Acta del Comité Nacional de Transparencia
PRI-CT-005-2024

ACUERDO MEDIANTE EL CUAL SE APRUEBAN LAS POLÍTICASINTERNAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DEL COMITÉ EJECUTIVO NACIONAL DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL

CONSIDERANDOS

1. Que el Congreso de la Unión, en cumplimiento al transitorio Segundo del Decretopor el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LeyGeneral), publicada el veintiséis de enero de dos mil diecisiete en el Diario Oficial de la Federación (DOF), entrando en vigor al día siguiente de su publicación de acuerdo a lo previsto en el Artículo Primero Transitorio de la referida Ley General.

2. Que el párrafo segundo del artículo 16 de la Constitución Política de los EstadosUnidos Mexicanos señala que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición al uso de su información personal, en los términos que fijela ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos personales, por razones de seguridad nacional, disposicionesde orden público, seguridad y salud públicas o para proteger los derechos de terceros.

3. Que con fecha veintiséis de enero de dos mil diecisiete se publicó en el DOF el Decreto por el que se expide la Ley General de Protección de Datos Personales enPosesión de Sujetos Obligados, la cual, de conformidad con su Artículo Primero Transitorio, entró en vigor el día siguiente de su publicación.

4. Que, tras la publicación en el DOF, y entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por medio de la cual se incluyeron como sujetos obligados a proteger los datos personales que obren en su poder a los Partidos Políticos, de conformidad con lo dispuesto en el artículo 1 de la referida Ley.

5. Que en materia de políticas de datos personales la normativa establece lo siguiente:

a. Ley General de Protección de Datos Personales en Posesión de Sujetos

Artículo 30. Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están,al menos, los siguientes:

I. Destinar recursos autorizados para tal fin para la instrumentación de programasy políticas de protección de datos personales;

II. Elaborar políticas y programas de protección de datos personales, obligatoriosy exigibles al interior de la organización del responsable;

…

Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, lassiguientes 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 devida de los datos personales, es decir, su obtención, uso y posterior supresión;
…

b. Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales):

Políticas y programas de protección de datos personales

Artículo 47. Con relación al artículo 30, fracciones I y II de la Ley General, el responsable deberá elaborar e implementar políticas y programas de protecciónde datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continúa.

Las políticas y programas de protección de datos personales a que se refiere el párrafo anterior del presente artículo deberán ser aprobados, coordinados y supervisados por su Comité de Transparencia.

El responsable deberá prever y autorizar recursos, de conformidad con la normatividad que resulte aplicable, para la implementación y cumplimiento de éstos.

Contenido de las políticas internas de gestión y tratamiento de los datospersonales

Artículo 56. Con relación a lo previsto en el artículo 33, fracción I de la LeyGeneral, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, almenos, lo siguiente:

I. El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los presentes Lineamientos generales;
II. Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen;
III. Las sanciones en caso de incumplimiento;
IV. La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados;
V. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y

VI. El proceso general de atención de los derechos ARCO.

6. Que el 11 de noviembre de 2020, el Pleno del INAI aprobó el Acuerdo mediante el cual se aprueba la adición de un Título Décimo a los Lineamientos Generales deProtección de Datos Personales para el Sector Público, el cual en su artículo 247, dispone que el INAI aprobará los Instrumentos Técnicos de Evaluación que sean necesarios para medir el desempeño de los responsables respecto al cumplimientode las obligaciones previstas en la Ley General y demás disposiciones aplicables en la materia; los cuales contemplarán, al menos el tipo de evaluación, la metodología los criterios, los formatos y los indicadores de cumplimiento que permitan la realización del ejercicio de evaluación que corresponda.

7. Que el artículo 248 de los Lineamientos Generales establece que el cumplimiento de las disposiciones contenidas en los instrumentos técnicos de evaluación es obligatorio para los responsables del ámbito federal a que se refiere el artículo primero de la normativa citada. Asimismo, en su artículo 250, establece que los responsables deberán habilitar en su portal de internet, un apartado denominado “Protección de datos personales” el cual será el medio idóneo que servirá a los responsables para rendir cuentas a los titulares y al INAI sobre el tratamiento de los datos personales en su posesión, permitiendo evaluar el cumplimiento de los principios, deberes y obligaciones; atendiendo a la obligatoriedad que les corresponde como responsables, en términos de lo previsto en los artículos 26, 29 y 30 de la Ley General Que de conformidad con lo que se establece en el artículo 16, último párrafo, 45,54, 72, 107 y 118 de los Lineamientos Generales, la carga de la prueba para acreditar el cumplimiento de los principios, deberes y obligaciones relativas a la protección de datos personales en su tratamiento, en todo momento, recaerá en elresponsable.

8. Que el 17 de noviembre de 2021, el Pleno del INAI aprobó el Acuerdo mediante el cual se aprueban los Instrumentos Técnicos a que se refiere el Título Décimo delos 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 (Instrumentos Técnicos), mismos que establecen en artículo Segundo Transitorio que los sujetos obligados del ámbito público federal deberán incorporar en su apartado virtual de protección de datos personales, los medios de verificación documentales y la información establecida en los instrumentos técnicos de evaluación, en relación con los tratamientos de datos personales que detentan, de conformidad con los criterios, formatos y plazos establecidos en los documentos técnicos de evaluación y en sus respectivosanexos, dentro de los primeros seis meses del ejercicio fiscal 2022.

9. Que el Partido Revolucionario Institucional es una entidad de interés pública, con personalidad jurídica y patrimonio propio que goza de facultades para regular su vida interna y determinar su organización interior y los procedimientos correspondientes, de conformidad con los artículos 3 y 23, numeral 1 inciso c de laLey General de Partidos Políticos.

10. Que el derecho a la protección de los datos personales es un derecho humanoque debe ser garantizado por los sujetos obligados.

11. Los Estatuto Generales del Partido Revolucionario Institucional establecen que el Comité Nacional de Transparencia y Protección de Datos Personales será el órgano responsable de garantizar los mecanismos para la protección de los datos personales que obren en su posesión, a través de su acceso, rectificación, cancelación y oposición en los términos previstos en lalegislación aplicable, así como, de establecer lineamientos y manuales que permitan hacer eficientes los procedimientos de solicitudes de acceso a la información y de protección de datos personales.

12. Que la Unidad de Transparencia, propone al Comité Nacional de Transparenciay Protección de Datos Personales del Partido Revolucionario Institucional el proyecto de Acuerdo mediante el cual se aprueban las políticas internas de gestión y tratamiento de los datos personales del Comité Ejecutivo Nacional del Partido Revolucionario Institucional.

Por lo expuesto en las consideraciones de hecho y de derecho, y con fundamento en lo dispuesto en los artículos 6o., apartado A, fracción I y II, y 16 de la ConstituciónPolítica de los Estados Unidos Mexicanos; artículos 30 fracciones I y II, 33, 83 y 84de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 3 y 23, numeral 1 inciso c de la Ley General de Partidos Políticos; Estatutos Generales del Partido Revolucionario Institucional; 47 y 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público; el Comité Nacional de Transparencia y Protección de Datos Personales del Partido Revolucionario Institucional emite el siguiente:

ACUERDO

PRIMERO. Se aprueban las políticas internas de gestión y tratamiento de los datospersonales del Comité Ejecutivo Nacional del Partido Revolucionario Institucional conforme al documento anexo que forma parte integral del presente Acuerdo.

SEGUNDO. Se instruye a la Unidad de Transparencia del Partido Revolucionario Institucional,realice las gestiones necesarias a efecto de que el presente Acuerdo y su anexo sepubliquen en la página oficial del partido.

TERCERO. Este Acuerdo y su anexo entrarán en vigor al día siguiente de su aprobación.

Así lo acordó, por unanimidad el Comité Nacional de Transparencia y Protección deDatos Personales del Partido Revolucionario Institucional, en sesión ordinaria celebrada el treinta de mayo de dos mil veinticuatro.

POLÍTICAS INTERNAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DEL COMITÉ EJECUTIVO NACIONAL DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL

Acta del Comité Nacional de Transparencia
PRI-CT-005-2024

Índice:

Acta del Comité Nacional de Transparencia
PRI-CT-005-2024

1. Marco Jurídico

Las presentes políticas se emiten en cumplimiento al artículo 6, inciso A, numeral II y III, artículo16 párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, artículos 30fracciones I y II y 33, fracción I, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los artículos 47 y 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

2. Objeto

Estas políticas tienen por objeto, establecer los elementos y actividades de dirección, operación y control de todos los procesos que, en el ejercicio de las funciones y atribuciones conferidas a este instituto político, que impliquen un tratamiento de datos personales a efectode proteger éstos de manera sistemática y continua.

3. Ámbito de Aplicación

Las políticas del presente documento son de observancia obligatoria por parte de todos los trabajadores y personal habilitado de todas las unidades administrativas del Comité Ejecutivo Nacional del Partido Revolucionario Institucional que, en el ejercicio de sus funciones obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean,manejen, aprovechen, divulguen, transfieran o dispongan de datos personales.

Por tanto, serán aplicables a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procedimiento, almacenamiento y organización.

Para los supuestos no previstos en las presentes políticas se aplicará lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como, enlos Lineamientos Generales de Protección de Datos Personales para el Sector Público.

4. Glosario

I.-Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales,a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

II. Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidadpara la cual fueron recabados, con el único propósito de determinar posibles responsabilidadesen 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 transcurridoéste, se procederá a su cancelación en la base de datos que corresponda;

III. Catálogo de disposición documental: Al registro general y sistemático que establece los valores documentales, la vigencia documental, los plazos de conservación y la disposición documental de las series documentales, mismas que se vinculan de los procesos y procedimientos institucionales.

IV. Ciclo vital: A las etapas (fase activa=archivo de trámite/ fase inactiva=archivo de concentración/ fase inactiva=Archivo Histórico o Baja documental) por las que atraviesan los documentos de archivo desde su producción o recepción hasta su baja documental o transferencia a un archivo histórico;

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

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

VII. 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;

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

IX. Documento de archivo: A aquel que registra un hecho, acto administrativo, jurídico, fiscal o contable producido, recibido y utilizado en el ejercicio de las facultades, competencias o funciones de las unidades administrativas y que deriva de un proceso y/o procedimiento, con independencia de su soporte documental.

X. Documento de seguridad: Instrumento que describe y da cuenta de manera general sobrelas medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable paragarantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

XI. 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 cuentadel responsable;

XII. Expediente: A la unidad documental compuesta por documentos de archivo, ordenados yrelacionados por un mismo asunto.

XIII. Gestión documental: Al tratamiento integral de la documentación a lo largo de su ciclo vital, a través de la ejecución de procesos de producción, organización, acceso, consulta, valoración documental y conservación;

XIV. INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de DatosPersonales.

XV. Ley General o LGPDPPSO: Ley General de Protección de Datos Personales en Posesiónde Sujetos Obligados;

XVI. Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público;

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

XVIII. 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 delpersonal, en materia de protección de datos personales;

XIX. 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 puedasalir de la organización, y
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimientoeficaz, que asegure su disponibilidad e integridad;

XX. 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 datospersonales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos,sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades querequiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo ymantenimiento del software y hardware, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursosinformáticos en el tratamiento de datos personales;

XXI. Partido: Comité Ejecutivo Nacional del Partido Revolucionario Institucional;

XXII. Plazo de conservación: Al periodo de guarda de la documentación en los archivos de trámite y concentración, que consiste en la combinación de la vigencia documental y, en su caso, el término precautorio y periodo de reserva que se establezcan de conformidad con la normatividad aplicable.

XXIII. Políticas: Políticas Internas de Gestión y Tratamiento de Datos Personales del Comité Ejecutivo Nacional del Partido Revolucionario Institucional;

XXIV. Responsable: El Comité Ejecutivo Nacional del Partido Revolucionario Institucional quien decide sobre el tratamiento de datos personales;

XXV. 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;

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

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

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

XXIX. Vigencia documental: Al periodo durante el cual un documento de archivo mantiene sus valores administrativos, legales, fiscales o contables, de conformidad con las disposicionesjurídicas vigentes y aplicables.

XXX. Vulnerabilidad. Falta o debilidad de seguridad en un activo o grupo de activos que puedeser explotada por una o más amenazas.

5. DE LOS PRINCIPIOS, DEBERES, DERECHOS Y OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

El derecho a la protección de los datos personales de conformidad con lo dispuesto en el artículo 16 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se regula a través de ocho principios, los cuales se traducen en obligaciones concretas para los responsables del tratamiento. Dichos principios son:

- **Licitud**
- **Finalidad**
- **Lealtad**
- **Consentimiento**
- **Calidad**
- **Proporcionalidad**
- **Información**
- **Responsabilidad**

A continuación, se explican cada uno de estos principios y, se identifican las obligaciones quese vinculan con los mismos.

1. Principio de licitud

Los datos personales tienen que ser tratados por el responsable de manera lícita, lo que supone que el responsable debe sujetarse a las facultades o atribuciones que la normatividadaplicable le otorga. En ese sentido, el responsable sólo podrá hacer con los datos personalesaquello que esté legalmente permitido.

Es decir, para dar cumplimiento al principio de licitud, el tratamiento que se dé a los datos personales deberá depender de las atribuciones o facultades que se tienen conferidas de conformidad con el marco normativo que resulte aplicable, en consecuencia, no deben tratarsedatos personales si no se tienen facultades previamente otorgadas.

En ese sentido, las obligaciones ligadas al principio en comento ser refieren a:

1) Tratar siempre los datos personales de conformidad con las atribuciones o facultadesconferidas por la normatividad, actuando con apego a la legislación mexicana, incluida la aplicable en materia de protección de datos personales y, en su caso, el derecho internacional.
2) El tratamiento se debe realizar tomando en consideración los derechos y libertades delos titulares y respetando la garantía de legalidad de los gobernados.

2. Principio de Finalidad

Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan losdatos personales.

Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades quehayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.Las finalidades deben ser concretas, explicitas, licitas y legitimas:

* **Concretas:** Cuando el tratamiento de los datos personales atiende a la consecución defines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.

* **Explícitas:** Tienen lugar cuando las finalidades se expresan y dan a conocer de maneraclara en el aviso de privacidad.

* **Lícitas:** Cuando las finalidades que justifican el tratamiento de los datos personales sonacordes con las atribuciones o facultades del responsable, conforme a lo previsto en lalegislación mexicana y el derecho internacional que le resulte aplicable.

* **Legítimas:** Cuando las finalidades que motivan el tratamiento de los datos personalesse encuentran habilitadas por el consentimiento del titular, salvo que se actualice algunade las causales de excepción previstas en el artículo 22 de la LGPDPPSO.

La finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

En ese sentido, se hace indispensable que en el aviso de privacidad se identifiquen y distinganlas finalidades del tratamiento. Asimismo, se deberá indicar el mecanismo habilitado para queel titular, si así lo desea, pueda manifestar su negativa al tratamiento de sus datos personalespara todas o algunas de las finalidades. Este mecanismo debe estar a disposición de los titulares previo a que su información personal sea tratada para dichos fines.

Al respecto, es importante mencionar que pueden surgir nuevas finalidades distintas a aquellasque motivaron su tratamiento original o que están previstas en el aviso de privacidad. Esto ocurre porque, de acuerdo con el artículo 10 de los Lineamientos Generales, el responsable deberá considerar 4 aspectos principales: la expectativa razonable de privacidad del titular basada en la relación que tiene con éste; la naturaleza de los datos personales; las consecuencias del tratamiento posterior de los datos personales para el titular; y las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y los Lineamientos Generales.

En todo caso, el titular de los datos personales puede negar o revocar su consentimiento, asícomo oponerse para el tratamiento de sus datos personales para las finalidades distintas a aquellas que motivaron su tratamiento original, sin que ello tenga como consecuencia la conclusión del tratamiento para las finalidades originarias.

Entre las obligaciones ligadas al principio de finalidad para los responsables se deberá atenderlo siguiente:

1) Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste;

2) Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean determinadas;

3) Identificar y distinguir en el aviso de privacidad entre las finalidades que dan origen al tratamiento de aquellas que son distintas a las que lo originaron, pero se consideran compatibles y/o análogas;

4) Ofrecer al titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidadessecundarias;

5) Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, como elcorreo postal, informar al titular que tiene cinco días hábiles, contados a partir de día siguiente a la notificación, para manifestar su negativa para el tratamiento de su información;

6) No condicionar el tratamiento para finalidades, distintas a las que dieron origen al tratamiento;

7) Tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiesen recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permitauna ley o reglamento, o se obtenga el consentimiento del titular de los datos

3. Principio de lealtad

El principio de lealtad implica que la obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos, lo que implica que:

* No se recabarán datos personales con dolo, mala fe o negligencia;

* No se tratarán los datos de tal manera que genere discriminación o un trato injustocontra los titulares.

* No se vulnerará la confianza del titular con relación a que sus datos personales serántratados conforme a lo acordado; y

* Se informarán todas las finalidades del tratamiento en el aviso de privacidad.

Con este principio no se permite el tratamiento tramposo, deshonesto y no ético de la información sobre los titulares, los derechos del titular dependen del responsable, para que, de esta manera, el titular pueda confiar en la buena fe del responsable, por ello, es sancionableesa confianza depositada en el responsable.

Con relación a este principio se tienen las siguientes obligaciones:

1) No hacer uso de medios engañosos o fraudulentos para la obtención de los datospersonales.

2) Respetar en todo momento la expectativa razonable de privacidad del titular.

4. Principio de consentimiento

Como regla general, el responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales. La solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir,el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general. Por ejemplo:

* **Correcto:** solicitar el consentimiento para el envío de información relacionada connuevos trámites sobre servicios que realiza el sujeto obligado.

* **Incorrecto:** solicitar el consentimiento para el uso de los datos personales en general,para cualquier finalidad que se le ocurra al responsable en el futuro. Por ejemplo: mencionar en el aviso de privacidad, sus datos personales serán recabados para las finalidades mencionadas y cualquier otra que se requiera.

El consentimiento debe ser informado, por lo que previo a su obtención, es necesario que el titular conozca el aviso de privacidad.

Además, el consentimiento debe ser libre tal y como lo refiere la Ley General, en el sentido que no medie error, mala fe, violencia o dolo que puedan afectar la voluntad del titular.

Cabe señalar que, el consentimiento puede ser tácito, expreso, o expreso y por escrito, dependiendo del tipo de datos personales que se tratarán.

Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o porcualquier otra tecnología.

El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario, y por regla general será válidoel consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

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

* Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la Ley de la materia.

* Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.

* Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

* Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

* Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

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

* Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;

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

* Cuando los datos personales se sometan a un procedimiento previo de disociación, o

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

El responsable tiene las siguientes obligaciones en torno al principio de consentimiento:

1) Obtener el consentimiento del titular para el tratamiento de los datos personales, cuandono se actualice alguno de los supuestos previstos en el artículo 22 de la Ley General;

2) Solicitar el consentimiento siempre ligado a finalidades específicas e informadas en el aviso de privacidad;

3) Determinar el tipo de consentimiento que se requiere: tácito, expreso o expreso y por escrito;

4) Solicitar el consentimiento expreso y por escrito para los datos personales sensibles, encaso de que no se actualice alguno de los supuestos del artículo 22 de la Ley General;

5) Solicitar el consentimiento expreso o expreso y por escrito cuando así lo requiera una ley o reglamento, se acuerde con el titular o lo determine conveniente el responsable;

6) Dar a conocer al titular el aviso de privacidad previo a la obtención del consentimiento;

7) Solicitar el consentimiento previo a la obtención de los datos personales, si éstos se recaban directamente del titular y no se actualiza alguno de los supuestos previstos enel artículo 22 de la Ley General;

8) Solicitar el consentimiento antes de utilizar los datos personales para las finalidades para las cuales se obtuvieron, si éstos se recabaron de manera indirecta y no se actualiza alguno de los supuestos previstos en el artículo 22 de la Ley General;

9) Implementar medios sencillos y gratuitos para la obtención del consentimiento, de acuerdo con el tipo de consentimiento que se requiera (tácito, expreso o expreso y porescrito);

10) Llevar un control para identificar a los titulares que negaron su consentimiento y a las finalidades concretas para las cuales no se podrán tratar los datos personales;

11) Esperar el plazo de cinco días hábiles que señala el artículo 15 de los Lineamientos Generales, para utilizar los datos personales, cuando éstos se hayan obtenido de manera indirecta, el aviso de privacidad se haya dado a conocer por un medio que no permita el contacto directo o personal con el titular y se requiera el consentimiento tácito;

12) Documentar su actuar para acreditar que se cumplió con el principio de consentimiento,y

13) Solicitar el consentimiento si hubo cambios en las finalidades informadas en el aviso deprivacidad y éstas lo requieren por no actualizarse alguno de los supuestos previstos enel artículo 22 de la Ley General.

5. Principio de calidad

El principio de calidad significa que, conforme a la finalidad o finalidades para las que se vayana tratar los datos personales, éstos deben ser exactos, correctos, completos y actualizados, por tanto:

* Los datos personales son **exactos y correctos** cuando en posesión del responsable nopresentan errores que pudieran afectar su veracidad.

* Los datos personales son **completos** cuando su integridad permite el cumplimiento delas finalidades que motivaron su tratamiento y de las atribuciones del responsable.

* Los datos personales están **actualizados** cuando los datos personales responden fielmente a la situación actual del titular.

En ese sentido, el partido debe adoptar las medidas que considere convenientes para procurarque los datos personales cumplan con estas características, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectadopor dicha situación.

Ahora bien, respecto a las obligaciones que se tienen que cumplir ligadas al principio de calidadse debe observar lo siguiente:

1) Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación;

2) Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo debloqueo;

3) Bloquear los datos personales antes de suprimirlos; por lo que, durante el periodo de bloqueo sólo serán tratados para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades;

4) Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación de conformidad con lo establecido por la Ley General de Archivos;

5) Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.

6) En caso de que se requiera, demostrar que los datos personales se conservan, bloquean y suprimen cumpliendo los plazos previstos para ello, o bien, en atención a una solicitud de ejercicio del derecho de cancelación.

6. Principio de Proporcionalidad

El principio de proporcionalidad establece la obligación del responsable de tratar sólo aquellosdatos personales que resulten necesarios, adecuados y relevantes en relación con lasfinalidades para las cuales se obtuvieron.

Por lo anterior, se deberá realizar esfuerzos razonables para que los datos personales tratadossean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron, las cuales, como se señaló anteriormente, deben ser acordes con las atribucionesconferidas al responsable y señaladas en el aviso de privacidad.

Las obligaciones por cumplir con respecto a este principio son:

1) Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantesen relación con las finalidades para las cuales se obtuvieron;

2) Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles; y

3) Crear bases de datos con datos personales sensibles sólo cuando se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidosen el artículo 22 de la Ley General en la materia.

7. Principio de Información

Los responsables se encuentran obligados a informar a los titulares, las características principales del tratamiento al que será sometida su información personal, lo que se materializaa través del aviso de privacidad. A fin de que los titulares puedan tomar decisiones informadasal respecto, y puedan ejercer su derecho a la protección de su información personal.

En ese sentido, todo responsable que trate datos personales, sin importar la actividad que realice, requiere elaborar y poner a disposición los avisos de privacidad que correspondan a los tratamientos que lleven a cabo.

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

Asimismo, resulta pertinente aclarar que los responsables deben tener el número de avisos deprivacidad que resulten necesarios de acuerdo con los tipos de tratamientos que realicen.

La puesta a disposición del aviso de privacidad implica publicar en un lugar visible, accesible y gratuito, en el cual el titular, de manera informada, cuente con la posibilidad de conocer el tratamiento que se les dará a sus datos personales. En ese sentido, el responsable no está obligado a entregar una copia del aviso de privacidad al titular, a menos que éste lo solicite.

El aviso de privacidad podrá difundirse, ponerse a disposición o reproducirse en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación. Por lo que, el aviso de privacidad deberá estar ubicado en unlugar visible y que facilite su consulta.

Las obligaciones ligadas al principio de información son:

1) Poner a disposición de los titulares el aviso de privacidad en los términos que fije la LeyGeneral en la materia y sus Lineamientos, aunque no se requiera el consentimiento delos titulares para el tratamiento de los datos personales;

2) Poner a disposición del titular el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera personal y directa del titular;

3) Poner a disposición del titular el aviso de privacidad al primer contacto que se tenga conéste, cuando los datos personales se hayan obtenido de una transferencia consentida, de una que no requiera el consentimiento, o bien de una fuente de acceso público;

4) Poner a disposición del titular el aviso de privacidad previo a iniciar tratamiento de los datos personales para la finalidad para la que se obtuvieron (aprovechamiento), cuandoéstos no se hayan obtenido de manera directa del titular, el tratamiento no requiera delcontacto con él y se cuente con datos para contactarlo;

5) Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades, cuando el responsable requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales losrecabó inicialmente;

6) Redactar el aviso de privacidad de manera que sea claro, comprensible, con una estructura y diseño que facilite su entendimiento; para su elaboración, tomar en cuentael perfil de los titulares y atender lo siguiente: no usar frases inexactas, ambiguas o vagas; no incluir textos o formatos que induzcan al titular a elegir una opción en específico; no pre-marcar casillas en las que se solicite el consentimiento, y no remitira textos o documentos que no estén disponibles;

7) Ubicar el aviso de privacidad en un lugar visible y que facilite su consulta, conindependencia del medio de difusión o reproducción que se utilice;

8) Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfieradatos personales;

9) Demostrar el cumplimiento del principio de información, en caso de que así se requiera;10)Cuando se utilice la modalidad integral del aviso de privacidad, incluir todos los elementos informativos previstos de la normatividad aplicable;

11) Cuando se utilice la modalidad simplificada del aviso de privacidad, incluir todos los elementos informativos correspondientes;

12) Elaborar y tener disponible para su consulta el aviso de privacidad integral, conindependencia de que se ponga a disposición de los titulares en su versión simplificadaprevio a la obtención o aprovechamiento de los datos personales;

13) No establecer cobros para la consulta del aviso de privacidad;

14) Cuando así ocurra, informar en el portal de Internet, a través de una comunicación o advertencia colocada en un lugar visible y a la cual se pueda acceder desde el momentoen que se ingresa a dicho portal, que están siendo utilizadas tecnologías de rastreo, que a través de éstas se pueden recabar datos personales y la forma en cómo se pueden deshabilitar, y

15) Poner a disposición de los titulares un nuevo aviso de privacidad en los siguientes casos: (i) cambie la identidad del responsable; (ii) se requiera recabar nuevos datos personales sensibles, patrimoniales o financieros y se requiera el consentimiento del titular; (iii) se requiera tratar los datos personales para nuevas finalidades que requieran el consentimiento del titular, y (iv) se requiera realizar nuevas transferencias que requieran el consentimiento del titular.

8. Principio de Responsabilidad

Este principio establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante los titulares y órganos garantes, que cumple con sus obligaciones en torno a la protección de los datos personales.

Bajo este principio, los responsables del tratamiento están obligados a velar por la protecciónde los datos personales aun y cuando los datos estén siendo tratados por encargados. Asimismo, este principio supone que el responsable tome las medidas suficientes para que lostérminos establecidos en el aviso de privacidad sean respetados por aquéllos con los que mantenga una relación jurídica, así como al momento de realizar transferencias nacionales o internacionales de datos personales.

En torno al principio de responsabilidad se tienen las siguientes obligaciones:

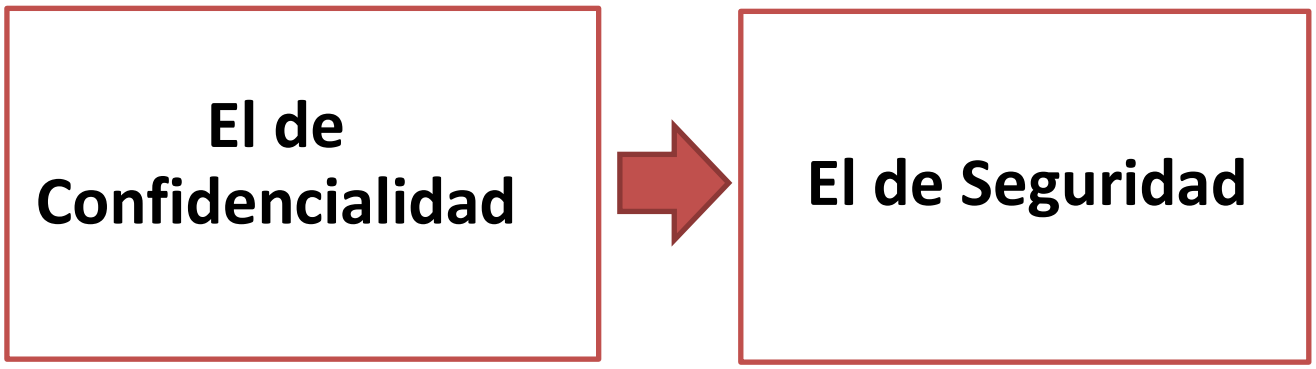
1) Velar por el cumplimiento de los principios y responder por el tratamiento de los datospersonales, aún por aquéllos comunicados a encargados;

2) Adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad, y

3) Tomar medidas para que los terceros con quienes mantiene una relación jurídica que implique el tratamiento de los datos personales, respeten el aviso de privacidad en el que se establezcan las condiciones de dicho tratamiento.

6. DE LOS DEBERES A CUMPLIR EN MATERIA DEPROTECCIÓN DE DATOS PERSONALES.

La protección de datos personas tiene como base dos deberes:



El **deber de confidencialidad** implica que se establezcan controles o mecanismos que tenganpor objeto que todas aquellas personas que traten datos personales, en cualquier fase del tratamiento, mantengan en secreto la información, así como evitar que la información sea revelada a personas no autorizadas y prevenir la divulgación no autorizada de la misma.

Implica la obligación de guardar secreto respecto de los datos personales que son tratados, para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información y hacer mal uso de esta.

Cuando se tratan datos personales, el responsable tiene que adoptar medidas para evitar quequienes tengan acceso a éstos, divulguen dicha información. Incluso la obligación de confidencialidad tiene que hacerse cumplir una vez que finalice la relación jurídica, a través decláusulas de confidencialidad establecidas en los instrumentos jurídicos suscritos entre el responsable del tratamiento y quien tenga acceso a los datos personales.

El **deber de Seguridad**, es básico para la verdadera protección de los datos personales y, esla implementación de un Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión), que permita planificar, implementar, monitorear y mejorar las medidas de seguridadde carácter administrativo, físico y técnico, a través de una serie de actividades interrelacionadas y documentadas tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

Así, se debe entender por Sistema de Gestión de Seguridad de los Datos Personales al conjunto de elementos y actividades relacionadas entre sí, que le permitirán al responsable planificar, implementar, monitorear y mejorar las medidas de seguridad de carácter administrativo, físico y técnico, tomando en consideración la normatividad aplicable, así como,los estándares a nivel nacional e internacional, en materia de protección de datos personales y seguridad.

Para adoptar un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), se debe hacer basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar). El responsable debe implementar un sistema de gestión contemplando cuando menos los siguientes aspectos:

a) Crear políticas internas para la gestión y tratamiento de los datos personales;

b) Elaborar un inventario de datos personales;

c) Definir funciones y obligaciones del personal que trate datos personales;

d) Realizar un análisis de riesgo de los datos personales, el cual deberá consideraramenazas, vulnerabilidades existentes y recursos involucrados en el tratamiento;

e) Realizar un análisis de brecha (consistente en comparar las medidas de seguridadexistentes contra las medidas de seguridad faltantes);

f) Elaborar un plan de trabajo para implementar las medidas de seguridad faltantes y elcumplimiento cotidiano de sus políticas de gestión;

g) Monitorear y revisar de manera periódica las medidas de seguridad implementadas; y

h) Diseñar y capacitar al personal del responsable.

Lo anterior, se materializa a través del documento de seguridad, siendo este el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicasy administrativas adoptadas por el responsable para garantizar la confidencialidad, integridady disponibilidad de los datos personales.

Al respecto, el documento de seguridad deberá actualizarse cuando ocurra alguno de los siguientes eventos:

* Se produzcan modificaciones sustanciales al tratamiento de datos personales, queimpliquen un cambio en el nivel de riesgo;

* Atendiendo a una mejora continua, por el monitoreo y revisión del sistema de gestión;

* Por un proceso de mejora, para disminuir el impacto de una vulneración a la seguridad;

* Como parte de las acciones preventivas y correctivas de una vulneración.

7. LOS DERECHOS ARCO

La Ley General, contempla cuatro derechos en materia de datos personales, **Acceso, Rectificación, Cancelación y Oposición**, mismos que pueden ser ejercidos en todo momentopor el titular o su representante. Por tanto, a continuación, se hace una breve descripción de en qué consiste cada uno de ellos.

El **Derecho de Acceso**, es el derecho que tiene el titular para solicitar el acceso a sus datos personales que se encuentren en las bases de datos, sistemas, archivos, registros o expedientes que posee el responsable, así como, de conocer información relacionada con el tratamiento que se da a su información.

Para ello, el titular deberá indicar la modalidad en la que prefiere se reproduzcan sus datos personales.

Derecho de Rectificación, es aquel que tiene el titular de solicitar la rectificación o corrección de sus datos personales, cuanto éstos sean inexactos o incompletos o no se encuentren actualizados. Es decir, el titular puede solicitar en cualquier momento que sus datos sean corregidos cuando advierta que los mismos son incorrectos, desactualizados o inexactos.

Así, el titular debe especificar las modificaciones que solicita a los datos personales, así como, aportar los documentos que sustenten su solicitud.

Derecho de Cancelación es el derecho que tienen los titulares de solicitar que sus datos personales se eliminen de los documentos de archivo, registros, expedientes, sistemas y/o bases de datos del responsable que los trata. Aunque hay que tomar en cuenta que no en todos los casos se podrán eliminar sus datos personales, principalmente cuando sean necesarios por alguna cuestión legal o para el cumplimiento de obligaciones.

Al respecto, es importante hacer notar que, con relación a una solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión (eliminación) de sus datos personales en los documentos de archivo, registros o bases de datos del responsable.

Derecho de Oposición este derecho tiene la finalidad de que el titular pueda solicitar que susdatos personales no se utilicen para una determinada finalidad. Sin embargo, no siempre se podrá impedir el uso de los datos, cuando estos sean necesarios por motivos legales o para elcumplimiento de obligaciones.

Asimismo, en caso de una solicitud de oposición, el 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 finalidadesespecíficas respecto de las cuales requiere ejercer el derecho de oposición.

Derivado de lo anterior, es necesario dejar en claro que, existen algunos límites a los derechosantes mencionados, por lo que a continuación, se mencionan las causas por las que se puedenegar el ejercicio de los derechos ARCO:

- El titular de los datos personales o su representante no hayan acreditado su identidad;
- El responsable no sea competente para atender la solicitud;
- Exista un impedimento legal;
- Se puedan afectar los derechos de terceras personas;
- Cuando el ejercicio de los derechos ARCO pudiera obstaculizar procesos judiciales oadministrativos;
- Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;
- Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridaspor el titular;
- Cuando los datos sean parte de información de las entidades sujetas a regulación ysupervisión financiera del sujeto obligado, o
- Cuando en función de las atribuciones legales de este sujeto obligado, el uso, resguardoy manejo sean necesarios para mantener la integridad, estabilidad y permanencia del Estado mexicano.

No obstante lo anterior, aun cuando resultara improcedente el ejercicio de los derechos ARCO,siempre se estará obligado a responder las solicitudes e informar a los titulares las causas deimprocedencia.

8. ROLES Y RESPONSABILIDADES ESPECÍFICAS DE LOSINVOLUCRADOS INTERNOS Y EXTERNOS DENTRO DE LA ORGANIZACIÓN.

De conformidad con lo dispuesto en el artículo 57 de los Lineamientos Generales, el Partido deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendiciónde cuentas de todas las personas que traten datos personales en la organización.

Por tanto, se deberán establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales al interior del partido conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como, las consecuencias de su incumplimiento.

De manera general, el personal del Partido que de tratamiento a los datos personales que obren bajo su resguardo deberá:

1. Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales,a los que hace referencia la Ley General de la materia.

2. Justificar por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normativa aplicable les confiera todo tratamiento que efectúe.

3. 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 veracidadde los mismos.

4. Las Unidades Administrativas deberán tener debidamente identificadas a las personasque, en el ejercicio de sus funciones, puedan realizar tratamiento de datos personales,garantizando la restricción de acceso a terceros no autorizados.

5. Las personas que tengan acceso a datos personales, no podrán reproducirlos ni difundirlos mediante ningún medio sea físico o electrónico, a menos que sea necesariopara el ejercicio de sus funciones.

6. La transferencia de datos personales que se realice podrá realizarse siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles y análogas con la finalidad que motivó el tratamiento.

7. Los trabajadores y/o funcionarios partidistas que participen en el tratamiento de datos personales, deberán cumplir con la capacitación en materia de protección de datos personales que al efecto apruebe el Comité de Transparencia.

8. El plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para cumplir con:

* Las disposiciones legales establecidas en la Ley General de Archivos;
* Las disposiciones aplicables en la materia de que se trate;
* Los aspectos administrativos, contables, fiscales, jurídicos e históricos de lainformación, y
* El periodo de bloqueo.

9. Deberá suprimir los datos personales, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos, siempre y 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.

10. En cuanto a los datos personales sensibles, el responsable debe realizar esfuerzos razonables para limitar el periodo de tratamiento al mínimo indispensable.

11. Establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyanlos periodos de conservación de estos.

12. Tratar sólo los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

13. Es responsabilidad de los titulares de las unidades administrativas el informar a la Unidad de Transparencia sobre las bases de datos personales a las que de tratamiento para que, en colaboración se cree el aviso de privacidad, se publique en el medio oficialdispuesto para ello y, se pueda registrar en el inventario correspondiente dicho tratamiento.

14. Informar al titular, a través del aviso de privacidad, la existencia y características del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

15. Establecer y mantener medidas de seguridad físicas, técnicas y administrativas para laprotección de los datos personales en contra de daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como, garantizar su confidencialidad,integridad y disponibilidad.

16. Deberá, en caso de una vulneración a la seguridad, analizar las causas por las cualesse presentó e implementar en su plan de trabajo las acciones preventivas y correctivaspara adecuar las medidas de seguridad y el tratamiento de los datos personales.

17. Llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas deforma inmediata y definitiva.

18. Informar al titular, y según corresponda, al INAI y a los Organismos garantes de las Entidades Federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y se hayan empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectadospuedan tomar las medidas correspondientes para la defensa de sus derechos.

19. Informar a toda persona que da tratamiento de datos personales en nombre del Partido que está impedida para divulgar dicha información, por lo que deberá guardar confidencialidad y preferentemente esta deberá estar establecida en los instrumentos jurídicos suscritos entre el partido y aquellos que tengan acceso a los datos personales.

20. El Comité de Transparencia tiene la responsabilidad de establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO.

Para el caso de personas externas al Partido que dan tratamiento a los datos personales quemaneja este, tendrán la figura de **encargado** siendo, por tanto, un prestador de servicios quelos trata a nombre y por cuenta del responsable. Esta figura tiene las siguientes características:

* Puede ser una persona física o jurídica;
* Del ámbito público o privado;
* Ajeno a la organización del responsable, es decir, los trabajadores que forman parte dela estructura del responsable no son encargados;
* Puede tratar los datos solo o de manera conjunta con otras personas;

Para el caso de los encargados, se deberá tener en cuenta lo siguiente:

1. El Partido está obligado a establecer la relación con el encargado a través de un documento que permita acreditar la existencia de la relación jurídica, su alcance y contenido; siempre con estricto apego a lo previsto en el aviso de privacidad que definiólas condiciones del tratamiento de los datos personales y nunca se deberá contravenirlo establecido en la Ley General.

2. El instrumento jurídico en el que se establezca la relación jurídica con el encargado deberá contemplar, al menos, las siguientes obligaciones:

   I. Realizar el tratamiento de los datos personales conforme a las instruccionesdel responsable;
   II. Abstenerse de tratar los datos personales para finalidades distintas a lasinstruidas por el responsable;
   III. Implementar las medidas de seguridad conforme a los instrumentos jurídicosaplicables;
   IV. Informar al responsable cuando ocurra una vulneración a los datospersonales que trata por sus instrucciones;
   V. Guardar confidencialidad respecto de los datos personales tratados;
   VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no existauna previsión legal que exija la conservación de los mismos, y
   VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente
   VIII. Permitir al INAI o al responsable, realizar verificaciones en el lugar o establecimiento donde se lleva a cabo el tratamiento de los datos personales;
   IX. Colaborar con el INAI en las investigaciones previas y verificaciones de acuerdo con lo dispuesto en la Ley General y los Lineamientos Generales, por lo que, el encargado tiene la obligación de proporcionar la información ydocumentación necesaria.

3. De acuerdo con el numeral 61 de la Ley General, el encargado puede llevar a cabo subcontrataciones, siempre que cuente con la autorización del responsable, es decir, que se establezca en el instrumento jurídico mediante el cual se haya formalizado la relación entre responsable y encargado, se contemplen la subcontratación de servicios.

   Por ello, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia,alcance y contenido.

4. En su caso, el encargado deberá prever en el instrumento jurídico correspondiente quela persona subcontratada asume las mismas obligaciones que se establezcan para el encargado.

5. El encargado será considerado responsable de los datos personales en los casos en que incumpla con las instrucciones del responsable, contenidas en el instrumento jurídico que celebran previamente, siendo aplicable la normatividad de datos personalesegún corresponda, es decir, la Ley General o la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

6. Las unidades administrativas que realicen transferencias de datos personales, dentro ofuera de México, deberán hacerlo del conocimiento del titular en el aviso de privacidad.

7. El titular deberá otorgar su consentimiento para que la transferencia se realice, salvo enlos casos de

excepción previstos en el artículo 22, 66 y 70 de la Ley General. Por su parte, el receptor en su carácter de responsable deberá cumplir con lo establecido en la normatividad aplicable en materia de datos personales, ya sea que pertenezca al sectorpúblico o privado.

8. Sólo se deberán hacer transferencias fuera del territorio nacional cuando el tercero receptor se obligue a proteger los datos personales conforme a los principios y deberesque establece la Ley General y demás disposiciones aplicables en la materia.

9. En caso de que la transferencia sea nacional, el receptor deber observar la confidencialidad y la obligación de utilizar los datos personales únicamente para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad.

9. SANCIONES EN CASO DE INCUMPLIMIENTO.

El incumplimiento a las obligaciones establecidas en la Ley General implica la vulneración al derecho humano de la protección de datos personales, lo que puede dar lugar a la imposiciónde medidas de apremio y sanciones.

Así, el INAI puede imponer como medidas de apremio la amonestación pública o una multa equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces del valor de la unidadde medida y actualización, **estas multas no podrán ser cubiertas con recursos públicos**.

Será causas de sanción por incumplimiento de las obligaciones establecidas en la Ley General,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 presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derechode que se trate;
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;
V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley General, según sea el caso, y demásdisposiciones que resulten aplicables en la materia;
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley General;
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos31, 32 y 33 de la Ley General;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley General;
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley General;
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 General;
XIII. No acatar las resoluciones emitidas por el INAI y
XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44,fracción VII de la Ley General de Transparencia y Acceso a la Información Pública,o bien, entregar el mismo de manera extemporánea.

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, seránconsideradas como graves para efectos de su sanción administrativa.

En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente.

Ante incumplimientos por parte de este Partido Político, el INAI dará vista al Instituto NacionalElectoral, para que resuelva lo conducente, sin perjuicio de las sanciones establecidas para los partidos políticos en las leyes aplicables.

10. IDENTIFICACIÓN DEL CICLO DE VIDA DE LOS DATOS PERSONALES.

El artículo 59 de los Lineamientos Generales dispone que, en el ciclo de vida de los datos personales, se debe considerar: la obtención; el almacenamiento; el uso de estos conforme asu acceso, manejo, aprovechamiento, monitoreo y procesamiento; su divulgación; el bloqueo que, en su caso proceda; la cancelación, supresión o destrucción de los datos personales.

Por lo que en el siguiente diagrama se puede observar el **ciclo de vida de los datos personales** identificado por este sujeto obligado:

En ese sentido, cabe destacar que en todo el ciclo de vida de los datos personales deben tomarse en consideración y observarse los principios y deberes para su tratamiento.

La **Obtención** es el momento en el que el partido comienza a dar tratamiento a datos personales entendiendo esto como, la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

En ese sentido, se deberá identificar a las personas, áreas, departamentos o direcciones del partido que realicen cualquiera de las actividades antes señaladas, así como, identificar qué actividad en concreto realizan con los datos personales, por ejemplo, si los recaban yalmacenan; si los recaban, transfieren o acceden a los mismos. En todos los casos, los datospersonales que se tratan podrán ser **almacenados** en soporte electrónico o físico.

Es necesario identificar cada una de las finalidades concretas para las cuales se tratan los datos personales, lo cual, se vincula de manera directa con las actividades en las cuales se **usan los datos personales**.

Así, durante el ciclo de vida el Partido puede comunicar datos a los encargados, para que estosden tratamiento a nombre y por cuenta de este instituto político, a esta comunicación de datospersonales se le denomina **remisión**.

La relación entre ambos deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa aplicable.

El encargado puede ser una persona física o jurídica, pública o privada, ajena a la organizacióndel responsable, que sola o conjuntamente trate datos personales.

Ahora bien, la comunicación de datos personales no solamente puede ser con encargados, también puede ser con el propio titular de los datos o con otro responsable, lo que se denomina**transferencia**.

De igual forma, en el ciclo de vida se deben tener en claro los plazos de conservación de los datos, mismos, que deben observarse en cumplimiento a la legislación en materia de gestión documental y administración de archivos, en conjunto con la Coordinación General de Archivoso área encargada de ello con la finalidad de identificar y determinar a través de un análisis deprocesos y procedimientos: los documentos de archivo y plazos de conservación de las seriesdocumentales establecidas en el Catálogo de disposición documental.

En ese sentido, es necesario prever el **bloqueo** de los datos personales en los casos que corresponda a efecto de que una vez identificados los plazos de conservación y cumplida la finalidad para la cual fueron recabados los datos, no se de tratamiento a estos por el responsable hasta que se concluya el plazo de prescripción legal o contractual de los datos yuna vez concluido este se deberá proceder a su cancelación.

Por último, la **supresión** de estos de conformidad con lo dispuesto en el artículo 23 de los Lineamientos Generales, establece la obligación del responsable de establecer políticas, métodos y técnicas orientadas a la supresión de los datos atendiendo los medios de almacenamiento, es decir, físicos o electrónicos y deberán tener las siguientes características:

* Ser irreversible: el proceso utilizado no permita recuperar los datos.
* Ser seguro y confidencial: la eliminación debe atender a los deberes de confidencialidady seguridad.
* Ser favorable al medioambiente: que el método utilizado produzca la menor cantidad deemisiones y desperdicios que afecten el medio ambiente.

Por tanto, para la cancelación, supresión o destrucción de los datos personales, se deberá atender lo dispuesto en las Políticas, Métodos y Técnicas orientadas a la supresión definitiva de datos personales que obren en el Comité Ejecutivo Nacional del Partido Revolucionario Institucional.

11. PROCESO GENERAL PARA EL ESTABLECIMIENTO,ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y MEDIDAS DE SEGURIDAD.

Las medidas de seguridad son el conjunto de acciones y actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales.Para determinar qué medidas de seguridad se deben implementar, se deberán tomar en cuenta los siguientes factores:

Factoresde Riesgo
Riesgo inherente a los datos personales.
Sensibilidad de los datos personales.Desarrollo tecnológico.
Las posibles consecuencias de una vulneración para los titulares.
Las transferencias de datos personales que se realicen.
Número de titulares.
Las vulneraciones previas ocurridas en los sistemas de tratamiento.
El riesgo por el valor cuantitativo y cualitativo respecto de una tercera persona no autorizada.

Tomando en consideración los factores de riesgo antes mencionados, se deberá monitoreary revisar las medidas de seguridad, de conformidad con lo dispuesto en el artículo 63 de losLineamientos Generales, a saber:

* Nuevos activos gestionados;
* Modificaciones necesarias;
* Nuevas amenazas dentro o fuera de la organización;
* Posibilidad de nuevas vulneraciones, por las amenazas correspondientes;
* Vulneraciones identificadas para determinar amenazas nuevas;
* Impacto de amenazas valoradas, vulnerabilidades y riesgos en conjunto;
* Incidentes y vulneraciones de seguridad ocurridas.

Por tanto, de conformidad con la Ley General se consideran como vulneraciones de la seguridad las siguientes:

A. La pérdida o destrucción no autorizada.

B. El robo, extravío o copia no autorizada.

C. El uso, acceso o tratamiento no autorizado.

D. El daño, la alteración o modificación no autorizada.

Dicho lo anterior, el monitoreo y revisión de las medidas de seguridad se realizará a través delas unidades administrativas en conjunto con la Unidad de Transparencia, siendo este el proceso de supervisar el funcionamiento del sistema de gestión y evaluar los objetivos, políticas, procesos y procedimientos establecidos en el mismo, con el fin de cumplir con la legislación en protección de datos personales.

De esta manera, cuando el partido sufra alguna vulneración a la seguridad, éste deberá actuarconforme a lo dispuesto en los artículos 37, 38, 39, 40 y 41 de la Ley General. Asimismo, parael caso de las notificaciones sobre vulneraciones, deberá observar los artículos 66, 67 y 68 delos Lineamientos Generales y, conforme a los mecanismos de monitoreo y revisión de las medidas de seguridad establecidos en el Documento de Seguridad del partido.

12. Proceso general de atención a los derechos ARCO.

El derecho a la protección de datos personales es un derecho personalísimo, solamente los titulares o sus representantes podrán solicitar el ejercicio de los derechos ARCO, por lo que es indispensable acreditar la identidad.

Para que un derecho sea ejercido no es necesario que se haya ejercido previamente otro, ni el ejercicio de uno impide que posteriormente se ejerza uno distinto.

La solicitud debe presentarse ante el responsable que posea los datos personales respecto delos cuales se requiera el acceso, rectificación, cancelación u oposición.

Para lo cual, de conformidad con el artículo 52 de la Ley General, se deberán tomar en consideración los siguientes requisitos:

* El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;
* Los documentos que acrediten la identidad del titular y, en su caso, la personalidad eidentidad de su representante;
* De ser posible, el área responsable que trata los datos personales y ante el cual sepresenta la solicitud;

- La descripción clara y precisa de los datos personales respecto de los que se buscaejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;
- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita eltitular, y
- Cualquier otro elemento o documento que facilite la localización de los datospersonales, en su caso.

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

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

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

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

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

Como se señaló, un requisito fundamental para el ejercicio de derechos ARCO es que el titularacredite, previo al ejercicio de estos que, es el titular de los datos personales y/o en su caso lapersonalidad de su representante legal, por ello, de conformidad con lo establecido en el artículo 76 de los Lineamientos Generales existen tres medios para acreditar la identidad:

I. Identificación oficial,
II. Instrumentos electrónicos o mecanismos de autenticación, como la FirmaElectrónica; y
III. Mecanismos establecidos por el responsable de manera previa, siempre y cuandopermitan de forma inequívoca la acreditación de la identidad del titular.

Por su parte el representante deberá acreditar su personalidad mediante:

I. Copia de identificación oficial del titular de los datos;
II. Identificación del representante, y
III. Instrumento notarial o Carta Poder (firmada por dos testigos y sus respectivas identificaciones)

No se omite mencionar que, la solicitud del ejercicio de los derechos ARCO se podrá presentarpor escrito libre, formatos, medios electrónicos o cualquier otro que establezca el INAI, en el ámbito de su competencia.

Transitorios

Primero. Estas políticas, internas de gestión y tratamiento de los datos personales del ComitéEjecutivo Nacional del Partido Revolucionario Institucional entrarán en vigor al día siguiente de su aprobación.

Segundo. Las presentes políticas deberán ser publicadas en el apartado de Protección de datos personales del partido, al que hace referencia el artículo 250 de los Lineamientos Generales, a más tardar el 15 de junio de 2024.