



Comisión Nacional del Agua

# PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES.

2022

Unidad de Transparencia  
1-6-2022

En pro





## PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES.

### ÍNDICE

	PÁGINA
1. INTRODUCCIÓN	1
2. OBJETIVO	2
3. ALCANCE	2
4. MARCO NORMATIVO	3
5. TÉRMINOS Y DEFINICIONES	3
6. ATRIBUCIONES Y OBLIGACIONES DE LAS UNIDADES ADMINISTRATIVAS	4
7. POLÍTICA PARA LA PROTECCIÓN DE DATOS PERSONALES	6
8. CUMPLIMIENTO DE LOS PRINCIPIOS Y OBLIGACIONES	7
8.1. Obligaciones Transversales	7
8.2. Principios	9
8.3. Otras Obligaciones	16
9. REVISIÓN Y AUDITORÍA	26
10. ACCIONES PARA LA MEJORA CONTINUA	29
11. SANCIONES	32
12. ANEXOS	
I. Política de Protección de Datos Personales en posesión de la Comisión Nacional del Agua.	
II. Observación de los principios y obligaciones.	
III. Documento de Seguridad.	
IV. Mecanismos Para Garantizar La Confidencialidad De Los Datos Personales	
V. Programa anual de Capacitación en materia de transparencia, acceso a la información y protección de datos personales.	
VI. Procedimiento de recepción y atención de Quejas y Denuncias que presenten los Titulares de Datos Personales.	
VII. Procedimiento de solicitud de consentimiento para el tratamiento de los Datos Personales.	





- VIII. Guía para el ejercicio de derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de Datos Personales
- IX. Mecanismos de Seguridad para la entrega de los Datos Personales
- X. Mecanismos de evaluación de calidad en la gestión de las solicitudes para el ejercicio de los Derechos ARCO
- XI. Programa de revisiones administrativas y auditorías 2022
- XII. Procedimiento para la gestión de las acciones preventivas y correctivas

En proceso de revisión del Comité de Transparencia





## 1. INTRODUCCIÓN

Un Sistema de Gestión es un conjunto de elementos que están interrelacionados o que interactúan para establecer políticas, objetivos y procesos, así como las actividades necesarias para lograr esos objetivos; en tal sentido, el Sistema para la Protección de Datos Personales es en esencia, el conjunto de estos elementos para garantizar la seguridad de dichos datos, durante todo el ciclo de vida en los tratamientos que se realizan.

Los elementos que integran el sistema de gestión son la estructura, los roles y responsabilidades, la planificación, procesos, políticas, objetivos, normas, así como el conocimiento y las actividades operativas para lograr esos objetivos en materia de protección de los Datos Personales.

La obligación de contar con un sistema de esta naturaleza se fundamenta en el artículo 34 de la Ley General de Protección de Datos personales en Posesión de Sujetos Obligados (LGPDPSO), el cual 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.

De igual manera, la estructura del sistema está definida en el artículo 65 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el cual indica que el sistema de gestión deberá permitir planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

De conformidad con lo anterior, el presente documento describe el *Sistema de Gestión de Seguridad de los Datos Personales en posesión de la Comisión Nacional del Agua*, y define el Programa para su implementación y mejora.

El Comité de Transparencia, en su carácter de autoridad máxima en materia de protección de datos personales de conformidad con el artículo 83, segundo párrafo y con las atribuciones conferidas por el artículo 84, fracción I, de la Ley General, establece el presente sistema como el mecanismo para coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales.



## 2. OBJETIVOS

El presente programa tiene como objetivos los siguientes:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión del sujeto obligado;
2. Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, así como la normatividad que derive de los mismos;
3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y
4. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en la organización, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

## 3. ALCANCE

El presente programa aplicará a todas las unidades administrativas de la Comisión Nacional del Agua a que refiere su Reglamento Interior y que realicen tratamiento de datos personales en ejercicio de sus atribuciones.

Asimismo, en virtud de que uno de los objetivos del Programa es cumplir con las obligaciones establecidas en la Ley General, se cubrirán todos los principios, deberes y obligaciones que establece dicha norma para los responsables del tratamiento.

Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 120 de la Ley General de Transparencia y Acceso a la Información Pública y numeral 117 de la Ley Federal de Transparencia y Acceso a la Información Pública,





## 4. MARCO NORMATIVO

- Artículos 6, Apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Lineamientos Generales de Protección de Datos Personales para el Sector Público
- Reglamento Interior de la Comisión Nacional del Agua.

## 5. TÉRMINOS Y DEFINICIONES

- **Áreas administrativas:** El segundo nivel que reporta a las Subdirecciones Generales y Coordinaciones Generales en el nivel central y en los Organismos de Cuenca y Direcciones Locales en el nivel regional hidrológico – administrativo de la Comisión Nacional del Agua.
- **CONAGUA:** Comisión Nacional del Agua.
- **INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- **Unidades Administrativas:** Las establecidas en el Reglamento Interior de la Comisión Nacional del Agua en el nivel central como los Organismos de Cuenca y Direcciones Locales en el nivel regional hidrológico – administrativo.
- **Ley General:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017.
- **Lineamientos Generales:** Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicada en el Diario Oficial de la Federación el 26 de enero de 2018.
- **Lineamientos para la Evaluación de Impacto:** Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, publicados en el Diario Oficial de la Federación el 23 de enero de 2018.
- **Lineamientos para la Portabilidad:** Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, publicado en el Diario Oficial de la Federación el 12 de febrero de 2018.



## 6. ATRIBUCIONES Y OBLIGACIONES DE LAS UNIDADES ADMINISTRATIVAS

Con fundamento en lo dispuesto por los artículos 83 y 84, fracción I de la Ley General y 47, segundo párrafo, y 48 de los Lineamientos Generales, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones con relación a este programa:

- I. Elaborar, aprobar, coordinar y supervisar el Programa, en conjunto con las áreas técnicas que estime necesario involucrar o consultar;
- II. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
- III. Dar a conocer el Programa al interior del sujeto obligado;
- IV. Coordinar la implementación del Programa en las unidades administrativas del sujeto obligado;
- V. Asesorar a las unidades administrativas en la implementación de este Programa, con el apoyo de la Unidad de Transparencia y las áreas técnicas que estime pertinente;
- VI. Presentar un informe anual al titular de la institución, en el que se describan las acciones realizadas para cumplir con lo dispuesto por este Programa;
- VII. Supervisar la correcta implementación del Programa;
- VIII. Elaborar, aprobar, coordinar y supervisar el programa anual de capacitación, en conjunto con las áreas técnicas que estime necesario involucrar o consultar, y
- IX. Las demás que de manera expresa señale el propio Programa.

El informe al que refiere la fracción VI anterior, deberá presentarse en las primeras dos semanas del mes de marzo de cada año y referirá al año inmediato anterior. Algunos de los elementos que pueden incluirse en el informe son:

- Estadística e información general sobre el cumplimiento de las obligaciones señaladas en el Programa de Protección de Datos Personales por parte de las unidades administrativas;
- Acciones realizadas por el Comité de Transparencia y la Unidad de Transparencia para cumplir con las obligaciones específicas que establece el Programa de Protección de Datos Personales, y
- Los resultados de las revisiones y auditorías.

Por su parte, en el ejercicio del presente Programa, la Unidad de Transparencia y las unidades administrativas, en esencia tendrán las siguientes funciones, además de sujetarse a lo indicado en el numeral VII.4:



### *Unidad de Transparencia*

- Proponer políticas y programas internos de protección de datos personales.
- Establecer un sistema de supervisión de vigilancia para comprobar el cumplimiento de las políticas en materia de datos personales.
- Resguardar la documentación del Sistema de Gestión de la Protección de Datos Personales y coordinar la elaboración del Documento de Seguridad.
- Documentar el Plan de Trabajo en materia de Protección de Datos Personales de la CONAGUA.

### *Unidades Administrativas*

- Observar los principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad y responsabilidad.
- Adoptar las medidas necesarias para mantener exactos, completos, pertinentes, correctos y actualizados los datos personales en su posesión.
- Mantener estricto control sobre los datos personales que obren en sus archivos, teniendo prohibido difundir o realizar un uso no autorizado de los datos personales, incluso finalizado el tratamiento.
- Documentar el cumplimiento del presente Programa en sus respectivos ámbitos de competencia.

Las unidades administrativas deberán realizar las acciones necesarias para cumplir con las obligaciones que establece este Programa, para lo cual deberán asignar los recursos materiales y humanos necesarios, y prever lo que se requiera en sus programas de trabajo.

Para ello, resulta fundamental que el Programa se conozca al interior del sujeto obligado, por lo que el Comité de Transparencia a través de la Unidad de Transparencia se encargará de difundirlo entre los servidores públicos.

Considerando lo anterior, y con la finalidad de alcanzar los objetivos planteados en el Sistema de Gestión, las políticas y directrices internas de protección de datos personales el Programa será **de observancia obligatoria para todos los servidores públicos de la Comisión Nacional del Agua que realicen el tratamiento de datos personales.**



## 7. POLÍTICA PARA LA PROTECCIÓN DE DATOS PERSONALES

El tratamiento de datos personales en la CONAGUA se deberá sujetar en todo momento a los principios y deberes dispuestos en la Ley General y en los Lineamientos Generales conforme a lo establecido en la “Política de protección de datos personales en posesión de la CONAGUA” (Anexo I), documento que establece de manera particular las pautas y criterios a las que se sujeta la protección de datos personales.

Es responsabilidad de las unidades administrativas el vigilar el estricto cumplimiento de los principios establecidos en el artículo 16 de la Ley General durante todo el **ciclo de vida de los datos personales**:

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

Durante las etapas que integran el ciclo de vida: **A) Obtención**; **B) Uso** (registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento divulgación, transferencia o disposición); y, **C) Eliminación**, se deberá guardar el debido respeto de los principios y los deberes previstos para el tratamiento de los datos personales.

Las Unidades Administrativas deberán asegurarse de observar los principios y deberes en cada una de las etapas conforme a lo siguiente:





Respecto de los deberes, el relativo a la **seguridad** implica que la CONAGUA debe establecer y mantener medidas de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión; mientras que en el de **confidencialidad**, se deben establecer controles para que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden la confidencialidad de éstos, obligación que subsistirá aún después de finalizar sus relaciones con éste Órgano Desconcentrado.

## 8. CUMPLIMIENTO DE LOS PRINCIPIOS Y OBLIGACIONES

A efecto de facilitar la comprensión de los principios y deberes en materia de protección de datos personales, en anexo se presenta la relación “*Observación de los principios y obligaciones*” (Anexo II), en la que se abordarán bajo los aspectos siguientes:

### 8.1. Obligaciones Transversales

#### **Deber de Seguridad**

##### **Obligación:**

Implementar medidas de seguridad físicas, técnicas y administrativas necesarias para proteger los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no autorizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales, mismas que se encuentran contenidas en el *Documento de Seguridad (Anexo III)* y se consideran parte integral del presente Sistema de Gestión e incluye los mecanismos a operar por las unidades administrativas para garantizar la confidencialidad<sup>1</sup>, integridad<sup>2</sup>, accesibilidad<sup>3</sup> y autenticidad<sup>4</sup> de los datos personales; así como para el monitoreo, revisión y auditoría por parte del Comité de Transparencia a través de la Unidad de Transparencia.

<sup>1</sup> **Confidencialidad:** Estado de disponibilidad de información solo para usuarios, procesos y dispositivos autorizados.

<sup>2</sup> **Integridad:** Ausencia de alteraciones no autorizadas, información agregada o destruida (La información debe estar protegida contra el borrado mediante métodos que aseguran la confidencialidad, la copia de seguridad, y la ausencia de distorsión).

<sup>3</sup> **Accesibilidad:** Provisión de acceso oportuno y confiable a la información y los servicios de información.

<sup>4</sup> **Autenticidad:** Capacidad de identificar de forma exclusiva al autor / fuente de información.



### **Cumplimiento:**

- Implementar las medidas de seguridad que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado; las cuales podrán ser de carácter administrativo, físico y técnico.
- Garantizar la confidencialidad, integridad y disponibilidad de los datos personales, e impedir que el tratamiento respectivo contravenga las disposiciones del marco normativo en la materia.
- Ante cualquier modificación de las medidas de seguridad establecidas, las unidades administrativas competentes deberán dar aviso al Comité de Transparencia, a fin de instruir las modificaciones pertinentes al Documento de Seguridad.
- Asegurar que los servidores públicos involucrados en el tratamiento conozcan el Programa, así como las consecuencias de su incumplimiento.

**Responsables:** Unidades administrativas que realicen el tratamiento de datos personales, Gerencia de Tecnología de la Información y Comunicaciones, Gerencia de Recursos Materiales (en términos de lo indicado en el Documento de Seguridad), y el Comité de Transparencia.

**Fundamento:** Artículos 31, 32, 33, 34, 35 y 36 de la Ley General y 55 al 65 de los Lineamientos Generales.

### **Deber de Confidencialidad**

#### **Obligación:**

Establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales guarden el debido sigilo, obligación que subsistirá aún después de finalizar sus relaciones con el mismo y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Los mecanismos administrativos se encuentran contenidos en el documento denominado "*Mecanismos Para Garantizar La Confidencialidad De Los Datos Personales*" (Anexo IV).

#### **Cumplimiento:**

- Implementar controles y medidas de seguridad que garanticen el sigilo y la protección de los datos personales.
- En caso de elaborar un contrato, establecer cláusulas que obliguen a la confidencialidad de los datos personales a los terceros que intervengan en su tratamiento.



**Responsables:** Unidades administrativas que realicen el tratamiento de datos personales y que suscriban contratos con los encargados; Gerencia de Tecnología de la Información y Comunicaciones, Gerencia de Recursos Materiales (en términos de lo indicado en el Documento de Seguridad); Subdirecciones Generales de Administración y Jurídica.

**Fundamento:** Artículo 42 de la Ley General y 71 de los Lineamientos Generales.

## 8.2. Principios

### ***Principio de Responsabilidad***

#### **Obligación:**

Autorizar y destinar recursos para instrumentación de programas y políticas de protección de datos personales exigibles al interior de la organización; así como diseñar, desarrollar e implementar procedimientos para atender solicitudes, dudas y quejas de los titulares; políticas públicas, programas, servicios, sistemas o cualquier otra tecnología que implique el tratamiento de datos personales, así como un programa de capacitación.

Las políticas y programas estarán sujetos a revisión para determinar las modificaciones que se requieran, así como supervisar y vigilar su cumplimiento.

Se deberán Implementar las medidas apropiadas para garantizar que las políticas, programas, servicios, sistemas o plataformas informáticas, cumplan por defecto con las obligaciones, y que se traten los datos personales estrictamente necesarios para los fines del tratamiento.

En materia de capacitación, el *"Programa anual de Capacitación en materia de transparencia, acceso a la información y protección de datos personales"* (Anexo V), mismo que considera los roles y responsabilidades asignadas para su tratamiento y seguridad de los datos personales y está sujeto a evaluación de su eficiencia y eficacia.

El programa anual que considera los siguientes niveles:

- a) Concienciación: de corto plazo para la difusión de la protección de datos personales;
- b) Entrenamiento: capacitación de mediano plazo dirigida al personal de acuerdo a sus funciones y responsabilidad, y





- c) Educación: de largo plazo para incluir la protección de los datos personales en la cultura organizacional.

Entre los mecanismos que deben adoptarse para cumplir con el principio de responsabilidad, se encuentra la implementación de un “*Procedimiento de recepción y atención de Quejas y Denuncias que presenten los Titulares de Datos Personales*” (Anexo VI).

En el ejercicio de los derechos ARCO, las respuestas a los titulares de los Datos Personales, deberán incluir los datos de contacto a través de los cuales podrán comunicarse ante dudas, cuestionamientos y quejas.

El cumplimiento de los principios, deberes y obligaciones deberá estar debidamente documentado.

#### **Cumplimiento:**

- Prever presupuesto para la instrumentación del programa de protección de datos personales.
- Elaborar un programa de protección de datos personales.
- Elaborar y aplicar un programa de capacitación y actualización de los servidores públicos en materia de protección de datos personales.
- Establecer un sistema de supervisión y vigilancia para comprobar el cumplimiento del Programa, incluyendo las medidas de seguridad, con un periodo de revisión de cada dos años como máximo.
- Establecer un procedimiento para atender dudas y quejas de los titulares.
- Diseñar o modificar las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de forma tal que prevean la privacidad por diseño y por defecto.
- Documentar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables.

**Responsables:** Subdirección General de Administración; Comité de Transparencia; Unidad de Transparencia; Gerencia de Tecnología de la Información y Comunicaciones; Unidades administrativas.

**Fundamento:** Artículos 29 y 30 de la LGPDPPSO y 46 al 54 de los Lineamientos Generales.



## ***Principio de Licitud***

### **Obligación:**

Sujetar la solicitud y recepción de los datos personales para su tratamiento a las atribuciones o facultades previstas en el Reglamento Interior de la Comisión Nacional del Agua y demás disposiciones jurídicas nacionales o internacionales que rigen su actuar.

### **Cumplimiento:**

- Identificar la disposición normativa que faculta a la instancia para realizar el tratamiento de los datos personales, considerando cada una de sus finalidades.
- El aviso de privacidad respectivo deberá incluir de manera precisa el fundamento legal que faculte a la instancia para llevar a cabo el tratamiento correspondiente.

**Responsables:** Unidades administrativas que se alleguen de datos personales para realizar su tratamiento, en el ámbito de sus respectivas competencias.

**Fundamento:** Artículo 17 de la Ley General, 8 de los Lineamientos Generales

## ***Principio de Lealtad***

### **Obligación:**

No obtener ni tratar datos personales a través de medios engañosos y fraudulentos (Uso con dolo, mala fe o negligencia).

Privilegiar la expectativa razonable de privacidad de los titulares evitando dar lugar a discriminación, trato injusto o arbitrario en su contra.

### **Cumplimiento:**

- Llevar a cabo el tratamiento de los datos personales únicamente para los fines comunicados al titular en el Aviso de Privacidad y evitar su obtención con dolo, mala fe o negligencia
- Elaborar los Avisos de Privacidad de conformidad con lo previsto en la Ley General y Lineamientos Generales y asegurar que su contenido es fiel a la realidad del tratamiento de los datos personales.
- Verificar que el tratamiento de los datos personales no provoque a su titular discriminación, un trato injusto o arbitrario en su contra.



**Responsables:** Unidades administrativas que realicen el tratamiento de datos personales.

**Fundamento:** Artículo 19 de la Ley General y 11 de los Lineamientos Generales.

### **Principio de Información**

#### **Obligación:**

A través del respeto al principio de información, los titulares deberán de conocer las características principales del tratamiento al que serán sometidos sus datos personales.

Tal conocimiento se concreta a través de la puesta a disposición del aviso de privacidad, que constituye el medio por el que los responsables de los datos personales hacen saber a los particulares la finalidad para la cual se recaba su información.

#### **Cumplimiento:**

- Previo a la obtención o recepción de los datos personales, poner a disposición del titular el aviso de privacidad.

**Responsables:** Unidades administrativas que tengan obligación de emitir el aviso de privacidad.

**Fundamento:** Artículos 3, fracción II, 26, 27, 28 y 29 de la Ley General y 26 a 45 de los Lineamientos Generales.

### **Medidas Compensatorias**

#### **Obligación:**

Instrumentar medidas compensatorias cuando resulte imposible dar a conocer al titular el aviso de privacidad simplificado de manera directa, o ello exija esfuerzos desproporcionados.

#### **Cumplimiento:**

- Cuando resulte imposible dar a conocer al titular el aviso de privacidad de manera directa, o ello exija esfuerzos desproporcionados dar a conocer el aviso de privacidad simplificado a través de la implementación de medidas compensatorias, previa evaluación de la autorización expresa del INAI.



**Fundamento:** Artículo 26 de la LGPDPSO y Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal.

## **Principio de Consentimiento**

### **Obligación:**

Al obtener los datos personales para realizar su tratamiento, las Unidades Administrativas deberán contar con el consentimiento de del titular (salvo que se actualice alguno de los supuestos previstos en el artículo 22 de la Ley General).

El consentimiento que se obtenga deberá ser libre, específico e informado ser concisa e inteligible. La solicitud del consentimiento deberá estar redactada en un lenguaje claro y sencillo acorde con el perfil del titular (de conformidad con lo dispuesto en el artículo 20 de dicha Ley General).

El consentimiento podrá manifestarse de forma tácita o expresa, ya sea que se obtengan de manera directa o indirecta del titular (observando lo establecido en el artículo 21 de la Ley General y los artículos 12 al 20 de los Lineamientos).

Atender las solicitudes de revocación a través del ejercicio de los derechos de oposición y cancelación.

El consentimiento podrá ser recabado de conformidad con lo establecido para esos efectos en el "*Procedimiento de solicitud de consentimiento para el tratamiento de datos personales*", que constituye el *Anexo VII* de este documento.

### **Cumplimiento:**

- Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.
- 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.
- Redactar las solicitudes de consentimiento en un lenguaje claro y sencillo acorde con el perfil del titular, de tal manera que sea libre, específico e informado.
- Habilitar los mecanismos necesarios para solicitar el consentimiento expreso, en los términos señalados en la columna anterior, así como documentar su obtención.



- Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.
- 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 no se obtengan directamente del titular, enviar al titular o su representante legal el aviso de privacidad.
- Prever en el Procedimiento para la atención de solicitudes de derechos ARCO lo relativo a la revocación del consentimiento.

**Responsables:** Unidades administrativas que realicen el tratamiento de datos personales.

**Fundamento:** Artículos 20, 21 y 22 de la Ley General y 12 al 20 de los Lineamientos Generales.

### ***Principio de Proporcionalidad***

#### **Obligación:**

Realizar el tratamiento de los datos personales sólo cuando resulten adecuados, relevantes y necesarios para la finalidad que los justifica.

Limitar los datos personales tratados al mínimo necesario, respecto de las finalidades que motivaron su tratamiento.

#### **Cumplimiento:**

- Las unidades administrativas deberán identificar los datos personales que se requieren para cada una de las finalidades del tratamiento.
- Analizar y revisar que se soliciten únicamente aquellos que resultan indispensables para las finalidades del tratamiento.
- Cuando la normatividad establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad, solo deberán solicitarse dichos datos.
- Los datos personales requeridos deberán ser los mínimos posibles para lograr las finalidades para las cuales se obtuvieron.

**Responsables:** Unidades administrativas que realicen el tratamiento de datos personales.

**Fundamento:** Artículo 25 de la Ley General y 24 y 25 de los Lineamientos Generales.

### ***Principio de Finalidad***



### **Obligación:**

Todo tratamiento de datos personales debe estar justificado en razón de finalidades concretas, lícitas, explícitas y legítimas (conforme al artículo 10 de los Lineamientos Generales):

Las finalidades deben ser acordes con las atribuciones normativas de la unidad administrativa que realice el tratamiento.

El tratamiento para finalidades distintas a las que motivaron el tratamiento original, requiere la valoración de los elementos indicados en el Artículo 10 de los Lineamientos Generales.

### **Cumplimiento:**

- Identificar las finalidades de cada tratamiento, y verificar que las mismas atiendan a fines específicos o determinados, y que sean acordes a las atribuciones de la unidad administrativa.
- Verificar que en los avisos de privacidad se informan de manera clara todas las finalidades del tratamiento e identificar aquellas que requieren consentimiento.
- Identificar el marco normativo que otorga las atribuciones a la unidad administrativa para el tratamiento.
- Cuando aplique, identificar las finalidades distintas a las informadas en el aviso de privacidad que se requieran llevar a cabo y asegurarse de que se cuenta con atribuciones legales para ello.
- Gestionar la emisión de un nuevo aviso de privacidad que incluya, en su caso, la solicitud del consentimiento de los titulares para el tratamiento para las finalidades adicionales.

**Responsables:** Unidades administrativas que realicen el tratamiento de datos personales.

**Fundamento:** Artículo 18 de la Ley General y, 9, 10 y 44, fracción III, de los Lineamientos Generales.

### **Principio de Calidad**

#### **Obligación:**

Las unidades administrativas deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales (en términos de los



descrito en los artículos 21 y 22 de los Lineamientos Generales), principalmente cuando se obtuvieron de manera indirecta del titular.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

### **Cumplimiento:**

- Las Unidades Administrativas deberán implementar acciones y medidas que estimen necesarias y que tengan como objetivo que los datos personales se actualicen y, en su caso, corrijan o completen, independientemente del medio en que se encuentren contenidos.
- Estas medidas deberán permitir que la modificación de los datos personales sea inmediata, una vez que se tenga conocimiento de la actualización o corrección a que haya lugar.
- Documentar la conservación y en su caso, supresión de los datos personales conforme a los procedimientos establecidos.

**Responsables:** Unidades administrativas que realicen el tratamiento de datos personales; Área coordinadora de archivos y Gerencia de Tecnología de la Información y Comunicaciones.

**Fundamento:** Artículos 23 y 24 de la Ley General, y 21 y 22 de los Lineamientos Generales.

## **8.3. Otras Obligaciones**

### **Transferencias**

#### **Obligación:**

Las transferencias de datos personales<sup>5</sup>, entendidas como todo traslado de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de: a) su titular, b) la CONAGUA, o c) los encargados contratados por ésta<sup>6</sup>, implican las siguientes

<sup>5</sup> **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

<sup>6</sup> **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.



obligaciones para las unidades administrativas en el ejercicio de sus funciones, las cuales deberán observar.

Formalizar las transferencias nacionales e internacionales mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, que permita demostrar el alcance del tratamiento de los datos personales.

Asegurar que en las transferencias fuera del territorio nacional se obligue al tercero receptor a proteger los datos personales conforme a la Ley General.

Comunicar el aviso de privacidad respectivo.

Solicitar el consentimiento para las transferencias (salvo en los casos indicados en el artículo 22 de la Ley General).

Asegurarse de tratar los datos que hayan sido transferidos al responsable para las finalidades para las cuales le hayan sido comunicados, según lo establecido en el aviso de privacidad proporcionado, así como garantizar la confidencialidad de los datos personales.

### **Cumplimiento:**

- Identificar las transferencias que se realizan que requieren la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico.
- Elaborar y suscribir las cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, cuando se requiera.
- Para las transferencias y remisiones internacionales, previo a que éstas ocurran, se deberá solicitar al tercero receptor que manifieste por escrito que se obliga a proteger los datos personales conforme a los principios y deberes que establece la Ley General.
- Comunicar el aviso de privacidad correspondiente (En la primera transferencia y en lo sucesivo, sólo las modificaciones al aviso de privacidad original, cuando existan).
- Atender lo relativo a los deberes de seguridad y confidencialidad, así como el principio de consentimiento y finalidad.

**Responsables:** Todas las unidades administrativas que realicen transferencias: Subdirección General Jurídica, en lo relativo a la elaboración y suscripción de las cláusulas contractuales, convenios de colaboración u otros instrumentos jurídicos.

**Fundamento:** Artículos 66, 67, 68, 69 y 70 de la Ley General y 113 a 118 de los Lineamientos Generales.





## **Relación con los Encargados**

### **Obligación:**

Cuando una persona física o jurídica, pública o privada, en calidad de *encargado*<sup>7</sup>, trate datos personales a nombre y por cuenta de la CONAGUA, incluida la *remisión de datos personales*<sup>8</sup>, se deberá:

- Formalizar la relación mediante contrato o instrumento jurídico, que permita acreditar su existencia, alcance y contenido.
- El contrato o instrumento jurídico, deberá al menos, contener las obligaciones indicadas en la Ley General y los Lineamientos Generales.
- Autorizar las subcontrataciones que realicen los encargados y que involucren el tratamiento de datos personales.
- Informar al encargado que el contrato o el instrumento jurídico mediante el cual se formalice la subcontratación deberá incluir cláusulas con las obligaciones antes señaladas.

### **Cumplimiento:**

- Formalizar las relaciones con los encargados mediante contrato o instrumento jurídico, que contenga las obligaciones y cláusulas de confidencialidad.
- Incluir en los contratos con los encargados la procedencia (autorizar, prohibir o bien, se podrá establecer que para la subcontratación será necesario que el encargado solicite autorización expresa al responsable, caso por caso.) en caso de que el encargado desee subcontratar servicios que involucren el tratamiento de datos personales.

**Responsables:** Subdirección General de Administración, Subdirección General Jurídica, y unidades administrativas requirentes.

**Fundamento:** Artículos 59 y 61 de la LGPDPPSO y 108 a 110 de los Lineamientos Generales.

## **Cómputo en la Nube**

### **Obligación:**

<sup>7</sup> **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.

<sup>8</sup> **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.



Cómputo en la nube<sup>9</sup>, se refiere a un modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales en recursos compartidos dinámicamente.

En caso de que la CONAGUA contrate dichos servicios, deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

En el supuesto de que la CONAGUA se adhiera a dichos servicios mediante condiciones o cláusulas generales de contratación, deberá:

- Contratar con proveedores que garanticen políticas y la debida protección de datos personales conforme a los principios y deberes establecidos en la Ley.
- Delimitar el tratamiento a través de cláusulas contractuales u otros instrumentos jurídicos.
- Contratar sólo servicios que cumplan, al menos, con las obligaciones y mecanismos establecidos en el artículo 64 de la Ley General

Cuando se tenga la posibilidad de convenir con el proveedor las condiciones y términos del servicio, se deberá incluir en el contrato o instrumento jurídico las obligaciones generales de cualquier encargado.

**En ningún caso**, la CONAGUA podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la Ley General, Lineamientos Generales y demás disposiciones que resulten aplicables en la materia.

### Cumplimiento:

- Verificar las cláusulas contractuales antes de la contratación, con objeto de garantizar que el servicio cumpla con los requisitos que establece la Ley General.
- Sólo contratar servicios de cómputo en la nube que garanticen dichos requisitos.
- En caso de que los contratos se hayan celebrado antes de la entrada en vigor de la Ley General, será necesario realizar su modificación o renovación.
- En su caso, incluir en el contrato o instrumento jurídico que formalice la contratación de los servicios, las obligaciones generales de cualquier encargado.

<sup>9</sup> **Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.



**Responsables:** Gerencia de Tecnología de la Información y Comunicaciones.  
Subdirección General de Administración y Subdirección General Jurídica.

**Fundamento:** Artículos 63 y 64 de la LGPDPPSO y 110 y 111 de los Lineamientos Generales.

## **Atención de Solicitudes de Ejercicio de Derechos ARCO**

### **Obligación:**

Los titulares de los datos personales, de conformidad con la Ley General y los Lineamientos Generales, cuentan con la prerrogativa de ejercer los siguientes derechos ARCO<sup>10</sup>.

- Acceso<sup>11</sup>.
- Rectificación<sup>12</sup>.
- Cancelación<sup>13</sup>.
- Oposición<sup>14</sup>.

Para la gestión de las solicitudes, la CONAGUA deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO.

El procedimiento deberá considerar las obligaciones relativas a la orientación a los titulares, los tramites y plazos internos, los medios habilitados para atender las solicitudes para el ejercicio de los derechos, los formatos, sistemas y otros métodos, incluyendo los destinados a las personas con algún tipo de discapacidad o grupos vulnerables.

El trámite de las solicitudes de ejercicio de los derechos referidos (derechos ARCO), será substanciado por la Unidad de Transparencia, de acuerdo con la "Guía para el ejercicio de derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de Datos Personales", que constituye el Anexo VIII de este documento.

<sup>10</sup> Ejercicio de Derechos ARCO: De conformidad con lo establecido en la fracción XI, de la Ley General.

<sup>11</sup> **Acceso:** es el derecho que tiene el titular de solicitar el acceso a sus datos personales que están en las bases de datos, sistemas, archivos, registros o expedientes del responsable que los posee, almacena o utiliza, así como de conocer información relacionada con el uso que se da a los datos personales.

<sup>12</sup> **Rectificación:** es el derecho que tiene el titular de solicitar la rectificación o corrección de sus datos personales, cuando éstos sean inexactos o incompletos o no se encuentren actualizados. En ese sentido, puede solicitar a quien posea o utilice sus datos personales que los corrija cuando los mismos sean incorrectos, estén desactualizados o inexactos.

<sup>13</sup> **Cancelación:** es el derecho que tiene el titular de solicitar que sus datos personales se eliminen de los archivos, registros, expedientes, sistemas, bases de datos del responsable que los posee, almacena o utiliza, cuando ello resulte procedente.

<sup>14</sup> **Oposición:** es el derecho que tiene el titular de solicitar que sus datos personales no se utilicen para ciertos fines, o de requerir que se concluya el uso de los mismos a fin de evitar un daño a su persona, cuando ello resulte procedente.



Documentar el ejercicio de los derechos ARCO, incluyendo la acreditación de la identidad, la atención a menores de edad y personas en estado de interdicción o incapacidad, o las relativas al ejercicio del derecho relativas a personas fallecidas conforme a los “**Mecanismos de Seguridad para la entrega de los Datos Personales**” (Anexo IX).

Acreditar el pago de los costos de reproducción y envío y, en su caso, las constancias que acrediten: la rectificación de los datos personales, la cancelación y/o el cese el tratamiento de datos personales.

Para efectos de la mejora de la atención al ejercicio de los derechos ARCO, la CONAGUA cuenta con instrumentos para la evaluación de la calidad de las respuestas conforme a los “*Mecanismos de evaluación de calidad en la gestión de las solicitudes para el ejercicio de los Derechos ARCO*” (Anexo X).

#### **Cumplimiento:**

- Establecer procedimientos internos para la atención de solicitudes de derechos ARCO conforme a lo previsto por la Ley General y los Lineamientos Generales.
- Establecer medios para que los titulares presenten sus solicitudes de ejercicio de derechos ARCO, que sean de fácil acceso.
- Elaborar formularios, sistemas y otros métodos simplificados para facilitar el ejercicio de los derechos ARCO, o utilizar los elaborados por el INAI.
- Prever las medidas pertinentes para que las personas con algún tipo de discapacidad o grupos vulnerables, incluyendo aquellos que pertenecen a grupos indígenas y con discapacidad visual, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.
- Documentar el ejercicio de los derechos ARCO conforme al procedimiento, incluyendo lo relativo a la acreditación de la identidad, el trámite en caso de tratarse de menores de edad y personas en estado de interdicción o incapacidad, o personas fallecidas.
- Prever la acreditación del pago de los costos de reproducción y envío correspondientes, en su caso, las constancias que acrediten: la rectificación de los datos personales, la cancelación y/o el cese el tratamiento de datos personales.

**Responsables:** Comité de Transparencia; Unidad de Transparencia; Unidades Administrativas que atiendan solicitudes de ejercicio de Derechos ARCO

**Fundamento:** Artículo 43 al 56, 85 y 86 de la Ley General y 73 al 107 de los Lineamientos Generales.



## **Portabilidad**

### **Obligación:**

Otorgar al titular una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos, cuando los mismos se traten en un formato con tales características.

### **Cumplimiento:**

- Atender las solicitudes del ejercicio del derecho de portabilidad según los criterios y parámetros establecidos por la Ley General y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, publicados en el Diario Oficial de la Federación el 12 de febrero de 2018.

**Responsables:** Unidad de Transparencia y unidades administrativas responsables de atender las solicitudes de ejercicio de derechos ARCO.

**Fundamento:** Artículo 57 de la LGPDPSO y en general los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

## **Supresión de los Datos Personales**

### **Obligación:**

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya su plazo de conservación.

El **bloqueo de los datos personales** (identificación y conservación de los datos una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con el periodo de su tratamiento, hasta que concluya el plazo de vigencia documental o en su caso, de prescripción legal), deberá corresponder a los periodos máximos de vigencia documental<sup>15</sup>, o en su caso, a los plazos

<sup>15</sup> **Vigencia documental:** Periodo durante el cual un documento de archivo mantiene sus valores administrativos, legales, fiscales o contables, de conformidad con las disposiciones jurídicas vigentes y aplicables.



de conservación<sup>16</sup>; periodo en el que, los datos personales no podrán ser objeto de tratamiento.

Una vez transcurrido el bloqueo de los datos personales procederá conforme a lo siguiente:

- Eliminar, los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades y una vez que concluya su plazo de conservación establecido, de conformidad con el procedimiento de baja archivística que la Subdirección General de Administración prevea para dicho propósito.

Cada Unidad Administrativa deberá mantener identificado el ciclo de vida de los datos personales y el periodo de bloqueo de la totalidad de los tratamientos que efectúen en ejercicio de sus funciones.

- Establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales de los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales en los que se atiendan los atributos de:
  - I. Irreversibilidad,
  - II. Seguridad y confidencialidad, y
  - III. Favorable al medio ambiente

### Cumplimiento:

- Identificar los plazos de conservación de las series documentales que contienen datos personales
- Incluir la etapa de bloqueo de los datos personales en el plazo de conservación y en el procedimiento de archivos.
- Desarrollar políticas, métodos y técnicas para la supresión definitiva de los datos personales, considerando los atributos de irreversibilidad; seguridad y confidencialidad y favorable al medio ambiente.
- Una vez concluido el plazo de conservación respectivo, proceder a la eliminación de los documentos correspondientes a dichas series documentales y documentar dicha eliminación.

**Responsables:** Área coordinadora de archivos, Gerencia de Tecnología de la Información y Comunicaciones y unidades administrativas que procedan a la supresión.

**Fundamento:** Artículo 23 de la Ley General y 23 de los Lineamientos Generales.

<sup>16</sup> **Plazo de conservación:** Al periodo de guarda de la documentación en los archivos de trámite y concentración, que consiste en la combinación de la vigencia documental y, en su caso, el término precautorio y periodo de reserva que se establezcan de conformidad con la normatividad aplicable.



## ***Evaluación de impacto en la Protección de Datos Personales***

### **Obligación:**

**Cuando se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio implique el tratamiento intensivo o relevante de datos personales**, se deberá realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el INAI, quien podrá emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

Se estará en presencia de un tratamiento intensivo o relevante de datos personales cuando ocurra alguna de las condiciones siguientes:

- a. Existan riesgos inherentes a los datos personales a tratar.
- b. Se traten datos personales sensibles.
- c. Se efectúen o pretendan efectuar transferencias de datos personales.

Las Unidades Administrativas que pretendan implementar o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio implique el tratamiento intensivo o relevante de datos personales, procederán conforme a lo siguiente:

- Remitir al Comité de Transparencia, 45 días hábiles previos a la fecha en que se considere poner en operación, informe que dé cuenta de los aspectos siguientes:
  - ✓ La descripción de la política, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretenda poner en operación o modificar.
  - ✓ La justificación de la necesidad de tal implementación o modificación.
  - ✓ La representación del ciclo de vida de los datos personales a tratar.
  - ✓ La identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales.
  - ✓ El análisis de cumplimiento normativo en materia de protección de datos personales de conformidad con la Ley General y la normativa aplicable.
  - ✓ Cualquier otra información o documentos que se considere conveniente.

El Comité, a través de la Unidad de Transparencia, analizará que el tratamiento de datos personales efectivamente actualice los supuestos de un tratamiento intensivo o relevante



en términos de lo previsto en la Ley General y los Lineamientos para la Evaluación de Impacto, lo que deberá hacer del conocimiento del Comité de Transparencia.

Al estar ante la presencia de un tratamiento intensivo o relevante de datos personales, la Unidad administrativa con el apoyo de la Gerencia de Tecnología de la Información y Comunicaciones y deberá:

- Realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el INAI.
- Atender el plazo de treinta días hábiles previos a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, para presentar la evaluación de impacto ante el INAI.

#### **Cumplimiento:**

Desarrollar el procedimiento para la evaluación de impacto en la protección de datos personales que prevea:

- Los elementos para detectar los casos en que se requiera la realización de la Evaluación de Impacto en la Protección de Datos Personales.
- Los mecanismos para la elaboración y presentación de las evaluaciones.
- Los medios para la atención de las observaciones que, en su caso, emita el INAI.

Documentar el proceso de presentación en tiempo y forma de las Evaluaciones que se requieran ante el INAI.

**Responsables:** Comité de Transparencia; Unidad de Transparencia; Gerencia de Tecnología de la Información y Comunicaciones

**Fundamento:** Artículos 74, 75, 77, 78 y 79 de la LGPDPPSO y 120 de los Lineamientos Generales. Tomando en consideración lo dispuesto en los artículos 75 y 79 de la LGPDPPP y 120 de los Lineamientos Generales.





## 9. REVISIÓN Y AUDITORÍA

Con objeto de monitorear y revisar la eficacia y eficiencia del sistema de gestión en que se basa este Programa, y de conformidad con lo dispuesto en los artículos 33, fracción VII, de la Ley General y 63 de los Lineamientos Generales, las disposiciones contenidas en el presente programa, de observancia obligatoria para las unidades administrativas, serán supervisadas, monitoreadas y revisadas a través de los siguientes mecanismos:

### 1) Auditorías.

De carácter interno a realizarse con el apoyo de las unidades administrativas relacionadas con el cumplimiento de las obligaciones de seguridad y confidencialidad, o externo a realizarse por auditores externos (sujeto a disponibilidad de presupuesto y la importancia del caso), o a través de auditorías voluntarias, realizadas por el INAI de conformidad con el artículo 151 de la LGPDPSO.

En el desarrollo de las auditorías se deberán incluir la revisión del cumplimiento de las obligaciones que tiene el Comité de Transparencia en cuanto a la aplicación de este Programa; evaluar su conformidad; incluir, cuando sea posible, cifras, indicadores y estadísticas relacionadas con los procedimientos a revisar, y emitir recomendaciones respecto del cumplimiento del Programa.

Las auditorías podrán ser integrales o parciales cuando resulten necesarias para supervisar y monitorear el cumplimiento de obligaciones específicas en tratamientos particulares.

Como resultado de las auditorías se deberá obtener el nivel de madurez de la CONAGUA en la protección de datos personales en su posesión, a fin de tenerlo como referencia y línea base para la mejora continua

En el caso de auditorías externas, el Comité de Transparencia deberá asegurar la objetividad e imparcialidad del auditor y el programa propuesto.

### 2) Revisiones administrativas.

A realizarse por el Comité de Transparencia con el apoyo de la Unidad de Transparencia y de las unidades administrativas relacionadas con el cumplimiento de las obligaciones de seguridad y confidencialidad.



Las revisiones administrativas deberán estar documentadas, y tendrán como objetivo supervisar

- a) el adecuado desarrollo y efectividad del Programa, y/o,
- b) el debido tratamiento en los cambios que afecten aspectos significativos en la protección de datos personales, como nueva normatividad, tecnología, o procesos o procedimientos.

La programación y ejecución de las revisiones administrativas y auditorías deberán estar debidamente documentada y se tomará en cuenta lo siguiente:

- La retroalimentación por parte de las unidades administrativas;
- Los riesgos identificados en el análisis de riesgos;
- Los resultados de auditorías;
- Los resultados de las revisiones anteriores;
- Las actualizaciones o cambios en la tecnología, normatividad y procesos aplicables e implementados;
- Los requerimientos por parte de autoridades;
- Las quejas, y
- Las vulneraciones de seguridad.

El Comité de Transparencia con el apoyo de la Unidad de Transparencia desarrolla el “Programa de revisiones administrativas y auditorías 2022” (Anexo XI), el cual ha sido aprobado por dicho Comité y que integra las acciones a realizar para verificar y evaluar el funcionamiento del Sistema de Gestión de la Protección de Datos Personales de la CONAGUA, y que contribuirá a identificar oportunidades de mejora en la efectividad y eficacia del Programa.

### **Acciones para la mejora continua del Programa**

En esta fase del Programa, se adoptarán las medidas preventivas y correctivas que hayan resultado de las auditorías y revisiones realizadas, o bien que se hayan obtenido de otras fuentes de información relevantes.

Los puntos de mejora de la implementación del Programa pueden ser de dos tipos:

**1. Acciones preventivas:** aquéllas encaminadas a evitar cualquier “no conformidad” (no cumplimiento) con relación a lo establecido en este Programa.

En las acciones preventivas se pueden incluir las siguientes actividades:

- El análisis y revisión de las posibles causas de no conformidad;

Avenida Insurgentes Sur número 2416, Colonia Copilco El Bajo, Alcaldía Coyoacán, Código Postal 04340,  
Ciudad de México. Teléfono: 55 5174 4000 [www.gob.mx/conagua](http://www.gob.mx/conagua)





- Determinar las no conformidades que podría desencadenarse a partir de ciertas situaciones de riesgo para el tratamiento de datos personales;
- Evaluar las acciones necesarias para evitar que la no conformidad ocurra;
- Determinar e implementar estas acciones;
- Documentar los resultados de las acciones tomadas, y
- Revisar la eficacia de las acciones preventivas tomadas.

**2. Acciones correctivas:** aquéllas encaminadas a eliminar las causas de la “no conformidad” con relación a lo previsto en este Programa.

Para la instrumentación de las acciones correctivas se deben llevar a cabo, al menos, las siguientes actividades:

- Analizar y revisar la no conformidad;
- Determinar las causas que dieron origen a la no conformidad;
- Evaluar las acciones necesarias para evitar que la no conformidad vuelva a ocurrir;
- Implementar estas acciones;
- Documentar los resultados de las acciones tomadas, y
- Revisar la eficacia de las acciones correctivas tomadas.

El objetivo de las acciones correctivas es eliminar la causa de la no conformidad, o bien, reducir su grado de prevalencia y correrán a cargo de las unidades administrativas en las que se haya identificado la no conformidad.

Para la sustanciación de las no conformidades detectadas, el Comité de Transparencia establecerá un plazo límite para su corrección, lo cual deberá documentarse como parte de la mejora continua en la implementación de este Programa.

El “*Procedimiento para la gestión de las acciones preventivas y correctivas*” se adjunta al presente Programa (*Anexo XII*) y se considera parte integrante del mismo.





## 10. ACCIONES PARA LA MEJORA CONTINUA

Este apartado se refiere a la forma en que se documentarán las acciones para la mejora continua de la protección de los datos personales en la CONAGUA.

Con la finalidad de que el presente Programa se mantenga en constante perfeccionamiento, deberán documentarse las acciones para su mejora continua.

En ese sentido, la Unidad de Transparencia, por sí o a petición de las Unidades Administrativas, dará cuenta al Comité de Transparencia de los puntos de mejora en materia de protección de datos personales que hayan sido advertidos de las auditorías y revisiones realizadas, o bien, que se estimen relevantes o de inmediata aplicación para perfeccionar las directrices incluidas en este Programa.

Por tanto, una vez identificados los puntos de mejora, deberán ser sometidos a conocimiento del Comité de Transparencia.

La Unidad de Transparencia, deberá documentar los resultados y revisiones de los puntos de mejora desarrollados.

## 11. SANCIONES

El incumplimiento de las obligaciones en materia de protección de datos personales o de las relativas al trámite del ejercicio de los derechos ARCO, son objeto de sanción conforme a lo siguiente:

### a) Incumplimiento de las obligaciones en materia de protección de datos personales

De conformidad con el artículo 163 de la Ley General, serán causas de sanción por incumplimiento de las obligaciones establecidas en la Ley General, las siguientes:

- I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.
- II. Incumplir los plazos de atención previstos en la Ley General 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 Ley General.
  - V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley General, según sea el caso, y 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 Ley General.
  - VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley General.
  - IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley General.
  - X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley General.
  - XI. Obstruir los actos de verificación del INAI.
  - XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley General.
  - XIII. No acatar las resoluciones emitidas por el INAI.
  - 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**.

#### **b) Incumplimiento por parte de las Unidades Administrativas en el ejercicio de los derechos ARCO**

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 deberá dar aviso al superior jerárquico de dicha unidad administrativa, para que le ordene realizar sin demora las acciones conducentes.

**MEDIO AMBIENTE**

SECRETARÍA DE MEDIO AMBIENTE Y RECURSOS NATURALES

**CONAGUA**

COMISIÓN NACIONAL DEL AGUA

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 al Órgano Interno de Control y, en su caso, se dé inicio el procedimiento de responsabilidad administrativo respectivo.

Cabe destacar que las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Las responsabilidades que resulten de los procedimientos administrativos correspondientes, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.





## ANEXOS

- Anexo I: Política de Protección de Datos Personales en posesión de la Comisión Nacional del Agua.
- Anexo II: Observación de los principios y obligaciones.
- Anexo III: Documento de Seguridad.
- Anexo IV: Mecanismos Para Garantizar La Confidencialidad De Los Datos Personales
- Anexo V: Programa anual de Capacitación en materia de transparencia, acceso a la información y protección de datos personales.
- Anexo VI: Procedimiento de recepción y atención de Quejas y Denuncias que presenten los Titulares de Datos Personales.
- Anexo VII: Procedimiento de solicitud de consentimiento para el tratamiento de los Datos Personales.
- Anexo VIII: Guía para el ejercicio de derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de Datos Personales
- Anexo IX: Mecanismos de Seguridad para la entrega de los Datos Personales
- Anexo X: Mecanismos de evaluación de calidad en la gestión de las solicitudes para el ejercicio de los Derechos ARCO
- Anexo XI: Programa de revisiones administrativas y auditorías 2022
- Anexo XII: Procedimiento para la gestión de las acciones preventivas y correctivas

