



**GOBIERNO DE  
MÉXICO**



**CONAHCYT**  
CONSEJO NACIONAL DE HUMANIDADES  
CIENCIAS Y TECNOLOGÍAS

**UNIDAD DE ASUNTOS JURÍDICOS  
UNIDAD DE TRANSPARENCIA**

# **PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES CONAHCYT**

Av. Insurgentes Sur No. 1582, Col. Crédito Constructor, CP. 03940, Benito Juárez, Ciudad de México.  
Tel: (55) 5322 7700 [www.conahcyt.mx](http://www.conahcyt.mx)





## CONTENIDO

### Presentación

- I. Objetivo
- II. Alcance
- III. Glosario
- IV. Marco Normativo
- V. Gestión de los datos personales
- VI. Lineamientos para la protección de datos personales a cargo del Conahcyt
- VII. Inventario de datos personales
- VIII. Documento de seguridad
- IX. Mecanismos para el cumplimiento de los principios de protección de datos personales en el Conahcyt
- X. Cumplimiento de los deberes de protección de datos personales en el Conahcyt
- XI. Ejercicio de los Derechos ARCO y la Portabilidad de los Datos Personales
- XII. Atención de Solicitudes de Ejercicio de Derechos ARCO
- XIII. Procedimiento y Requisitos de la Solicitud de Ejercicio de Derechos ARCO
- XIV. Facultades y atribuciones del Comité de Transparencia en materia de protección de datos personales
- XV. Facultades y atribuciones Unidad de Transparencia en materia de protección de datos personales
- XVI. Documento de seguridad
- XVII. Mejores Prácticas
- XVIII. Revisiones y Auditorías
- XIX. Sanciones por incumplimiento



GOBIERNO DE  
MÉXICO



CONAHCYT  
CONSEJO NACIONAL DE HUMANIDADES  
CIENCIAS Y TECNOLOGÍAS

UNIDAD DE ASUNTOS JURÍDICOS  
UNIDAD DE TRANSPARENCIA

## PRESENTACIÓN

El Conahcyt, en su calidad de sujeto obligado, es responsable de asegurar la correcta gestión de los datos personales y de velar por el cumplimiento de este Programa. Al desarrollar y adoptar mejores prácticas, el Conahcyt puede garantizar la protección efectiva de los datos personales relativos a los tratamientos realizados.

De acuerdo con lo estipulado en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSSO), en su artículo 34 establece que las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión al que para mejor entendimiento denominaremos Programa. Este Programa se encuentra conformado por el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales recabados por el Consejo Nacional de Humanidades, Ciencias y Tecnologías (Conahcyt) de conformidad con lo previsto en la LGPDPSO y las demás disposiciones que le resulten aplicables en la materia emitidas por el Sistema Nacional de Transparencia o por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Para la elaboración e implementación del Programa de protección de datos personales del Conahcyt deberá considerarse el modelo PHVA el cual incluye las fases de planificar, hacer, verificar y actuar. Este modelo, de acuerdo con los marcos teóricos es un enfoque utilizado en la gestión de la calidad y mejora continua de los procesos, de manera general cada fase se define de la forma siguiente:

*Planificar:* Establece los objetivos y metas a alcanzar, identificando los procesos y recursos necesarios, y elaborar un plan de acción definiendo los criterios de evaluación.

*Hacer:* Implementar el plan de acción y realizar la ejecución de las actividades previstas recopilando los datos necesarios para su evaluación.

*Verificar:* Analizar y evaluar los resultados obtenidos comparándolos con los objetivos establecidos en la fase de planificación, utilizando técnicas de medición y análisis de datos para verificar si se han alcanzado los resultados esperados.

*Actuar:* Tomar las decisiones basadas en los resultados obtenidos durante la fase de verificación, e implementar cambios y mejoras necesarias en los procesos, así como realizar ajustes, utilizando la retroalimentación obtenida para la planificación de futuras acciones.

El diseño de este Programa, tomando como base el modelo PHVA, permitirá, eventualmente, al Conahcyt mejorar sus procesos y alcanzar altos estándares en la protección de los datos personales a su cargo.



## I. OBJETIVO

El propósito de la emisión del presente Programa es proporcionar un marco integral que permita al Conahcyt cumplir con sus obligaciones y proteger los datos personales que utiliza en la realización de sus actividades cotidianas. Este Programa abarca una serie de políticas, procedimientos y controles diseñados para garantizar el cumplimiento normativo y mitigar los posibles riesgos asociados al manejo de datos personales, con ella se establecen e implementan los principios, deberes y obligaciones que deben seguirse para garantizar la correcta protección y confidencialidad de los datos personales que sean recopilados, tratados y almacenados por el Conahcyt.

Estas disposiciones serán comunicadas a todas las personas servidoras públicas, así como al personal involucrado en el tratamiento de datos personales, debiendo fomentar la capacitación continua para garantizar su comprensión y cumplimiento, incluyendo mecanismos de evaluación y mitigación de riesgos para garantizar su efectividad y proteger la privacidad de los ciudadanos a través de su implementación.

## II. ALCANCE

Este Programa es de observancia obligatoria para todas las personas servidoras públicas de las áreas y unidades administrativas que conforman al Consejo Nacional de Humanidades, Ciencias y Tecnologías que realicen tratamiento de datos personales en ejercicio de sus facultades.

## III. GLOSARIO

*Auditoría:* Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

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

*Bases de datos:* Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

*Comité de Transparencia:* Órgano colegiado al que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

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

*Datos personales sensibles:* Aquellos que se refieran a la esfera más íntima de su titular, cuya utilización indebida pueda dar origen a actos de discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, preferencias sexuales y de identidad de género, creencias religiosas, filosóficas y morales, opiniones, entre otras.

*Derechos ARCOP:* Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.



GOBIERNO DE  
MÉXICO



CONAHCYT  
CONSEJO NACIONAL DE HUMANIDADES  
CIENCIAS Y TECNOLOGÍAS

UNIDAD DE ASUNTOS JURÍDICOS  
UNIDAD DE TRANSPARENCIA

**Documento de Seguridad:** Instrumento que describe y da cuenta, de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

**Encargado:** Persona física o jurídica, pública, privada o social, ajena a la organización del responsable que por sí o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

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

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

**Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional que incluye la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal en materia de protección de datos personales.

**Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

**Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se sirven de la tecnología para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

**Portabilidad de datos personales:** Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento, en un formato estructurado, que le permita seguir utilizándolos por un responsable distinto.

**Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado dentro o fuera del territorio mexicano.

**Responsable:** Para efectos de los presentes lineamientos, se entenderá como responsable a la unidad administrativa del sujeto obligado que decide sobre el tratamiento de los datos personales.

**Revisión:** Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

**Riesgo:** Combinación de la probabilidad de un evento y su consecuencia desfavorable.

**Titular:** Persona física a quien corresponden los datos personales.

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

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

**Unidad administrativa:** Área de la estructura orgánica del Conahcyt a la que se le confieren facultades y atribuciones específicas en el Estatuto Orgánico, Manuales Específicos u Operativos o normatividad análoga y a quien para efectos de los presentes lineamientos se les señala como responsables.



*Unidad de Transparencia:* Instancia a la que hace referencia el artículo 85 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

#### IV. MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General en materia de Humanidades, Ciencias, Tecnologías e Innovación.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Estatuto Orgánico del Consejo Nacional de Humanidades, Ciencias y Tecnologías.
- Manual de Organización General del Consejo Nacional de Humanidades, Ciencias y Tecnologías.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.
- Lineamientos que establecen los parámetros, modalidades y procesamiento para la portabilidad de datos personales.

#### V. GESTIÓN DE LOS DATOS PERSONALES

En el cumplimiento del presente Programa las personas servidoras públicas de todas las áreas y unidades administrativas del Conahcyt deberán cumplir con los principios, deberes y obligaciones que establece la LGPDPPSO para ello ajustarán su actuación respetando el ciclo de vida de los datos personales.

El ciclo de vida de los datos personales se compone de las siguientes fases: Obtención, uso y eliminación. En su obtención se deberá de cumplir, en todo momento, con los principios de licitud, información, consentimiento, proporcionalidad, seguridad y confidencialidad que establece la LGPDPPSO. El tratamiento de los datos personales engloba: registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia y disposición, debiendo velar por el cumplimiento de los principios de calidad, finalidad, lealtad, seguridad y confidencialidad. Mientras que la eliminación de los datos personales debe considerar los métodos necesarios y suficientes que garanticen su supresión de los sistemas donde hubiesen sido registrados; esta fase garantiza el cumplimiento de los principios de calidad y seguridad.

De manera general, los principios que rigen el tratamiento y la protección de los datos personales pueden definirse de la siguiente forma:

*Principio de licitud:* la obtención de los datos personales se efectuará únicamente por el área o unidad administrativa que cuente con las facultades expresas para requerirlos.

*Principio de finalidad:* los datos personales que se obtengan para la realización de trámites y procedimientos, serán recabados para un fin concreto, de tal manera que no se genere incertidumbre a sus titulares sobre el uso que se dará y quedarán plasmadas en el Aviso de Privacidad. No podrán tratarse datos para finalidades distintas y, en el caso de los datos personales sensibles, se procurará limitar el periodo de tratamiento al mínimo indispensable.

*Principio de lealtad:* el tratamiento de los datos personales debe apegarse a las finalidades para las que fueron obtenidos, tomando en consideración la expectativa razonable de privacidad y sin que para ello se utilice algún medio engañoso o fraudulento.



*Principio de consentimiento:* es la prerrogativa que tiene el titular para que, de manera voluntaria, libre, sin que medie error, mala fe, violencia o dolo que pudiera afectar su voluntad, de manera específica e informada ceda para un determinado fin el uso de sus datos personales.

*Principio de calidad:* los datos personales recabados deberán ser exactos, correctos, completos y actualizados de manera periódica por su titular a fin de que no se altere la veracidad de estos.

*Principio de proporcionalidad:* los datos recabados deberán ser estrictamente necesarios, apropiados, indispensables y no excesivos para el cumplimiento de las finalidades para las que fueron obtenidos.

*Principio de información:* es la obligación que tienen las personas servidoras públicas del Conahcyt para comunicar a los titulares las características del tratamiento a los que serán sometidos sus datos personales.

*Principio de responsabilidad:* constituye la obligación de las personas servidoras públicas del Conahcyt para adoptar e implementar mecanismos y medidas necesarias a su alcance que garanticen el cumplimiento de los principios, deberes y obligaciones en el tratamiento de los datos personales que recaba.

## VI. LINEAMIENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES A CARGO DEL CONAHCYT

**Lineamiento 1.** Corresponde a la totalidad de personas servidoras públicas, así como aquellas que realicen cualquier tipo de labor, incluidas las de apoyo, cargos honorarios, prestadores de servicio social o prácticas profesionales y en general, a cualquier categoría de persona que, para el desempeño de un encargo o encomienda requiera utilizar datos personales, la observancia obligatoria de los presentes lineamientos.

Estos lineamientos serán aplicables a la totalidad de datos personales recopilados, almacenados, procesados o transferidos por el Conahcyt, contenidos en cualquier tipo de archivo, ya sea en su forma física o digital, sin importar el área o unidad administrativa responsable.

**Lineamiento 2.** El objeto de los presentes lineamientos es otorgar la máxima protección y seguridad a los datos personales con los que cuenta el Conahcyt, así como garantizar la privacidad de los titulares de los datos personales de acuerdo con los estándares normativos emitidos por el Sistema Nacional de Transparencia y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

En todo tratamiento de datos personales, las personas titulares de las unidades administrativas y las personas servidoras públicas a su cargo, deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

**Lineamiento 3.** Al interior del Conahcyt, las personas titulares de las unidades administrativas son los responsables del tratamiento de los datos personales de acuerdo con el ámbito de las facultades y atribuciones que tengan conferidas de conformidad con el Estatuto Orgánico del Conahcyt, el Manual de Organización General del Conahcyt y demás disposiciones análogas.

En su calidad de responsables, deberán informar a la Unidad de Transparencia y a la Coordinación de Repositorios, Investigación y Prospectiva, los nombres completos de las personas servidoras públicas que realizarán tratamiento de datos personales, el perfil y la denominación del puesto que ostentan, el listado de los datos personales a los que tendrá acceso, el rol que realicen dentro del trámite o procedimiento a desarrollar y los privilegios asignados para el desarrollo de sus labores. En el caso de que alguna persona servidora pública cause baja, deberá informar de manera inmediata el hecho a fin de que se realice la revocación de accesos a plataformas y sistemas.



La baja o el término de la relación laboral con la persona servidora pública o bien, la terminación del encargo o cargo honorario, no exime a la persona del deber de confidencialidad respecto de los datos personales a los que tuvo acceso por lo que subsistirá la obligación aún después de finalizada la relación laboral.

Para asegurar que las personas que tengan conocimiento de datos personales en posesión del Conahcyt se concienticen respecto del control, manejo y resguardo de ellos, de manera preventiva, suscribirán cartas responsivas respecto del manejo de la información confidencial. El resguardo y control de las cartas responsivas signadas para el tratamiento de datos personales quedará a cargo de la Unidad de Transparencia.

**Lineamiento 4.** Son obligaciones de las personas responsables del tratamiento de los datos personales:

- I. Justificar mediante finalidades concretas, lícitas, explícitas y legítimas el tratamiento de los datos personales. Estas finalidades deberán estar relacionadas con las facultades y atribuciones que tengan conferidas;
- II. Tratar y obtener los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento;
- III. Informar al titular de los datos personales, a través del Aviso de Privacidad, la existencia y características principales del tratamiento al que serán sometidos con el objeto de que pueda externar su consentimiento;
- IV. Abstenerse, por sí o a través de las personas servidoras públicas a su cargo o de terceros, de obtener y tratar datos personales utilizando medios engañosos, fraudulentos o no autorizados por el Conahcyt;
- V. Privilejarán en todo momento, la protección de los intereses de los titulares así como la expectativa razonable de su privacidad y, ante la duda proteger cada dato personal;
- VI. Contar con el consentimiento previo del titular otorgado de forma libre, específica e informada.

Para la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada, deberán ser consideradas las disposiciones para representación previstas en la legislación en materia civil.

En la manifestación del consentimiento serán válidas la forma expresa y la tácita. Se entenderá por forma expresa cuando la voluntad del titular se manifieste por escrito, por medios electrónicos, ópticos, con el uso de cualquier tecnología o de forma verbal siempre y cuando demuestre signos inequívocos para proporcionar sus datos. El consentimiento será tácito cuando, habiéndose puesto a disposición del titular el Aviso de Privacidad, éste no manifieste su voluntad en sentido contrario; esta forma será válida por regla general salvo que la ley exija que la voluntad deba manifestarse de forma expresa;

- VII. En el caso de los datos personales sensibles, deberán obtener el consentimiento por escrito considerándose como válida su obtención con la firma autógrafa, electrónica (a través del uso de la e.firma o firma con CURP) o cualquier otro mecanismo de autenticación establecido por el Conahcyt, y
- VIII. Elaborar los proyectos de Aviso de Privacidad para sanción y validación por parte de la Unidad de Transparencia.

**Lineamiento 5.** Para dar cumplimiento al principio de información, las unidades administrativas deberán remitir a la Unidad de Transparencia los proyectos de Aviso de Privacidad Integral y Aviso de Privacidad Simplificado para sanción y en su caso validación.



Una vez sancionado por la Unidad de Transparencia, al Aviso de Privacidad Integral, se le asignará un número inequívoco a fin de contar con un registro actualizado de los mismos. Los Avisos de Privacidad Integral y Simplificado deberán ser puestos a disposición del titular de los datos personales considerando lo siguiente:

- a) En el caso del Aviso de Privacidad Integral su divulgación se realizará a través de la Unidad de Transparencia en la página web <https://conahcyt.mx/transparencia/proteccion-de-datos-personales/avisos-de-privacidad/>;
- b) En el caso de que, para recabar los datos personales se utilicen formularios o medios electrónicos, la forma de difusión del Aviso de Privacidad Simplificado, quedará a cargo de las personas responsables del tratamiento quienes deberán articular de manera conjunta con la Coordinación de Repositorios, Investigación y Prospectiva su implementación y divulgación como mecanismo manifestación del consentimiento de sus titulares para el tratamiento, y
- c) En el caso de que los datos personales se utilicen formularios en formatos físicos, la difusión del Aviso de Privacidad Simplificado quedará a cargo de las personas responsables del tratamiento y quienes deberán implementar los mecanismos que aseguren que los titulares de los datos personales han sido informados respecto del uso que se dará a sus datos.

Con independencia de lo anterior, es obligación de las personas responsables del tratamiento difundir el Aviso de Privacidad por medios electrónicos, físicos, ópticos, sonoros, visuales o a través de cualquier tecnología que permita su eficaz comunicación.

**Lineamiento 6.** Los titulares de las unidades administrativas no estarán obligadas a recabar el consentimiento cuando:

- I. Una ley así lo disponga;
- II. Las transferencias se utilicen para el ejercicio de facultades compatibles o análogas con la finalidad que motivo el tratamiento;
- III. Exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- IV. Resulten necesarios para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- V. Los datos se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- VI. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
- VII. Los datos sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria;
- VIII. Los datos personales figuren en fuentes de acceso público;
- IX. Los datos personales sean sometidos a un procedimiento previo de disociación, y
- X. El titular de los datos personales sea una persona reportada como desaparecida en los términos de la norma correspondiente.

**Lineamiento 7.** Los titulares de las unidades administrativas deberán adoptar las medidas técnicas y de organización necesarias para mantener exactos, completos, correctos y actualizados los datos personales sometidos a tratamiento a fin de que no se altere la veracidad de estos.

Las personas titulares de las unidades administrativas deberán implementar mecanismos para mantener la calidad de los datos personales proporcionados por su titular hasta en tanto subsista un interés particular para que el Conahcyt haga uso de su información.

**Lineamiento 8.** Los titulares de las unidades administrativas, en coordinación con la Unidad de Transparencia, deberán establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de



los datos personales en los cuales se deberán contemplar los periodos de conservación considerando los aspectos administrativos, contables, fiscales, jurídicos e históricos establecidos en el Catálogo de Disposición Documental.

En el caso de que los datos personales sean recabados a través de medios electrónicos, adicionalmente, deberán solicitar la intervención de la Coordinación de Repositorios, Investigación y Prospectiva a fin de garantizar la supresión segura de los datos personales.

**Lineamiento 9.** En el caso de que los datos personales sean tratados de forma física, los titulares de las unidades administrativas, deberán establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para su protección con el objeto de prevenir cualquier tipo de daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

**Lineamiento 10.** Los titulares de las unidades administrativas deberán realizar, cuando menos una vez al año, la revisión de los trámites, procesos y procedimientos con los que realiza el tratamiento de datos personales así como del marco normativo que les aplica a fin de determinar y establecer, en coordinación con la Unidad de Asuntos Jurídicos, la Coordinación de Repositorios, Investigación y Prospectiva, el Área Coordinadora de Archivos y la Unidad de Transparencia, las medidas para realizar la corrección de datos inexactos, la periodicidad de conservación, bloqueo y procedimientos de eliminación segura de los mismos.

Los titulares de las unidades administrativas deberán asegurarse de que los datos personales sólo sean tratados durante el tiempo necesario para cumplir con las finalidades para los que fueron recabados, a menos que demuestre ante la Unidad de Transparencia, de manera fundada y motivada, requiera una retención más prolongada.

**Lineamiento 11.** Los titulares de las unidades administrativas deberán, ante cualquier tipo de vulneración, dar aviso por escrito y sin dilación a la Unidad de Transparencia y a la Coordinación de Repositorios, Investigación y Prospectiva a fin de que esta última ejecute las acciones de seguridad aplicables al sistema que haya sido vulnerado.

La Coordinación de Repositorios, Investigación y Prospectiva levantará el reporte correspondiente de la vulneración a la seguridad en la bitácora correspondiente en la que deberá incluir la fecha en que sucedieron los hechos, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

La Coordinación de Repositorios, Investigación y Prospectiva remitirá una copia certificada de la bitácora, así como el reporte por escrito de las acciones implementadas a la Unidad de Transparencia a fin de que, por su conducto, se informe a las personas integrantes del Comité de Transparencia.

**Lineamiento 12.** Al presentarse la vulneración a la seguridad de los datos personales, los titulares de las unidades administrativas a través de la Coordinación de Repositorios, Investigación y Prospectiva, deberán informar a las personas titulares, al menos, lo siguiente:

- I. La naturaleza del incidente;
- II. Los datos personales comprometidos;
- III. Las recomendaciones que el titular de los datos pueda adoptar para proteger sus intereses;
- IV. Las acciones correctivas realizadas de forma inmediata y,
- V. Los medios donde puede obtener más información al respecto.

**Lineamiento 13.** Una vez que el Comité de Transparencia tome conocimiento de la vulneración de los datos personales determinará el grado o nivel de vulneración e identificará a las posibles personas servidoras públicas involucradas de acuerdo con los registros de la Unidad de Transparencia.



**Lineamiento 14.** Cualquier persona servidora pública que reciba alguna solicitud, escrito físico o electrónico de un titular que requiera ejercer cualquiera de los derechos ARCOP, deberá remitir la petición a la Unidad de Transparencia a fin de que ésta realice el registro correspondiente en la Plataforma Nacional de Transparencia, verifique la identidad de la persona solicitante, se asegure que la unidad administrativa facultada pueda proporcionar la atención correspondiente en el tiempo establecido por ley y, que la información sea entregada a su titular o a su representante legal.

**Lineamiento 15.** No será procedente el ejercicio de los derechos ARCO cuando:

- I. El titular o su representante no estén debidamente acreditados para ello;
- II. Los datos personales no se encuentren en posesión de los sistemas a cargo del Conahcyt o que los mismos hayan sido recabados por otro sujeto obligado;
- III. Exista un impedimento legal;
- IV. Se lesionen los derechos de un tercero;
- V. Se obstaculicen actuaciones judiciales o administrativas;
- VI. Exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;
- VII. La cancelación u oposición haya sido previamente realizada;
- VIII. El Conahcyt no sea competente para realizar el tratamiento;
- IX. Sean necesarios para proteger intereses jurídicamente tutelados del titular;
- X. Sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;
- XI. Cuando, en función de sus atribuciones legales, el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado Mexicano y,
- XII. Sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

En los casos anteriores, los responsables deberán informar a los titulares de los datos personales y a la Unidad de Transparencia, el motivo de su determinación en un plazo no mayor de diez días hábiles y, en su caso, deberán acompañar las pruebas que resulten necesarias.

**Lineamiento 16.** Las unidades administrativas sólo podrán realizar transferencias o remisiones de datos personales fuera del territorio nacional cuando el tercer receptor o el encargado se obligue a proteger los datos personales conforme a los principios y deberes que establece la LGPDPPSO.

En este caso, de manera paralela a la solicitud de sanción del convenio de colaboración, convenio marco o cualquier otro instrumento legal por parte de la Subdirección de Convenios y Asesoría Institucional, deberá solicitar la revisión de las cláusulas respectivas o sus anexos a la Unidad de Transparencia.

**Lineamiento 17.** Las personas titulares de las unidades administrativas podrán realizar transferencias de datos personales sin necesidad de requerir el consentimiento de su titular en los supuestos siguientes:

- I. Cuando la transferencia esté prevista en la LGPDPPSO, leyes, convenios o tratados internacionales suscritos y ratificados por México;
- II. Cuando la transferencia se realice entre sujetos obligados siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;



- V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
- VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;
- VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
- VIII. Cuando se trate de los casos en los que las personas titulares de las Unidades administrativas no estén obligadas a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales,
- o
- IX. Cuando la transferencia sea necesaria por razones de seguridad nacional.

La actualización de algunas de las excepciones señaladas con anterioridad, no exime al titular de la Unidad Administrativa de cumplir con las obligaciones previstas en los presentes lineamientos que resulten aplicables.

**Lineamiento 18.** El Comité de Transparencia del Conahcyt es la máxima autoridad en materia de protección de datos personales, además de las facultades y atribuciones que le confiere la Ley General de Transparencia y Acceso a la Información Pública, contará con las siguientes atribuciones:

- I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en el Conahcyt;
- II. Establecer e implementar procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCOP;
- III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCOP;
- IV. Establecer y supervisar la aplicación de criterios específicos en materia de protección de datos personales;
- V. Supervisar el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
- VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;
- VII. Establecer programas de capacitación y promover la actualización de las personas servidoras públicas en materia de protección de datos personales, y
- VIII. Dar vista al Órgano Interno de Control Específico en el Conahcyt en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales, particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables en las unidades administrativas.

**Lineamiento 19.** En materia de protección de datos personales, además de las funciones que prevé la Ley General de Transparencia y Acceso a la Información, corresponde a la Unidad de Transparencia lo siguiente:

- I. Auxiliar y orientar al titular de los datos personales respecto de lo requiera en relación al ejercicio de los derechos ARCOP;
- II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;
- III. Establecer mecanismos para asegurar que los datos personales sólo se entreguen a su titular o su representante debidamente acreditado;
- IV. Informar al titular de los datos personales el monto de los costos a cubrir por concepto de reproducción con base en lo establecido en las disposiciones normativas aplicables;
- V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCOP;
- VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCOP;



- VII. Asesorar a las personas titulares de las unidades administrativas y a las personas servidoras públicas a ellas adscritas en materia de protección de datos personales, y
- VIII. Demostrar ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cumplimiento de la normatividad en materia de protección de datos personales.

**Lineamiento 20.** De acuerdo con lo establecido en el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales las siguientes:

- I. Actuar con negligencia, dolo o mala fe durante la sustanciación de solicitudes para el ejercicio de los derechos ARCOP;
- II. Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCOP o para hacer efectivo el derecho de que se trate;
- III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, encargo o comisión;
- IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO;
- V. Faltar al deber de informar al titular de los datos personales de la existencia del Aviso de Privacidad;
- 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;
- VIII. Omitir el establecimiento de las medidas de seguridad;
- IX. Reportar vulneraciones cuya causa encuadre en la falta de implementación de medidas de seguridad;
- X. Realizar transferencias en contravención a estos lineamientos;
- XI. Obstruir los actos de verificación de la autoridad;
- XII. Crear o realizar duplicados de bases de datos personales fuera de los registros informados a la Unidad de Transparencia, y
- XIII. Omitir acatar las resoluciones emitidas por el Comité de Transparencia, la Unidad de Transparencia o el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales.

**Lineamiento 21.** El Comité de Transparencia podrá imponer como sanciones las siguientes:

- I. Dar vista al superior jerárquico a fin de que la persona servidora pública atienda sin dilación a lo requerido por la Unidad de Transparencia;
- II. Dar vista al Órgano Interno de Control Específico del Conahcyt de la falta cometida a fin de que se inicie con el procedimiento de responsabilidad correspondiente;
- III. Tratándose de sanciones económicas determinadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el monto correspondiente no podrá ser cubierto con recursos públicos, e
- IV. Informar a la Dirección de Personal de la sanción impuesta a la persona servidora pública responsable de la vulneración de las medidas de seguridad a fin de que sea incorporada la resolución en el expediente laboral.

En el supuesto de que, con motivo de vulneraciones a las medidas de protección, los titulares de derechos interpongan recursos legales en materias civil, penal o administrativo, se procederá a dar vista a la Dirección de Estrategias y Procesos Jurídicos quien dependiendo la gravedad del asunto podrá, sin responsabilidad para el Conahcyt, dar por terminada la relación laboral con la persona servidora pública de conformidad con la normativa aplicable a dicha materia.



**Lineamiento 22.** Los presentes lineamientos serán revisados una vez al año o bien, en el momento en que sean emitidas nuevas disposiciones por el Sistema Nacional de Transparencia y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

**Lineamiento 23.** Estos lineamientos entrarán en vigor a partir de la fecha de aprobación por parte del Comité de Transparencia del Conahcyt.

**Lineamiento 24.** En caso de duda respecto del sentido de alguna disposición de los presentes Lineamientos o sobre su aplicabilidad, la Unidad de Transparencia establecerá su interpretación y alcance.

## VII. INVENTARIO DE DATOS PERSONALES

En materia de protección de datos personales, el inventario consiste en una lista detallada de todos los datos personales que son tratados a través de sistemas, subsistemas y aplicativos del Conahcyt que son utilizados por las diferentes unidades administrativas para el cumplimiento de las facultades y atribuciones a su cargo.

De acuerdo con lo reportado por las unidades administrativas, así como el registro en posesión de la Coordinación de Repositorios, Investigación y Prospectiva, el Inventario de Datos Personales del Conahcyt contiene de manera enunciativa, más no limitativa, entre otra la información siguiente:

- a) Unidad administrativa responsable del tratamiento;
- b) Identificación de los datos personales recabados;
- c) Fuentes de obtención de los datos personales;
- d) Propósito del tratamiento;
- e) Ubicación y almacenamiento;
- f) Categorización de datos sensibles;
- g) Forma en que se recabó el consentimiento;
- h) Identificación sobre el nivel para gestión de riesgos;
- i) Registro de actividades de tratamiento, y
- j) Apartado sobre actualización del inventario.

El inventario de los datos personales a cargo del Conahcyt y sus actualizaciones serán publicados en <https://conahcyt.mx/transparencia/proteccion-de-datos-personales/>.

## VIII. DOCUMENTO DE SEGURIDAD

El artículo 3, fracción XIV, de la LGPDPPSO define al documento de seguridad como el instrumento que describe de manera general las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Conahcyt para garantizar la confidencialidad, integridad y disponibilidad de los datos personales sujetos a tratamiento.

El Documento de Seguridad del Conahcyt contiene de manera enunciativa, más no limitativa, entre otra la información siguiente:

- a) El inventario de datos personales y de los sistemas de tratamiento;
- b) Las funciones y obligaciones de las personas servidoras públicas del Conahcyt que realizan el tratamiento de datos personales;
- c) El análisis de riesgo;
- d) El análisis de brecha;
- e) El plan de trabajo;



- f) Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- g) El programa general de capacitación.

La versión pública del Documento de seguridad del Conahcyt será publicado en <https://conahcyt.mx/transparencia/proteccion-de-datos-personales/>.

## IX. MECANISMOS PARA EL CUMPLIMIENTO DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES EN EL CONAHCYT

Para la debida constancia del cumplimiento de los principios en materia de protección de datos personales que establece la ley de materia, se establecerán los procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.

El Conahcyt, en su calidad de sujeto obligado, podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines previa autorización del Comité de Transparencia.

### a) Principio de información

Como se ha dicho, los responsables del tratamiento se encuentran sujetos al cumplimiento del principio de información, el cual se materializa a través de la puesta a disposición de los diversos Avisos de Privacidad al titular de los datos personales a fin de que, como su nombre lo indica, se le informe sobre los aspectos relacionados con el manejo de sus datos, cómo se están utilizando y cuáles son sus derechos en relación con ellos, por lo tanto, asegurar que tengan el control sobre su información.

#### *El Aviso de Privacidad*

El artículo 26 de la LGPDPSO establece que el responsable del tratamiento de los datos personales debe informar al titular, a través del Aviso de Privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos; tiene por objeto que el titular esté en condiciones de tomar decisiones informadas respecto del tratamiento, los alcances y condiciones generales del tratamiento, el Aviso se pondrá a disposición del titular en dos modalidades: simplificado e integral.

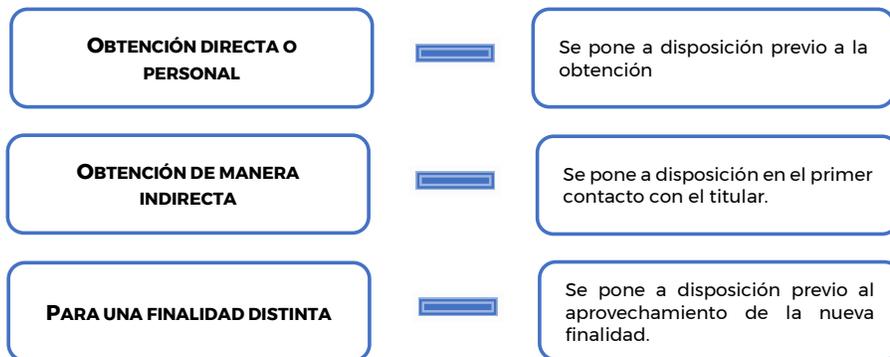
Para que el Aviso de Privacidad cumpla con su esencia y objeto, conforme a los Lineamientos para la Protección de Datos Personales a cargo del Conahcyt, las personas responsables del tratamiento deberán remitir a la Unidad de Transparencia los proyectos de Avisos de Privacidad Integral y Simplificado, a fin de garantizar que los mismos sean generados conforme lo siguiente:

- o Redacción y estructura clara y sencilla;
- o Contendrá únicamente información necesaria;
- o Expresado en lenguaje comprensible;
- o Estructura y diseño que facilite su entendimiento, y
- o Atenderá al perfil de los titulares de los datos personales a los que está dirigido.

De conformidad con lo dispuesto por el artículo 19 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en todos los casos, la persona responsable del tratamiento debe ubicar el Aviso de Privacidad en un lugar visible que facilite al titular su consulta y que permita acreditar fehacientemente su cumplimiento.



El último párrafo del artículo 27 de la LGPDPSO refiere que el Aviso de Privacidad debe ser puesto a disposición, previo al tratamiento de los datos personales, y el artículo 43 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, señalan que, en caso de que los datos se obtengan indirectamente, el aviso debe ponerse a disposición en el primer contacto con el titular. Para clarificar lo anterior puede visualizarse la siguiente tabla:



De acuerdo con la normativa que regula la protección de datos personales, existen dos modalidades en que el aviso de privacidad puede materializarse, esto es la modalidad integral y la simplificada, las cuales pueden diferenciarse a partir de lo siguiente:

Requisitos para el aviso de privacidad en su modalidad simplificada:

ELEMENTOS	DESCRIPCIÓN
Denominación del responsable.	Es obligatorio señalar la denominación completa y sin abreviaturas.
Abreviatura o acrónimo.	Se puede incluir la denominación, abreviaturas o acrónimos con los que usualmente se identifica al responsable por el público.
Finalidades del tratamiento.	Es necesario que se describan cada una de las finalidades que serán aplicadas a los datos personales, las cuales tendrán que distinguirse entre las que requieren del consentimiento del titular y las que no lo requieren. Las finalidades deben redactarse de manera completa y no utilizar frases inexactas, ambiguas o vagas; deben ser precisas, redactadas con claridad y que no den lugar a confusión.
Transferencias de datos personales que requieran consentimiento del titular.	Se deben precisar de los sujetos responsables receptores lo siguiente: a) Si pertenecen al sector público o privado, b) Si son nacionales o internacionales, c) Identificar por nombre, denominación o razón social, y d) Señalar las finalidades de la transferencia a realizar y por cada una de ellas su fundamento legal.
Transferencias de datos personales que no requieren del consentimiento del titular.	Se deben precisar de los sujetos responsables receptores lo siguiente: a) Si pertenecen al sector público o privado, b) Si son nacionales o internacionales, c) Identificar por nombre, denominación o razón social, y d) Señalar las finalidades de la transferencia a realizar y por cada una de ellas el fundamento legal que faculta a la unidad administrativa para realizar la transferencia.
Mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento.	Puede valerse de casillas u opciones de marcado o cualquier medio, siempre y cuando, el mismo esté disponible y se permita manifestar la negativa previo al tratamiento o transferencia.





Sitio donde se podrá consultar el Aviso de Privacidad Integral.	Se debe indicar la fecha de elaboración, o bien, de última actualización.
---	---

*Requisitos para el aviso de privacidad en su modalidad integral:*

ELEMENTOS	DESCRIPCIÓN
Denominación del responsable.	Es obligatorio señalar la denominación completa y sin abreviaturas.
Abreviatura o acrónimo.	Se puede incluir la denominación, abreviaturas o acrónimos con los que usualmente se identifica al responsable por el público.
Domicilio del responsable.	Ubicación geográfica del lugar donde se encuentran las oficinas del responsable; se considera como obligatorio incluir calle, número, colonia, ciudad, municipio o alcaldía, código postal y entidad federativa.
Datos personales que serán sometidos a tratamiento.	Se deben indicar los datos personales sometidos a tratamiento. Este requisito se puede cumplir señalando cada dato personal o por tipo de datos.
Identificación de datos personales sensibles.	Se debe distinguir y señalar los datos personales sensibles sometidos al tratamiento.
Fundamento legal que faculta al responsable para llevar a cabo el tratamiento.	Es necesario señalar con exactitud el precepto legal, esto es, se debe indicar artículo, apartado, fracción, inciso y nombre del ordenamiento con fecha de publicación o última reforma o modificación.
Finalidades del tratamiento.	Es necesario que se describan cada una de las finalidades que serán aplicadas a los datos personales, las cuales tendrán que distinguirse entre las que requieren del consentimiento del titular y las que no lo requieren. Las finalidades deben redactarse de manera completa y no utilizar frases inexactas, ambiguas o vagas; deben ser precisas, redactadas con claridad y que no den lugar a confusión.
Transferencias de datos personales que requieran consentimiento del titular.	Se deben precisar de los sujetos responsables receptores lo siguiente: a) Si pertenecen al sector público o privado, b) Si son nacionales o internacionales, c) Identificar por nombre, denominación o razón social, y d) Señalar las finalidades de la transferencia a realizar y por cada una de ellas su fundamento legal.
Transferencias de datos personales que no requieren del consentimiento del titular.	Se deben precisar de los sujetos responsables receptores lo siguiente: a) Si pertenecen al sector público o privado, b) Si son nacionales o internacionales, c) Identificar por nombre, denominación o razón social, y d) Señalar las finalidades de la transferencia a realizar y por cada una de ellas el fundamento legal que faculta a la unidad administrativa para realizar la transferencia.
Mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento.	Puede valerse de casillas u opciones de marcado o cualquier medio, siempre y cuando, el mismo esté disponible y se permita manifestar la negativa previo al tratamiento o transferencia.
Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO.	Se debe informar los mecanismos, medios y procedimientos habilitados para tal efecto, entre los que se encuentran: a) Requisitos de la solicitud; b) Medios de presentación de la solicitud; c) Formularios, sistemas o métodos implementados; d) Medios de respuesta; e) Modalidad o medios de reproducción; f) Plazos de atención, y g) El derecho de la presentación del recurso de revisión.
Domicilio de la Unidad de Transparencia.	Ubicación geográfica del lugar donde se encuentran las oficinas de la Unidad de Transparencia del responsable; se considera como obligatorio incluir calle, número, colonia, ciudad, municipio o alcaldía, código postal y entidad federativa. Asimismo, se debe incluir número y extensión telefónica.



Medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.	Se debe hacer la referencia de los medios habilitados para informar a los titulares de derechos sobre los cambios o actualizaciones de los avisos de privacidad integral y simplificados.
Derecho de portabilidad.	En el caso de que la modalidad se encuentre disponible, se deberá informar al titular de los derechos sobre la posibilidad que tiene para solicitar la portabilidad de sus datos personales y su alcance; debiendo señalar de manera clara y precisa los tipos o categorías de datos personales que técnicamente sean portables; el o los tipos de formatos estructurados y comúnmente utilizados disponibles para obtener o transmitir sus datos personales, así como los mecanismos, medios y procedimientos disponibles para que el titular pueda solicitar la portabilidad de sus datos personales.

El artículo 54 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establecen que la carga de la prueba del cumplimiento de los principios recae en todo momento en el responsable del tratamiento.

Para el cumplimiento del principio de información, es fundamental que el responsable del tratamiento deba probar cada uno de los puntos previstos ya que, como se ha señalado, el responsable tiene la carga de la prueba respecto de la puesta a disposición del aviso de privacidad de que se trate.

**b) Principio de responsabilidad**

Corresponde a todas las áreas y unidades administrativas del Conahcyt velar por el cumplimiento del principio de responsabilidad, el cual, como se ha señalado constituye la obligación de las personas servidoras públicas para adoptar e implementar mecanismos y medidas necesarias a su alcance que garanticen el cumplimiento de los principios, deberes y obligaciones en el tratamiento de los datos personales que recaba.

Con independencia de lo establecido en los Lineamientos para la protección de datos personales a cargo del Conahcyt, las personas titulares de las unidades administrativas deberán implementar, al interior de ellas, la realización de las acciones tendientes al cumplimiento del deber de responsabilidad, las cuales, de manera enunciativa más no limitativa, deberán contemplar lo siguiente:

- 1) Diseñar e implementar políticas internas claras que establezcan los procedimientos y las prácticas que deben seguirse para garantizar el cumplimiento de las normativas de protección de datos y de salvaguarda de la privacidad de las personas;
- 2) Establecer un plan de respuesta a incidentes de seguridad que incluya procedimientos para notificar y gestionar vulneraciones a datos; en caso de que ocurran, establecimiento de un sistema de supervisión y vigilancia interna, para comprobar el cumplimiento de las políticas de protección de datos personales;
- 3) Proponer revisiones de las políticas y programas de seguridad y del sistema de vigilancia implementado al menos una vez al año, salvo que se realicen modificaciones a los tratamientos y que ameriten una revisión previa;
- 4) Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales, que sea de fácil acceso y con la mayor cobertura posible;
- 5) Cuando se realicen actividades de tratamiento de datos que puedan suponer un alto riesgo para los derechos y libertades de las personas, colaborar y proponer a la Unidad de Transparencia la realización de evaluaciones de impacto para identificar y mitigar los riesgos asociados;





- 6) Colaborar con la Unidad de Transparencia a fin de propiciar entre las personas servidoras públicas la capacitación y actualización de las obligaciones y demás deberes en materia de protección de datos personales, y
- 7) Brindar las facilidades necesarias a la Unidad de Transparencia con motivo de la práctica de auditorías y la revisión de los procesos de protección de datos para evaluar el cumplimiento de las normativas de protección de datos y realizar ajustes y mejoras según sea necesario.

En todos los casos, las personas responsables deberán generar las pruebas necesarias y suficientes para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPPSO, los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos para la protección de datos personales a cargo del Conahcyt.

<b>MECANISMOS PARA EL CUMPLIMIENTO DEL PRINCIPIO DE RESPONSABILIDAD</b>	
Recursos	Destinar recursos económicos y humanos para instrumentar políticas y programas de protección de datos personales.
Políticas y programas	Elaborar y aplicar políticas y programas obligatorios, contar con revisiones periódicas, al menos una vez al año o antes si hubiere cambios sustanciales en el tratamiento de los datos personales. Los mismos deben ser aprobados, coordinados y supervisados por el comité de vigilancia que corresponda.
Capacitación	Colaborar con la Unidad de Transparencia para el cumplimiento del programa de capacitación y actualización para las personas servidoras públicas encargadas del tratamiento.
Dudas y quejas	Contar con procedimientos para atender dudas y quejas en la materia y dirigido a los titulares de datos personales, tomando en consideración que, el mismo debe ser de fácil acceso y con la mayor cobertura posible.
Desarrollo tecnológico	Alineado a la normatividad en materia de protección de datos personales; debe privilegiarse la protección de datos desde el diseño de aplicaciones y contar con mecanismos que garanticen la protección de datos por defecto.

## **X. CUMPLIMIENTO DE LOS DEBERES DE PROTECCIÓN DE DATOS PERSONALES EN EL CONAHCYT**

La protección de los datos personales se centra en requisitos legales que deben ser observados por las personas responsables del tratamiento a efecto de que la información que identifica o hace identificables a personas físicas se realice bajo parámetros que aseguren que el titular de dicha información siga manteniendo su control, por lo tanto, la ley en materia de protección de datos personales refiere al tratamiento de datos personales bajo la luz de los deberes de confidencialidad y medidas de seguridad.

*Deber de confidencialidad.* El deber de confidencialidad es entendido como la obligación que tiene cualquier persona que intervenga en el tratamiento de los datos personales de guardar la secrecía de estos, incluso esta obligación subsistente al término de la relación entre las personas servidoras públicas y el sujeto obligado o bien, persiste este deber a la conclusión de la relación del sujeto obligado con el encargado. Este deber se encuentra vinculado, además de la obligación de mantener la privacidad con la seguridad respecto de la información personal que recaba y procesa.

*Deber de medidas de seguridad.* De conformidad con lo dispuesto en el artículo 3 fracción XX, de la Ley General de Protección Datos Personales en Posesión de los Sujetos Obligados las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales, por lo cual a efecto de proteger los datos personales contra pérdidas, daños, alteraciones, destrucciones o tratamientos no autorizados y asegurar que la información conserve los atributos de





confidencialidad, integridad y disponibilidad, deben ser adoptadas y armonizadas medidas de seguridad físicas, técnicas y administrativas.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas, conforme al artículo 33 de la LGPDPSO.

- I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;
- II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;
- III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
- IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;
- V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
- VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
- VII. 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, y
- VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Las medidas de seguridad físicas son las medidas, mecanismos y controles que se adoptan para proteger el entorno físico en el que los datos personales son tratados, incluyendo incluso la disposición de medios de almacenamiento.

Las medidas de seguridad técnicas se refieren a las medidas, mecanismos y controles tecnológicos para protección de los datos personales tratados en entornos digitales y los recursos que se involucran en su tratamiento.

Las medidas de seguridad administrativa, entendidas como el conjunto de medidas, mecanismos y controles que se traducen en políticas y procedimientos cuyo fin es que a nivel organizacional se protejan los datos personales sometidos a tratamiento.

Se identificará el nivel de medidas de seguridad que serán adoptadas para la salvaguardar los datos personales.

El **riesgo inherente** a los datos personales. Se deben documentar las probabilidades de que una amenaza se configure con respecto a que las medidas de seguridad sean vulneradas y los datos personales sean expuestos o pierdan sus características de confidencialidad, disponibilidad e integridad.

La **sensibilidad** de los datos personales.



- Si se trata de datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y referencia sexual.
- Se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

Debido a lo anterior, atendiendo a la clasificación que se realice, se deberá ponderar el nivel de sensibilidad de los datos personales sometidos a tratamiento.

**Desarrollo tecnológico.** El criterio debe ser considerado en dos dimensiones:

- El desarrollo comercial existente.
- El desarrollo que es aplicado por sujeto obligado que realiza el tratamiento de los datos personales, el que debe estar justificados técnica y económicamente.

Las posibles **consecuencias de una vulneración** a los titulares. Este criterio está íntimamente relacionado con el riesgo inherente, pues se deben documentar las posibilidades y consecuencias de una vulneración a los datos personales de los titulares, la que se debe realizar tomando en cuenta el tipo de dato y las características de sus titulares.

Las **transferencias** de datos personales que se realicen. Se deben considerar las comunicaciones que se realizan a terceros ajenos a la organización bajo la figura de transferencia.

El **número de titulares**. Se trata de un criterio importante, pues del mismo se desprende la cantidad de datos tratados, que mientras más elevado sea en número, mayor es el atractivo para su vulneración.

Las **vulneraciones previas** que hubieren ocurrido a los datos personales.

El **riesgo por el valor potencia cuantitativo o cualitativo** que los datos personales pueden tener para volverse atractivos a ser vulnerados.

Actividades de cumplimiento a las medidas de seguridad		
<b>Medidas de seguridad físicas</b>	Protección del entorno físico de los datos personales y los recursos involucrados en su tratamiento.	<ol style="list-style-type: none"> <li>1. Control de acceso en el perímetro de la organización, sus instalaciones, áreas críticas, recursos e información.</li> <li>2. Acciones para prevenir el daño o interferencia a instalaciones físicas, áreas críticas, recursos e información.</li> <li>3. Acciones de protección y, en su caso, de mantenimiento, respecto de los medios de soportes físicos o electrónicos que puedan salir de la organización.</li> </ol>





<b>Medidas de seguridad técnicas</b>	Protección del entorno digital de los datos personales.	<ol style="list-style-type: none"> <li>1. Acceso controlados a bases de datos o a información.</li> <li>2. Esquema de privilegios para la ejecución de actividades.</li> <li>3. Configuración y mantenimiento de la seguridad de <i>software</i> y <i>hardware</i>.</li> <li>4. Gestión de las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos involucrados en el tratamiento de datos personales.</li> </ol>
<b>Medidas de seguridad administrativas</b>	Acciones de protección a nivel organizacional.	<ol style="list-style-type: none"> <li>1. Políticas y procedimientos para la gestión, soporte y revisión de la seguridad.</li> <li>2. Identificación, clasificación y borrado seguro de la información.</li> <li>3. Sensibilización y capacitación.</li> </ol>

*Tabla Actividades de cumplimiento a las medidas de seguridad*

### **XIII. EJERCICIO DE LOS DERECHOS ARCO Y LA PORTABILIDAD DE LOS DATOS PERSONALES**

#### **DERECHOS ARCO**

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, establece que *“Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”*.

El artículo 43 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, refiere que *“En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen”*.

**DERECHO DE ACCESO.** El derecho con el que se cuenta para solicitar el acceso a los datos personales que obren en los sistemas de archivos del Sujeto Obligado, así como conocer la información relacionada con las condiciones y generalidades del tratamiento.

**DERECHO DE RECTIFICACIÓN.** El derecho de rectificación tiene lugar, para los casos en que los datos personales sometidos al tratamiento no cumplen con el principio de calidad, por estar incompletos, inexactos o desactualizados, y sus titulares desean que se realice la corrección o rectificación de estos.





**DERECHO DE CANCELACIÓN.** El derecho de cancelación es la prerrogativa que tienen los titulares de datos personales para solicitar a los responsables del tratamiento, a efecto de sus datos personales dejen de ser tratados y ya no estén en su posesión. Esto es, que los mismos sean eliminados de sus registros.

**DERECHO DE OPOSICIÓN.** El derecho de oposición al tratamiento de los datos personales presupone el cese del tratamiento y no de su supresión.

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

La portabilidad de datos personales tiene por objeto que el titular solicite:

**I.** Una copia de sus datos personales que hubiere facilitado directamente al responsable, en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a otro responsable para su reutilización y aprovechamiento en un nuevo tratamiento, sin que lo impida el responsable al que el titular hubiere facilitado los datos personales, y

**II.** La transmisión de sus datos personales a un responsable receptor, siempre y cuando sea técnicamente posible, el titular hubiere facilitado directamente sus datos personales al responsable transmisor y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.

#### XIV. ATENCIÓN DE SOLICITUDES DE EJERCICIO DE DERECHOS ARCO

La Unidad de Transparencia dará trámite a todas las solicitudes de ejercicio de derechos ARCO y entregará el acuse de recibido que corresponda, asimismo, deberá turnar las solicitudes admitidas a las unidades administrativas que puedan poseer los datos personales según sus atribuciones, competencias, facultades o funciones.

Se deberán registrar las solicitudes para el ejercicio de los derechos ARCO que se presenten mediante escrito libre en el sistema electrónico habilitado para tal efecto.

En caso de que la solicitud para el ejercicio de los derechos ARCO en escrito libre se presente directamente ante una unidad administrativa distinta a la Unidad de Transparencia, la Unidad Administrativa deberá remitir la solicitud a la Unidad de Transparencia a más tardar al día siguiente de su presentación y se tendrá por recibida en la fecha en que fue presentada en la unidad administrativa, procediendo al registro en la Plataforma Nacional de Transparencia.

El plazo de respuesta de las solicitudes de ejercicio de derechos ARCO no deberá exceder de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, el plazo podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

En caso de resultar procedente el ejercicio de los derechos ARCO, se deberá hacer efectivo en un plazo que no podrá exceder de 15 días contados a partir del día siguiente en que se haya notificado la respuesta al titular.

Previo a hacer efectivo el ejercicio del derecho que corresponda, se deberá acreditar la identidad del titular y, en su caso, la identidad y personalidad del responsable, así como verificar los pagos de los costos de reproducción, envío o certificación que se hayan establecido.



En la atención de las solicitudes se deberá prever dar trámite a todas las solicitudes y entregar al titular el acuse correspondiente, previendo el turno de las solicitudes a todas las unidades administrativas que pudieran tener los datos personales.

## XV. PROCEDIMIENTO Y REQUISITOS DE LA SOLICITUD DE EJERCICIO DE DERECHOS ARCO

Para ejercer ante el Consejo Nacional de Humanidades, Ciencias y Tecnologías, cualquier derecho de acceso, rectificación, cancelación u oposición de datos personales, y en su caso el derecho de portabilidad, denominados derechos ARCO, se debe tomar en cuenta que solo el titular de los datos personales o en su caso su representante podrán ejercerlo, de la forma siguiente:

El procedimiento para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales (derechos ARCO) así como los datos de contacto de la Unidad de Transparencia del Conahcyt pueden consultarse en <https://conahcyt.mx/transparencia/acceso-ala-informacion/unidad-de-transparencia/>

La solicitud de ejercicio de derechos ARCO podrá presentarse en la Unidad de Transparencia del Conahcyt de manera física, a través del correo electrónico [ley\\_transparencia@conahcyt.mx](mailto:ley_transparencia@conahcyt.mx) o bien en la Plataforma Nacional de Transparencia en <http://www.plataformadetransparencia.org.mx>.

La solicitud de ejercicio de derechos ARCO deberá contener lo siguiente:

- Nombre del titular de los datos personales.
- Documentos que acrediten la identidad del titular.
- En su caso, nombre del representante del 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 quieren rectificar, cancelar u oponerse a su tratamiento.
- Descripción del derecho que se quiere ejercer o de lo que solicita el titular.
- En su caso, documentos o información que faciliten la localización de los datos personales, entre ella, el área responsable del tratamiento.

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

**Derecho de ACCESO:** la modalidad en la que prefiere que se reproduzcan los datos personales solicitados.

**Derecho de RECTIFICACIÓN:** las modificaciones que solicita que se realicen a los datos personales, así como aportar los documentos que sustenten la solicitud.

**Derecho de CANCELACIÓN:** las causas que motivan la petición de que se eliminen los datos de los archivos, registros o bases de datos del responsable del tratamiento.

**Derecho de OPOSICIÓN:** las causas o la situación que lo llevan a solicitar que finalice el tratamiento de sus datos personales, así como el daño o perjuicio que le causaría que dicho tratamiento continúe; o bien, deberá indicar las finalidades específicas respecto de las cuales desea ejercer este derecho.

Si la solicitud no cuenta con la información referida, se podrá solicitar la información faltante por medio de una prevención, la cual se deberá emitir en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud, y se tendrán 10 días hábiles, después de recibir la prevención, para proporcionar la información requerida, de lo contrario se tendrá como no presentada su solicitud.



Para acreditar la identidad del titular y en su caso, la de su representante, así como la personalidad de este último, en la solicitud se deberá anexar copia simple de una identificación oficial del titular de los datos personales, así como la de su representante en su caso.

Se podrá acreditar personalidad con identificaciones oficiales válidas:

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

La identidad de los menores de edad se podrá acreditar mediante:

- Acta de nacimiento
- Clave Única de Registro de Población
- Credenciales expedidas por instituciones educativas o instituciones de seguridad social
- Pasaporte
- Cualquier otro documento oficial utilizado para tal fin.

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

- Acta de nacimiento
- Clave Única de Registro de Población
- Pasaporte
- Cualquier otro documento o identificación oficial expedida para tal fin.

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

Si el representante es persona física

- La presentación de una carta poder simple suscrita ante dos testigos, anexando copia simple de sus identificaciones oficiales;
- Mediante instrumento público (documento suscrito por un Notario Público)
- Acudiendo usted y su representante a declarar en comparecencia ante el responsable.

La personalidad de un representante persona moral

- Mediante instrumento público.

La identidad del titular, así como la personalidad de su representante, deberá quedar debidamente acreditada 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.

Para solicitudes de ejercicio de derechos ARCO de datos personales de menores de edad:

Si los padres ejercen la patria potestad y son los que presentan la solicitud:

- Documento que acredite la identidad de menor.



- Acta de nacimiento del menor.
- Identificación oficial del padre o de la madre, que pretenda ejercer el derecho.
- Carta en la que se manifieste, bajo protesta de decir verdad, que el padre o la madre es quien ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

Si una persona distinta a los padres es quien ejerce la patria potestad, y es quien presenta la solicitud:

- Documento que acredite la identidad de menor.
- Acta de nacimiento del menor.
- Documento legal que acredite la posesión de la patria potestad.
- Identificación oficial de quien presenta la solicitud y posee la patria potestad.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la patria potestad del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la patria potestad.

Cuando un tutor es quien ejerce la patria potestad:

- Documento que acredite la identidad de menor.
- Acta de nacimiento del menor.
- Documento legal que acredite la tutela
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela del menor, y que no se encuentra dentro de alguno de los supuestos legales de suspensión o limitación de la tutela.

Para solicitudes de derechos ARCO de datos personales de personas en estado de interdicción o incapacidad legal:

- Documento que acredite la identidad del titular de los datos personales.
- Instrumento legal de designación del tutor.
- Identificación oficial del tutor.
- Carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de lo alguno de los supuestos legales de suspensión o limitación de la misma.

Para solicitudes de derechos ARCO de datos personales de personas fallecidas:

- Identificación oficial de la persona a quien pertenecían los datos personales.
- Acta de defunción correspondiente.
- Documento(s) que acrediten el interés jurídico de quien presenta la solicitud; aquél donde el titular de los datos personales hubiere expresado fehacientemente su voluntad de que esta persona ejerza los derechos ARCO con relación a sus datos personales, o el mandato judicial que en su caso exista para dicho efecto.
- Documento de identificación oficial de quien presenta la solicitud

El interés jurídico es aquel derecho subjetivo derivado de una ley que permite a una persona actuar a nombre de otra que por su situación le es imposible, a efecto de una solicitud de ejercicio de derechos ARCO, pueden alegarlo entre otros, el albacea, los herederos, los legatarios o cualquier persona que haya sido designada previamente por el titular para ejercer los derechos ARCO en su nombre, lo que se acreditará con copia simple del documento delegatorio, pasado ante la fe de notario público o suscrito ante dos testigos.



GOBIERNO DE  
MÉXICO



CONAHCYT  
CONSEJO NACIONAL DE HUMANIDADES  
CIENCIAS Y TECNOLOGÍAS

UNIDAD DE ASUNTOS JURÍDICOS  
UNIDAD DE TRANSPARENCIA

En el supuesto de que el titular sea un menor de edad, el interés jurídico se acreditará con la copia del acta de defunción, de las identificaciones del menor y de quien ejercía la patria potestad y/o tutela, así como una carta en la que el requirente manifieste, bajo protesta de decir verdad, que no se encontraba dentro de alguno de los supuestos legales de suspensión o limitación de la misma.

En el supuesto de que el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, el interés jurídico se acreditará con la copia de su acta de defunción, el documento de su identificación oficial y de quien ejercía la tutela, el instrumento legal de designación del tutor, así como carta en la que se manifieste, bajo protesta de decir verdad, que ejerce la tutela, y que no se encuentra dentro de lo alguno de los supuestos legales de suspensión o limitación de la misma.

En ambos supuestos, se deberá acompañar una carta en la cual se expresen los motivos por los cuales solicita el acceso, rectificación, cancelación u oposición de los datos de la persona fallecida. Una vez presentada la solicitud y que ésta cumplió con los requisitos, el Conahcyt, en un plazo de 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, deberá informarle si procede o no el ejercicio del derecho solicitado.

En caso de que haya procedido el ejercicio del derecho, deberá llevar a cabo las acciones necesarias para hacerlo efectivo, en un plazo de 15 días hábiles, contados a partir del día siguiente en el que le haya notificado la respuesta anterior. Los plazos antes señalados se pueden ampliar por un periodo igual, cuando esté justificado y se le informe de ello.

Los plazos se pueden ampliar por un periodo igual, cuando esté justificado y se le informe de ello.

El ejercicio de los derechos ARCO es gratuito, y sólo se realizarán cobros para recuperar los costos de reproducción, certificación o envío de información.

El solicitante podrá proporcionar un medio magnético, electrónico o el mecanismo necesario para la reproducción de sus datos personales, asimismo, la información deberá ser entregada sin costo cuando implique la entrega de no más de 20 hojas simples.

### **Derecho de Portabilidad**

En la solicitud de portabilidad de datos personales los requisitos son los siguientes:

Es posible solicitar una copia de sus datos personales en un formato estructurado y comúnmente utilizado, o bien, transmitir sus datos personales a un responsable receptor. La explicación general de la situación de emergencia en la que se encuentra el titular, a efecto de que los plazos de respuesta sobre la procedencia o improcedencia de su solicitud y en su caso, para hacer efectiva la portabilidad de sus datos personales sean menores.

La denominación del responsable receptor y el documento que acredite la relación jurídica entre el responsable y el titular; el cumplimiento de una disposición legal o el derecho que pretende ejercer, en caso de solicitar la transmisión de sus datos personales.

Si se solicita una copia de sus datos personales en un formato estructurado y comúnmente utilizado podrá acompañar a su solicitud el medio de almacenamiento para la elaboración de la copia correspondiente.

En caso de que usted no proporcione el medio de almacenamiento, podrá ser proporcionado por este Consejo con el costo razonable que esto implique.

El plazo que se tiene para que pueda presentar el medio de almacenamiento para la elaboración de la copia de sus datos personales en un formato estructurado y comúnmente utilizado, no podrá exceder de tres días contados

Av. Insurgentes Sur No. 1582, Col. Crédito Constructor, CP. 03940, Benito Juárez, Ciudad de México.  
Tel: (55) 5322 7700 [www.conahcyt.mx](http://www.conahcyt.mx)





a partir del día siguiente en que se le hubiere notificado la respuesta o el costo del medio de almacenamiento para la elaboración de la copia de los datos personales en un formato estructurado y comúnmente utilizado que, en su caso, corresponda, siempre y cuando usted no lo proporcione.

Se destaca que el artículo 11 de “Los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales”, señala que “en el aviso de privacidad integral a que se refiere el artículo 28 de la Ley General o los que correspondan en las legislaciones estatales en la materia, el responsable deberá informar al titular sobre la posibilidad que tiene de solicitar la portabilidad de sus datos personales y su alcance; los tipos o categorías de datos personales que técnicamente sean portables; el o los tipos de formatos estructurados y comúnmente utilizados disponibles para obtener o transmitir sus datos personales, así como los mecanismos, medios y procedimientos disponibles para que el titular pueda solicitar la portabilidad de sus datos personales”.

### XVIII. IMPLEMENTACIÓN DE MEJORAS

El artículo 72 de la LGPDPPSO, señala que, para el cumplimiento de las obligaciones previstas, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto:

- I. Elevar el nivel de protección de los datos personales;
- II. Armonizar el tratamiento de datos personales en un sector específico;
- III. Facilitar el ejercicio de los derechos ARCO por parte de los titulares;
- IV. Facilitar las transferencias de datos personales;
- V. Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales, y
- VI. Demostrar ante el Instituto o, en su caso, los Organismos garantes, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

### XIX. REVISIONES Y AUDITORÍAS

Con objeto de monitorear y revisar la eficacia y eficiencia del sistema de gestión en que se basa este Programa, se contará con un programa para llevar a cabo dos tipos de acciones:

- Auditorías y
- Revisiones administrativas.

El monitoreo de los tratamientos de datos personales es esencial para garantizar que el Conahcyt cumpla con las leyes de la materia de protección de datos personales y a efecto de supervisar el tratamiento de datos personales, se establece lo siguiente:

**Auditorías Internas:** El Conahcyt deberá llevar a cabo auditorías internas periódicas para evaluar la conformidad con las políticas internas y la ley de la materia, dichas auditorías abordarán aspectos como la seguridad de los datos, el consentimiento, la finalidad y otros principios clave.



GOBIERNO DE  
MÉXICO



CONAHCYT  
CONSEJO NACIONAL DE HUMANIDADES  
CIENCIAS Y TECNOLOGÍAS

UNIDAD DE ASUNTOS JURÍDICOS  
UNIDAD DE TRANSPARENCIA

**Evaluaciones de Impacto en la Privacidad:** Especialmente cuando el tratamiento de datos personales implica riesgos significativos para los derechos y libertades de los titulares, el Conahcyt podrá realizar evaluaciones de impacto.

**Registros de Actividades de Tratamiento:** Se mantendrán registros detallados de todas las actividades relacionadas con el tratamiento de datos personales. Estos registros pueden incluir detalles sobre la recopilación, el procesamiento y el almacenamiento de datos, así como el acceso y cualquier divulgación realizada.

- Revisar y realizar las actualizaciones correspondientes a los procesos que traen aparejado el tratamiento de datos personales.
- Actualizar los avisos de privacidad, para el caso de que cambien las finalidades, así como mantener actualizadas cada una de las funciones y obligaciones del personal que trata datos personales.
- Realizar evaluaciones, registrando cualquier cambio respecto de las amenazas o vulnerabilidades detectadas.
- Mantener actualizados los sistemas de datos personales, así como realizar las actualizaciones correspondientes respecto del análisis de riesgos y de brecha.

**Revisiones por Parte de Autoridades:** De conformidad con el artículo 151 de la LGPDPPSO, el Conahcyt podrá voluntariamente someterse a la realización de auditorías por parte del Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles implementados por el responsable, identificar sus deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan.