



GOBIERNO DE  
**MÉXICO**



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

**UNIDAD DE ASUNTOS JURÍDICOS**

**DIRECCIÓN DE CONSULTA Y ESTUDIOS NORMATIVOS**  
**SUBDIRECCIÓN DE TRANSPARENCIA Y SEGUIMIENTO LEGISLATIVO**

# POLITICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES

## CONAHCYT



## **I. OBJETIVO**

El objetivo general de las políticas internas para la gestión y tratamiento de datos personales es garantizar el cumplimiento de las leyes y regulaciones relacionadas con la privacidad y protección de datos personales, así como establecer estándares y procedimientos para el manejo adecuado y seguro de la información personal de los titulares. Estas políticas buscan proteger la privacidad de los datos personales, asegurar su confidencialidad, integridad y disponibilidad, así como promover la transparencia en el uso y tratamiento de esta información. Además, estas políticas internas sirven para fomentar una cultura de responsabilidad y compromiso con la protección de los datos personales en posesión del Consejo Nacional de Humanidades Ciencias y Tecnologías.

## **II. AMBITO DE APLICACIÓN**

Estas políticas aplicaran a todas las Unidades Administrativas que conforman el Consejo Nacional de Humanidades Ciencias y Tecnologías, que realicen tratamiento de datos personales en ejercicio de sus atribuciones.

Las Unidades Administrativas que conforman el Consejo Nacional de Humanidades Ciencias y Tecnologías que deberán observar estas políticas internas de Protección de Datos Personales son las siguientes:

1. Dirección General
2. Coordinación de Comunicación y Cooperación Internacional
3. Coordinación de Repositorios, Investigación y Prospectiva
4. Dirección Adjunta de Investigación Humanística y Científica
5. Coordinación de Programas para la Formación y Consolidación de la Comunidad
6. Dirección Adjunta de Desarrollo Tecnológico, Vinculación e Innovación
7. Unidad de Articulación Sectorial y Regional
8. Unidad de Asuntos Jurídicos
9. Unidad de Administración y Finanzas
10. Secretaría Ejecutiva de la CIBIOGEM



### III. DISPOSICIONES GENERALES

- I.** Garantizar la máxima protección y seguridad de los datos personales y privacidad de los ciudadanos y empleados, de acuerdo con las leyes de protección de datos aplicables.
- II.** Esta política se aplica a todos los datos personales recopilados, almacenados, procesados o transferidos por el Conahcyt, ya sea en formato físico o digital.
- III.** El Conahcyt, obtendrá el consentimiento informado de los ciudadanos antes de recopilar cualquier dato personal.
- IV.** Se limitará la recopilación y el almacenamiento de datos personales solo a aquellos necesarios para los fines especificados.
- V.** Se mantendrá la precisión de los datos personales adoptando las medidas razonables para corregir o eliminar datos inexactos.
- VI.** Solo se mantendrán los datos personales durante el tiempo necesario para cumplir con los fines para los que se recopilaron, a menos que se requiera una retención más prolongada, cuando así lo establezca la normatividad aplicable.
- VII.** Se cumplirá con los derechos de los ciudadanos sobre sus datos personales, incluido el derecho de acceso, rectificación, cancelación, oposición y en su caso portabilidad.
- VIII.** Solo se procesarán los datos personales para los fines específicos para los que fueron recopilados y previamente informados a los ciudadanos.
- IX.** Se aplicarán medidas de seguridad adecuadas para proteger los datos personales contra cualquier forma de procesamiento no autorizado o ilegal.
- X.** No se transferirán datos personales a terceros sin el consentimiento previo de los individuos, a menos que la ley lo requiera o sea necesario para la prestación de los servicios requeridos.
- XI.** Solo se utilizarán los datos personales de manera justa y legítima, sin exceder las finalidades para las que se recopilaron.



**XII.** El Conahcyt, establecerá procedimientos para el consentimiento informado y el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación, Oposición y en su caso Portabilidad) por parte de los titulares de los datos personales.

**XIII.** El Conahcyt, establecerá procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.

**XIV.** Se responderá de manera oportuna y adecuada a cualquier solicitud de ejercicio de derechos de los ciudadanos, respecto de sus datos personales.

#### IV. PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES

Los principios de protección de datos personales se establecen en el artículo 16 de la LGPDPSO, con la finalidad de observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, a fin de garantizar la privacidad y seguridad de la información personal de las personas y proteger sus derechos y libertades fundamentales en relación con el procesamiento de sus datos personales.

**LICITUD.** Los datos personales se deben obtener y tratarse de manera lícita, apegándose a la normativa aplicable, tanto en la legislación mexicana, como en el derecho internacional, con pleno cumplimiento de la legalidad, respeto, la buena fe y los derechos de los ciudadanos, respecto de la información que es sujeta a tratamiento, sujetándose a las facultades o atribuciones que la normatividad aplicable le confiera.

**FINALIDAD.** El tratamiento se limitará al cumplimiento de las finalidades para las cuales se hayan obtenido los datos, y deben estar previstas en el Aviso de Privacidad. No podrán tratarse los datos para finalidades distintas y en el caso de datos personales sensibles, se procurará limitar el periodo de tratamiento al mínimo indispensable.

**LEALTAD.** En el tratamiento de los datos personales, se debe apegar a las finalidades, tomando en cuenta la expectativa razonable de privacidad y la obtención, no debe realizarse por medios engañosos o fraudulentos.



**CONSENTIMIENTO.** El tratamiento de los datos, estará sujeto al consentimiento del titular, cuando no se actualicen las causales de excepción previstas en el artículo 22 de la LGPDPPSO, el consentimiento deberá otorgarse de forma Libre, sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular; específica, referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e informada, que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Por regla general será válido el consentimiento tácito, como la forma de autorización que se da de manera implícita, es decir, a través de la conducta o acciones de una persona, en lugar de ser otorgado de manera explícita mediante una declaración verbal o escrita, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

Tratándose de datos personales sensibles se deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de la LGPDPPSO.

**CALIDAD.** Los datos personales deben ser pertinentes y correctos para la finalidad para la cual fueron recabados, adoptando las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, a fin de que no se altere la veracidad de éstos. Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Asimismo, 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 conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.





Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

Se deberán incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales.

**PROPORCIONALIDAD.** De conformidad a lo establecido en el artículo 25 de la LGPDPPSO, sólo se deberán tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento. Las características del tratamiento necesario, adecuado y relevantes se cumple cuando se justifica que los datos personales sometidos al procedimiento son los que se requieren para el cumplimiento de las finalidades para las cuales los datos personales han sido obtenidos y sometidos a tratamiento, prevalece el equilibrio entre la información que se solicita, contra la que realmente se necesita obtener.

**INFORMACIÓN.** Existe la obligación de hacer del conocimiento a los titulares la información que se recaba de ellos, para que fines y el tratamiento que se dará.

En este principio los titulares de los datos deben ser informados de manera clara, precisa y oportuna sobre el tratamiento que se dará a su información personal, esto incluye el propósito del tratamiento, las finalidades del mismo, los mecanismos para el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) garantizando que los titulares de la información sean plenamente informados y tengan control sobre el tratamiento de sus datos personales. Esto es informando al titular a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

**RESPONSABILIDAD.** Se velará en todo momento por el cumplimiento de los principios establecidos en la Ley, adoptando las medidas necesarias para garantizar que el Aviso de Privacidad sea respetado; por lo cual se rendirán cuentas al titular en caso de incumplimiento, este principio es garantía para el titular de los datos, respecto de los tratamientos llevados a cabo.

Bajo este principio se establecerán los procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales, el responsable podrá valerse de estándares,



mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.

## V. DEBERES PARA LA PROTECCIÓN DE DATOS PERSONALES

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

**Deber de confidencialidad.** El deber de confidencialidad es fundamental y está vinculado con la obligación de mantener la privacidad y seguridad de la información personal que se recaba y procesa. Este deber implica que se deberán adoptar medidas para prevenir el acceso no autorizado, la divulgación no autorizada y el uso indebido de dicha información, el deber de confidencialidad es entendido como la obligación que cualquier persona que intervenga en el tratamiento de los datos personales debe guardar la secrecía de estos, esta obligación es subsistente aún después de la relación entre las personas y el responsable, e incluso el encargado, hubieren concluido

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

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

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;



- III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
- IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;
- V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
- VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
- VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y
- VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

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

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

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

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

El **riesgo inherente** a los datos personales. Se deben documentar las probabilidades de que una amenaza se configure con respecto a que las medidas de seguridad sean vulneradas y





los datos personales sean expuestos o pierdan sus características de confidencialidad, disponibilidad e integridad.

La **sensibilidad** de los datos personales.

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

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

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

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

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

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

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

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



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

## **VI. ATENCIÓN DE SOLICITUDES DE EJERCICIO DE DERECHOS ARCO**

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

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

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

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

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

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

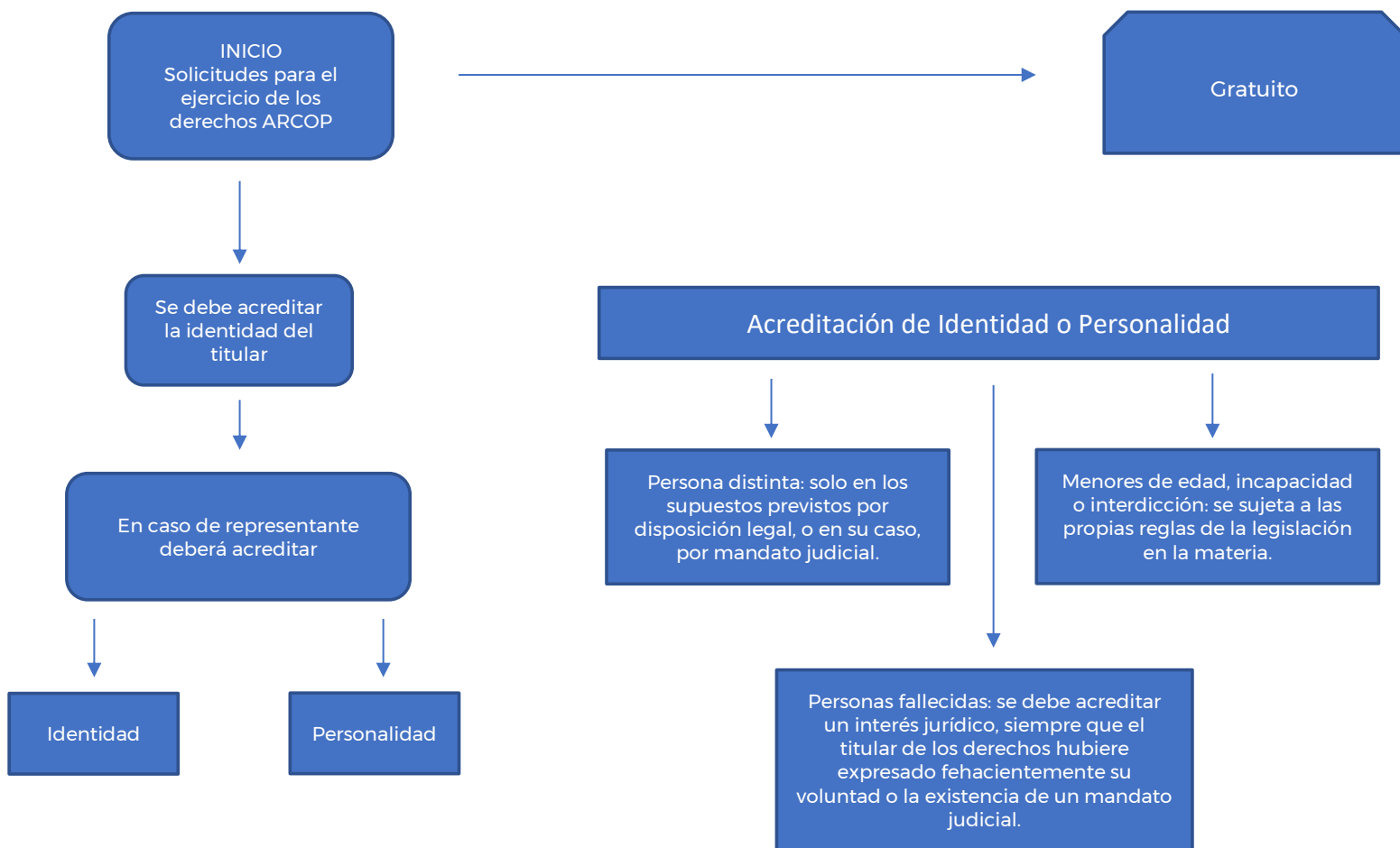
En la atención de las solicitudes se deberá prever dar trámite a todas las solicitudes y entregar al titular el acuse correspondiente, previendo el turno de las solicitudes a todas las unidades administrativas que pudieran tener los datos personales.



## PLAZOS

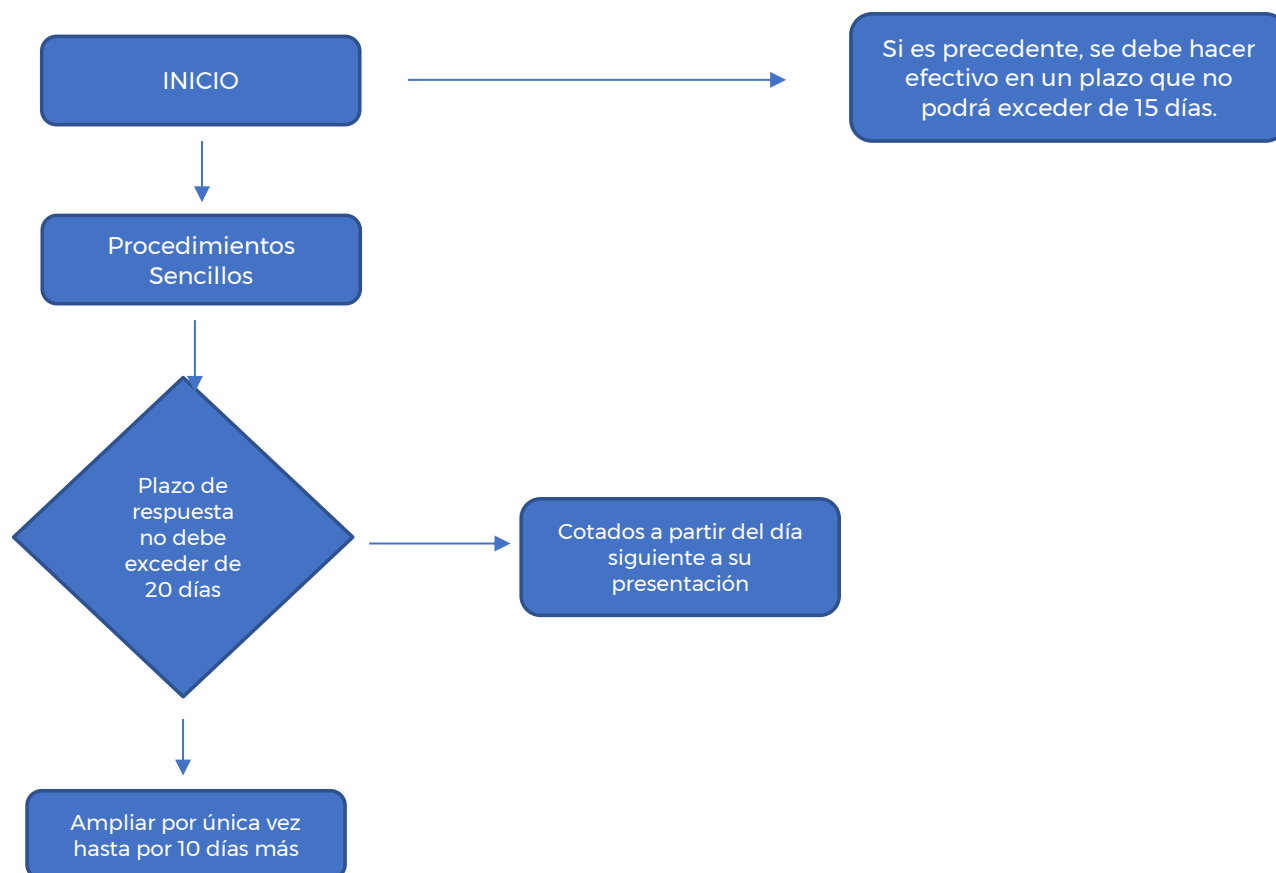
Solicitud de derechos ARCO	No competencia	Prevención	Información disponible públicamente	Respuesta Final	Recurso de revisión
	3 días	5 días	5 días	20 días (+10)	15 días

## SOLICITUDES PARA EL EJERCICIO DE LOS DERECHOS ARCO



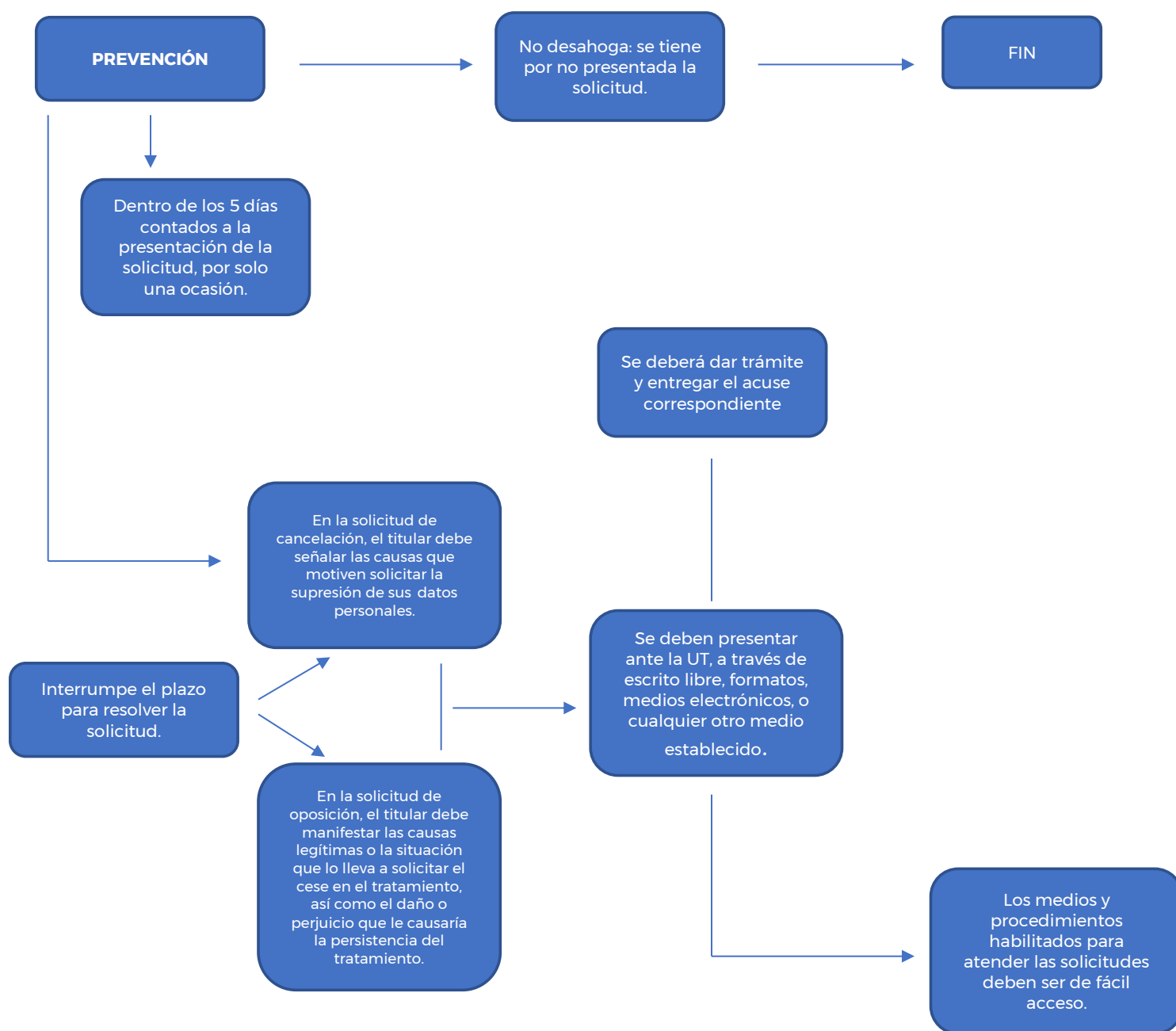


## PLAZO DE RESPUESTA





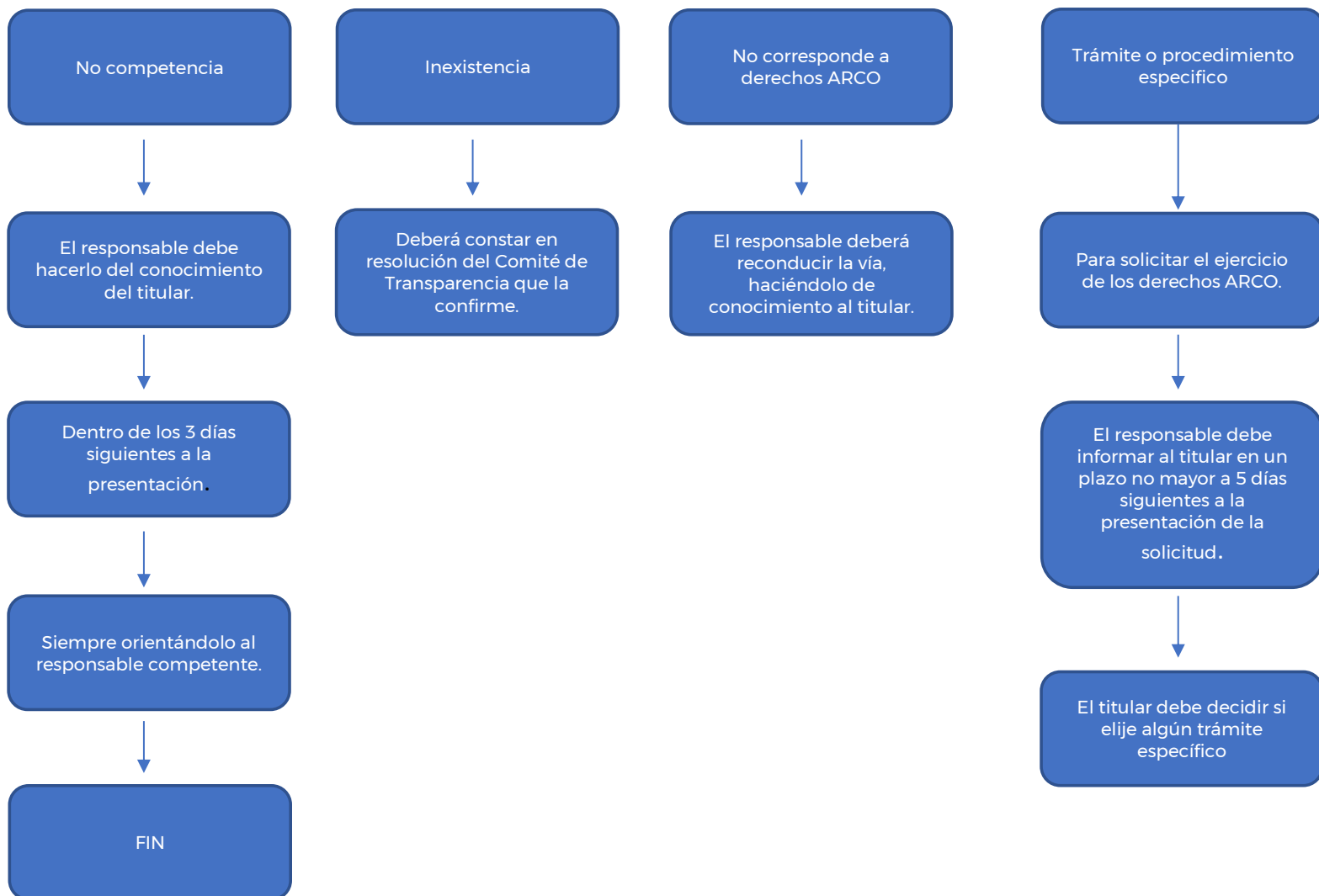
## PREVENCIÓN







## NO COMPETENCIA, INEXISTENCIA, RECONDUCCIÓN, TRÁMITE ESPECÍFICO





## IMPROCEDENCIA

### CAUSALES DE IMPROCEDENCIA

