



CULTURA
SECRETARÍA DE CULTURA

INBAL

POLÍTICAS INTERNAS DE GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES DEL INSTITUTO NACIONAL DE BELLAS ARTES Y LITERATURA

Av. Juárez No. 101, Esq. Av. Paseo de la Reforma, Torre Prisma, 8° Piso, Col. Centro, Alcaldía de Cuauhtémoc,
C.P. 06040, Ciudad de México, Tel: 1000 4622 Ext. 1910, 1913 y 1354, correo electrónico:
unidadenlace@inba.gob.mx.





Contenido

I. Introducción	1
II. Cumplimiento de los principios, deberes y derechos	2
A) Principios en materia de protección de datos personales que deben cumplir los centros de trabajo del INBAL.....	2
I. Principio de Licitud;.....	2
II. Principio de Finalidad;.....	3
III. Principio de Lealtad;	3
IV. Principio de Consentimiento:.....	4
V. Principio de Calidad;	4
VI. Proporcionalidad;	5
VII. Principio de Información,.....	5
VIII. Principio de Responsabilidad.....	6
B) Deberes en materia de protección de datos personales que deben cumplir los centros de trabajo del INBAL.....	6
I. Deber de seguridad	6
II. Deber de confidencialidad	7
C) Derechos de los titulares que deben cumplir los centros de trabajo del INBAL	7
III. Los roles y responsabilidades de los involucrados con los tratamientos de datos personales	8
IV. Las sanciones en caso de incumplimiento;	8
VI. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad	11
VII. El proceso general de atención de los derechos ARCO.	12





I. Introducción

Con este documento se busca asegurar la aplicación de los principios y responsabilidades en la protección de datos personales dentro de los procesos internos de gestión y tratamiento de datos personales dentro del Instituto Nacional de Bellas Artes y Literatura (en adelante referido como “INBAL”) en concordancia con lo establecido en el artículo 30, fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados¹ (en adelante referida como “LGPDPPO”) y en los términos del artículo 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público² (en adelante referidos como “Lineamientos Generales”).

Esta política, es vinculante para las servidoras y los servidores públicos del INBAL que, en el ejercicio de sus funciones, manejen datos personales. Los responsables de cada centro de trabajo deben definir y documentar los roles y responsabilidades del personal a su cargo. Además, en colaboración con la Unidad de Transparencia del INBAL, deberán asegurar que todas las personas involucradas en el tratamiento de datos personales conozcan sus obligaciones, y las consecuencias de su incumplimiento. Para facilitar esto, deben designar a un enlace ante la Unidad de Transparencia del INBAL, quien supervisará la implementación y el cumplimiento de estas políticas con la ayuda de los centros de trabajo.

En resumen, estas políticas se centran en proteger los datos personales tratados por el Instituto y asegurar que se utilicen de manera adecuada. Cumplir con estas políticas garantizará la protección de la información contra cualquier daño, pérdida, alteración, destrucción o acceso no autorizado.

¹ **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:

(...)

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

(...)

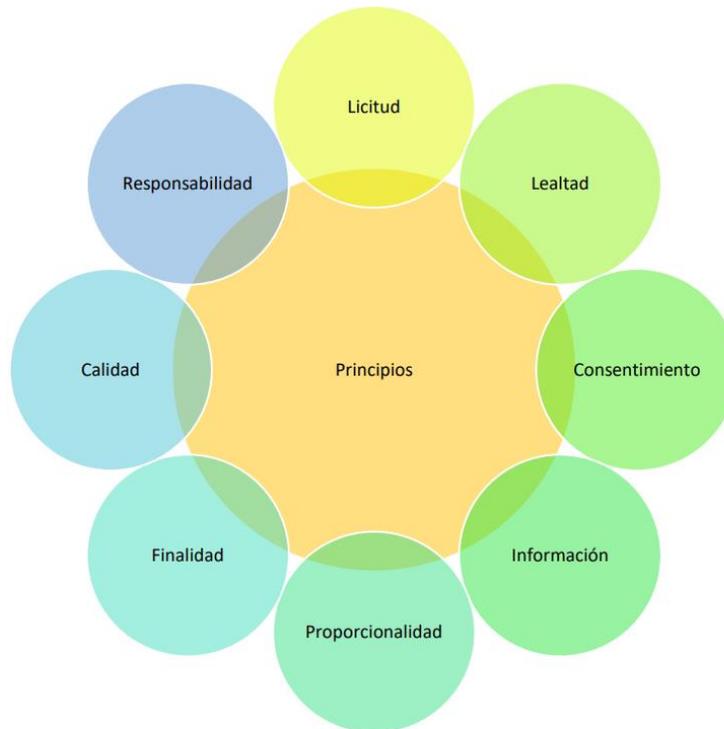
² **Artículo 56.** Con relación a lo previsto en el artículo 33, fracción I de la Ley General, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, al menos, lo siguiente:

- 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.

II. Cumplimiento de los principios, deberes y derechos

A) Principios en materia de protección de datos personales que deben cumplir los centros de trabajo del INBAL

De conformidad con lo previsto en la LGPDPPSO y los Lineamientos Generales, en todo tratamiento de datos personales el responsable deberá observar los siguientes principios rectores de la protección de datos personales:



2

3

I. Principio de Licitud;

El INBAL deberá tratar los datos personales que posea sujetándose a las atribuciones o facultades que la normatividad aplicable le confiera, así como con estricto apego y cumplimiento de lo dispuesto en la LGPDPPSO, los Lineamientos generales, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos de los titulares.

Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Revisar que los datos se traten conforme a la LGPDPPSO, los Lineamientos Generales y demás normativa aplicable.
- Conocer la normativa que en lo particular regule sus atribuciones, funciones y responsabilidades con relación al tratamiento de los datos personales que realice.

³ La imagen forma parte de las políticas internas para la gestión y tratamiento de datos personales del INAI.



- Cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.

II. Principio de Finalidad;

Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta. Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.

Las finalidades para el tratamiento de datos personales deberán ser:

- **Concretas:** cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados.
- **Explícitas:** cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
- **Lícitas:** cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.
- **Legítimas:** cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta.
- Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma clara.
- Identificar y distinguir en el aviso de privacidad entre las finalidades primarias⁴ y secundarias⁵.
- Ofrecer a la persona 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 finalidades secundarias.

III. Principio de Lealtad;

Refiere a la obligación de las personas servidoras públicas del INBAL de actuar de manera leal y transparente en el tratamiento de datos personales. Esto implica que deban ser honestos y claros con los titulares sobre cómo se utilizarán sus datos personales, evitando la obtención de los datos personales a través de medios engañosos o fraudulentos, se entenderá por medios engañosos o fraudulentos aquellos que el responsable utilice para tratar los datos personales con dolo, mala fe o negligencia.

⁴ **Finalidades Primarias:** propósitos principales y esenciales para los cuales se recopilan los datos personales. Estas finalidades están directamente relacionadas con el tratamiento.

⁵ **Finalidades Secundarias:** Estas finalidades suelen ser complementarias a las establecidas como finalidades primarias y no están directamente relacionadas con la razón principal por la que se recopilaron los datos.



Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Revisar los procedimientos y formatos utilizados para recabar datos personales, para verificar que en éstos no se utilicen prácticas que lleven a la obtención de los datos de manera dolosa, de mala fe o con negligencia.
- Dar vista a la oficina de representación en el INBAL antes Órgano Interno de Control en caso del uso de prácticas dolosas, de mala fe o negligentes para la obtención de los datos personales.
- Respetar en todo momento la expectativa razonable de privacidad de la persona titular de los datos personales.
- Tratar los datos conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la LGPDPSO y los Lineamientos generales.
- Verificar los tratamientos, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.
- Elaborar avisos de privacidad con todos los elementos informativos que establece la LGPDPSO, y con información que corresponda a la realidad del tratamiento que se efectúa.
- Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta, para que no haya lugar a confusión al respecto

IV. Principio de Consentimiento:

Previo al tratamiento de los datos personales, el responsable deberá obtener el consentimiento del titular, de manera libre, específica e informada, el cual deberá ir siempre relacionado a las finalidades del tratamiento que se informen en el aviso de privacidad.

Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.
- Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.
- Redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.
- Definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento y habilitar los mecanismos necesarios para solicitar el consentimiento.

V. Principio de Calidad;

El principio de calidad significa que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser:

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



Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, pertinentes, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que la persona titular se vea afectada por dicha situación.
- 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 de bloqueo.
- Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.
- Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación.

VI. Proporcionalidad;

Los centros de trabajo del INBAL que realicen tratamiento de datos personales deberán tratar solo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Deben evaluar cuidadosamente el propósito para el cual se recopilan y procesan los datos personales. Es fundamental que este propósito esté claramente definido y sea legítimo, es decir, que esté relacionado con las funciones y actividades encomendadas.
- Deben limitar la cantidad de datos personales recopilados a lo estrictamente necesario para cumplir con la finalidad establecida. Se debe evitar la recopilación de datos innecesarios o excesivos que no estén directamente relacionados con la finalidad del tratamiento.
- Una vez recopilados los datos necesarios, se debe minimizar su uso y tratamiento. Esto implica utilizar únicamente los datos que sean relevantes y necesarios para alcanzar la finalidad del tratamiento, evitando cualquier forma de procesamiento adicional que no esté justificada por la finalidad establecida.

VII. Principio de Información,

Establece que las personas tienen derecho a recibir información clara, completa y transparente sobre cómo se recopilan, utilizan, procesan y protegen sus datos personales. Este principio garantiza que los titulares puedan tomar decisiones informadas sobre el manejo de sus datos y ejercer sus derechos de privacidad de manera efectiva.

Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Poner a disposición de los titulares el aviso de privacidad en los términos dispuestos en la LGPDPPSO, y demás normativa aplicable
- Facilitar a los titulares el ejercicio de sus derechos de privacidad, como el derecho de acceso, rectificación, cancelación y oposición (derechos ARCO).

VIII. Principio de Responsabilidad.

Este principio establece la obligación de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la autoridad, que se cumple con las obligaciones en torno a la protección de los datos personales. Esto implica que se deban tomar medidas proactivas para asegurar que los datos personales sean tratados de manera adecuada y que se respeten los derechos de privacidad de los individuos.

Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Cumplir con el programa de capacitación y actualización aprobado por el Comité de Transparencia.
- Analizar los riesgos que implica todo tratamiento de datos personales.
- Designar enlaces para coordinar las actividades relacionadas con la protección de datos personales.
- Reportar y gestionar incidentes de seguridad de manera adecuada.

B) Deberes en materia de protección de datos personales que deben cumplir los centros de trabajo del INBAL

Los deberes de **seguridad** y **confidencialidad** deben observarse especialmente en cualquier etapa del ciclo de vida de los datos personales.

6

I. Deber de seguridad

Este deber refiere a la obligación de establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales en posesión del INBAL, con el objeto de impedir daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado de los datos personales.

Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Establecer y mantener medidas de seguridad administrativas⁶, físicas⁷ y técnicas⁸.
- Tomar en cuenta el riesgo inherente asociado con cada tipo de dato personal; las posibles consecuencias para las personas titulares en caso de una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico con el que cuenta la Institución.
- Notificar a las personas titulares las vulneraciones de seguridad que se presenten de manera oportuna, proporcionando la información con la que se cuente.
- Llevar a cabo las acciones correctivas que sean necesarias con el objetivo de mitigar cualquier impacto negativo.

⁶ Las medidas de seguridad **administrativas** corresponden a todas las acciones encaminadas a la protección de la información y que están relacionadas con la gente y los procesos.

⁷ Las medidas **físicas** incluyen todas las acciones que tienen que ver con el entorno físico de la información y de los elementos físicos asociados a la misma.

⁸ Las medidas de seguridad **técnicas** se apoyan en infraestructura tecnológica (hardware y software).



II. Deber de confidencialidad

Esta obligación indica que se deberán establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo, evitando causar un daño al titular de los datos.

Para cumplir con este principio, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Guardar confidencialidad en cualquier fase del tratamiento de los datos personales y limitar el acceso a la información solo a aquellos que necesiten acceder a ella para realizar sus funciones.
- Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste, para lo cual se deberá incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas de confidencialidad y para que quienes tengan acceso a los datos personales en posesión del responsable cumplan con esta obligación de confidencialidad.
- Capacitar al personal para que conozca sus obligaciones con relación al tratamiento de datos personales y la importancia de mantener la confidencialidad de la información.
- Establecer procedimientos para evitar fuga de información, el acceso indebido a los datos personales y para responder adecuadamente a cualquier violación de la confidencialidad de los datos.

C) Derechos de los titulares que deben cumplir los centros de trabajo del INBAL

En todo momento el titular de los datos personales o su representante podrán ejercer los derechos ARCO, solicitando el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen en términos de lo referido en la LGPDPSO en los artículos transcritos a continuación:

*“Artículo 44. El titular tendrá derecho de **acceder** a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.*

*Artículo 45. El titular tendrá derecho a solicitar al responsable la **rectificación** o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.*

*Artículo 46. El titular tendrá derecho a solicitar la **cancelación** de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.*

*Artículo 47. El titular podrá **oponerse** al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:*

I. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y

II. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.”





La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO que se formulen a este INBAL, se sujetarán al procedimiento establecido en el capítulo “Del ejercicio de los derechos de acceso, rectificación, cancelación y oposición” de los Lineamientos Generales y al Procedimiento para la atención de solicitudes para el ejercicio de los derechos ARCO del INBAL.

III. Los roles y responsabilidades de los involucrados con los tratamientos de datos personales

Las presentes políticas internas de protección de datos personales son de observancia obligatoria para todo aquel que intervenga en cualquier fase de tratamiento realizado dentro de las siguientes áreas del INBAL y los centros de trabajo que dependen de ellas:

1. Dirección General.
2. Subdirección General de Administración.
3. Subdirección General del Patrimonio Artístico Inmueble.
4. Subdirección General de Bellas Artes.
5. Subdirección General de Educación e Investigación Artísticas.
6. Dirección de Difusión y Relaciones Públicas.
7. Área Coordinadora de Archivos.

Las funciones y obligaciones de las personas que tratan datos personales en el INBAL se han identificado detalladamente en el Programa de Protección de Datos Personales de este INBAL y a través de los inventarios que se desarrollaron por cada uno de los tratamientos, en los cuales se identificó el personal que realiza el tratamiento, el centro de trabajo al que está adscrito y la finalidad de dicho tratamiento, mismos que forman parte integrante del documento de seguridad en sus anexos 1 y 2.

IV. Las sanciones en caso de incumplimiento;

Cuando el Comité de Transparencia del INBAL tenga conocimiento del incumplimiento de alguna obligación prevista en estas políticas, deberá realizar al centro de trabajo correspondiente un exhorto para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos futuros o situaciones de riesgo que los pudieran ocasionar.

De manera adicional, es importante que los servidores públicos que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones establecidas en dicha ley, 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 LGPDPPSO 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 LGPDPPSO;

Av. Juárez No. 101, Esq. Av. Paseo de la Reforma, Torre Prisma, 8° Piso, Col. Centro, Alcaldía de Cuauhtémoc, C.P. 06040, Ciudad de México, Tel: 1000 4622 Ext. 1910, 1913 y 1354, correo electrónico: unidadenlace@inba.gob.mx

- 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 LGPDPPSO, 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 LGPDPPSO;
- VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;
- 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 LGPDPPSO;
- X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;
- 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 LGPDPPSO;
- XIII. No acatar las resoluciones emitidas por el Instituto, y
- XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 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, serán consideradas como graves.

9

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

Si persiste la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento del Comité de Transparencia para que, a su vez, dé vista a la oficina de representación antes órgano interno de control, y, en su caso, dé inicio el procedimiento de responsabilidad administrativo respectivo.

V. Ciclo de vida de los datos personales

La identificación del ciclo de vida de los datos personales tiene como finalidad asegurar el cumplimiento de los principios y deberes en cada etapa.

El ciclo de vida de los datos personales se refiere a todas las etapas que atraviesan los datos personales desde el momento en que son recolectados hasta su eliminación definitiva. Este ciclo incluye varias etapas, en cada una se deberá asegurar que la información se maneje de manera segura, eficiente y conforme a la normativa de protección de datos. En términos del artículo 59 de los Lineamientos Generales, se deberá considerar el ciclo de vida de los datos personales conforme a lo siguiente:

- La obtención de los datos personales;

Av. Juárez No. 101, Esq. Av. Paseo de la Reforma, Torre Prisma, 8° Piso, Col. Centro, Alcaldía de Cuauhtémoc, C.P. 06040, Ciudad de México, Tel: 1000 4622 Ext. 1910, 1913 y 1354, correo electrónico: unidadenlace@inba.gob.mx

- El almacenamiento de los datos personales;
- El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
- La divulgación de los datos personales considerando las remisiones⁹ y transferencias¹⁰ que, en su caso, se efectúen;
- El bloqueo de los datos personales, en su caso, y
- La cancelación, supresión o destrucción de los datos personales.



Por lo anterior, los centros de trabajo del INBAL deberán ajustarse a las siguientes recomendaciones:

- Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen.
- Elaborar un inventario de datos personales relacionando el tipo de tratamiento con el ciclo de vida.
- Bloquear, cancelar, suprimir o destruir los datos personales, en los casos establecidos en la normatividad aplicable.

⁹ La comunicación o divulgación de datos personales entre un responsable y un encargado (la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable).

¹⁰ Toda comunicación de datos personales realizada a persona distinta del titular, del responsable o del encargado.

VI. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad

El artículo 33, fracción VII de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

En ese sentido, el artículo 35, fracción VI, de la Ley General establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad, por lo que forman parte del documento de seguridad del INBAL como anexo 5.

Mecanismo de monitoreo y supervisión: La Unidad de Transparencia será la encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, a través de los siguientes ejes:

I. Etapa de Monitoreo. La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración del respectivo reporte.

II. Etapa de Supervisión: La Unidad de Transparencia analizará los reportes de las áreas, verificando aquellos puntos en los que se hubiera reportado “No” como respuesta y se emitirá un dictamen o ficha técnica en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

Mecanismos de actuación ante vulneraciones a la seguridad de los datos personales: El artículo 33, fracción VII, de la Ley General, dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

En ese sentido, el artículo 63, fracción VII, de los Lineamientos Generales, entre otras disposiciones estipula que, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, se deberán monitorear las vulneraciones de seguridad ocurridas.

Por ello, la Unidad de Transparencia deberá monitorear y revisar de manera periódica las medidas de seguridad, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual se podrá auxiliar de la Dirección de Servicios Informáticos y/o cualquier centro de trabajo del INBAL.

En el documento “Guía para registrar y reportar vulneraciones de datos personales” se concentran las actividades que deben realizarse cuando se materialice una vulneración de seguridad en cualquier fase del tratamiento de datos personales.

Mecanismos de auditoría en materia de datos personales: Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 30, fracción V, de la LGPDPPSO, establece que se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías.

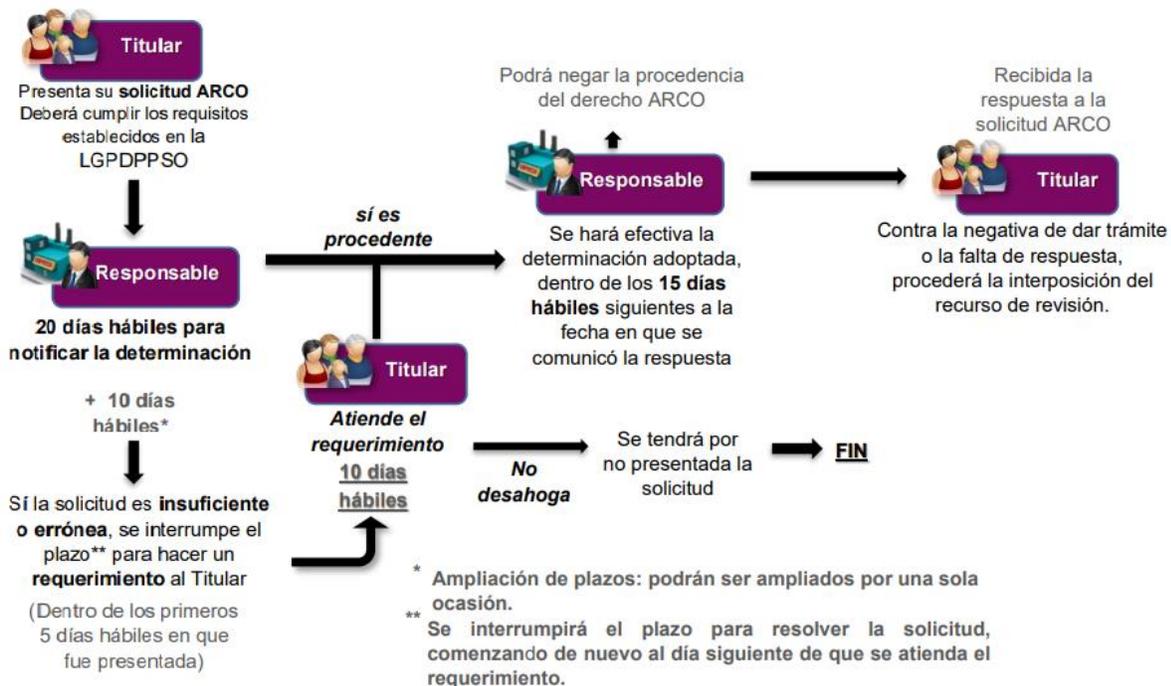
El artículo 63 de los Lineamientos Generales, dispone que además del monitoreo y supervisión periódica de las medidas de seguridad, se deberá contar con un programa de auditoría para revisar la eficacia y eficiencia del sistema de gestión.

Por tanto, resulta necesario establecer un mecanismo que permita dar cumplimiento a las disposiciones antes citadas, mismo que se desarrolla de la siguiente manera:

Las auditorías en materia de datos personales tendrán como finalidad verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la LGPDPPSO y los Lineamientos Generales.

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

La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO que se formulen a este INBAL, se sujetarán al procedimiento establecido en el capítulo “Del ejercicio de los derechos de acceso, rectificación, cancelación y oposición” de los Lineamientos Generales y al Procedimiento para la atención de solicitudes para el ejercicio de los derechos ARCO del INBAL.



El Titular de los Datos Personales Podrá presentar su solicitud para ejercer los derechos ARCO través de los siguientes medios:

- A través de la Plataforma Nacional de Transparencia, disponible en la siguiente liga: <http://www.plataformadetransparencia.org.mx/>

¹¹ El diagrama forma parte de las políticas internas para la gestión y tratamiento de datos personales del INAI.



- En las instalaciones de la Unidad de Transparencia del INBAL ubicadas en Av. Juárez, Número 101, esquina Av. Paseo de la Reforma, piso 8, Torre Prisma, Col. Centro, alcaldía Cuauhtémoc, C.P. 06040, Ciudad de México.
- A través del correo electrónico del INBAL: unidadenlace@inba.gob.mx

APROBACIÓN

El presente documento fue aprobado por el Comité de Transparencia en la Décima Sexta Sesión Extraordinaria 2024, de fecha veintitrés de mayo de dos mil veinticuatro mediante acuerdo AR04-16SECT-2024, de conformidad con lo dispuesto en los artículos 83 y 84 de la LGPDPPSO

