CULTURA
SECRETARÍA DE CULTURA

POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES

Secretaría de Cultura

OBJETIVO GENERAL

Implementar los principios y deberes en materia de protección de datos personales en los procesos internos de gestión y tratamiento de datos personales la Secretaría de Cultura, conforme a lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos de Protección de Datos Personales para el Sector Público.

ÁMBITO DE APLICACIÓN

El presente documento es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas de la Secretaría que conforme a sus atribuciones realicen tratamiento de datos personales.

DISPOSICIONES GENERALES

1. Se debe realizar el tratamiento de datos personales con base en las atribuciones conferidas a cada una de las áreas de la Secretaría dentro del marco legal en la materia y del consentimiento de la persona titular.

2. Previo a recabar datos personales, se debe mostrar el aviso de privacidad integral y/o simplificado, según sea el caso; el aviso de privacidad debe encontrarse en un lugar visible.

3. Al momento de recabar datos personales, se deberá hacer del conocimiento de la persona titular la finalidad con la cual se reciben.

4. Las áreas solo deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de atribuciones y funciones.

5. Se deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que se reciban en ejercicio de las atribuciones otorgadas a las unidades administrativas de la Secretaría.

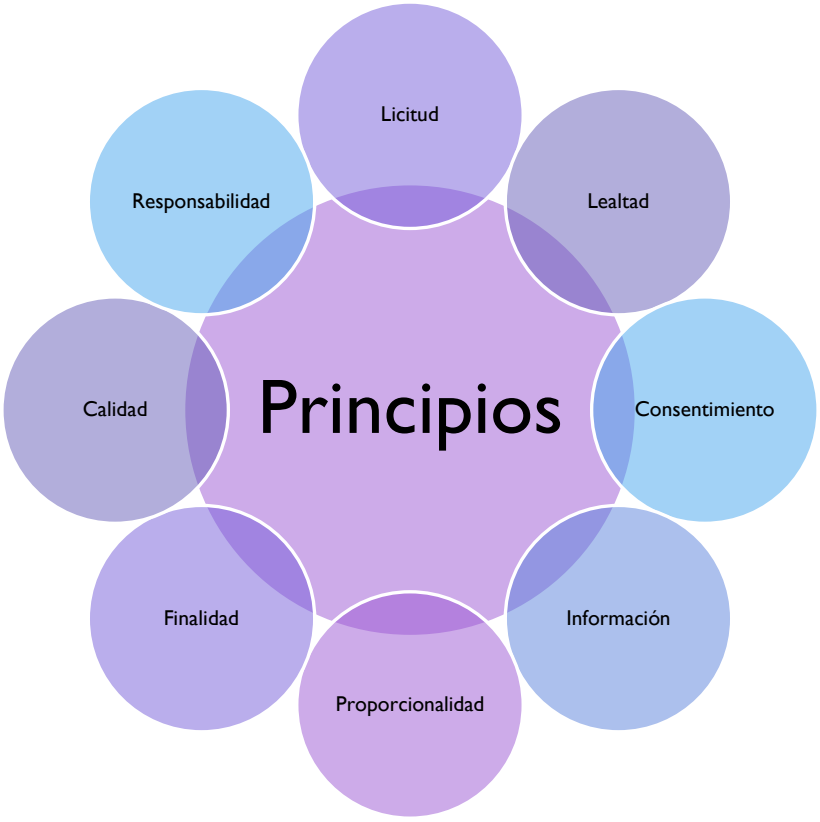
6. Es obligación de todas las personas servidoras públicas de la Secretaría de Cultura que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.

7. Cuando se recaben datos personales de menores de edad se deberá obtener el consentimiento expreso de quien o quienes ejerzan la patria potestad o tutela sobre éstos.

8. Las unidades administrativas deberán identificar todos los avisos de privacidad que se requieren, según los tratamientos que realicen.

9. Los avisos de privacidad deberán ser elaborados en sus dos modalidades: simplificado e integral y contener todos los elementos informativos que exige la norma, además de estar redactados de manera clara y sencilla.

10. Las áreas deberán verificar que sus avisos de privacidad simplificados e integrales se difundan en el portal de internet de la Secretaría de Cultura y estar disponibles para su consulta por parte de las personas titulares.



PRINCIPIOS, DEBERES Y DEMÁS OBLIGACIONES

PRINCIPIOS

1. Principio de Licitud

Los datos personales tienen que ser tratados de manera lícita, esto es, el tratamiento se debe sujetar a las facultades y/o atribuciones que la normatividad aplicable le confiera.

Para cumplir con este principio, las unidades administrativas deberán ajustarse a las siguientes recomendaciones:

a. Revisar que los datos se traten conforme a la LGPDPPSO, Lineamientos Generales de Protección de Datos Personales para el Sector Públicos y demás normativa aplicable.
b. Conocer la normativa que en lo particular regule sus atribuciones, funciones y responsabilidades con relación al tratamiento de los datos personales que realice.
c. Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.

2. Principio de Lealtad

La obtención de los datos personales no podrá hacerse a través de medios engañosos o fraudulentos.

Para cumplir con este principio, las Unidades Administrativas deberán:

a. 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.
b. 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.
c. Respetar en todo momento la expectativa razonable de privacidad de la persona titular de los datos personales.
d. Tratar los datos conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la LGPDPPSO y los Lineamientos generales.
e. Verificar los tratamientos, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.
f. Elaborar avisos de privacidad con todos los elementos informativos que establece la LGPDPPSO, y con información que corresponda a la realidad del tratamiento que se efectúa.
g. 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

3. 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, las Unidades Administrativas deberán ajustarse a las siguientes recomendaciones:

a. Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.
b. Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.
c. 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.
d. 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.
e. Habilitar los mecanismos necesarios para solicitar el consentimiento expreso.
f. Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.

g. Solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad, cuando los datos personales se obtengan directamente de su titular o representante.
h. Cuando los datos personales no los proporcione personal o directamente el titular o su representante, deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado. Asimismo, deberá informarles que cuentan con un plazo de 5 días hábiles para en su caso manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran su consentimiento. Si el titular no manifiesta su negativa en el plazo de cinco días antes señalado, entonces podrá suponer que cuenta con el consentimiento tácito.
i. En el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso de privacidad o en un instrumento aparte. No podrán tratar los datos personales si no cuenta con el consentimiento expreso del titular.

4. Principio de Información

Las Unidades Administrativas que realizan tratamientos de datos personales se encuentran obligadas a informar a las personas titulares de los datos personales, a través de los avisos de privacidad integral y simplificado, las características principales del tratamiento al que serán sometidos sus datos personales es decir cómo se recopilan, utilizan, procesan y protegen sus datos personales, a fin de que pueda tomar decisiones informadas sobre el manejo de sus datos y ejercer sus derechos de privacidad de manera efectiva.

Para cumplir con este principio, las Unidades Administrativas deberán ajustarse a las siguientes recomendaciones:

a. Poner a disposición de los titulares el aviso de privacidad en los términos dispuestos en la LGPDPPSO, y demás normativa aplicable
b. Redactar el aviso de privacidad de manera que sea claro, comprensible y con una estructura y diseño que facilite su entendimiento.
c. Facilitar a los titulares el ejercicio de sus derechos de privacidad, como el derecho de acceso, rectificación, cancelación y oposición (derechos ARCO).

5. Proporcionalidad

Las Unidades Administrativas 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, las Unidades Administrativas deberán:

a. Tratar el menor número posible de datos personales.
b. Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles.
c. Crear bases de datos con datos personales sensibles sólo cuando:
   - Obedezca a un mandato legal;

- Se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o
- Lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

d. Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.
e. Cuando una normativa establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, sólo deberán solicitarse dichos datos.

6. 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 primarias (propósitos principales y esenciales para los cuales se recopilan los datos personales. Estas finalidades están directamente relacionadas con el tratamiento) y 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.)
- 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.

- Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, informar a la persona titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información para finalidades secundarias.
- No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias

7. 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:** Cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles
- **Completos:** Cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular
- **Pertinentes:** Cuando corresponden efectivamente al titular.
- **Actualizados:** Cuando los datos personales responden fielmente a la situación actual del titular.
- **Correctos:** Cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados y estos no presentan errores que pudieran afectar su veracidad.

Para cumplir con este principio, las Unidades Administrativas de la Secretaría de Cultura 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.

8. Principio de Responsabilidad.

A este principio se le conoce también como el principio de “rendición de cuentas” ya que 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, las áreas deberán:

- 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.

DEBERES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

La protección de los datos personales se basa en dos deberes: el de **confidencialidad** y el de **seguridad**, los cuales se traducen también en obligaciones concretas para el responsable. A continuación, se abordarán estos deberes

1. 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 administrativas, físicas y técnicas.
    - **Administrativas** corresponden a todas las acciones encaminadas a la protección de la información y que están relacionadas con la gente y los procesos.
    - **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.
    - **Técnicas** se apoyan en infraestructura tecnológica (hardware y software).
- 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.

2. Deber de confidencialidad

Este deber implica la obligación de guardar la confidencialidad respecto de los datos personales que son tratados. Este deber debe cumplirse para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información.

Para cumplir con este principio, las áreas deberán:

- Guardar confidencialidad en cualquier fase del tratamiento de los datos personales y limitar el acceso a la información solo a aquellos casos en 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.
- 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.
- 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.

3. Deber de seguridad

Este deber se refiere a la obligación de establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Para cumplir con este deber, las áreas deberán:

1. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas.
2. No adoptar medidas de seguridad menores a aquéllas que mantengan para el manejo de su información.
3. Tomar en cuenta el riesgo inherente por tipo de dato personal; las posibles consecuencias para las personas titulares por una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico.
4. Notificar a las personas titulares las vulneraciones de seguridad que se presenten, con la información y en el momento antes señalado;
5. Llevar a cabo las acciones correctivas que sean necesarias.

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;
- 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 remisiones (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) y transferencias (Toda comunicación de datos personales realizada a persona distinta del titular, del responsable o del encargado) 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 las unidades administrativas deberán ajustarse a las siguientes recomendaciones:

1. 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.
2. Elaborar un inventario de datos personales relacionando el tipo de tratamiento con el ciclo de vida.
3. Bloquear, cancelar, suprimir o destruir los datos personales, en los casos establecidos en la normatividad aplicable.

ROLES Y RESPONSABILIDADES

Con relación a lo dispuesto en el artículo 33, fracción II de la LGPDPPSO, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.

SANCIONES

Serán causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales las establecidas en el artículo 163 de la LGPDPPSO:

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;

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;

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.

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.

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.

De acuerdo con la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

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 General de Tecnologías de la Información y/o cualquier unidad administrativa de la Secretaría de Cultura.

En el documento "Guía para registrar y reportar vulneraciones de datos personales" se concentran las actividades que deben realizare 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.

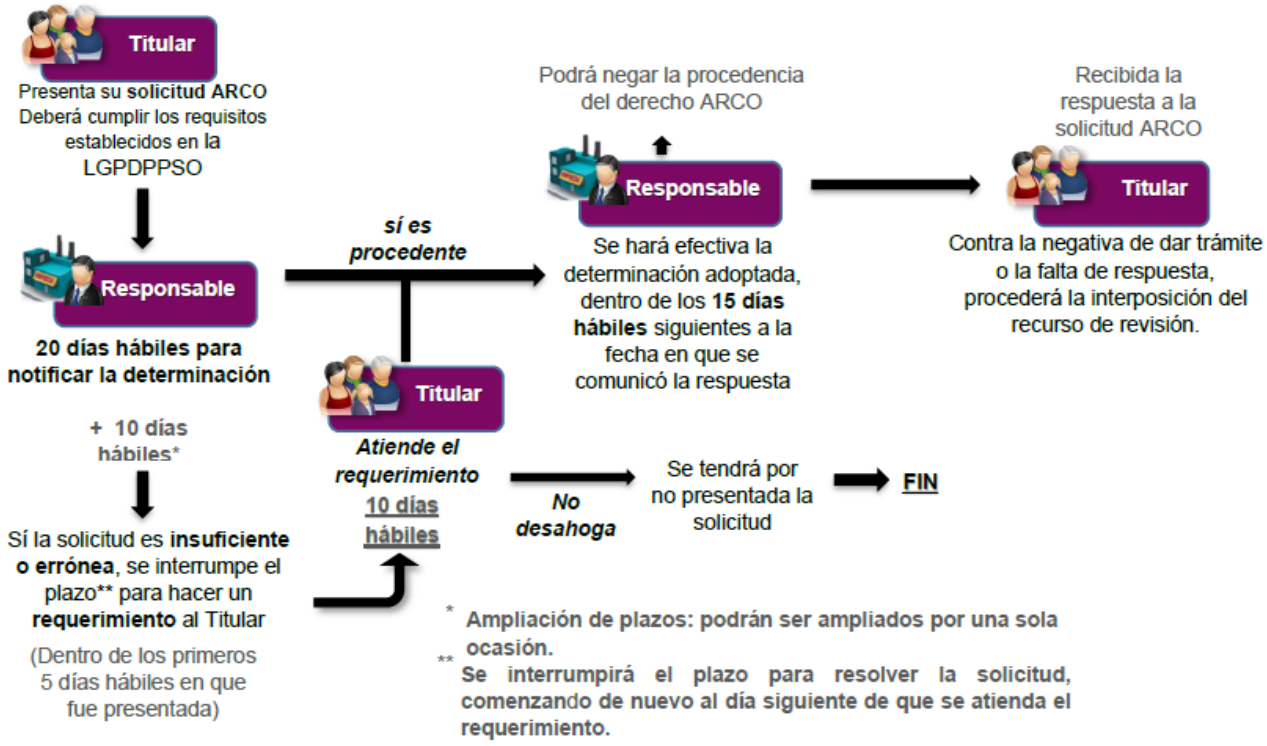
Por tanto, resulta necesario establecer un mecanismo que permita dar cumplimiento a las disposiciones antes citadas, mismo que se desarrolla de la siguiente manera:

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.

Proceso General de Atención de los Derechos Arco.

La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO, 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 de la Secretaría de Cultura.

Solicitud de derechos ARCO	No Competencia (3 días)
	Prevención (5 días)
	Información disponible públicamente (5 días)
	Respuesta terminal (20 días (+10))
	Recurso de Revisión (15 días)



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/

- En las instalaciones de la Unidad de Transparencia de la Secretaría de Cultura ubicadas en Av. Paseo de la Reforma 175, PB Col. Cuauhtémoc, alcaldía Cuauhtémoc, C.P. 06500, Ciudad de México.

- A través del correo electrónico de la Unidad de Transparencia de la Secretaría de Cultura unidadenlace@cultura.gob.mx