

# Política de Protección de Datos Personales

**Versión agosto dos mil veintitrés**

- I. Glosario de términos comunes
- II. Presentación
- III. Objetivo
- IV. Referencias
- V. Alcance del Programa
- VI. Disposiciones Generales
- VII. De los Principios de Protección de Datos Personales
- VIII. De los Deberes para la Protección de Datos Personales
- IX. Documentos para la Protección de Datos Personales
- X. Ejercicio de los Derechos ARCO y la Portabilidad de los Datos Personales
- XI. Supervisión en materia de Protección de Datos Personales

## Glosario de términos comunes

**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 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:** Instancia a la 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, o cuya utilización indebida pueda dar origen a 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, creencias religiosas, filosóficas y morales, opiniones.

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

**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 o privada, ajena a la organización del responsable, que sola o juntamente con otras trate datos personales a nombre y por cuenta del responsable.

**Evaluación de impacto en la protección de datos personales:** Evaluación mediante la cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

**Instituto o INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

**COFAA-IPN:** Comisión de Operación y Fomento de Actividades Académicas del Instituto Politécnico Nacional.

**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, 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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

**Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus obligaciones;
- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
- d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

**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.

**Programa:** Programa de Protección de Datos Personales.

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

**Responsable:** Sujeto obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados 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.

**SNT:** Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

**Sujeto obligado:** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

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

**Transferencias:** 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 a la que se le confieren atribuciones específicas en el Estatuto Orgánico de la COFAA-IPN, incluidas las ponencias de los Comisionados.

**Unidad de Transparencia:** Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

## Presentación

La Comisión de Operación y Fomento de Actividades Académicas del Instituto Politécnico Nacional, en adelante COFAA-IPN, en su carácter de organismo público descentralizado, con personalidad jurídica y patrimonio propios, es sujeto obligado en términos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Por ello, es responsable de proteger los datos personales que trate, garantizando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, los deberes de seguridad y confidencialidad, y las obligaciones derivadas de la Ley General.

El presente documento constituye una política interna de la COFAA-IPN, elaborado en observancia al principio de responsabilidad, el cual prevé que la o el responsable del tratamiento de los datos personales deberá implementar mecanismos para el cumplimiento de los principios, deberes y obligaciones establecidos en las disposiciones en materia de protección de datos personales.

Estos mecanismos, prevé la ley que deben tener por objeto establecer los elementos y las actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continua.

Los responsables del tratamiento de los datos personales, para el caso en concreto de la Comisión, no sólo debe tomar las medidas necesarias para cumplir con los principios, deberes y obligaciones antes señaladas, sino que además es deseable que realice un esfuerzo adicional para observar las mejores prácticas y estándares en la protección de datos personales, y para que rinda cuentas con relación al uso y cuidado de la información personal que esté en su posesión.

Para ello, existe la autorregulación, mediante la cual, de manera voluntaria, los responsables pueden adoptar un mecanismo que les ayude a mejorar el tratamiento y cuidado de los datos personales.

En este tenor, la instrumentación de esta Política de Protección de Datos Personales, facilitará a las personas Titulares de las Unidades Administrativas de esta dependencia a realizar un tratamiento de datos personales en estricto apego a los principios, deberes y obligaciones establecidos en la Ley General y demás disposiciones aplicables, lo cual permitirá garantizar la adecuada protección de los datos personales y el ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición "ARCO" y Portabilidad al tratamiento de datos personales por parte de sus titulares.

## Objetivos

Garantizar el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales, establecer mejores prácticas y estándares, así como elementos y actividades de dirección, operación y control en los procesos en que las Unidades Administrativas de la comisión, que en el ejercicio de sus atribuciones realicen el correcto tratamiento de datos personales.

Garantizar el acceso a la información pública y la protección a los datos personales a fin de que el personal de la COFAA-IPN y externos ejerzan su derecho constitucional. Fomentar la cultura de transparencia impulsando programas de capacitación que permita implementar en el personal de la comisión un actuar conforme a Derecho.

## Referencias:

- Constitución Política de los Estados Unidos Mexicanos, artículo 6º, Base Ay segundo párrafo del artículo 16.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Lineamientos que establecen los parámetros, modalidades y procesamiento para la portabilidad de datos personales.
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

## Alcance

La presente Política de Protección de Datos Personales es de observancia general para todo los Servidores Públicos de la Comisión de Operación y Fomento de Actividades Académicas del Instituto Politécnico Nacional (COFAA-IPN), así como al Personal con interés jurídico y/o involucrados en el tratamiento de datos personales.

La aplicación y cumplimiento de la presente Política de Protección de Datos Personales, es obligatoria para los Titulares de las Unidades Administrativas responsables de cualquier tratamiento de datos personales con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, así como establecer las medidas necesarias que garanticen la seguridad de los datos personales que el ámbito de su competencia posean, recaben o transmitan, a fin de evitar su alteración, daño, destrucción o su uso, acceso o tratamiento no autorizado, pérdida y transmisión, debiendo asegurar su manejo para los propósitos para los cuales se hayan obtenido.

## Disposiciones Generales

**Artículo 1.-** La presente Política de Protección de Datos Personales es de observancia general para todo el personal de la Secretaría involucrado en el tratamiento de datos personales.

El Comité de Transparencia como autoridad máxima en la materia velará por el debido cumplimiento y aplicación de la presente Política.

**Artículo 2.-** La Dirección General de Transparencia y Gobierno Abierto asesorará a las Unidades Administrativas en materia de protección de datos personales conforme a los principios, deberes y obligaciones establecidos en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

**Artículo 3.-** Para las actividades señaladas en la presente Política, será necesario contar con personas servidoras públicas que actúen como enlaces en materia de datos personales.

Las personas Titulares de las Unidades Administrativas designarán a una persona servidora pública como enlace en materia de protección de datos personales, para establecer un canal de comunicación efectivo entre la Unidad de Transparencia y las Áreas Administrativas.

**Artículo 4.-** Las personas Titulares de las Unidades Administrativas son los responsables del tratamiento de los datos personales en el ámbito de sus facultades y atribuciones; y, por lo tanto, tendrán la obligación de cumplir los principios, deberes y obligaciones establecidos en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

**Artículo 5.-** El Comité de Transparencia y/o la Dirección General podrán sugerir a las Unidades Administrativas que realicen o dejen de hacer ciertas acciones con el fin de prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales.

**Artículo 6.-** El Comité de Transparencia cuando adviertan un hecho que pueda constituir una probable falta administrativa en materia de datos personales en términos de la normativa aplicable, darán vista al Órgano Interno de Control para su conocimiento.

## De los Principios de Protección de Datos Personales

Los principios de protección de datos personales, son las herramientas para garantizar la efectiva protección de los datos personales de sus titulares cuando son tratados; herramientas de uso obligatorio para interpretar y aplicar la Ley General y demás normativa aplicable y representar un límite al tratamiento de datos personales que se encuentran en posesión de sujetos obligados.

El derecho a la protección de datos personales se regula a través de ocho principios, que son los siguientes:

Las personas Titulares de las Unidades Administrativas de la Secretaría, responsables del tratamiento de datos personales deberán observar los siguientes principios rectores de la protección de datos personales:

- I. Licitud
- II. Finalidad
- III. Lealtad
- IV. Consentimiento
- V. Calidad
- VI. Proporcionalidad
- VII. Información
- VIII. Responsabilidad

### PRINCIPIO DE LICITUD

El tratamiento de datos personales por parte de las personas Titulares de las Unidades Administrativas de la Secretaría debe ser realizado de conformidad con las atribuciones o facultades que previamente se otorgan en la normativa aplicable que le confiera, en este sentido, no deben tratarse datos personales si no se sujetan a las facultades previamente conferidas.

### PRINCIPIO DE FINALIDAD

Todo tratamiento de datos personales efectuado por las personas Titulares de las Unidades Administrativas de la Secretaría tendrá que estar justificado por las finalidades concretas, explícitas, lícitas y legítimas. Para tal efecto, se entenderá que las finalidades son:

- I. **Concretas:** Atender el tratamiento de los datos personales con los fines específicos o determinados para los que fueron recabados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión a su titular;

- II. **Explícitas:** Señalar y dar a conocer de manera clara en el aviso de privacidad las finalidades relativas al tratamiento de datos personales;
- III. **Lícitas:** Las finalidades que justifiquen el tratamiento de los datos personales deben ser acordes con las atribuciones o facultades de la Unidad Administrativa conforme a la normatividad aplicable;
- IV. **Legítimas:** Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran autorizadas por el consentimiento de su titular, salvo que se actualicen las excepciones previstas en la Ley General, en la presente Política y demás normativa aplicable.

## PRINCIPIO DE LEALTAD

Las personas Titulares de las Unidades Administrativas de la Secretaría se abstendrán de obtener y tratar datos personales a través de medios engañosos o fraudulentos. Con este principio no se permite un tratamiento tramposo, deshonesto y no ético de los datos personales de los y las titulares.

### Obligaciones vinculadas al Principio de Lealtad

Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que tratan datos personales, son las siguientes:

- I. Verificar que los datos personales no se recaben con dolo, mala fe o negligencia;
- II. Comprobar que el tratamiento de los datos personales no genere discriminación o un trato injusto o arbitrario contra sus titulares;
- III. Evitar quebrantar la confianza de los y las titulares en relación con sus datos personales que serán tratados conforme a lo acordado;

## PRINCIPIO DE CONSENTIMIENTO

Previo al tratamiento de los datos personales, las personas Titulares de las Unidades Administrativas deberán obtener el consentimiento de las y los titulares de los datos personales de manera libre, específica, inequívoca e informada, salvo que no sea requerido, en virtud de las siguientes causales de excepción:

- o Cuando una ley así lo disponga, en cuyo caso, los supuestos de excepción deberán ser acordes con las bases, principios y disposiciones establecidos en la Ley General que, en ningún caso, podrán contravenirla;
- o Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- o Para el reconocimiento o defensa de derechos de la titular ante autoridad competente;
- o Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el o la titular y la Secretaría.
- o Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

- Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria;
- Cuando los datos personales figuren en fuentes de acceso público;
- Cuando los datos personales se sometan a un procedimiento previo de disociación.
- Cuando la o el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

La actualización de alguno de los supuestos no exime a las personas Titulares de las Unidades Administrativas responsables del tratamiento de datos personales del cumplimiento de las demás obligaciones establecidas en la Ley General, en la presente Política y demás normativa aplicable.

### **PRINCIPIO DE INFORMACIÓN**

Las personas Titulares de las Unidades Administrativas de la comisión, que traten datos personales, se encuentran obligadas a informar a las personas titulares, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad. En ese sentido, se deberá elaborar y poner a disposición los avisos de privacidad simplificado e integral que correspondan al tratamiento que lleven a cabo, en los términos establecidos en la Ley General, en la presente Política y demás normativa aplicable, independientemente de que se requiera o no el consentimiento del o la titular.

### **PRINCIPIO DE PROPORCIONALIDAD**

Las personas Titulares de las Unidades Administrativas de la Secretaría, recabarán aquellos datos personales que resulten necesarios, adecuados y relevantes para la finalidad que justifica su tratamiento. Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas.

### **PRINCIPIO DE CALIDAD**

Las personas Titulares de las Unidades Administrativas de la Secretaría, deberán mantener los datos personales conforme a la finalidad o finalidades para las que se hayan recabado y adoptar las medidas necesarias para mantenerlos exactos, correctos, completos y actualizados a fin de que no se altere su veracidad. Se puntualiza que estas características de los datos personales tienen el siguiente alcance:

**Exactos:** se considera que los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles;



**Correctos:** son correctos cuando no presentan errores que pudieran afectar su veracidad;

**Completos:** cuando la integridad de los datos personales permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del o la responsable;

**Actualizados:** cuando los datos personales responden fielmente a la situación actual de su titular.

## PRINCIPIO DE RESPONSABILIDAD

Conforme al principio de responsabilidad, las personas Titulares de las Unidades Administrativas velarán por el cumplimiento del resto de los principios, adoptar medidas necesarias como estándares y mejores prácticas para su aplicación y demostrar ante las y los titulares y al Órgano garante que cumple con sus obligaciones en torno a la protección de datos personales.

Asimismo, el Principio de Responsabilidad también es conocido por el principio de rendición de cuentas, ya que como bien se dijo en el párrafo anterior, establece la obligación de velar por el cumplimiento del resto de los principios, así como los deberes que establece la normativa aplicable para dar cuenta a los y las titulares y la autoridad de que se cumple con las obligaciones de protección de datos personales.

### Obligaciones vinculadas al Principio de Responsabilidad

**Artículo 31.-** Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales, son las siguientes:

- I. Participar en los programas de capacitación y actualización en materia de protección de datos personales;
- II. Establecer procedimientos para recibir y responder dudas y quejas de los y las titulares;
- III. Cumplir con los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

## De los Deberes para la Protección de Datos Personales

### Deber de Confidencialidad

La protección de los datos personales además de los principios y las obligaciones ya expuestas, prevé dos deberes, el de confidencialidad y el de seguridad.

La importancia de estos deberes es proteger los datos personales de cualquier amenaza de riesgo con potencial para provocarles un daño o perjuicio, como el robo, extravío o copia no autorizada, pérdida o destrucción no autorizada, uso o acceso no autorizado, daño, alteración o modificación no autorizado.

Con estos deberes, se garantiza:

- Integridad
- Confidencialidad
- Disponibilidad

Las personas Titulares de las Unidades Administrativas de la Secretaría que traten datos personales deberán establecer controles o mecanismos de observancia obligatoria para las personas servidoras públicas que intervengan en cualquier fase del tratamiento, mantengan en secreto la información, así como evitar que los datos personales sean revelados a personas no autorizadas y prevenir la divulgación no autorizada de los mismos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Es así que, dicho deber implica la obligación de guardar secreto respecto de los datos personales que son tratados por las personas Titulares de las Unidades Administrativas de esta comisión, para evitar causar un daño a su titular.

### Deber de Seguridad

Las personas Titulares de las Unidades Administrativas de la Secretaría, adoptarán e instrumentarán las medidas físicas, técnicas y administrativas a través de las cuales garantice la protección de datos personales.

#### Obligaciones vinculadas al Deber de Seguridad

**Artículo 44.-** Las obligaciones para su cumplimiento por parte de las personas Titulares de las Unidades Administrativas que traten datos personales son:

- Generar e implementar políticas de gestión, en las cuales se considere el tipo de datos personales recabados, el tratamiento que se les dará y el ciclo de vida, es decir, su obtención, uso y posterior supresión;
- Establecer las personas servidoras públicas que podrán intervenir en el tratamiento de los datos personales y definir las funciones y obligaciones que tendrán;
- Realizar un análisis de riesgo de los datos personales tratados, así como de los sistemas físicos y/o electrónicos en los cuales se desarrolle dicho tratamiento;

- Desarrollar acciones de prevención y mitigación de amenazas o vulneraciones de datos personales;
- Monitorear y revisar las medidas de seguridad adoptadas para garantizar la protección de datos;
- Incentivar la capacitación de las personas servidoras públicas involucradas en el tratamiento de datos personales, conforme al nivel de responsabilidad que tengan asignado

## Documentos para la Protección de Datos Personales

Para la Protección de Datos Personales, la Comisión de Operación y Fomento de Actividades Académicas del Instituto Politécnico Nacional, contará con los siguientes documentos:

### Programa de Capacitación

Documento en el cual se prevén actividades de capacitación y actualización para todo el personal de la comisión, considerando sus roles y responsabilidades asignadas para el tratamiento de datos personales y la carga de información en el SIPOT.

### Documento de Seguridad

Documento elaborado en coordinación con las Áreas Administrativas de la comisión, cuyo propósito es establecer las medidas administrativas, físicas y técnicas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

### Avisos de Privacidad

Instrumento generado por las Áreas Administrativas de la Comisión, para dar a conocer a las y los titulares los datos personales que son recabados y las finalidades de su tratamiento.

## Ejercicio de los Derechos ARCO y la Portabilidad de los Datos Personales

Los Derechos Arco es el conjunto de derechos a través de los cuales la Ley Orgánica de Protección de Datos de Carácter Personal, garantiza a las personas el poder de control sobre sus datos personales. Se refiere a aquel **derecho que tiene un titular de datos personales, para solicitar el acceso, rectificación, cancelación u oposición sobre el tratamiento de sus datos, ante el Sujeto Obligado que esté en posesión de los mismos.**

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, de conformidad con lo establecido en el presente Título. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro.

- El titular tendrá derecho de **acceder** a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.
- El titular tendrá derecho a solicitar al responsable la **rectificación** o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.
- El titular tendrá derecho a solicitar la **cancelación** de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.
- El titular podrá **oponerse** al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:
  - I. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y
  - II. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

### **Supervisión en materia de Protección de Datos Personales**

Para el debido cumplimiento de los principios, deberes y obligaciones que establecen la Ley General, los Lineamientos Generales y la normativa aplicable en materia de protección de datos personales, el Comité de Transparencia supervisará a las Áreas de esta comisión para garantizar el derecho a la protección de datos personales.

Se realizará una supervisión de protección de datos personales se sustanciará mediante requerimientos de información sobre el tratamiento de datos personales, así como de sugerencias a las Unidades Administrativas para prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales.