PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES CONSEJO NACIONAL PARA PREVENIR LA DISCRIMINACIÓN

Fecha de dictaminación de la Dirección de Asuntos Jurídicos	Fecha de aprobación Comité de Transparencia
05 de marzo del 2025	07 de marzo del 2025

I. OBJETIVO

De conformidad con los deberes establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de **Protección de Datos Personales para el Sector Público**, así como las normas que de los mismos derivan, se elabora el presente documento con la finalidad de presentar las acciones de trabajo para la protección de los datos personales que se encuentran bajo conocimiento y resguardo del Consejo Nacional para Prevenir la Discriminación.

II. APLICABILIDAD

El presente programa de protección de datos personales será aplicable para todas las Unidades Administrativas del Conapred que realicen tratamientos de datos personales en ejercicio de sus atribuciones y funciones.

Asimismo, en virtud de que uno de los objetivos del Programa es cumplir con las obligaciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), se cubrirán todos los principios, deberes y obligaciones que establece la Ley para los responsables del tratamiento.

III. MARCO JURÍDICO

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)
- Lineamientos Generales de Protección de Datos Personales para el Sector Público
- Diccionario de Protección de Datos Personales. Conceptos Fundamentales.
- Ley General de Transparencia y Acceso a la Información Pública (LGTAIP)
- Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP)
- Ley General de Archivos (LGA)

IV. RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

- Comité de Transparencia
- Unidad de Transparencia
- Unidades Administrativas
- Encargados

Así mismo, además de las funciones y obligaciones con las que cuentan las Unidades Administrativas involucradas, de manera general todas las personas servidoras públicas que tengan acceso al tratamiento de datos personales tendrán que observar lo siguiente:

Obligaciones Generales	
Deberes	**Funciones**
• Tratar los datos personales con responsabilidad y las medidas de seguridad que se hayan establecido para tal fin;	• Garantizar la confidencialidad de la información que conozcan a través del desarrollo de sus funciones y actividades en especial cuando se traten de datos que puedan ser vulnerables para la integridad de las personas físicas.
• Capacitarse en materia de protección de datos personales	• Conocer el tratamiento de los datos personales, así como las medidas de protección a fin de salvaguardarlos ante amenazas, dando aviso inmediato a sus superiores jerárquicos, ante cualquier eventualidad que ponga en riesgo la confidencialidad, integridad y disponibilidad de los datos personales, o bien, al observar alguna vulneración a la seguridad de estos.

Por otra parte, se debe tener en cuenta que, de conformidad con las funciones, atribuciones, cargos y designaciones de las personas servidoras públicas de las unidades administrativas del Conapred, se catalogan tres niveles básicos a través de los cuales se podría vulnerar la seguridad en el tratamiento de los datos personales.

Es por lo que, el deber de garantizar la seguridad y su confidencialidad en el tratamiento de la información recabada tendrá que procurarse entre los involucrados que intervengan en el tratamiento de los datos personales, aún y cuando hayan finalizado su participación en el mismo, hayan cambiado sus funciones o se termine su relación con el Conapred.

V. ALCANCE

Las Unidades Administrativas que forman parte del Conapred, mismos que deberán observar el Programa de Protección de Datos Personales son las siguientes:

- Presidencia
- Coordinación de Vinculación, Cultura y Educación
- Dirección General Adjunta de Quejas
- Coordinación de Estudios, Legislación y Políticas Públicas
- Dirección de Asuntos Jurídicos
- Dirección de Planeación, Administración y Finanzas
- Dirección de Apoyo a Órganos Colegiados y Coordinación Interinstitucional
- Subdirección de Comunicación Social
- Subdirección de Gestión
- Oficina de Representación en el Consejo Nacional para Prevenir la Discriminación del Órgano Interno de Control en la Secretaría de Gobernación.

VI. GESTIÓN DE DATOS PERSONALES

Las Unidades Administrativas del Conapred encargadas de llevar a cabo el tratamiento de datos personales, deberán cumplir con los principios, deberes y obligaciones que prevé la Ley General de Transparencia y Acceso a la Información Pública, para lo cual se tendrán que guiar con las directrices establecidas en las normas aplicables y el presente documento general.

En ese sentido, es necesario reiterar que, es obligación de todas las personas servidoras públicas, salvaguardar cualquier información que se encuentre en su poder concerniente a una persona física identificada (que sabemos quién es) o identificable (que fácilmente podemos determinar quién es); esto es, cuando su identidad se determina a través de cualquier información, aún y cuando pertenezcan a servidores públicos. Por tal motivo, se tendrán que observar en todo momento los principios en la materia, siendo estos el principio de *licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad*,

según sea el ciclo de vida de los datos personales dentro de los tratamientos que tengan a su cargo.

VII. CUMPLIMIENTO DE LAS OBLIGACIONES

Para el acatamiento de las normas en la materia, deberán participar todas las Unidades Administrativas del Conapred, que intervengan en el tratamiento de datos personales en ejercicio de sus atribuciones y funciones, con la finalidad de preservar la confidencialidad, reserva, integridad y disponibilidad de la información que manejan los usuarios de las diferentes áreas del Conapred.

A continuación, se hace mención, de manera enunciativa más no limitativa, el fundamento y obligaciones que tendrán los responsables del tratamiento de datos personales para el cumplimiento de cada principio rector:

- **PRINCIPIO DE LICITUD**

Artículo 16, 17 de la LGPDPPSO.

Los datos personales deberán tratarse con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional. El tratamiento de los datos personales que realicen las personas servidoras públicas deberá sujetarse a las facultades o atribuciones que la normativa aplicable les confiera.

Debe tenerse en consideración que no se podrán tratar datos personales sensibles, salvo consentimiento expreso, o excepciones señaladas en el *artículo 22 de la LGPDPPSO.*

- **PRINCIPIO DE FINALIDAD**

Artículo 16, 18 de la LGPDPPSO

Todo tratamiento de datos personales que se efectúe deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

Se podrán tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, sólo pueden ser tratados para cumplir con la finalidad que hayan sido informadas en el aviso de privacidad y para aquellas

finalidades que sean compatibles, para ello se deberán realizar tratamientos justificados.

- **PRINCIPIO DE LEALTAD**

Artículo 16, 19 de la LGPDPPSO

No se deberán obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Los datos personales que nos sean proporcionados serán tratados conforme a lo acordado y lo señalado por la normatividad y el aviso de privacidad.

- **PRINCIPIO DE CONSENTIMIENTO**

Artículos 7, 16, 20 al 22 de la LGPDPPSO.

Se deberá recabar el consentimiento del titular para el tratamiento de sus datos personales, salvo en los casos de excepción previstos en el artículo 22 de la LGPDPPSO, según resulte.

Este principio permite a los titulares de datos personales decidir de manera libre y especifica si quieren compartir su información con otras personas.

En caso de que se requiera el consentimiento del titular para el tratamiento de sus datos personales deberá ser redactada en lenguaje claro y sencillo. El titular podrá manifestar su consentimiento de manera expresa o tácita. Por regla general el consentimiento será tácito, salvo excepciones de ley.

El consentimiento se entenderá como tácito cuando habiéndose puesto a disposición el aviso de privacidad, el titular no manifieste su voluntad en sentido contrario.

El consentimiento será expreso cuando la voluntad del titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o cualquier tecnología. Para su obtención, se deberá facilitar un medio a través del cual se le permita acreditar de manera indubitable que otorgó su consentimiento a través de una declaración o una acción afirmativa clara.

En los casos en que se manifieste la negativa del tratamiento de los datos, se deberá documentar dicho pronunciamiento.

❖ **PRINCIPIO DE CALIDAD**
Artículos 16, 23 y 24 de la LGPDPPSO.

Se entenderá que los datos personales son:

- *Exactos y correctos,* cuando no presentan errores que pudieran afectar su veracidad.
- *Completos*: Cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento.
- *Actualizados*: Cuando los datos personales responden a la situación del titular.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular hasta que éste no manifieste y acredite lo contrario. Se tendrán que adoptar los mecanismos para procurar que cuenten con las características, a fin de que no se altere la veracidad de la información.

Cuando los datos personales dejen de ser necesarios deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de estos, por tanto, se tendrán que conservar los datos personales, hasta en tanto la finalidad para la cual se recabaron, haya sido satisfecha y por el tiempo establecido en las disposiciones legales aplicables.

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.

Se tendrá que documentar el proceso de supresión, bloqueo y, en su caso, eliminación.

❖ **PRINCIPIO DE PROPORCIONALIDAD**
Artículo 16, 25 de la LGPDPPSO.

Solo se tratarán los datos personales necesarios, adecuados y relevantes, emitiéndose por estos como los apropiados, indispensables y no excesivos para el

cumplimiento de las finalidades que motivaron su obtención para la finalidad concreta, explícita lícita y legítima que justifica su tratamiento, de acuerdo con las atribuciones aplicables.

En dicho sentido se deberá limitar el número de datos personales recabados, procurando sean los mínimos indispensables solo con la finalidad para las que se hayan obtenido y que se encuentren previstas en el aviso.

- **PRINCIPIO DE INFORMACIÓN**

Artículos16, 26 al 28 de la LGPDPPSO.

Se tendrán que comunicar al titular de los datos personales las características principales del tratamiento de su información, así como los medios para ejercer sus derechos, lo que se materializa a través del Aviso de Privacidad.

Es responsabilidad de los servidores públicos responsables el elaborar y poner a disposición de los titulares el aviso de privacidad, previo a la obtención de los datos personales, o en el momento que se considere oportuno.

El aviso contendrá los elementos que establecen los *artículos 27 y 28 de la LGPDPPSO*. Debiendo realizarse en una redacción sencilla, con la información necesaria, con un lenguaje claro y comprensible, y con una estructura y diseño de fácil entendimiento; asimismo en caso de realizar transferencias de datos personales, se deberá hacer de conocimiento de manera expresa a los titulares.

VIII. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES.

Con la finalidad de dar atención a las obligaciones establecidas en el artículo 33, fracción III de la LGPDPPSO, el cual señala la obligación de establecer las medidas de seguridad para la protección de datos personales, el Consejo Nacional para Prevenir la Discriminación elaborará un inventario de datos personales y de los sistemas de tratamiento, mismo que da atención al artículo 35 de la Ley anteriormente señalada.

Por lo anterior, se solicitará a las Unidades Administrativas proporcionen información sobre los sistemas electrónicos, bases de datos, programas, así como soportes físicos que se encuentran en funcionamiento dentro del Conapred, donde

se efectué el tratamiento de datos personales, permitiendo con ello que la Unidad de Transparencia dé seguimiento a las actividades de actualización del Documento de Seguridad y conformación del inventario que señala el artículo 33 de la Ley que nos rige en la materia.

Al respecto, la información requerida se presentará por las Áreas adscritas a cada una de las Direcciones, Coordinaciones o Subdirecciones, en caso de que exista más de un tratamiento en cada Unidad Administrativa.

El inventario de los sistemas se integrará de la siguiente manera:

1. Medios de Obtención: Formatos en los que se recaban y almacenan los datos personales.
2. Tipos de Datos.
3. Finalidades del tratamiento
4. Formato y ubicación de los datos.
5. Servidores públicos con acceso a los datos (Lista de servidores públicos que tienen acceso a los sistemas).
6. Encargado (en caso de Transferencia de datos, nombre completo del encargado y el instrumento jurídico que formaliza la presentación de los servicios que brinda al responsable.)
7. Transferencias de Datos
8. Difusión de Datos
9. Procedimiento de bloqueo, supresión y cancelación de los Datos**.**

IX. MEDIDAS DE SEGURIDAD

Las Unidades Administrativas del Conapred, deberán implementar las medidas de seguridad necesarias para garantizar la protección de los datos personales en su posesión.

Para tal fin, las medidas de seguridad se entenderán como el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales, las cuales se abordan en tres modalidades.

- **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.

- **Medidas de seguridad administrativas:** se traducen en 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 técnicas**: son 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 el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
  c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
  d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

X. PROGRAMA GENERAL DE CAPACITACIÓN

Entre las atribuciones del Comité de Transparencia tal como lo estipula el artículo 44 de la LGTAIP, en especial la fracción V, se encuentra la de promover la capacitación y actualización de las personas servidoras públicas continua en la materia.

Derivado de lo anterior, cada ejercicio se elabora un *Programa de Capacitación* con el propósito de brindar a los servidores públicos de este Consejo Nacional, los conocimientos básicos en materia de transparencia, acceso a la información, protección de datos personales y archivo, al ser temas interrelacionados con las funciones que llevan a cabo en su actuar cotidiano, los cursos se llevarán a cabo en la modalidad ***Presencial a Distancia*****,** mediante el Sistema para la Administración de la Capacitación Presencial (SACP) del INAI, a través de la convocatoria que haga de conocimiento la Unidad de Transparencia.

XI. DOCUMENTO DE SEGURIDAD

A fin de garantizar el cumplimiento de los principios de protección de datos personales, así como garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales y verificar que los datos de los titulares sean tratados conforme a los principios de licitud, finalidad, legalidad, consentimiento, calidad, proporcionalidad, información y responsabilidad que enmarca la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), este Consejo Nacional, de conformidad a lo establecido en el artículo 35 de la Ley General en la materia, realizará el Documento de Seguridad mediante el cual se analizarán las medidas de seguridad que se han implementado a cada una de las bases de datos en posesión del Conapred.

Dicho documento tendrá por objeto establecer de manera general las medidas de seguridad técnicas, físicas y administrativas que habrán de adoptarse para garantizar el cumplimiento de los principios en la materia.

De la misma manera, contemplará los siguientes:

I. El inventario de datos personales y de los sistemas de tratamiento;

II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

Debe tenerse en consideración que la actualización del Documento procederá de conformidad con el artículo 36 de la LGPDPPSO, cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Los trabajos de conformación de la información y seguimiento se llevarán a cabo por la Unidad de Transparencia, con apoyo de las Unidades Administrativas Responsables, quienes facilitarán la información, medios, recursos y lo necesario para la integración, seguimiento y evaluación de las actividades a su cargo.

La Unidad de Transparencia generará las acciones u observaciones correspondientes a cada Unidad, con la finalidad de que las deficiencias detectadas sean atendidas, corregidas o bien, derivado del análisis realizado, se propongan acciones de mejora.

Las actividades relacionadas con el Documento de Seguridad se informarán oportunamente al Comité de Transparencia.

XII. VULNERACIONES O AMENAZAS

Las vulneraciones de seguridad que pudieran presentarse a partir de una amenaza o debilidad de alguno de los soportes electrónicos o físicos en los que se encuentran almacenados los datos personales recabados por este Consejo Nacional, se consideran como aquellas que de no ser solventadas de forma inmediata y correcta, son factibles de convertirse en un riesgo, incidente de seguridad o bien, ser la causa del establecimiento de medidas de apremio o sanciones por incumplimiento de las obligaciones estipuladas en la LGPDPPSO (Articulo 163, fracción VII y IX).
A través del presente se enuncian los parámetros necesarios que se deberán seguir en caso de materializarse alguna vulneración, en los sistemas que contienen datos personales.

Para los efectos mencionados, las vulneraciones de seguridad se deberán entender en los siguientes términos:

1. Afecten los sistemas relacionados con los datos personales en cualquier fase de su tratamiento, e
2. Impacten de manera característica los derechos patrimoniales o morales de los titulares de los datos personales.
3. La pérdida o eliminación no autorizada. Se refiere a la pérdida definitiva o irremediable de un activo o parte de este.
4. El robo, extravío o copia no autorizada. Se refiere a la desaparición de un activo, o bien al copiado parcial o total de la información.
5. El uso o acceso no autorizado. Se refiere a la intrusión a un sistema de tratamiento, en formato físico o electrónico.
6. El daño, la alteración o modificación no autorizada. Se refiere a la afectación parcial, o cambio en la naturaleza, las condiciones, o las características de un activo.

PROCEDIMIENTO EN CASO DE VULNERACIONES

1. **Notificación al interior del Conapred.**

En caso de existir alguna vulneración y/o amenaza, de la cual tenga conocimiento la Subdirección de Informática, ésta tiene la obligación de comunicarlo por escrito

al área responsable del tratamiento de los datos personales y al Comité de Transparencia de este Consejo, el mismo día hábil de haber tenido conocimiento, con la finalidad de que el área responsable dé cumplimiento a los artículos 39 y 40 de la LGPDPPSO, los cuales estipulan los deberes que se tienen con el titular de los datos personales vulnerados o amenazados.

En caso de que la Subdirección de Informática no notifique el informe de vulneraciones o amenazas al área responsable y al Comité de Transparencia, en el plazo estipulado anteriormente, se dará vista al superior jerárquico. En ese sentido, en un término de un día hábil, el superior jerárquico deberá remitir el soporte informando la amenaza o vulneración existente, a fin de que el Comité de Transparencia vote la procedencia de dar vista al Órgano Interno de Control.

Ahora bien, si es que el área responsable del tratamiento es la primera instancia en detectar la vulneración o amenaza al sistema, deberá de consultar con la Subdirección de Informática la gravedad de la afectación, esto con el objetivo de que, a más tardar al día siguiente, se comience con el proceso para llevar a cabo la protección de datos y notificación a los titulares de los datos personales, de ser necesario.

2. Notificación a los titulares de los datos personales.

Cuando se materialice una vulneración, y las áreas involucradas hayan notificado el hecho al Comité de Transparencia, el área responsable deberá de dar aviso por medio de oficio, correo electrónico u algún otro medio acreditado con el titular de los datos personales afectados, respecto de las vulneraciones sufridas, de conformidad con el artículo 41 de la LGPDPPSO, haciendo de su conocimiento, lo siguiente:

I. La naturaleza del incidente o vulneración ocurrida,
II. Los datos personales comprometidos,
III. Las recomendaciones dirigidas al titular sobre las medidas que este pueda adoptar para proteger su interés,
IV. Las acciones correctivas realizadas de forma inmediata,
V. Los medios puestos a disposición del titular para que puedan obtener más información al respecto,

VI. La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular de los datos personales a entender el impacto del incidente, y
VII. Cualquier otra información y documentación que se considere conveniente para la adaptación de los datos personales.

1. Notificación al Órgano Garante.

La notificación de las vulneraciones sufridas se informará al órgano garante por el área responsable y deberá ser por escrito, mencionando el domicilio del Instituto o domicilio del lugar donde se ubique la base donde se haya sufrido la vulneración, dicha notificación tendrá que hacerse de conocimiento del Comité y la Unidad de Transparencia y deberá de contener la siguiente información:

a. La hora y fecha de la identificación de la vulneración,
b. La hora y fecha del inicio de la investigación de la vulneración,
c. La naturaleza del incidente o vulneración ocurrida,
d. La descripción detallada de la circunstancia (s) en relación con la vulneración y/o amenaza ocurrida,
e. Los números aproximados de los titulares de los datos personales afectados,
f. El nombre del sistema y el tipo de datos personales afectados,
g. Las acciones ya implementadas inmediatamente,
h. La descripción de las posibles consecuencias de vulneración de seguridad ocurridas,
i. Las recomendaciones que ya anteriormente se pusieron a disposición del titular de los datos personales,
j. El nombre y contacto del responsable, con el objetivo de que en caso de dudas o comentario el órgano garante pueda ponerse en contacto y
k. Cualquier otra información y/o documentación que considere conveniente de hacer conocimiento al órgano garante.

2. Bitácora de vulneraciones.

Las áreas responsables de los tratamientos deberán elaborar una bitácora de las vulneraciones que lleguen a sufrir, la cual tendrá que contener:

1. Descripción de la vulneración sufrida, datos afectados y número estimado de titulares en riesgo,
2. Fecha en que ocurrió,
3. Motivo que la generó,
4. Acciones implementadas para su solución y respuesta, documentando las gestiones realizadas.

La Unidad de Transparencia analizará el impacto de la amenaza y acompañará a las Unidades Administrativas, a fin de realizar los procesos óptimos ante los titulares y el Órgano Garante.

XIII. ACCIONES DE MEJORA

Las acciones de mejora se verán encaminadas a la generación, seguimiento o actualización de los documentos, procesos o actividades que coadyuven al perfeccionamiento de los mecanismos implementados en la institución para la procuración en la protección de los datos personales y el cumplimiento de las normas que rigen en la materia.

La Unidad de Transparencia podrá verificar el cumplimiento de las disposiciones aplicables y medidas de seguridad implementadas con la finalidad de reportar al Comité de Transparencia los resultados, y en su caso, observaciones detectadas, en el cumplimiento de cada Unidad Administrativa, durante cada ejercicio; lo anterior, con la finalidad de corroborar la eficacia de las medidas adoptadas en la protección de datos personales a su cargo y el desarrollo de las actividades y obligaciones presentadas mediante el presente programa, así como las vulneraciones que se hayan llegado a suscitar, y en su caso, emitir recomendaciones para posibles mejoras.

Las acciones determinadas en el marco de este contexto podrán ser preventivas, a fin de subsanar los errores y omisiones detectadas. También se podrán emitir acciones correctivas, cuando se detecte la falta total o incumplimiento de las obligaciones en la materia, las normas aplicables, o las disposiciones internas que tengan como finalidad el garantizar la protección a los datos personales.

XIV. POLÍTICAS GENERALES DE SEGURIDAD.

Con la finalidad de mejorar las medidas de seguridad aplicadas en el tratamiento de los datos personales, se deberá procurar que las áreas responsables del Conapred observen lo siguiente:

Como medidas físicas:

- Protección de los expedientes que contengan datos personales, su entorno y los recursos involucrados en su tratamiento, homologando los métodos de resguardo en cada una de las instalaciones de las Oficinas de las Unidades Administrativas donde se concentren, los cuales pueden comprender, entre otras puertas con control de acceso, letreros de acceso restringido, control de acceso a través de personal autorizado, dispositivos biométricos, tarjetas inteligentes, personal de seguridad.
- Para el respaldo de documentos en formato físico, se debe considerar la digitalización de estos.
- Se deben establecer políticas de seguridad para el traslado de soportes físicos y electrónicos que contengan datos personales, una vez que salgan de las instalaciones de resguardo, garantizando la seguridad de la información.

Como medidas administrativas:

- Contar con capacitación específica sobre la LGPDPPSO, a fin de que los servidores públicos designados, conozcan los principios rectores en el tratamiento de datos personales, así como establecer un plan de capacitación y capacitación relacionada con cada sistema en el que tengan injerencia.
- Permitir el acceso a los sistemas solo mediante usuario y contraseña.
- Instruir a cada usuario en la responsabilidad de guardar su contraseña o mecanismos correspondientes para el acceso a los sistemas en que se encuentre habilitado, por lo que se tendrá que implementar la firma de instrumentos que los obliguen a mantener sus contraseñas en confidencialidad.
- Elaborar guías o recomendaciones para la creación y mantenimiento de contraseñas seguras.

- Revisar semestralmente los controles de seguridad implementados, a fin de corroborar su correcto funcionamiento, así como las posibles amenazas y vulnerabilidades relacionadas.
- Para la autorización de usuarios, habilitar a solo una persona con los permisos para modificaciones a los datos en los registros de los sistemas.
- Contar con responsables del resguardo y clasificación archivística de los soportes físicos.
- Exhibir en un lugar visible el aviso de privacidad, en particular, en el caso de los tratamientos en los que se recaben los datos personalmente del titular, es decir, con la presencia física de este ante el Conapred.
- Verificar que los contratos de servicios celebrados con prestadores de servicios externos y que tengan injerencia en el trato de los datos personales, contengan una cláusula de confidencialidad, con la finalidad de salvaguardar la información tratada.

Como medidas técnicas:

- Establecer políticas de equipos sin atender.
- Realizar respaldos proporcionales al manejo de datos personales del Conapred. Llevar un control sobre la periodicidad de generación de respaldos y el almacenaje de los soportes físicos o electrónicos, así como identificar el proceso a realizar en caso de que sea necesario restaurar un respaldo electrónico, probando los respaldos periódicamente para asegurar su correcto funcionamiento.
- Verificar que los sistemas que soportan el tratamiento de datos personales cuentan con configuraciones seguras en el hardware, sistema operativo, base de datos y aplicaciones, debiendo tener identificadas las necesidades de nuevos sistemas, actualizaciones o nuevas versiones. Es recomendable realizar pruebas antes de implementar cualquiera de ellos.
- Implementar políticas y procedimientos para el uso de soportes informáticos extraíbles como memorias USB, discos, cintas magnéticas, a fin de evitar la reproducción de datos personales.
- Contar con un plan de incidentes por cada tratamiento electrónico y realizar procedimientos relacionados al monitoreo, reporte, mitigación y documentación de un incidente de seguridad, tal que se pueda verificar la ocurrencia de una vulneración para darle un adecuado seguimiento e implementar las medidas de seguridad correctivas.

Las políticas descritas, se identifican como aplicables a la mayoría de los tratamientos de datos personales a cargo del Conapred, por lo cual, su desarrollo deberá ser coordinado por la Unidad de Transparencia con la finalidad de que sean implementadas en los tratamientos bajo responsabilidad de cada área; no obstante, se podrá solicitar el apoyo para resolver cuestionamientos técnicos y operativos de los sistemas administrados, a cada una de las Unidades Administrativas.

XV. ATENCIÓN A SOLICITUDES DE ACCESO A LA INFORMACIÓN, EJERCICIO DE DERECHOS ARCO.

Los derechos arco son, los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, por lo que todas las Unidades Administrativas se encuentran obligadas a la búsqueda de la información que obre en sus archivos, una vez que sean requeridos a través de una solicitud de ejercicio de los derechos ARCO.

¿Qué es una solicitud de acceso a la información?

Es un escrito que las personas particulares presentan ante la Plataforma Nacional de Transparencia o las Unidades de Transparencia de los Sujetos Obligados, a través del cual pueden requerir el acceso a información pública o ejercer el derecho de Acceso, Rectificación, Cancelación u Oposición y Portabilidad de los datos personales que se encuentren en posesión de los sujetos obligados dentro de los documentos que se generen, obtengan, adquieran, transformen o conserven en nuestros archivos.

¿Cómo atender correctamente una solicitud de acceso a datos personales?

Los enlaces serán el único canal de comunicación entre las Unidades Administrativas y la Unidad de Transparencia.

- Primero, la Unidad de Transparencia deberá hacer la revisión diaria en la Plataforma Nacional de Transparencia (PNT), a fin de detectar las solicitudes de ejercicio de derechos ARCO ingresadas, que puedan ser de su competencia.

- Una vez teniendo la petición correspondiente, la Unidad de Transparencia deberá analizar la descripción de esta y verificar si es competencia de las Unidades Administrativas que conforman al sujeto obligado, así como los detalles proporcionados para atender la solicitud de información.
- Si se detecta que existen datos incompletos o erróneos, los enlaces deberán formular un requerimiento de información adicional (RIA) al solicitante, debiendo informar a la Unidad de Transparencia en un término no mayor a 3 días hábiles. Una vez transcurrido el tiempo, no se podrá enviar ampliación alguna, por tanto, se tendrá que emitir respuesta por el área tal y como lo haya requerido el solicitante.
- Si se considera que la información solicitada tiene que ser clasificada como reservada o confidencial, se deberá remitir al Comité de Transparencia la solicitud mediante oficio firmado por el titular de la Unidad Administrativa, mediante el cual funde y motive la clasificación, señalando los motivos por los cuales se llegó a esa conclusión en particular. Así mismo, es importante mencionar que,—para la clasificación de información confidencial o reservada, se tendrá que aplicar una prueba de daño.

REQUISITOS PARA LA PRESENTACIÓN DE UNA SOLICITUD DE EJERCICIO DE DERECHOS ARCO.

Información general.

Toda solicitud de ejercicio de derechos ARCO deberá contener la siguiente información:

- Nombre de la persona titular de los datos personales.
- Documentos que acrediten la identidad de la persona titular.
- En su caso, nombre del representante de la persona titular y documentos para acreditar su identidad y personalidad.
- Domicilio, o cualquier medio para recibir notificaciones.
- Descripción clara y precisa de los datos personales que se requieran tener acceso, rectificar, cancelar u oponerse a su tratamiento.
- Descripción del derecho que se quiere ejercer, o de lo que solicita la persona titular.
- En su caso, documentos o información que faciliten la localización de los datos personales, entre ella, el área responsable del tratamiento.

Información específica.

Además de la información general antes señalada, dependiendo del derecho que desee ejercer, deberá incluir la siguiente información en la solicitud:

- Derecho de **ACCESO**: Es la facultad de solicitar el acceso a los datos personales que se encuentran en las bases de datos, sistemas, archivos, registros o expedientes del Conapred, que los almacena o utiliza, así como conocer la información relacionada con las condiciones y generalidades del tratamiento que se da, con fundamento en los artículos 44 de la Ley General y 92 de los Lineamientos Generales.
- Derecho de **RECTIFICACIÓN**: La corrección de los datos personales en su posesión, cuando éstos sean inexactos o incompletos o no se encuentren actualizados, con fundamento en los artículos 45 de la Ley General y 93 de los Lineamientos Generales.
- Derecho de **CANCELACIÓN**: Es la facultad de solicitar que los datos personales sean suprimidos o eliminados de los archivos, registros, expedientes, sistemas, bases de datos del sujeto obligado y dejen de ser tratados por esta última. Lo anterior, con fundamento en los artículos 46 de la Ley General y 94 de los Lineamientos Generales.

  De ser procedente la cancelación, los datos deberán ser bloqueados y, posteriormente, suprimidos de los archivos, registros, expedientes, sistemas o bases de datos en que se encuentren.

  Sin embargo, no en todos los casos se podrán eliminar los datos personales, principalmente cuando sean necesarios para el cumplimiento a las atribuciones del Conapred, y de obligaciones legales.

  Derecho de **OPOSICIÓN**: Es la facultad de solicitar al Conapred que se abstenga de utilizar información personal para ciertos fines, por ejemplo, la publicación de datos personales en alguna fuente de acceso público, o de requerir que se concluya el uso de estos a fin de evitar un daño o afectación a su persona, con fundamento en los artículos 47 de la Ley General y 95 de los Lineamientos Generales.

  Al igual que para la cancelación de datos, no siempre se podrá impedir el tratamiento de los datos personales, debido a que pueden ser necesarios para el cumplimiento a las atribuciones del Conapred, y de obligaciones legales.

El ejercicio de los derechos ARCO no será procedente cuando:

- La persona titular de los datos personales, o su representante, no hayan acreditado su identidad.
- Los datos personales no se encuentren en posesión del Conapred.
- Exista un ordenamiento legal que impida su ejercicio.
- Lesione o afecte los derechos de otra persona.
- Pudiera obstaculizar procesos judiciales o funciones de una autoridad administrativa.
- Exista una resolución de autoridad competente que impida el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de estos.
- La cancelación u oposición de datos personales haya sido previamente realizada.
- El Conapred no sea competente para atender la solicitud.
- Los datos personales sean necesarios para proteger intereses jurídicamente tutelados de la persona titular.
- Los datos personales sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por la persona titular.
- El tratamiento de los datos personales sea por cuestiones de seguridad nacional; orden, seguridad y salud públicos.

En estos casos, el Conapred deberá responder por escrito la solicitud e informar las causas de la improcedencia, además de que dicha improcedencia deberá ser confirmada por su Comité de Transparencia.

De la solicitud del ejercicio de los Derechos ARCO

La solicitud se presenta por medio de escrito libre, verbalmente, medios electrónicos, o cualquier otro que establezca el Organismo Garante competente para tal fin, a través de los siguientes mecanismos:

- **Personalmente:**
  En la Unidad de Transparencia en el Conapred, ubicada en:
  Calle Londres, número 247, Colonia Juárez, Alcaldía Cuauhtémoc, Código Postal 06600, Planta Baja, en un horario de lunes a jueves de 09:00 a 17:30 horas y viernes de 09:00 a 15:00 horas.

- **Medios electrónicos:**
  A través de la Plataforma Nacional de Transparencia (PNT), en la siguiente dirección electrónica:
  https://www.plataformadetransparencia.org.mx/Inicio, en dónde señale como sujeto obligado al Consejo Nacional para Prevenir la Discriminación; o
  Enviando correo electrónico a la cuenta siguiente:
  unidaddetransparencia@conapred.org.mx

Acreditar la identidad de la persona titular o de su representante, así como la personalidad de esta última.

La solicitud se deberá acompañar de copia simple de una identificación oficial de la persona titular de los datos personales, así como de su representante, en caso de que éste sea quien presente la solicitud.

Entre las identificaciones oficiales válidas (vigentes), se encuentran:

- Credencial para votar
- Pasaporte
- Cartilla militar
- Cédula profesional con fotografía
- Licencia para conducir
- Documento migratorio.

La identidad de las personas menores de edad se podrá acreditar mediante:

- Acta de nacimiento,
- Clave Única de Registro de Población (CURP),

- Credenciales expedidas por instituciones educativas o instituciones de seguridad social,
- Pasaporte, o
- Cualquier otro documento oficial utilizado para tal fin.

La identidad de las personas en estado de interdicción, o incapacidad declarada por ley, se podrá acreditar mediante:

- Acta de nacimiento,
- CURP,
- Pasaporte o cualquier otro documento, o
- Identificación oficial expedida para tal fin.

La personalidad de la persona representante, en su caso, se podrá acreditar de la siguiente forma:

- Si la persona representante es **persona física**, se podrá elegir cualquiera de las siguientes tres opciones:

  1) Presentación de una carta poder simple suscrita ante dos testigos, anexando copia simple de sus identificaciones oficiales;
  2) Mediante instrumento público (documento suscrito por un Notario Público), o
  3) Acudiendo la persona y su representante a declarar en comparecencia ante la persona responsable.

- La personalidad de un representante de **persona moral**, sólo se podrá acreditar mediante instrumento público.

Es importante tener en cuenta que la identidad de la persona titular y su representante, así como la personalidad de este último, deberán quedar debidamente acreditadas previo al ejercicio del derecho de que se trate, en caso de que resulte procedente, mediante la presentación de los documentos originales antes señalados o copia certificada de los mismos, para su cotejo

Plazos y procedimiento para la atención de las solicitudes de ejercicio de derechos ARCO.

Una vez que se presentó la solicitud y que ésta cumplió con los requisitos antes descritos, el sujeto obligado ante el cual se presentó deberá realizar lo siguiente:

- En un plazo de **20 días hábiles**, contados a partir del día siguiente a la recepción de la solicitud, deberá informar a la persona solicitante si procede o no el ejercicio del derecho solicitado.
- Dicho plazo, podrá ser ampliado por una sola vez hasta por **10 días hábiles** cuando así lo justifique las circunstancias, siempre y cuando se le notifique a la persona titular dentro del plazo de respuesta inicial.
- En caso de resultar procedente el ejercicio de los derechos ARCO, la Unidad de Transparencia deberá hacerlo efectivo en un plazo que no podrá exceder de **15 días hábiles** contados a partir del día siguiente en que se haya notificado la respuesta a la persona titular de los datos personales.
- En caso de que el ejercicio de los derechos ARCO no sea procedente, se deberá informar al titular el motivo de la determinación, en el plazo de hasta **20 días hábiles** contados a partir del día siguiente a la recepción de la solicitud. En la respuesta se deberá explicar las causas de la improcedencia y acompañar la confirmación del Comité de Transparencia al respecto.
- En caso de que los datos personales objeto del ejercicio de los derechos ARCO, no sean de la competencia de este Consejo, se informará a la persona titular dentro de los **3 días hábiles** posteriores a la recepción de la solicitud y, en caso de poder determinarlo, se le señalarán el o los sujetos obligados competentes para atender su solicitud.
- Si hay un trámite específico para el ejercicio de los derechos ARCO, se deberá informar sobre su existencia en un plazo máximo de **3 días hábiles**, a partir del día siguiente de la solicitud, para que la persona solicitante decida si presentará su solicitud de acuerdo con el trámite o con base en el procedimiento aquí descrito.
- En caso de que la solicitud de ejercicio de derechos ARCO corresponde a un derecho diferente, se reconducirá la vía haciéndolo del conocimiento a la persona titular dentro de los **3 días hábiles** siguientes a la solicitud.

Modalidad de reproducción de los datos personales.

En los casos en que resulte procedente el ejercicio de los derechos ARCO, la información podrá ponerse a disposición de la persona titular de los datos personales, o en su caso, de su representante, previa acreditación de la identidad respectiva, en cualquiera de las modalidades siguientes:

- **Consulta directa.** - Se realizará ante la instancia correspondiente, sin costo.
- **Copia certificada**. - Las primeras 20 fojas serán gratuitas.
- **Copia simple**. - Las primeras 20 fojas serán gratuitas.
- **Disco compacto CD o DVD.-** Con costo
- **Documento electrónico. –** Las primeras 20 fojas serán gratuitas.
- **Dispositivo de almacenamiento. -** Sin costo, siempre y cuando éste sea proporcionado por la persona solicitante y la instancia competente cuente con los datos personales en formato electrónico.

RECURSOS DE REVISIÓN A SOLICITUDES DE DERECHO ARCO

El recurso de revisión se podrá presentar ante el Organismo Garante competente, a través de la PNT, dentro de los **15 días hábiles** siguientes a la fecha de la notificación de la respuesta, o del vencimiento del plazo para su notificación.

El recurso de revisión procederá en los siguientes supuestos:

- Se clasifiquen como confidenciales los datos personales.
- Se declare la inexistencia de los datos personales.
- El Conapred se declare incompetente para atender la solicitud.
- Se entreguen datos personales incompletos.
- Se entreguen datos personales que no correspondan con lo solicitado.
- Se niegue el acceso, rectificación, cancelación u oposición de datos personales.
- No se dé respuesta a la solicitud dentro de los plazos ya señalados.

- Se entreguen o pongan a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible.
- El titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales.
- Se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia, y
- No se dé trámite a una solicitud para el ejercicio de los derechos ARCO.

El escrito de interposición del recurso de revisión debe contener:

- La persona responsable ante quien se presentó la solicitud para el ejercicio de los derechos ARCO.
- El nombre de la persona titular, o de su representante y tercero interesado si lo hay.
- Domicilio o medio para recibir notificaciones.
- La fecha en que fue notificada la respuesta, o en caso de falta de respuesta, la fecha de la presentación de la solicitud para el ejercicio de los derechos ARCO.
- El acto o hecho respecto del cual surge la queja y lo que se solicita al respecto, así como las razones o motivos de inconformidad.
- En su caso, copia de la respuesta que se impugna o con la que no se está conforme y de la notificación correspondiente, y
- Los documentos que acrediten la identidad de la persona titular o la personalidad e identidad de su representante.

Por último, si la normatividad aplicable al tratamiento de datos personales en cuestión establece un trámite o procedimiento específico para el ejercicio de los derechos ARCO, el sujeto obligado deberá informar la existencia de dicho trámite o procedimiento en un plazo máximo de **3 días hábiles**, contados a partir del día siguiente de la presentación de la solicitud, a fin de que la persona titular de los datos decida si presentará su solicitud de acuerdo con el trámite específico o con base en el procedimiento aquí descrito.

Es importante mencionar que, es criterio constante de dicho Organismo Garante competente, que en materia de datos personales **cualquier información relacionada con los mismos constituye propiamente un dato personal** y, por lo tanto, este Consejo Nacional para Prevenir la Discriminación no podría afirmar

o negar la existencia, o incluso notificar al peticionario el detalle de la documentación que obra en nuestros archivos, de manera electrónica y/o por ningún medio de mensajería.

En este sentido, este sujeto obligado informará a la persona titular, que las consideraciones respecto al ejercicio de los derechos de acceso, rectificación, cancelación u oposición de datos personales, conocidos como derechos ARCO, **se harán de su conocimiento una vez que acuda éste o su representante legal** a las instalaciones del Conapred, el día de su elección, ubicadas en *Londres número 247, Colonia Juárez, Alcaldía Cuauhtémoc, Código Postal 06600, Planta Baja, en un horario de lunes a jueves de 09:00 a 17:30 horas y viernes de 09:00 a 15:00 horas*, debiendo acreditar su personalidad o la de su representante; toda vez que, **es el ÚNICO medio para llevar a cabo el cotejo de la copia de la identificación que sea presentada**, con el documento en versión original de la misma, siendo que para el caso que hoy nos ocupa no obra evidencia de que el particular haya acudido a las oficinas indicadas para acreditar su identidad y poder recibir el pronunciamiento de este Sujeto Obligado, con respecto a su solicitud inicial.

En el supuesto de no contar con la debida acreditación de la identidad en el momento de la presentación del ejercicio de derechos ARCO, y dicha acreditación sea un requisito necesario para su ejercicio, se podrá prevenir a la persona titular para subsanar la falta de dicho requisito, y en caso de persistir la ausencia de dicha acreditación, la solicitud pudiera tenerse como no presentada en términos del artículo 52 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 87 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Asimismo, a la falta de acreditación de identidad, en términos del artículo 55, fracción I de Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, se tendrá que actualizar también una causal de improcedencia de la solicitud en caso de que la documentación presentada no permita acreditar fehacientemente la identidad o la personalidad en representación, por lo que, de actualizarse se deberá informar lo conducente en términos de lo que dispone la normatividad.

Por lo anterior, y de conformidad con el artículo 91 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establece que la acreditación de la identidad de la persona titular y, en su caso, la identidad y personalidad del representante, se deberá llevar a cabo mediante la presentación de los documentos originales que correspondan, siempre y cuando la persona titular o su representante se presenten en la Unidad de Transparencia, ubicado en *Londres número 247, Colonia Juárez, Alcaldía Cuauhtémoc, Código Postal 06600, Planta Baja, en un horario de lunes a jueves de 09:00 a 17:30 horas y los viernes de 09:00 a 15:00 horas*, y esta situación se deje asentada en la constancia que acredite los derechos ARCO.

XVI. MEDIDAS DE APREMIO O SANCIONES POR INCUMPLIMIENTO DE LAS OBLIGACIONES.

Reiterando que para este Consejo Nacional para Prevenir la Discriminación es imperante garantizar la confidencialidad sobre la información que las Unidades Administrativas Responsables conozcan a través del desarrollo de sus funciones y actividades, así como el implementar las medidas de protección suficientes a fin de salvaguardarlos contra daños, pérdidas, alteraciones, destrucción, uso, divulgación, acceso o tratamiento no autorizado, las personas servidoras públicas deben tener presentes las obligaciones que los constriñen, dando aviso inmediato a sus superiores jerárquicos ante cualquier eventualidad que ponga en riesgo la confidencialidad, integridad y disponibilidad de los datos personales, o bien, al observar alguna vulneración a la seguridad de los mismos. Tales deberes deberán tenerse presentes aún y cuando haya finalizado su participación en el tratamiento de estos, o bien, hayan cambiado funciones o se termine la relación laboral con el Conapred.

Igualmente destaca que, en caso de omisión a lo anteriormente señalado, del incumplimiento a las obligaciones en materia de protección de datos personales y al cometer alguno de los siguientes supuestos, se estaría incurriendo en una posible falta administrativa susceptible de ser sancionada de conformidad con lo previsto en la fracción V del Artículo 49, de la Ley General de Responsabilidades Administrativas (LGRA):

- 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.
- Dar tratamiento intencional a los datos personales en contravención a los principios y deberes establecidos en la Ley General.
- Incumplir el deber de confidencialidad
- No establecer las medidas de seguridad
- Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad.
- Llevar a cabo la transferencia de datos personales, en contravención de lo previsto por la Ley General.

En ese sentido resulta necesario reiterar que es obligación de todas las personas servidoras públicas resguardar, mantener la confidencialidad y no hacer mal uso de los documentos, expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, contratos, convenios, boletines, archivos físicos y/o electrónicos de información recabada, estadísticas o bien, cualquier otro registro o información relacionada con las funciones que desempeñan en sus funciones, o de los cuales tienen conocimiento.

Al respecto, queda prohibido difundir, distribuir, comercializar, usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, sin causa legítima, la información que se encuentre bajo custodia de los servidores públicos o de la cual tienen conocimiento con motivo de su empleo, cargo o comisión conforme a las facultades correspondientes.

Por otra parte, el artículo 163 de la LGPDPPSO, señala de manera literal que serán motivo de sanción las conductas siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

II. Incumplir con 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 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 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 presente Ley, 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 42 de la presente Ley;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;

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 presente Ley;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;

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 presente Ley;

XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.

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

En este contexto todo el personal adscrito al Consejo Nacional para Prevenir la Discriminación, deberán dar continuidad a las acciones que coadyuven al cumplimiento de las obligaciones que constriñen a este Consejo, ya que, **en caso de advertir alguna conducta contraria a lo estipulado por la Ley, se dará vista inmediata** a la autoridad fiscalizadora o instancia equivalente, para que en el ámbito de sus atribuciones determine lo conducente.

Las responsabilidades que resulten de los procedimientos administrativos son independientes a las de cualquier otro tipo que se puedan derivar por los mismos hechos.