacionados con la Ley General de Transparencia y Acceso a la Información Pública y la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

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.

Datos personales: La 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, entre otra, la relativa a su origen étnico o racial,o que esté referida a las características físicas, morales o emocionales, asu vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o

[1] Algunas de las definiciones se toman con base en el artículo 3º de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y el Reglamento de Transparencia del PT

filosóficas, el estado de salud físico o mental, las preferencias sexuales, u otras análogas que afecten su intimidad.

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 ARCOP: Los derechos de acceso, rectificación, cancelación y oposición de datos personales. Además, se entenderá por:

a) **Acceso:** poner a disposición del titular sus datos personales;
b) **Rectificación:** revisión que solicita el titular de los datos, por serinexactos o incompletos;
c) **Cancelación:** supresión que solicita el titular de los datos, de uno ovarios datos personales en el sistema o base de que se trate;
d) **Oposición:** negativa del titular de los datos personales al tratamientode los mismos.
e) **Portabilidad:** El derecho a la portabilidad de datos permite a la persona titular, obtener de forma segura del Partido del Trabajo como responsable de la posesión de los datos personales, una copia electrónica de los datos objeto de tratamiento, en un formato estructurado, comúnmente utilizado y sin afectar su uso, para sus propios fines.

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: Persona física o moral, pública o privada, ajena al responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

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

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

Inventario de datos personales: Documento que describe el contenido del sistema de tratamiento.

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

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.

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.

Órgano Interno Responsable: Área a la que se le confieren atribuciones específicas en la estructura interna de los Estatutos del Partido del Trabajo -PT-.

PT: Partido del Trabajo.

Persona colaboradora: Persona operativa designada por la persona Titular de la Unidad de Transparencia para auxiliar en la coordinación las Órganos Internos Responsables para el cumplimiento de las presentes Políticas.

Políticas: Las directrices estratégicas establecidas en este documento para la gestión y tratamiento de datos personales, alineadas a las atribuciones del Partido del Trabajo -PT-, incluyendo la elaboración y emisión interna de programas, entre otros documentos regulatorios.

Responsable: El Partido del Trabajo a través de sus Órganos Internos Responsables y/o personas colaboradoras administrativas., de conformidad con lo que refiere el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que deciden sobre el tratamiento de datos personales.

Sistema de Tratamiento: Archivo físico y/o electrónico que contenga datos personales que se hayan recabado para el ejercicio de las funciones de las Órganos Internos Responsables.

Sistema de Gestión: Sistema de Gestión de Seguridad de Datos personales en posesión del Partido del Trabajo -PT-, conformado por el conjunto de elementos y actividades interrelacionadas para establecer,

implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la Ley de Datos Personales y las demás disposiciones que le resulten aplicables en la materia.

Sistema Nacional: El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

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

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. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Transferencia: Toda comunicación de datos realizada a persona distinta de la persona titular, responsable o encargado del tratamiento, dentro o fuera del territorio nacional.

Unidad de Transparencia: Área técnico-administrativa del Partido encargada de garantizar el acceso a la información pública y la protección y ejercicio de derechos ARCOP de los datos personales de titulares, en posesión del Partido del Trabajo, de las personas solicitantes y titulares, cumplir las obligaciones de conservación y actualización de la información pública del Partido en el SIPOT de la PNT, dar trámite a los asuntos en materia de transparencia ante la Autoridad Garante y lo demás a lo que hacen referencia los artículos 41 de la Ley General de Transparencia y Acceso a la Información Pública y 79 a Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

3. PRINCIPIOS RECTORES DE LA GESTIÓN DE DATOS PERSONALES

En su política de gestión de datos, el Partido del Trabajo sigue los principios de datos personales reconocidos por la comunidad internacional, que son recogidos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en el Título Segundo, Capítulo I:

- **Principio de límites de la recolección.** Deben existir limitaciones para la recolección de datos personales, y en todo caso deben ser obtenidos haciendo uso de medios lícitos y, en determinados casos, con el conocimiento y consentimiento de las personas titulares.
- **Principio de la calidad de datos o principio de preservación de la integridad de datos personales.** Los datos personales deben ser relevantes para el propósito para el cual se usan y, en la medida de lo posible respecto de dichos propósitos, deben ser adecuados, completos y actuales.

  Principio de especificación de propósito. Los propósitos para los cuales se recolectan datos personales deben ser especificados al momento de su obtención, y el uso subsecuente de ellos

debe limitarse al cumplimiento de tales propósitos u otros que no sean incompatibles con estos y que sean especificados en cada ocasión en que varíen los propósitos iniciales.

- **Principio de limitación de uso.** Los datos personales no deben ser divulgados o puestos a disposición de terceros para usos diferentes a los declarados por quien los obtuvo.
- **Principio de salvaguardas de seguridad.** Los datos personales deben ser protegidos mediante salvaguardas de seguridad razonables, contra riesgos de pérdida o de acceso, destrucción, uso, modificación o divulgación no autorizados.
- **Principio de apertura.** Debe existir una política pública abierta respecto al desarrollo, prácticas y políticas prevalecientes en relación con la recolección y uso de los datos personales.
- **Principio de participación individual.** Toda persona debe tener derecho: I) A obtener información de los sujetos obligados, o la confirmación de que un determinado sujeto obligado no tiene información sobre la persona solicitante; II) A que se le indique en tiempo y de manera gratuita, en una forma adecuada, la información que se mantenga de ella; y III) A que se le hagan saber de las razones de cualquier negativa a contestar un requerimiento de información, así como a solicitar que se elimine, rectifique, complete o modifique información que se tenga de ella
- **Principio de responsabilidad.** Todo sujeto obligado en la ley, debe ser responsable de cumplir con las medidas que se adopten para hacer eficientes los principios antes mencionados.
- **Principio de prevención del daño.** Debe reconocerse el interés de la persona a sus expectativas legítimas de privacidad, por lo que la legislación debe prevenir y sancionar el uso ilegitimo de la información.
- **Principio de obligación de dar aviso.** Los sujetos obligados por la legislación deben dar aviso en términos claros y entendibles a las personas titulares de la información, respecto de las prácticas de privacidad de los que gozará la información que comparta.
- **Principio de acceso y derecho de corrección.** Las personas titulares de información personal deben tener derecho a: I) obtener confirmación por parte de los sujetos obligados por la ley, respecto de si tienen o no información personal que les concierna; II) que se les haga saber la información que tengan en su conocimiento, en un tiempo y a un costo razonable, con los medios adecuados que les permita entenderla; y III) controvertir la exactitud de la información y, en su caso, solicitar su rectificación.
- **Principio de proporcionalidad.** Los datos personales solicitados deben estar completamente relacionados con los propósitos para los cuales se recolectaron, por ningún motivo deben ser excesivos e irrelevantes.

4. INSTANCIAS ENCARGADAS DE LA GESTIÓN DE DATOS PERSONALES

El Comité de Transparencia del Partido del Trabajo es el Órgano colegiado creado por la Comisión Ejecutiva Nacional y la autoridad máxima en materia de acceso a la información pública y la protección y ejercicio de derechos ARCOP de los datos personales de titulares, en posesión del Partido, que conoce de los asuntos más relevantes para este sujeto obligado. También tiene la última palabra en lo relativo a la supervisión de la gestión de datos personales y resuelve todas las peticiones de derechos ARCOP que tramita el Oficial de Protección de Datos Personales.

El Comité de Transparencia y el Oficial de Protección de Datos Personales tienen su dirección en

Avenida Cuauhtémoc número 47, colonia Roma Norte, C.P. 06700, Demarcación territorial Cuauhtémoc, Ciudad de México y cuenta con la dirección de correo electrónico: unidadtransparenciaptnal@gmail.com y número telefónico 5555118983.

5. FORMA EN LA QUE SE OBTIENEN LOS DATOS PERSONALES

El Partido del Trabajo obtiene, almacena y trata los datos personales en virtud de la relación de participación política que existe entre este instituto político nacional y la ciudadanía afín a su ideología. El Partido del Trabajo también es responsable de resguardar los datos personales que dimanen de sus actividades administrativas.

Los datos personales que la persona titular proporcione deben ser correctos, completos, veraces, exactos y actuales. El Partido del Trabajo tiene la obligación de mantener la veracidad de los datos bajo su resguardo, pero la persona titular tiene también el derecho a rectificar y corregirlos vía los mecanismos que señala la Ley.

El tratamiento de datos personales que el Partido del Trabajo lleve a cabo debe apegarse a la legislación, respetar los derechos humanos y ceñirse a las mejores prácticas existentes, operando también con una expectativa razonable de privacidad. Esta actividad debe realizarse guardando confidencialidad y respetando en todo momento los intereses de las personas titulares de datos personales; para tal efecto, deben existir controles de confidencialidad adecuados.

Los datos personales no deben obtenerse ni tratarse por medio del fraude y del engaño, sin que medie dolo, mala fe o negligencia en la información proporcionada a la persona titular sobre el tratamiento de sus datos y del ejercicio de sus derechos ARCOP.

Los datos personales obtenidos deben ser los necesarios para el cumplimiento de las funciones del Partido del Trabajo como entidad de interés público en términos del artículo 41 de la Constitución Política de los Estados Unidos Mexicanos y ello implica que la finalidad de la obtención y tratamiento de datos personales debe hacerse saber por medio de un aviso de privacidad, de forma clara e indubitable; este es el instrumento para la obtención del consentimiento de la persona titular de los datos personales. Este debe de ser libre, específico, informado e inequívoco.

Para lograr su propósito, el Partido del Trabajo obtiene datos personales por parte de la ciudadanía cuya categoría se relaciona con su identificación, ubicación física, contacto, académicos, biométricos, laborales y patrimoniales. La afinidad política no puede considerarse en este contexto como dato personal sensible, a razón de que se presupone al manifestar una afinidad con el Partido del Trabajo y su ideología.

Son datos personales atenientes a la **Ubicación física** su dirección; **de Identificación**: el nombre, estado civil, firma autógrafa y, en su caso, electrónica, RFC, CURP, lugar y fecha de nacimiento, nacionalidad, fotografía, edad, etc.; **de Contacto**: correo electrónico, número telefónico fijo y celular; **Académicos:** idioma, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, etc.; **Biométricos:** huellas dactilares; **Laborales**: puesto y lugar de trabajo, experiencia, datos de contacto, correo y teléfono institucional, etc. y **Patrimoniales:** saldos bancarios, estados y número de cuenta, bienes muebles e inmuebles, información fiscal, ingresos, de colaboradores y proveedores.

6. FORMA EN LA QUE SE RESGUARDAN LOS DATOS PERSONALES

El Partido del Trabajo posee medidas de seguridad administrativas, técnicas y físicas suficientes y adecuadas para proteger sus datos personales, evitando así su daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Las personas colaboradoras encargadas de recabar, usar, registrar, organizar, conservar, difundir, almacenar, poseer, manejar, aprovechar, divulgar y de ser necesario, transferir datos personales tienen la obligación de guardar confidencialidad sobre los mismos. El respeto a la dignidad y la privacidad de las personas titulares de datos personales es un compromiso fundamental para el Partido del Trabajo.

El Partido del Trabajo no realiza transferencia de datos personales, por lo que los involucrados en su tratamiento deberán abstenerse de hacer transferencias de datos personales, salvo en el caso de que así lo determine una autoridad competente.

La obtención, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, copia, destrucción, daño, alteración y/o modificación no autorizada de los datos personales proporcionados al Partido del Trabajo traerá como consecuencia una investigación por parte del Comité de Transparencia y la Contraloría Interna, con el propósito de dar turno a la Autoridad Garante a efecto de que procese y sancione a quienes resulten responsables.

En caso de darse una vulneración, el Partido del Trabajo deberá notificar a las personas titulares y a la Autoridad Garante, además de tomar las medidas necesarias para reducir daños y corregir la vulneración. Asimismo, se adoptará el procedimiento de contingencia adecuado.

Las solicitudes de ejercicio de derechos ARCOP que presenten las personas titulares de datos personales serán recibidas por Unidad de Transparencia, procesadas por el Oficial de Protección de Datos Personales y resueltas de forma definitiva por el Comité de Transparencia del Partido del Trabajo, el que emitirá la respectiva Resolución. Para el ejercicio de estos derechos -Acceso, Rectificación, Cancelación y Oposición- será necesario que la persona titular o su representación legal, acredite su identidad.

El Partido del Trabajo velará porque los datos que hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el Aviso de Privacidad, sean suprimidos mediante técnicas de borrado seguro.

7. SANCIONES

El incumplimiento de estas políticas conlleva una violación a la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, pudiendo actualizarse las causales de sanción contenidas en el artículo 132 de la misma. Esto tiene como consecuencia la vista a la Autoridad Garante para que determine la responsabilidad correspondiente y en su caso, imponga o ejecute una sanción.

POLÍTICA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I
De los Principios Generales del tratamiento y la protección de datos personales en posesión del Partido del Trabajo

Artículo 1. En el tratamiento de datos personales, el PT, los Órganos Internos Responsables y las personas colaboradoras administrativas deberán justificar las finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera; observando en todo momento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, en términos de la Ley de Datos Personales y demás disposiciones normativas aplicables.

Artículo 2. Las personas Titulares de los Órganos Internos Responsables designarán una persona colaboradora administrativa custodio para los Sistemas de Tratamiento que les correspondan, quién tendrá las siguientes funciones:

I. Adoptar, aplicar y vigilar el cumplimiento de las medidas y estándares de seguridad para la conservación y resguardo de los Sistemas de Tratamiento bajo su responsabilidad, de manera que se evite su alteración, pérdida o acceso no autorizado;
II. Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico o disposición normativa, el acceso a otros usuarios y llevar una relación actualizada de las personas que tengan acceso a los Sistemas de Tratamiento a su cargo; y
III. Las demás que establezcan las presentes Políticas.

Artículo 3. Los Órganos Internos Responsables y las personas colaboradoras administrativas custodios, deberán 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. Para efectos de lo anterior, se entenderá que los datos personales son:

I. Exactos y correctos: cuando los datos personales en posesión de la persona responsable no presentan errores que pudieran afectar su veracidad
II. Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable; y
III. Actualizados: cuando los datos personales responden fielmente a la situación actual de la persona titular.

Artículo 4. Las personas colaboradoras administrativas custodios están obligadas en todo momento a garantizar las condiciones y requisitos necesarios para el adecuado tratamiento, así como la debida administración y custodia de los datos personales que se encuentren bajo su resguardo, con el objeto de maximizar el ejercicio de los derechos ARCOP.

Artículo 5. Los datos personales serán confidenciales, independientemente de que hayan sido obtenidos por el PT directamente de su titular o por cualquier otro medio.

Artículo 6. Los datos personales sensibles, son aquellos que posee el PT en sus archivos, concernientes a una persona física identificada o identificable, 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, los cuales se describen a continuación de manera enunciativa y no limitativa:

I. Origen racial o étnico;
II. Estado de salud presente o futuro;
III. Información genética;
IV. Creencias religiosas;
V. Creencias morales;
VI. Preferencia sexual; y
VII. Otros asociados

Artículo 7. Los datos personales que se recaben en cumplimiento a las facultades, competencias y funciones establecidas en los procedimientos sustantivos del PT, señalados en la Ley General de Instituciones y Procedimientos Electorales y en la Ley General de Partidos Políticos, no formarán parte de ningún sistema de tratamiento de datos personales, en virtud de que el resguardo y protección de dicha información se encuentra regulada en términos de esas Leyes, de la Ley General de Transparencia, del Reglamento del Instituto Nacional Electoral en materia de Transparencia y Acceso a la Información Pública, de la normatividad del PT y demás normativa de acceso a la información.

CAPÍTULO II
Del tratamiento de los datos personales

Artículo 8. Los Órganos Internos Responsables y/o las personas colaboradoras administrativas del PT, que reciban u obtengan datos personales deberán obtener el consentimiento de la persona titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

I. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad de la persona titular;
II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e
III. Informada: Que la persona titular tenga conocimiento del Aviso de Privacidad previo al tratamiento a que serán sometidos sus datos personales.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

Artículo 9. El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad de la persona titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

El consentimiento será tácito cuando habiéndose puesto a disposición de la persona titular el Aviso de Privacidad, ésta 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 de la persona titular se manifieste expresamente.

Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito de la persona titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca.

Artículo 10. Las Órganos Internos Responsables y/o las personas colaboradoras administrativas del PT, que

reciban u obtengan datos personales deberán informar a la persona titular, a través del Aviso de Privacidad, la existencia y características principales del sistema de tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Por regla general, el Aviso de Privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable.

Para que el Aviso de Privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla, atendiendo las especificaciones establecidas en los artículos 20, 21 y 22 de la Ley de Datos Personales.

Artículo 11. El Aviso de Privacidad a que se refiere el artículo anterior se pondrá a disposición de la persona titular en dos modalidades: simplificado e integral.

El Aviso de Privacidad en su modalidad simplificada deberá contener la siguiente información:

I. La denominación y el domicilio del responsable;
II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento de la persona titular;
I. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
II. a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y
b) Las finalidades de estas transferencias;
III. Los mecanismos y medios disponibles para que la persona titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento de la persona titular; y
IV. El sitio donde se podrá consultar el Aviso de Privacidad integral.

Artículo 12. El Aviso de Privacidad integral, deberá contener, al menos, la siguiente información:

I. La denominación y el domicilio del responsable;
II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento de la persona titular;
V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
VI. El domicilio de la Unidad de Transparencia;
VII. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:
a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y
b) Las finalidades de estas transferencias;
VIII. Los mecanismos y medios disponibles para que la persona titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento de la persona titular, y
IX. Los medios a través de los cuales el responsable comunicará a las personas titulares los cambios al aviso de privacidad.

Los mecanismos y medios a los que se refiere la fracción VIII de este artículo deberán estar disponibles para que la persona titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias que requieran su consentimiento, previo a que ocurra dicho tratamiento.

Artículo 13. La Unidad de Transparencia pondrá a disposición de los Órganos Internos Responsables y de las personas colaboradoras administrativas del PT los formatos de Avisos de Privacidad simplificado e integral, para que los adopten de acuerdo con el ámbito de sus competencias y conforme al tratamiento de los datos personales que requieran.

Los Avisos de Privacidad deben ser aprobados por el Comité y deberán atender el procedimiento establecido en el segundo párrafo del siguiente artículo.

Artículo 14. Las Órganos Internos Responsables y/o las personas colaboradoras administrativas del PT podrán implementar, modificar, actualizar o cancelar los sistemas de tratamiento de datos personales que consideren necesarios para el ejercicio de sus funciones.

Para efecto de lo anterior, deberán remitir al Comité a través de la persona colaboradora designada, los siguientes documentos para su aprobación:

I. El inventario de datos personales que se traten, que contenga lo siguiente:
   a) Nombre de la Órgano Interno Responsable.
   b) Fecha de implementación, modificación, actualización o cancelación.
   c) Nombre del tratamiento de datos personales.
   d) Fundamento jurídico que habilita el tratamiento.
   e) El listado de datos personales que se recaban para el procedimiento, señalando si son sensibles o no.
   f) Los medios por los cuales se obtienen.
   g) Señalar el formato de la base de datos: físico y/o electrónico.
   h) Ubicación de la base de datos.
   i) El sección, serie y subserie a la que corresponde el tratamiento.
   j) Finalidades del tratamiento.
   k) Indicar si se requiere consentimiento expreso.
   l) Nombre, cargo y área de adscripción del colaborador administrativo custodio designado.
   m) Nombre, cargo y área de adscripción de las personas colaboradoras administrativas que tendrán acceso a la base de datos, así como la finalidad del acceso.
   n) Nombre del encargado y datos del instrumento jurídico que regula la relación con el encargado.
   o) Señalar si se realizan transferencias de datos personales y, en su caso, el nombre del tercero al que se le transfieren los datos personales, las finalidades de la transferencia, información del consentimiento para la transferencia, así como de la suscripción de instrumentos jurídicos
   p) Indicar si se realiza la difusión de los datos personales y su fundamento jurídico.
   q) El plazo de conservación y bloqueo
   r) Cualquier otro dato que sea relevante

II. Descripción del ciclo de vida de los datos personales desde la obtención hasta la cancelación o supresión y las medidas de seguridad adoptadas para el tratamiento;
III. Los Avisos de Privacidad, simplificado e integral correspondientes al tratamiento correspondiente;
IV. En caso de tratarse de la cancelación del sistema de tratamiento, se deberá remitir además un oficio signado por la persona titular de la Órgano Interno Responsable en el que manifieste:
   1. Las razones por las que se solicita la cancelación del sistema de tratamiento de datos personales,
   2. La fecha en que concluye el periodo de conservación de los datos personales, y

3. La fecha en que se llevó a cabo la supresión de la totalidad de los datos personales que fueron recabados para el tratamiento.

El Comité determinará en la sesión inmediata siguiente si se cumplen las formalidades establecidas en la Ley de Datos Personales para implementar, modificar, actualizar o cancelar los sistemas de tratamiento de datos personales.

En caso de no aprobarse, se deberán asentar en el Acta correspondiente las razones y, en su caso, señalar los elementos que deben subsanarse para que sea aprobada en la próxima sesión del Comité.

Artículo 15. La relación entre el PT y el encargado deberá estar formalizada mediante cualquier instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

En el instrumento jurídico a que hace referencia el presente artículo se deberán prever, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

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

Los acuerdos entre el PT y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la Ley de Datos Personales y demás disposiciones aplicables, así como lo establecido en el Aviso de Privacidad correspondiente.

Artículo 16. Las remisiones de datos personales que se realicen entre responsable y encargado no requerirán ser informadas a la persona titular, ni contar con su consentimiento.

Artículo 17. Las transferencias de datos personales se encuentran sujetas al consentimiento de su titular, salvo las excepciones previstas en los artículos 16, 60 y 64 de la Ley de Datos Personales.

Toda transferencia de datos personales que realicen los Órganos Internos Responsables y/o las personas colaboradoras administrativas del PT, 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 y que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes, atendiendo lo establecido en el Aviso de Privacidad correspondiente.

Artículo 18. En toda transferencia de datos personales, el PT, sus Órganos Internos Responsables y/o las personas colaboradoras administrativas deberán comunicar el Aviso de Privacidad al receptor de los datos personales, conforme al cual se tratan los mismos.

CAPÍTULO III
De la protección de los datos personales

Artículo 19. Corresponderá a las personas Titulares de los Órganos Internos Responsables establecer las medidas de seguridad físicas, técnicas y administrativas necesarias para proteger los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no automatizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

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

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

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

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

Por su parte, las **medidas de seguridad administrativas** refieren a las 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 de las personas colaboradoras en materia de protección de datos personales.

Artículo 20. En cualquier momento, el Comité podrá monitorear y/o revisar los sistemas de tratamiento, mecanismos y medidas de seguridad adoptadas por los Órganos Internos Responsables; así como solicitar el establecimiento y actualización de las que considere pertinentes, de conformidad con los programas de capacitación, auditoría y mejora continua.

Artículo 21. En caso de que ocurra una vulneración a la seguridad, se deberán analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

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

Artículo 22. Las Órganos Internos Responsables y/o las personas colaboradoras administrativas deberán informar sin dilación alguna al Comité, a la persona titular y a la Autoridad Garante, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que se haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que las personas titulares afectadas puedan tomar las medidas correspondientes para la defensa de sus derechos.

En atención a lo anterior, se deberá informar a la persona titular al menos lo siguiente:

I. La naturaleza del incidente;
II. Los datos personales comprometidos;
III. Las recomendaciones a la persona titular acerca de las medidas que ésta pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata;
V. Los medios donde puede obtener más información al respecto;
VI. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden a la persona titular a entender el impacto del incidente, y
VII. Cualquier otra información y documentación que considere conveniente para apoyar a las personas titulares.

Artículo 23. El Comité deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa la misma, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

Artículo 24. 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, una vez que concluya el plazo de conservación de estos.

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.

Artículo 25. Los Órganos Internos Responsables y/o las personas colaboradoras administrativas deberán establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleven a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en los artículos 17 y 18 de la Ley de Datos Personales.

En los procedimientos a que se refiere el párrafo anterior, se deberán incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión

periódica sobre la necesidad de conservar los datos personales.

CAPÍTULO IV
Del ejercicio de los derechos ARCOP

Artículo 26. En todo momento la persona titular o su representante podrán solicitar, el acceso, rectificación, cancelación, oposición o portabilidad al tratamiento de los datos personales que le conciernen y estén en posesión del PT. El ejercicio de cualquiera de los derechos ARCOP no es requisito previo, ni impide el ejercicio de otro.

Las solicitudes para el ejercicio de los derechos ARCOP deberán presentarse ante la Unidad de Transparencia del PT, a través de escrito libre, formato del PT establecido con base en los artículos 3, 46 y Título Tercero, Capítulo II de la Ley de Protección de Datos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto.

El PT deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCOP y entregar el acuse de recibo que corresponda.

Artículo 27. Para el ejercicio de los derechos ARCOP será necesario acreditar la identidad de la persona titular y, en su caso, la identidad y personalidad con la que actúe el representante.

El ejercicio de los derechos ARCOP por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

En el ejercicio de los derechos ARCOP de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.

Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el Título Tercero, Capítulo II de la Ley de Protección de Datos, siempre que la persona titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto.

Artículo 28. El ejercicio de los derechos ARCOP deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío.

Cuando la persona titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo a ésta.

La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples y la Unidad de Transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas de la persona titular.

Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, la persona titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos, ejerciendo el derecho de portabilidad.

Artículo 29. La solicitud de ejercicio de derechos ARCO deberá contener lo siguiente:

a) Nombre de la persona titular de los datos personales.
b) Documentos que acrediten la identidad de la persona titular y, en su caso, la personalidad e identidad de su representante;
c) De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;
d) La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCOP, salvo que se trate del derecho de acceso;
e) La descripción del derecho ARCOP que se pretende ejercer, o bien, lo que solicita la persona titular;
f) Domicilio o cualquier medio para recibir notificaciones
g) En su caso, documentos o información que faciliten la localización de los datos personales, en su caso.

Tratándose de una solicitud de acceso a datos personales, la persona titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan. El responsable 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 personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

Artículo 30. El Partido es responsable del tratamiento de datos personales, por lo que el Comité de Transparencia será la autoridad máxima en materia de protección de datos personales y la Unidad de Transparencia, la instancia responsable de atender las solicitudes de ejercicio de derechos ARCOP de datos personales: acceso, rectificación, cancelación, oposición y portabilidad. Además, se entenderá por:

- Derecho de Acceso: la modalidad en la que la persona titular prefiere que se reproduzcan los datos personales solicitados.
- Derecho de Rectificación: las modificaciones que la persona titular solicita que se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.
- Derecho de Cancelación: las causas que motivan la petición de que se eliminen los datos personales de los archivos, registros o bases de datos del responsable del tratamiento.
- Derecho de Oposición: las causas o la situación que llevan a la persona titular a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.
- Derecho de Portabilidad: la persona titular obtiene de forma segura del Partido del Trabajo como responsable de la posesión de los datos personales, una copia electrónica de los datos objeto de tratamiento, en un formato estructurado, comúnmente utilizado y sin afectar su uso, para sus propios fines.

Con relación a una solicitud de cancelación, la persona titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable.

En el caso de la solicitud de oposición, la persona titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.

Artículo 31. En caso de que la solicitud no cuente con la información antes descrita, la Unidad de Transparencia podrá solicitar la información faltante por medio de una prevención, la cual se emitirá en un plazo máximo de cinco días hábiles contados a partir del día siguiente de la presentación de la solicitud, y la persona titular de los datos personales, o en su caso, la persona representante, tendrá un plazo de diez días

hábiles, después de recibir la prevención, para proporcionar la información pública requerida.

La prevención tendrá el efecto de interrumpir el plazo que tiene el responsable para resolver la solicitud de ejercicio de los derechos ARCOP.

Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCOP.

Artículo 32. Cuando el responsable no sea competente para atender la solicitud para el ejercicio de los derechos ARCOP, deberá hacer del conocimiento de la persona titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud, y en caso de poderlo determinar, orientarlo hacia el responsable competente.

En caso de que el responsable advierta que la solicitud para el ejercicio de los derechos ARCOP corresponda a un derecho diferente de los previstos en este Capítulo, deberá reconducir la vía haciéndolo del conocimiento a la persona titular.

Artículo 33. En caso de que el responsable declare inexistencia de los datos personales en sus archivos, registros, sistemas o expediente, dicha declaración deberá constar en una Resolución del Comité que confirme la inexistencia de los datos personales.

Artículo 34. Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCOP, el responsable deberá informar a la persona titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCOP, a efecto de que esta último decida si ejerce sus derechos a través del trámite específico, o bien, por medio del procedimiento del ejercicio de los derechos ARCOP.

Artículo 35. Las únicas causas en las que el ejercicio de los derechos ARCO no serán procedente son:

I. Cuando la persona titular o su representante no estén debidamente acreditadas 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 de la persona titular;
X. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por la persona 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.

En todos los casos anteriores, el responsable deberá informar a la persona titular el motivo de su determinación, en el plazo de hasta veinte días a los que se refiere el primer párrafo del artículo 45 de la presente Ley, y por

el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes.

Artículo 36. Contra la negativa de dar trámite a toda solicitud para el ejercicio de los derechos ARCOP o por falta de respuesta del responsable, procederá la interposición del recurso de revisión a que se refiere el artículo 94 de la Ley de Datos Personales.

CAPÍTULO V
De las sanciones

Artículo 37. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la Ley de Datos Personales, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCOP;
II. Incumplir los plazos de atención previstos en la Ley de Datos Personales para responder las solicitudes para el ejercicio de los derechos ARCOP o para hacer efectivo el derecho de que se trate;
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley de Datos Personales;
V. No contar con el Aviso de Privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 21 de la Ley de Datos Personales, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
VII. Incumplir el deber de confidencialidad establecido en el artículo 29 de la Ley de Datos Personales;
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 25, 26 y 27 de la Ley de Datos Personales;
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 25, 26 y 27 de la Ley de Datos Personales;
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley de Datos Personales;
XI. Obstruir los actos de verificación de la autoridad;
XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley de Datos Personales;
XIII. No acatar las resoluciones emitidas por el Instituto, y
XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 40, fracción VI de la Ley de Transparencia, o bien, entregar el mismo de manera extemporánea.

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

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

Artículo 38. Para las conductas a que se refiere el artículo anterior se dará vista a la autoridad competente para que imponga o ejecute la sanción.

Artículo 39. Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 123 de la Ley de Datos Personales, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.

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

Para tales efectos, el Instituto podrá denunciar ante las autoridades competentes cualquier acto u omisión violatoria de la Ley de Datos Personales y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

Artículo 40. En aquellos casos en que la persona presunta infractora tenga la calidad de colaborador administrativo, el PT deberá remitir a la Autoridad Garante o autoridad competente, junto con la denuncia correspondiente, un Expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa.

La autoridad que conozca del asunto, deberá informar de la conclusión del procedimiento y, en su caso, de la ejecución de la sanción, a la Autoridad Garante.

A efecto de sustanciar el procedimiento citado en este artículo, el Instituto deberá elaborar una denuncia dirigida al órgano interno de control o equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la Ley de Datos Personales y que pudieran constituir una posible responsabilidad.

Asimismo, deberá elaborar un expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.

La denuncia y el Expediente deberán remitirse al órgano interno de control o equivalente dentro de los quince días siguientes a partir de que el Instituto tenga conocimiento de los hechos.

Artículo 40. En caso de que el incumplimiento de las determinaciones del Instituto implique la presunta comisión de un delito, el propio Instituto deberá denunciar los hechos ante la autoridad competente

TRANSITORIO. El presente documento que contiene la Política de gestión de datos personales surtirá efectos legales internos inmediatamente después de ser aprobado por el Comité de Transparencia del PT.