SENER
SECRETARÍA DE ENERGÍA

POLÍTICAS INTERNAS DE LA SECRETARÍA DE ENERGÍA PARA LA GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES

OBJETIVO GENERAL

Implementar los principios y deberes en materia de protección de datos personales en los procesos internos de gestión y tratamiento de datos personales de la Secretaría de Energía, 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.

AMBITO DE APLICACIÓN

El presente documento es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas de la Secretaría de Energía (SENER) que conforme a sus atribuciones realicen tratamiento de datos personales.

DISPOSICIONES GENERALES

1. Se debe realizar el tratamiento de datos personales con base en las atribuciones conferidas a cada una de las áreas de la Secretaría 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 áreas solo deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de 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 áreas de la Secretaría.

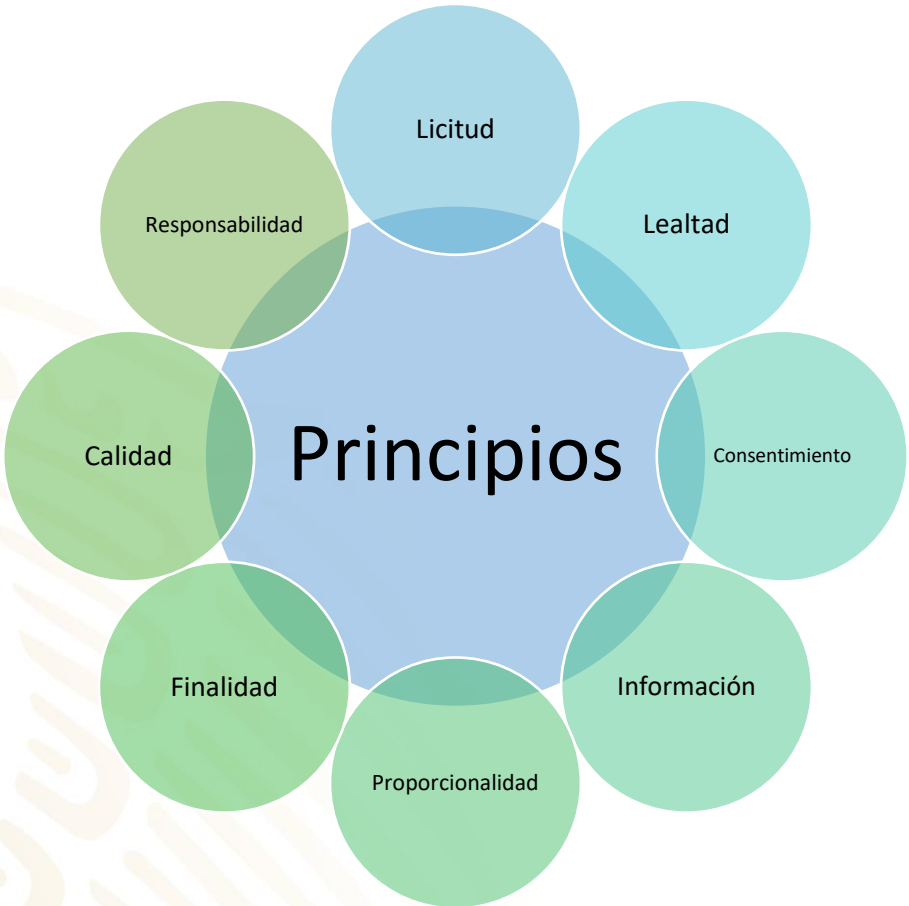
6. Es obligación de todas las personas servidoras públicas de la Secretaría que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.

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 áreas 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 áreas deberán verificar que sus avisos de privacidad simplificados e integrales se difundan en el portal de internet del INAI y estar disponibles de manera impresa en las instalaciones de la Secretaría, en un lugar visible y de fácil consulta por parte de las personas titulares.



PRINCIPIOS, DEBERES Y DEMÁS 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 áreas 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 áreas 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.

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 áreas 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. 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.

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

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

6. 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 del titular o representante.

7. 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.

8. 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 áreas 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 áreas 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 persona 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 áreas 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 áreas 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: (i) obedezca a un mandato legal; (ii) se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o (iii) 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 áreas 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	Completos	Pertinentes	Actualizados	Correctos
• Los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles	• 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	• Los datos personales son pertinentes cuando corresponden efectivamente a su titular	• Los datos están actualizados cuando están al día y coresponden a la situación real de su titular	• 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 áreas 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 áreas 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 áreas 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 áreas 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 áreas 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.

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;

El artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de establecer un sistema de supervisión y vigilancia que permita comprobar el cumplimiento de las políticas de protección de datos personales.

En ese sentido, el artículo 35, fracción VI de la Ley General establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad.

Al respecto, el artículo 33, fracción VII de la Ley General, dispone que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

1. Las medidas de seguridad implementadas en la protección de datos personales.
2. Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales

El artículo 63 de los Lineamientos Generales de protección de datos personales para el sector público establece que 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 anterior, el responsable deberá monitorear continuamente lo siguiente:

1. Los nuevos activos que se incluyan en la gestión de riesgos.
2. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.
3. Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.
4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
6. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
7. Los incidentes y vulneraciones de seguridad ocurridos.

Asimismo, 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.

En ese sentido, el INAI desarrollará el cumplimiento de dicha obligación a través de los siguientes mecanismos:

A. Mecanismo de monitoreo y supervisión

La Unidad de Transparencia será la encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, a través de los siguientes ejes:

I. Etapa de Monitoreo. La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, el llenado de los formatos adjuntos al presente documento.
II. Etapa de Supervisión. La Unidad de Transparencia analizará los reportes de las áreas, y emitirá un documento en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

B. Mecanismos de actuación ante vulneraciones a la seguridad de los datos personales

El artículo 33, fracción VII de la Ley General, dispone que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá 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.

En ese sentido, el artículo 63, fracción VII de los Lineamientos Generales de Protección de Datos Personales para el Sector Publico, entre otras disposiciones estipula que, para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, se deberán monitorear las vulneraciones de seguridad ocurridas.

Por ello, la Unidad de Transparencia deberá monitorear y revisar de manera periódica las medidas de seguridad, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual se podrá auxiliar de todas las unidades administrativas que estime necesarias.

Adicionalmente, resulta oportuno contar con un mecanismo que permita monitorear las alertas de seguridad de los datos personales, como posibles incidentes de seguridad, mismo que se desarrollará a través de las siguientes actividades:

1. Verificar si el hecho o evento podía dar como consecuencia una vulneración a la seguridad (posible incidente de seguridad), esto es:

- Que exista una amenaza que, de haberse concretado, hubiera producido sus efectos en el tratamiento de los datos personales.
- Que dichos efectos, de haberse materializado, hubieran representado un daño en los activos.

2. El área que advirtió de la alerta de seguridad deberá enviar un reporte a la Unidad de Transparencia, en un plazo no mayor a 72 horas, en el que deberá informar:

- Circunstancias de modo, tiempo y lugar en que se detectó la amenaza.
- Sistema de Tratamiento de Datos Personales, conforme al Inventario, en el que se detectó la amenaza.
- Datos personales involucrados.
- Datos de identificación y de contacto de la persona servidora pública responsable del tratamiento de los datos personales.
- Actuaciones que pueden evitar la explotación de la amenaza.
- Descripción de los controles físicos o electrónicos involucrados en la amenaza.

3. La Unidad de Transparencia registrará la alerta de seguridad y analizará el impacto de la amenaza y, de ser posible, determinará una estrategia de prevención, para lo cual, podrá apoyarse de las áreas técnicas y normativas de la SENER, con la finalidad de evitar que la alerta de seguridad pueda desencadenarse.

C. Mecanismos de supervisión y vigilancia en materia de datos personales

Entre los mecanismos que se deben adoptar para cumplir con el principio de responsabilidad el artículo 30, fracción V de la Ley General de Datos Personales en Posesión de Sujetos Obligados, establece que se deberá

mantener un sistema de supervisión y vigilancia que permita comprobar el cumplimiento de las políticas de datos personales.

PROCESO GENERAL DE ATENCIÓN DE LOS DERECHOS ARCO

SOLICITUD DE DERECHOS ARCO

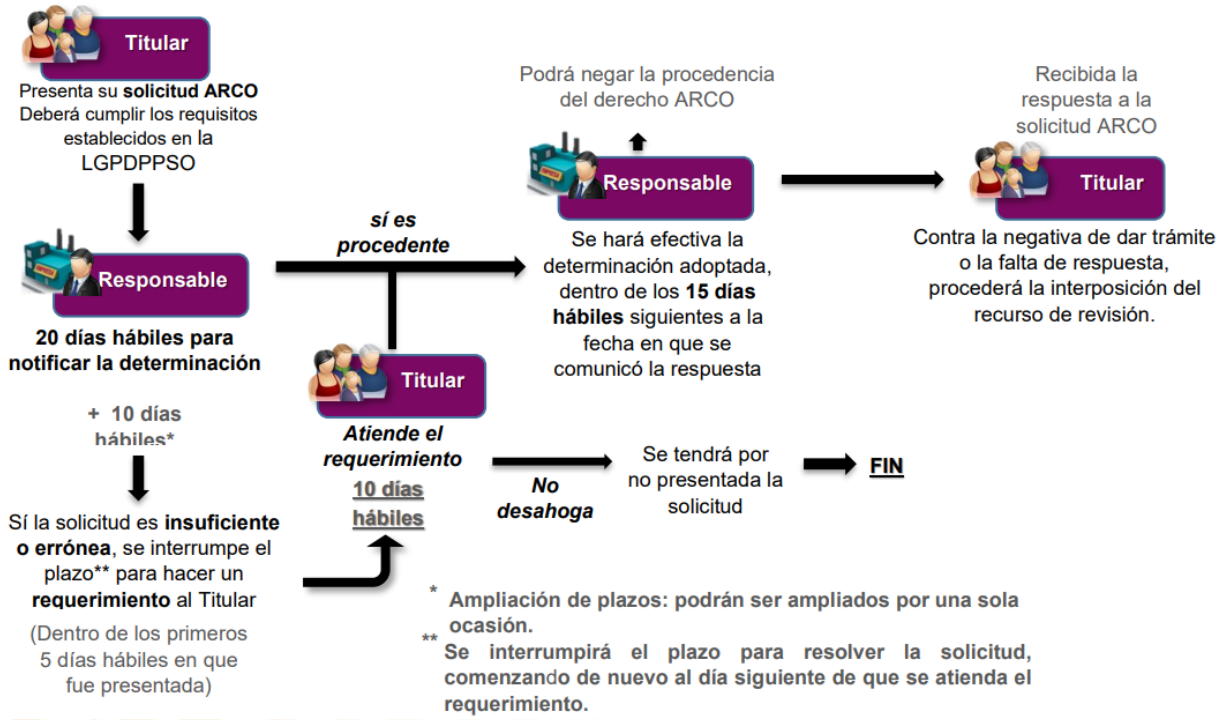
No Competencia (3 días)

Prevención (5 días)

Información disponible públicamente (5 días)

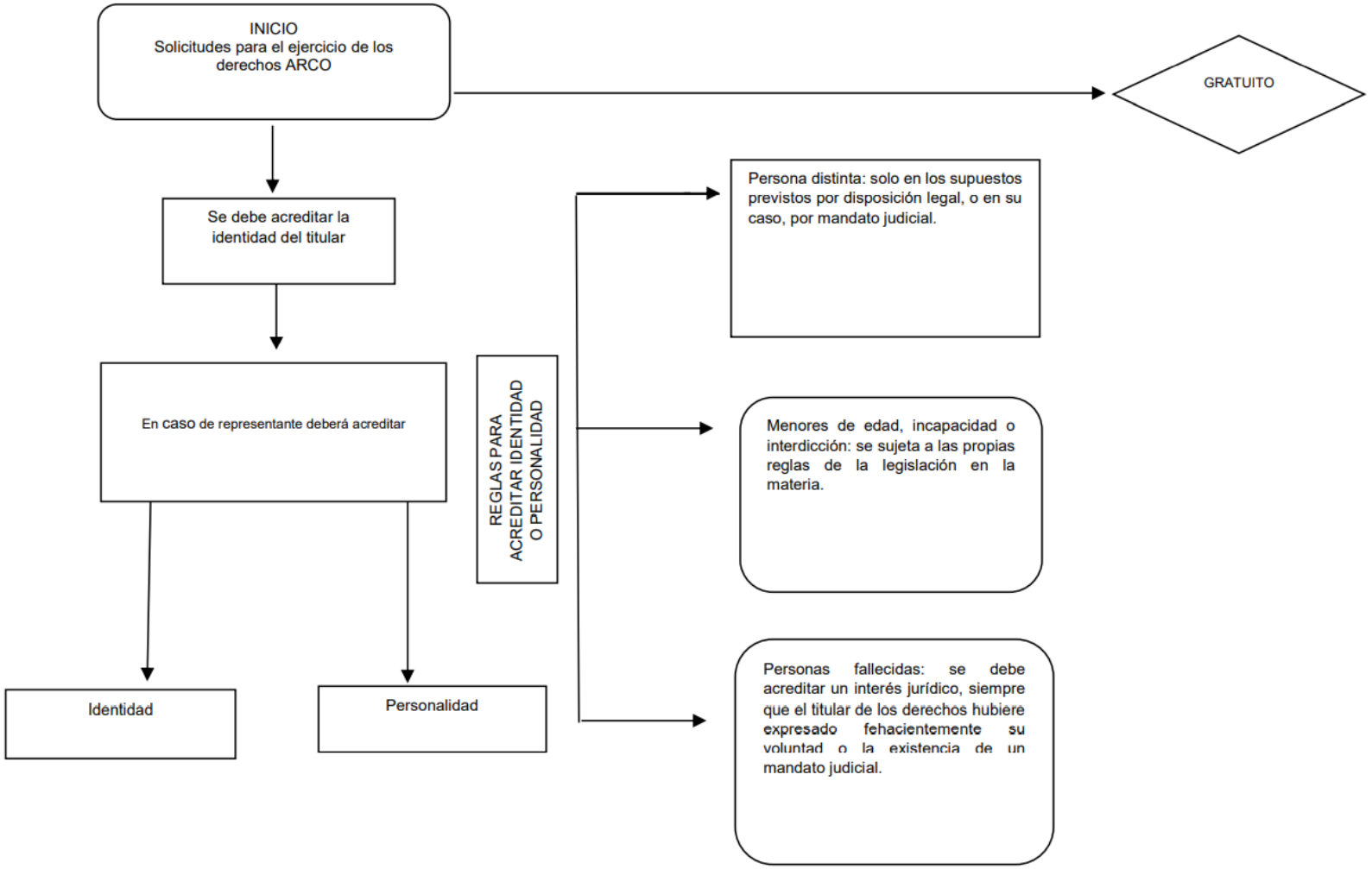
Respuesta terminal (20 días(+10))

Recurso de Revisión (15 días)



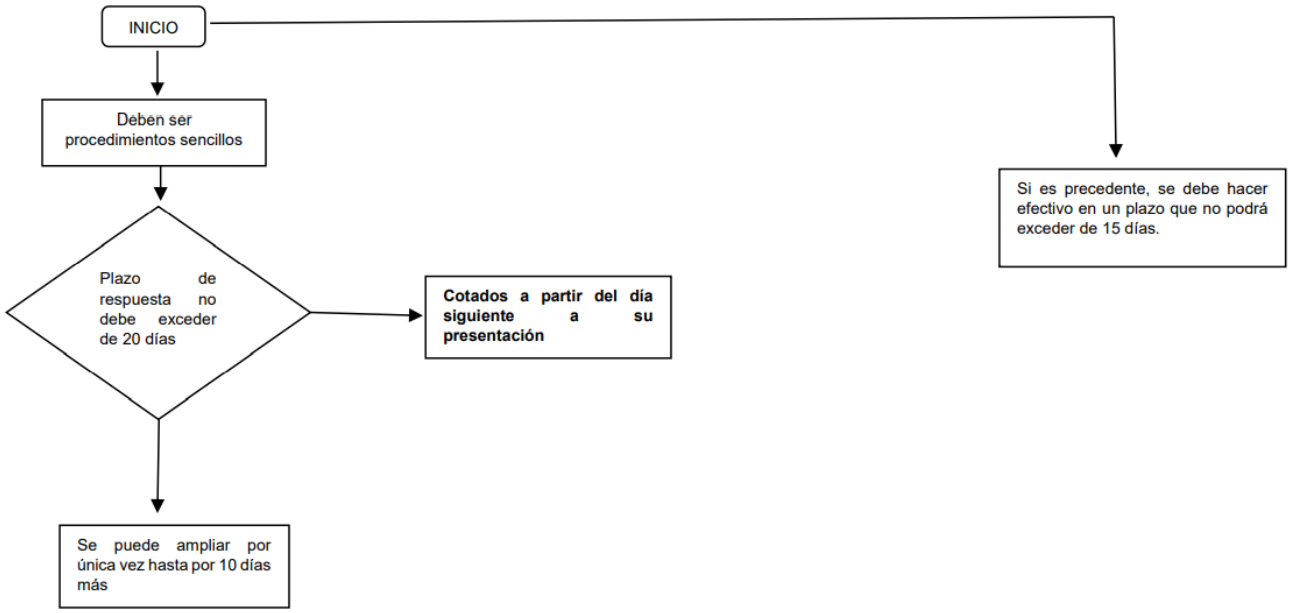
SENER
SECRETARÍA DE ENERGÍA

INICIO SOLICITUDES PARA EL EJERCICIO DE LOS DERECHOS ARCO

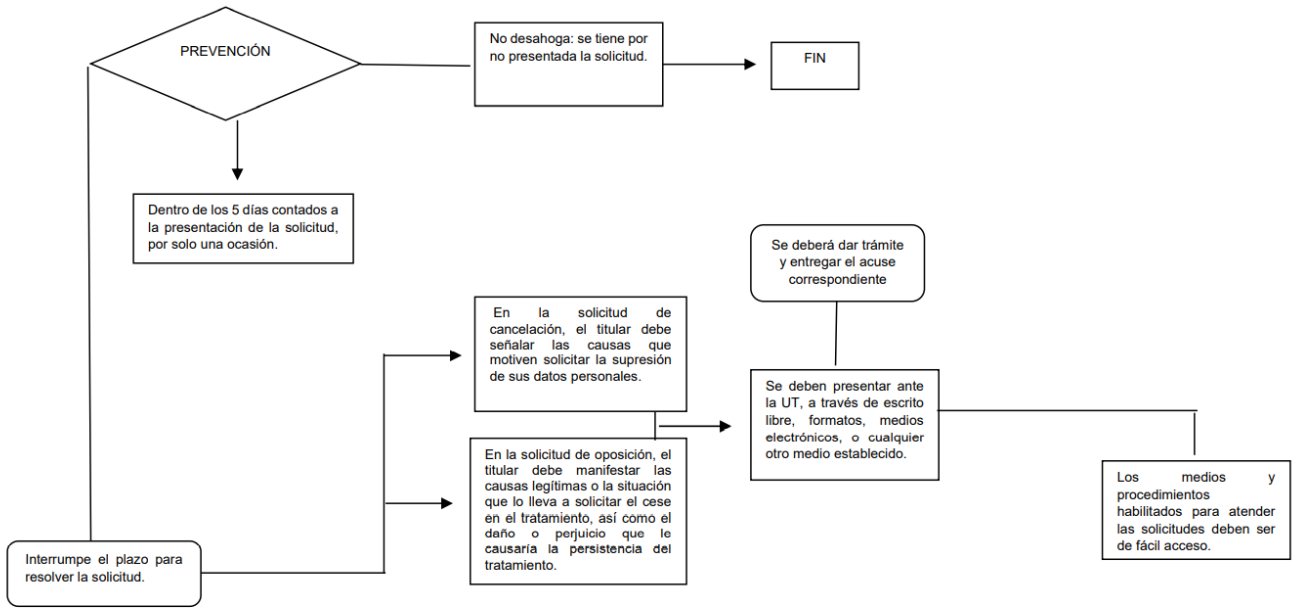


Insurgentes Sur 890, Del Valle, C.P. 03100. Benito Juárez, CDMX
t: (55) 5000.6000 www.gob.mx/sener

PLAZO DE RESPUESTA

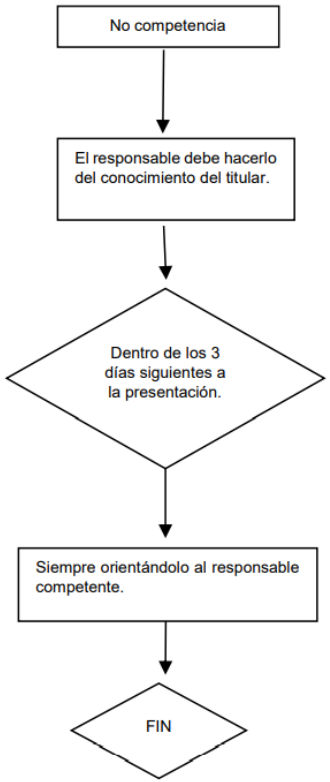


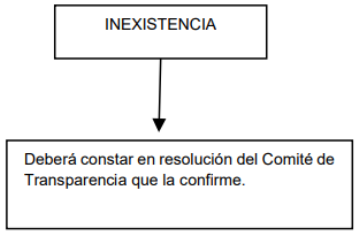
PREVENCIÓN

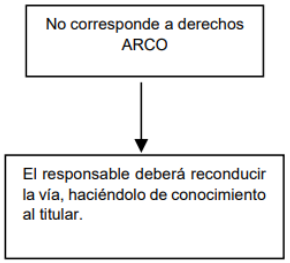


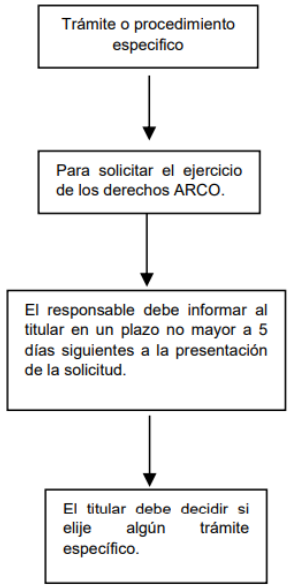
SENER
SECRETARÍA DE ENERGÍA

NO COMPETENCIA, INEXISTENCIA, RECONDUCCIÓN, TRÁMITE O PROCEDIMIENTO ESPECÍFICO





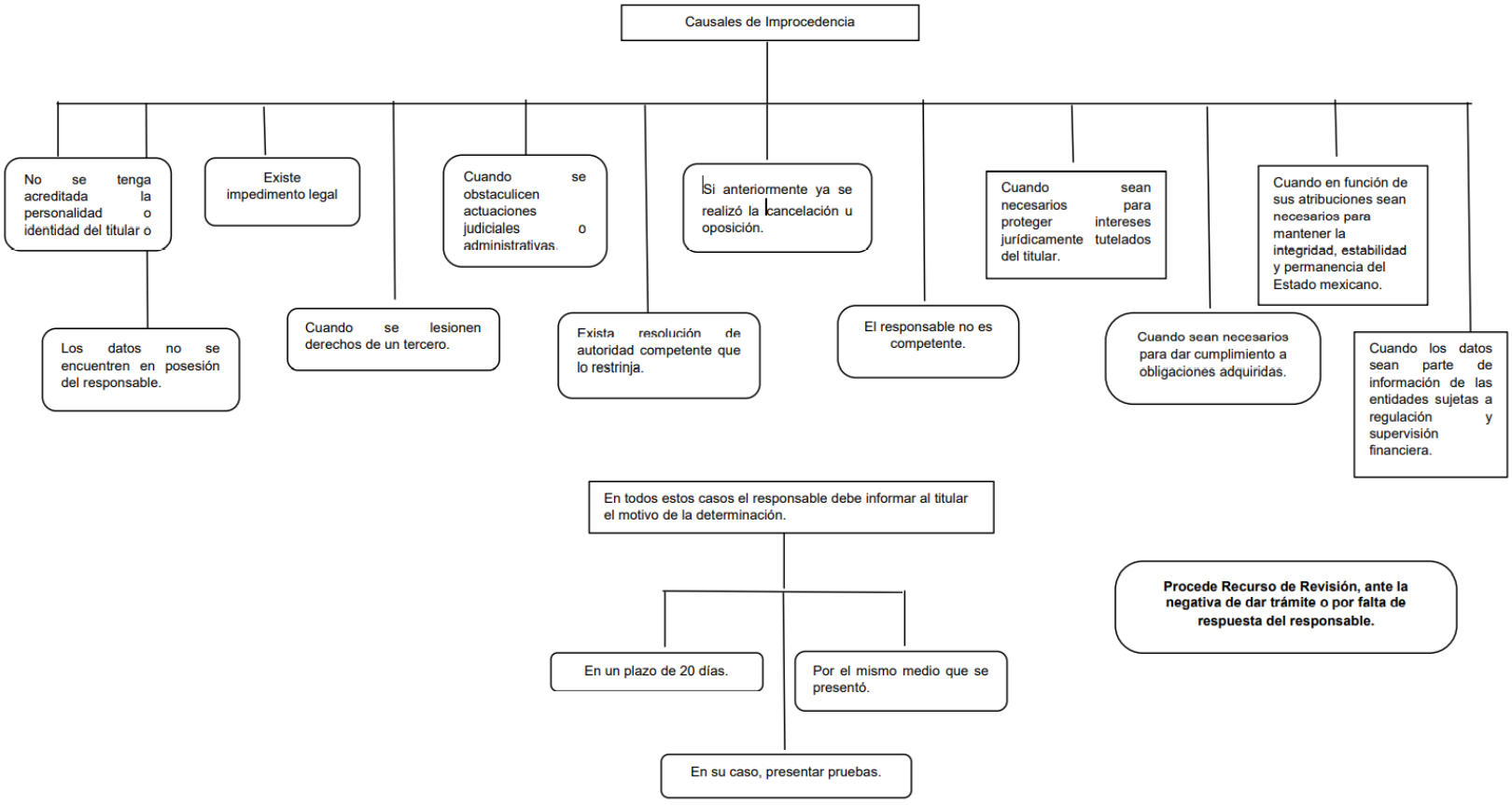




Insurgentes Sur 890, Del Valle, C.P. 03100. Benito Juárez, CDMX
t: (55) 5000.6000 www.gob.mx/sener

SENER
SECRETARÍA DE ENERGÍA

IMPROCEDENCIA



Insurgentes Sur 890, Del Valle, C.P. 03100, Benito Juárez, CDMX
t: (55) 5000.6000 www.gob.mx/sener