GOBIERNO DE MÉXICO | CONAHCYT CONSEJO NACIONAL DE HUMANIDADES CIENCIAS Y TECNOLOGÍAS | CIATEQ

## CIATEQ, A.C. Centro de Tecnología Avanzada.

# Políticas de Protección de Datos Personales

**Índice**

## Introducción.

CIATEQ A.C., Centro de Tecnología Avanzada, en adelante "CIATEQ" es una Asociación constituida mediante escritura pública número 19,276 de fecha 9 de noviembre de 1978, cuenta con personalidad jurídica y patrimonio propio. Tiene su domicilio fiscal en Avenida del Retablo, número 150, Colonia Constituyentes FOVISSSTE, C.P. 76150, en la Ciudad de Santiago de Querétaro, Estado de Querétaro; y cuenta con sedes establecidas en los Estados de Aguascalientes, Estado de México, Hidalgo, Jalisco, Querétaro, San Luis Potosí y Tabasco.

Es un Centro Público de Investigación Humanística y Científica, Desarrollo Tecnológico e Innovación, perteneciente al Sistema Nacional de Centros Públicos del Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT), con autonomía técnica y de gestión, de conformidad con los artículos 4, fracción IV, 75, 81, 82, 84 y 91 de la Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación. Además; reconocida como Entidad Paraestatal asimilada al régimen de las Empresas de Participación Estatal Mayoritaria a que se refieren la Ley Orgánica de la Administración Pública Federal y la Ley Federal de las Entidades Paraestatales.

Tiene por objeto entre otros, realizar actividades de investigación y desarrollo tecnológico en el área manufactura avanzada; sistemas mecánicos; procesos de manufactura, diseño y desarrollo de productos; ingeniería y construcción de plantas; plásticos y materiales avanzados; sistemas de medición; telecomunicaciones; tecnologías de la información, control y electrónica; ingeniería virtual, confiabilidad y disciplinas afines.

En estricto apego a lo dispuesto por la Constitución Política de los Estados Unidos Mexicanos, en su artículo 6, Apartado A, fracciones I y ll, la información que posee "CIATEQ" se regirá por el principio de máxima publicidad y la información concerniente a los datos personales será protegida en los términos y excepciones que fijan las leyes de la materia. Por lo tanto, de conformidad con lo establecido por la Ley General de Protección Datos de Personales en Posesión de Sujetos Obligados, cuyo objeto es establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados, el "CIATEQ", atiende a los principios de accesibilidad a la información, transparencia, objetividad e independencia, y tiene como obligación, el realizar acciones que deberán llevar a cabo las unidades administrativas en la protección, tratamiento y conservación de los datos personales; así como aquellas que coadyuven a identificar y adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal; su adopción es de obligado cumplimiento para las diversas áreas que conforman este Centro de Investigación, las cuales conforme a sus funciones, facultades y atribuciones dan tratamiento a datos personales.

De esta forma, las presentes Políticas de Protección de Datos Personales, son un instrumento necesario para asegurar el adecuado tratamiento de los datos personales en posesión del "CIATEQ".

## Objetivo.

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

## Ámbito de Aplicación.

El presente documento es de aplicación y observancia general y obligatoria para todas las personas que desempeñan un cargo o comisión en **"CIATEQ"** y que conforme a sus atribuciones y competencias realizan tratamiento de datos personales.

## Marco Jurídico

**I.** Constitución Política de los Estados Unidos Mexicanos;

**II.** Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) y su Protocolo adicional;

**III.** Ley General de Transparencia y Acceso a la Información Pública (LGTAIP);

**IV.** Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP);

**V.** Ley General de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO);

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

**VII.** Acuerdo mediante el cual se aprueba la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público;

## Glosario

**Aviso de privacidad**: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el "CIATEQ", 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.

**Datos personales**: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificada cuando se acredita su identidad a través de cualquier información relacionada ella, por ejemplo, su nombre, teléfono, domicilio, fotografía, huellas dactilares o cualquier otro dato personal. Asimismo, será una persona 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.

**Acceso**: Derecho del titular para acceder a sus datos personales que obren en posesión del **"CIATEQ"**, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.

**Rectificación**: Derecho del titular para solicitar al **"CIATEQ"** la corrección de sus da-tos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

**Cancelación**: Derecho del titular para solicitar al **"CIATEQ"** que sus datos personales sean bloqueados y, posteriormente, suprimidos de los archivos, registros, expedientes y sistemas institucionales, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados.

**Oposición**: Derecho del titular para solicitar al **"CIATEQ"**, cuando éste pretenda realizar el tratamiento de datos personales, que se abstenga de hacerlo en determina-das situaciones o para que cese el tratamiento.

**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, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

**Encargado**: Es la persona física o moral, pública o privada, ajena al **"CIATEQ"**, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

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

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

**Inventario de datos personales**: Catálogo de sistemas de datos con independencia de su forma de almacenamiento.

**Ley General de Datos de Personales o LGPDPPSO**: 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**: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

**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:

- Prevenir el acceso no autorizado al perímetro del **"CIATEQ"**, sus instalaciones físicas, áreas críticas, Centros de Datos y de Telecomunicaciones, recursos e información;
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas del "CIATEQ", recursos e información;
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir del "CIATEQ"; y
- 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:

- Asegurar que el acceso a los servidores y equipos en Centros de Datos y de Telecomunicaciones, bases de datos, sistemas informáticos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

- Generar un esquema de privilegios con base en roles y perfiles definidos para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

- Prevenir que los medios de transacción de información digital y datos personales se realice mediante canales seguros de telecomunicaciones.

- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware; y

- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

**Políticas**: Directrices estratégicas para la gestión y tratamiento de datos personales, alineadas a las atribuciones del **"CIATEQ"**. Incluye la elaboración y emisión interna de programas, entre otros documentos regulatorios.

**Responsable**: El **"CIATEQ"** a través de las unidades administrativas que se le adscriben, en tanto que deciden sobre el tratamiento de datos personales acorde a las funciones, facultades y atribuciones conferidas en sus Estatuto y demás ordenamientos normativos.

**Servidor público vinculado**: El o los servidores públicos que desempeñan un cargo o comisión en **"CIATEQ"** y que tienes a su cargo el tratamiento de datos personal, dentro de sus áreas de adscripción.

**Sistema de Datos**: Archivo físico o electrónico que contenga datos personales que se hayan recabado para el ejercicio de las funciones, facultades y atribuciones de las Unidades Administrativas.

**Titular**: La persona física a quien corresponden los datos personales.

**Unidades Administrativas**: Áreas administrativas previstas en el Manual de Organización de **"CIATEQ"**, las cuales conforme a sus funciones, facultades y atribuciones dan tratamiento a datos personales.

**Unidad de Transparencia**: Instancia a la que hacen referencia los Artículos 45 de la Ley General de Transparencia y Acceso a la Información Pública; 61 de la Ley Federal de Transparencia y Acceso a la Información Pública; y 85 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

**Vulneraciones**: La pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

## POLÍTICAS PARA EL TRATAMIENTO DE DATOS PERSONALES.

### I. Principios generales para la protección y tratamiento de datos personales.

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

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

3. Al momento de recabar datos personales, se deberá hacer del conocimiento de la persona titular la finalidad con la cual se reciben.
4. Las unidades administrativas solo deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de sus atribuciones y funciones.

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

6. Es obligación de todas las personas servidoras públicas del **"CIATEQ"** que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla ni difundirla por cualquier medio físico y/o electrónico a terceros.

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

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

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

sencilla.

10. Las unidades administrativas del **"CIATEQ"** deberán verificar que sus avisos de privacidad simplificados e integrales se difundan en el portal de internet del Organismo y estar disponibles de manera impresa en las instalaciones, en un lugar visible y de fácil consulta por parte de las personas titulares.

## Principios, Deberes y Obligaciones

**Principio de licitud**. Los datos personales tienen que ser tratados de manera lícita, esto es, debe sujetarse a las facultades o atribuciones que la normatividad aplicable le otorga.

Para cumplir con este principio, las unidades administrativas del **"CIATEQ"** deberán ajustarse a las siguientes recomendaciones:

1. Revisar que los datos se traten conforme a la LGPDPPSO, Lineamientos Generales de Protección de Datos Personales para el Sector Públicos y demás normativa aplicable.

2. Conocer la normativa que en lo particular regule sus atribuciones, funciones y responsabilidades con relación al tratamiento de los datos personales que realice.

3. Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.

**Principio de lealtad**. La obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos.

Para cumplir con este principio, las unidades administrativas deberán:

1. Revisar los procedimientos y formatos utilizados para recabar datos personales, para verificar que en éstos no se utilicen prácticas que lleven a la obtención de los datos de manera dolosa, de mala fe o con negligencia.

2. Dar vista al Órgano Interno de Control en caso del uso de prácticas dolosas, de mala fe o negligentes para la obtención de los datos personales.

3. Respetar en todo momento la expectativa razonable de privacidad de la persona titular de los datos personales.

4. Tratar los datos conforme lo acordado e informado a la persona titular de los datos personales.

5. Verificar los tratamientos, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.

6. Elaborar avisos de privacidad con todos los elementos informativos que establece la LGPDPPSO, y con información que corresponda a la realidad del tratamiento que se efectúa.

7. Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta, para que no haya lugar a confusión al respecto.

**Principio del consentimiento**. Como regla general, las áreas que realicen tratamiento de datos personales deberán contar con el consentimiento del titular para el tratamiento de sus datos personales, el cual deberá ir siempre ligado a las finalidades concretas del tratamiento que se informen en el aviso de privacidad.

Para cumplir con este principio, las unidades administrativas deberán:

1. Identificar las finalidades para las cuales se requiere el consentimiento de los titulares.

2. Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.

3. Redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.

4. 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.

5. Habilitar los mecanismos necesarios para solicitar el consentimiento expreso.

6. Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.

7. Solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad, cuando los datos personales se obtengan directamente de su titular o representante.

8. Cuando los datos personales no los proporcione personal o directamente el titular o su representante, deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado. Asimismo, deberá informarles que cuentan con un plazo de 5 días hábiles para en su caso manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran su consentimiento. Si el titular no manifiesta su negativa en el plazo de cinco días antes señalado, entonces podrá suponer que cuenta con el consentimiento tácito.

9. En el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso de privacidad o en un instrumento aparte. No podrán tratar los datos personales si no cuenta con el consentimiento expreso del titular.

**Principio de información**. Las unidades administrativas del **"CIATEQ"** que realizan tratamientos de datos personales se encuentran obligadas a informar a las personas titulares de los datos personales, a través de los avisos de privacidad integral y simplificado, las características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Para cumplir con este principio, las unidades administrativas deberán:

1. Poner a disposición de los titulares el aviso de privacidad en los términos dispuestos en la LGPDPPSO, y demás normativa aplicable.

2. Poner a disposición del titular el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera directa o personal del titular.

3. Poner a disposición de la persona titular el aviso de privacidad al primer contacto que se tenga con éste, cuando los datos personales se hayan obtenido de una transferencia consentida, de una que no requiera el consentimiento, o bien de una fuente de acceso público.

4. Poner a disposición de la persona titular el aviso de privacidad previo a iniciar el uso de los datos personales para la finalidad para la que se obtuvieron, cuando éstos no se hayan obtenido de manera directa de la titular, el tratamiento no requiera del contacto con ésta y se cuente con datos para contactarle.

5. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades (aprovechamiento), cuando requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente.

6. Redactar el aviso de privacidad de manera que sea claro, comprensible y con una estructura y diseño que facilite su entendimiento.

7. Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfiera datos personales.

8. Demostrar el cumplimiento del principio de información, en caso de que así se requiera.

**Principio de proporcionalidad**. Las unidades administrativas que realicen tratamiento de datos personales deberán tratar solo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

Para cumplir con este principio, las unidades administrativas deberán:

1. Tratar el menor número posible de datos personales.

2. Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles.

3. Crear bases de datos con datos personales sensibles sólo cuando:

    a. Obedezca a un mandato legal;
    b. Se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o
    c. Lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

4. Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.

5. Cuando una normativa establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, sólo deberán solicitarse dichos datos.

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

Para cumplir con este principio, las unidades administrativas deberán:

1. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta.

2. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean determinadas.

3. Identificar y distinguir en el aviso de privacidad entre las finalidades primarias y secundarias.

4. Ofrecer a la persona titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias.

5. Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, informar a la persona titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información para finalidades secundarias.

6. No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias

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

- **Exactos**. Los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles.
- **Completos**. Los datos personales están completos cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio a su titular.
- **Pertinentes**. Los datos personales son pertinentes cuando corresponden efectivamente a su titular.
- **Actualizados**. Los datos están actualizados cuando están al día y corresponden a la situación real de su titular.
- **Correctos**. Los datos personales son correctos cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

Para cumplir con este principio, las unidades administrativas deberán:

1. Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, pertinentes, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que la persona titular se vea afectada por dicha situación.

2. Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo.

3. Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.

4. Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación.

**Principio de responsabilidad**. A este principio se le conoce también como el principio de “rendición de cuentas”, ya que establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales.

Para cumplir con este principio, las unidades administrativas deberán:

1. Cumplir con el programa de capacitación y actualización aprobado por el Comité de Transparencia.

2. Analizar los riesgos que implica todo tratamiento de datos personales.

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

Para cumplir con este deber, las unidades administrativas deberán:

1. Guardar confidencialidad en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con la persona titular.

2. Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste.

3. Capacitar al personal para que conozca sus obligaciones con relación al tratamiento de datos personales.

4. Establecer procedimientos para evitar fuga de información o el acceso indebido a los datos personales.

5. Incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas de confidencialidad y para que quienes tengan acceso a los datos personales en posesión del responsable cumplan con esta obligación de confidencialidad.

6. Realizar verificaciones o supervisiones periódicas al trabajo realizado por los encargados, a fin de verificar que se cumplan con sus obligaciones en torno a la protección de los datos personales.

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

Para cumplir con este deber, las unidades administrativas deberán:

1. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas.

2. No adoptar medidas de seguridad menores a aquéllas que mantengan para el manejo de su información.

3. Tomar en cuenta el riesgo inherente por tipo de dato personal; las posibles consecuencias para las personas titulares por una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico.

4. Notificar a las personas titulares las vulneraciones de seguridad que se presenten, con la información y en el momento antes señalados;

5. Llevar a cabo las acciones correctivas que sean necesarias

### Ciclo de vida de los Datos Personales.

Las unidades administrativas que realizan tratamiento de datos personales deberán:

1. Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen.

2. Elaborar un inventario de datos personales relacionando el tipo de tratamiento con el ciclo de vida.

3. Bloquear, cancelar, suprimir o destruir los datos personales, en los casos establecidos en la normatividad aplicable.

### Roles y Responsabilidades

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

En el **"CIATEQ"**, las funciones y obligaciones de las personas que tratan datos personales se han identificado en dos niveles:

I. De manera general, a través de la implementación del Programa de Protección de Datos Personales, en el cual se describirán todas las obligaciones que establece la Ley General y los Lineamientos Generales y éstas se asociaron con el área responsable de su cumplimiento, y

II. De forma específica, a través de los inventarios que se desarrollaron por cada uno de los tratamientos de datos personales por unidad administrativa, en los cuales se identificó el personal que, conforme a sus facultades y atribuciones realiza el tratamiento de datos personales, así como la finalidad de dicho tratamiento.

### Sanciones

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

**I.** Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

**II.** Incumplir los plazos de atención 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 presente Ley;

**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 presente Ley, 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;

**VII.** Incumplir el deber de confidencialidad;

**VIII.** No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;

**IX.** Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;

**X.** Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;

**XI.** Obstruir los actos de verificación de la autoridad;

**XII.** Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;

**XIII.** No acatar las resoluciones emitidas por el Instituto y los Organismos garantes; y

**XIV.** Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea;

### Proceso General Para el Establecimiento, Actualización, Monitoreo y Revisión de Los Mecanismos y Medidas de Seguridad.

El artículo 33, fracción VII de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera

periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

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

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

Monitoreo y supervisión periódica de las medidas de seguridad implementadas

Artículo 63. Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

**I.** Los nuevos activos que se incluyan en la gestión de riesgos;

**II.** Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

**III.** Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;

**IV.** La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

**V.** Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

**VI.** El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y

**VII.** Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda este Sujeto Obligado.

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad del "CIATEQ":

**I.** Mecanismos de Monitoreo**.**

Para los tratamientos de datos personales del **"CIATEQ"**, se consideran los siguientes tipos de monitoreo:

1) Revisión de cumplimiento de las políticas internas, relacionadas con el tratamiento de datos personales. Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la Ley General, los Lineamientos Generales, y demás normatividad que resulte aplicable.

   Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

**a.** Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.

**b.** Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.

**c.** Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.

**d.** Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

2) Revisión del riesgo. Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:

**a.** **Monitoreo del entorno físico**. Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con: (I) personal de vigilancia en los accesos a las instalaciones del "CIATEQ", (II) control de acceso del personal con credencial laboral vigente, (III) control de acceso a través de bitácoras para visitantes y personal del "CIATEQ" que olvidó su credencial, (IV) control de asistencia a través listas, y (V) Control de acceso sólo a personal autorizado a Centros de Datos y Comunicaciones propios o arrendados.

**b.** **Monitoreo del entorno electrónico**. Para la detección continua de amenazas y vulnerabilidades, la Gerencia de Cómputo y Comunicaciones, cuenta con herramientas automatizadas de monitoreo (activo y pasivo), así como con bitácoras de los sistemas informáticos, bases de datos y configuraciones de los componentes.

**c.** **Actualización del plan de trabajo**. Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración de la Unidad de Transparencia, la Gerencia de Cómputo y Comunicaciones y el Comité de Transparencia.

**d.** **Revisión de avances del plan de trabajo**. A través de los mecanismos que determine la Unidad de Transparencia, la Gerencia de Cómputo y Comunicaciones y el Comité de Transparencia, se hará una revisión de los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

**e.** **Actualización tecnológica**. Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará de manera anual una actualización del análisis de riesgo, análisis de vulnerabilidades y plan de trabajo.

**f.** **Vulneraciones a la seguridad de los datos personales**. En caso de identificar un incidente de seguridad que involucre datos personales, la Unidad de Transparencia, la Gerencia de Cómputo y Comunicaciones y el Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

## II. Mecanismos de Supervisión y Revisión

Además del monitoreo continuo de las medidas de seguridad, se requiere realizar una supervisión periódica de las mismas, a través de auditorías las cuales pueden ser realizadas de manera interna; desarrolladas por el propio Centro o en su caso por el Órgano Interno de Control Específico del CONAHCYT; o bien de forma externa, a través

de la contratación de proveeduría externa; o bien, a través de las Auditorias Voluntarias establecidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Respecto del programa de auditoría mencionado en el último párrafo del artículo 63 de los Lineamientos Generales, se tiene contemplada la realización de una auditoría en materia de protección de datos personales, al menos una vez cada año. Dicha auditoría se puede llevar a cabo por terceros según la disponibilidad presupuestal con al que cuente el **"CIATEQ"**; o bien, de forma interna conforme a lo determine el Comité de Transparencia.

El programa de auditoría será aquél que determine el Comité de Transparencia en el Programa de Protección de Datos Personales del **"CIATEQ"**.

**Sistema de Gestión y Documento de Seguridad.**

La Unidad de Transparencia documentará el sistema de gestión previsto en el artículo 34 de la Ley General de Datos Personales, y elaborará el documento de seguridad a que se refiere el artículo 35 de dicho ordenamiento, el cual se integrará con la información señalada en el artículo anterior.

Cada Unidad Administrativa designará una persona responsable que esté vinculado a las bases de datos personales, quién será el encargado de apoyar al Titular de cada Unidad Administrativa de su adscripción para realizar lo establecido en las presentes Políticas y tendrá las siguientes funciones:

I. Adoptar las medidas de seguridad para el resguardo del o los sistemas de datos personales bajo su responsabilidad, en soporte físico, de manera que se evite su alteración, pérdida o acceso no autorizado;

II. Autorizar expresamente, en los casos en que no esté previsto por un instrumento jurídico o disposición normativa, a los usuarios, y llevar una relación actualizada de las personas que tengan acceso a las bases o los sistemas de datos personales que se encuentran en soporte físico, y

III. Aplicar y vigilar el cumplimiento de las medidas y estándares de seguridad para la conservación y resguardo de las bases o sistemas de datos personales del **"CIATEQ"**, que para tal efecto determine el Comité de Transparencia, a través de las disposiciones normativas específicas de observancia general para las Unidades Administrativas que cuenten con los referidos sistemas o bases.

**I.** Inventario de datos personales**.**

Las Unidades Administrativas, con la asesoría de la Unidad de Transparencia, deberán elaborar un inventario con la información básica de cada tratamiento de datos personales en posesión del **"CIATEQ",** considerando, al menos, los siguientes elementos:

1. Fundamento jurídico que habilita el tratamiento;

2. Las facultades, atribuciones y funciones que la normatividad aplicable les confiera para dar tratamiento a datos personales;

3. Listado de datos personales sujetos a tratamiento, en su caso, aquellos sensibles;

4. Los medios a través de los cuales se obtienen los datos personales;

5. Las finalidades de cada tratamiento de datos personales;

6. Los formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;

7. Los servidores públicos que tienen acceso a las bases o sistemas de tratamiento;

8. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda a **"CIATEQ"**, y

9. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

La actualización del inventario de datos personales deberá realizarse por las Unidades Administrativas responsables de su administración, el Titular de éstas, remitirá a la Unidad de Transparencia en el formato que establezca para tal efecto la modificación, actualización o cancelación de dichas bases.

### **II.** Seguridad de datos personales**.**

Corresponderá al Titular de cada Unidad Administrativa responsable establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar su relación con el mismo. Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

Con independencia del tipo de sistema en el que se encuentren los Datos Personales o el tipo de tratamiento que se efectúe, el Titular de la Unidad Administrativa responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico pudiendo solicitar apoyo de la Gerencia de Cómputo y Comunicaciones para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

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

1. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

2. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

3. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

4. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

5. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

6. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

7. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

8. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales que implementen las Unidades Administrativas responsables de las bases de datos personales deberán estar documentadas y contenidas en el sistema de que se trate, en términos de lo dispuesto por la Ley General de Datos de Personales y demás disposiciones administrativas aplicables.

Corresponderá a las Unidades Administrativas, con la asesoría de la Unidad de Transparencia, llevar una bitácora de las vulneraciones a la seguridad, a que hace referencia el artículo 39 de la Ley General de Datos de Personales, en la que se describa la fecha en la que ocurrió, el motivo y las acciones correctivas implementadas de forma inmediata y definitiva.

### **III.** Transferencia de datos personales**.**

Toda transferencia de datos personales se encontrará sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70, de la Ley General de Datos de Personales.

Toda transferencia de datos personales que realicen las Unidades Administrativas del "CIATEQ", en ejercicio de sus atribuciones o funciones, deberán ser formalizadas mediante convenios de colaboración, convenio de confidencialidad, no divulgación, reserva y resguardo de información o cualquier otro instrumento jurídico en el que se incluyan cláusulas que permitan demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes atendiendo a lo establecido en el Aviso de Privacidad correspondiente.

El instrumento que formalice la transferencia en términos de este artículo deberá contener al menos, lo siguiente:

1. Identificación del Sistema de Datos Personales, del transmisor y del destinatario de estos;

2. Finalidad de la transferencia, así como el tipo de datos que son objeto de la misma;

3. Las medidas de seguridad y custodia que fueron adoptadas por la Unidad o Área Administrativa y el destinatario;

4. Plazo por el que conservará el destinatario los datos que le hayan sido transmitidos, el cual podrá ser ampliado mediante aviso al "CIATEQ", y

5. Señalar si una vez concluidos los propósitos de la transmisión, los datos personales deberán ser destruidos o devueltos al "CIATEQ", al igual que cualquier soporte o documento en que conste algún Dato Personal objeto de la transmisión.

### **IV.** Remisiones de datos personales.

Las Remisiones nacionales e internacionales de datos personales que se realicen entre la Unidad Administrativa responsable y el Encargado no requerirán ser informadas al titular, ni contar con su consentimiento, en términos de lo dispuesto por el artículo 71, de la Ley General de Datos Personales.

Corresponderá a las Unidades Administrativas responsables de bases o sistemas de datos personales tomar las medidas necesarias para que cualquier relación jurídica entre el "CIATEQ" y terceros que funjan como Encargados en términos del Título Cuarto de la Ley General de Datos Personales, se formalice en cumplimiento a lo previsto por el Ordenamiento antes citado, mediante contratos o instrumentos jurídicos que garanticen el debido resguardo de los datos personales, a través de la implementación de mecanismos que en la medida de lo posible limiten las remisiones o transferencias al mínimo indispensable para la prestación del servicio de que se trate y garanticen el resguardo de la confidencialidad de los datos personales en los términos previstos por la legislación y normatividad administrativa aplicable al "CIATEQ".

Corresponderá a la Gerencia de Cómputo y Comunicaciones, cerciorarse de que para el debido tratamiento de Datos Personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias en las que el "CIATEQ" se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, se dé cumplimiento a lo previsto por el artículo 64 de la Ley General de Datos Personales.

## Proceso General de Atención de los Derechos ARCO

### I. Ejercicio de los derechos ARCO

Los servidores públicos vinculados están obligados en todo momento a garantizar las condiciones y requisitos necesarios para el adecuado tratamiento, así como la debida administración y custodia de los datos personales que se encuentren bajo su resguardo, con el objeto de maximizar el ejercicio de los derechos ARCO.

Para registrar, tramitar y dar respuesta a las solicitudes de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, la Unidad de Transparencia y los servidores públicos vinculados deberán atender lo que señala la Ley General de Datos Personales, así como en los Lineamientos Generales y el Procedimiento para ejercer los Derechos ARCO autorizado por el Comité de Transparencia del "CIATEQ".

Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el INAI en términos de las disposiciones normativas aplicables. El "CIATEQ" deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO y entregar el acuse de recibo que corresponda.

Los medios y procedimientos habilitados por el "CIATEQ" en su carácter de responsable para atender las solicitudes para el ejercicio de los derechos ARCO, deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con el responsable.

### II. Requisitos mínimos de la solicitud para el ejercicio de los derechos ARCO

En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes:

6. Nombre del titular de los datos personales.
7. Documentos que acrediten la identidad del titular.
8. En su caso, nombre del representante del titular y documentos para acreditar su identidad y personalidad.
9. Domicilio o cualquier medio para recibir notificaciones.
10. Descripción clara y precisa de los datos personales que se quieran rectificar, cancelar u oponerse a su tratamiento.
11. Descripción del derecho que se quiere ejercer o de lo que solicita el titular.
12. En su caso, documentos o información que faciliten la localización de los datos personales, entre ella, el área responsable del tratamiento.

Tratándose de una solicitud de acceso a datos personales, el titular o su representante deberán señalar la modalidad en la que prefiere que éstos se reproduzcan. Las Unidades Administrativas deberán atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

### III. Requerimiento de información adicional

En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere este artículo y el "CIATEQ" no cuente con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación.

Transcurrido dicho plazo sin que el titular o su representante desahoguen la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO. La prevención tendrá el efecto de interrumpir el plazo que tiene el "CIATEQ", para resolver la solicitud de ejercicio de derechos ARCO.

### **IV.** Medios para la acreditación de la identidad del titular y representante legal

Al promover solicitudes de ejercicio de los derechos ARCO, los titulares de dichos datos personales o su representante legal, deberán acreditar su identidad, mediante identificación oficial vigente con fotografía y tratándose del representante legal deberá acompañar además el documento con el que acredite su personalidad a través de instrumento público; carta poder simple firmada ante dos testigos anexando copia simple

de las identificaciones oficiales de quienes intervengan en la suscripción del mismo, o declaración en comparecencia ante la Unidad de Transparencia o el servidor público vinculado correspondiente atendiendo a lo establecido en el Procedimiento para ejercer los Derechos ARCO autorizado por el Comité de Transparencia del "CIATEQ" .

### **V.** Reproducción de datos personales

El ejercicio de los derechos ARCO será gratuito y el "CIATEQ" sólo podrá realizar cobros para recuperar los costos de reproducción o envío, conforme a la normatividad que resulte aplicable.

Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos le deberán ser entregados sin costo.

La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples o certificadas.

### **VI.** Plazo de respuesta

El plazo para dar respuesta a las solicitudes del ejercicio de los derechos ARCO en el "CIATEQ", no podrá ser mayor a veinte días hábiles contados a partir del día siguiente a la recepción de la solicitud.

### **VII.** Notoria incompetencia para atender la solicitud derechos ARCO

Cuando la Unidad de Transparencia determine la notoria incompetencia del **"CIATEQ"** para atender la solicitud para el ejercicio de alguno de los derechos ARCO, deberá comunicar tal situación al titular en el plazo de tres días hábiles siguientes a la presentación de la solicitud, y en su caso, orientarlo con el responsable competente, sin que sea necesario una resolución del Comité de Transparencia que confirme la notoria incompetencia.

### **VIII.** Causales de improcedencia del ejercicio de los derechos ARCO

Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente, serán aquellas a que hacen referencia el artículo 55, de la Ley General de Datos Personales, por lo que en caso de materializarse alguno de los supuestos contemplados en la referida

disposición, el "CIATEQ" por conducto del Comité de Transparencia de manera fundada y motivada, deberá hacerlo constar en una resolución que confirme la improcedencia del ejercicio de los derechos ARCO.

### **IX.** Inexistencia de los datos personales

Las resoluciones del Comité que confirmen modifiquen o revoquen la inexistencia de datos personales, deberá contar con los elementos mínimos que permitan al titular tener la certeza de que se utilizó un criterio de búsqueda exhaustivo; así como señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y la unidad administrativa competente de contar con los mismos, situaciones que se harán constar en resoluciones emitidas por dicho órgano colegiado.

**X.** Derecho de rectificación

El titular podrá solicitar al "CIATEQ" la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados, cuya obligación se dará por cumplida mediante constancia que acredite la corrección solicitada.

**XI.** Derecho de cancelación y oposición

Con relación a una solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del "CIATEQ". En el caso de la solicitud de oposición, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.

## Interpretación de las Políticas

Las Unidades Administrativas podrán solicitar asesoría al Comité de Transparencia sobre la aplicación de la Ley General de Datos de Personales y de las presentes Políticas, quien es a autoridad máxima en materia de protección de datos personales, acorde a lo dispuesto en los artículos 83 y 84, de la Ley General de Datos de Personales.