El ABC de los esquemas de MEJORES PRÁCTICAS en materia de protección de datos personales

–SECTOR PÚBLICO–

inai

DIRECTORIO

Blanca Lilia Ibarra Cadena
Comisionada Presidenta

Francisco Javier Acuña Llamas
Comisionado

Adrián Alcalá Méndez
Comisionado

Norma Julieta Del Río Venegas
Comisionada

Oscar Mauricio Guerra Ford
Comisionado

Rosendoevgueni Monterrey Chepov
Comisionado

Josefina Román Vergara
Comisionada

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Av. Insurgentes Sur 3211,
Col. Insurgentes Cuicuilco,
Alcaldía Coyoacán,
C.P. 04530,
Ciudad de México.

Edición, noviembre de 2021

ÍNDICE

INTRODUCCIÓN

El presente documento tiene por objetivo orientar a los responsables o encargados que requieren demostrar el cumplimiento en materia de protección de datos personales, teniendo la oportunidad de elevar su nivel establecido por la normatividad, mediante la realización de acciones preventivas como lo son **Esquemas de Mejores Prácticas** en Protección de Datos Personales, los cuales pueden adoptarse en el ámbito federal, estatal y municipal, ya sea por cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Los responsables o encargados pueden optar por inscribir sus **Esquemas de Mejores Prácticas** en materia de protección de datos personales a los que se refiere los artículos 72 y 73 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), y 119 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos).

Para obtener la **validación y reconocimiento de los Esquemas de Mejores Prácticas** por parte del Instituto, el responsable o encargado deberá acreditar el cumplimiento de los Parámetros de Mejores Prácticas en materia de protección de datos personales del sector público (Parámetros), así como las Reglas de Operación del Registro de Esquemas de Mejores Prácticas (Reglas) que ha emitido el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Instituto) y que se señalan en el presente documento. Como parte del reconocimiento el Instituto los publicará en el micrositio **Registro de Esquemas de Mejores Prácticas (REMP)** de acuerdo con diferentes modalidades como las Reglas para adaptar la normativa, sistemas de gestión validados, entidades de acreditación, organismos de certificación y las certificaciones reconocidas por el Instituto u Órgano Garante.

Por último, es importante señalar que el **REMP** permitirá a los interesados conocer a los responsables y encargados que han adoptado Esquemas de Mejores Prácticas, a través del REMP, donde se publicará información relacionada con dichos Esquemas que el Instituto y los Órganos Garantes consideren de interés general y que no se encuentre clasificada en términos de la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública o las legislaciones estatales en la materia.

GLOSARIO

ACREDITACIÓN	Acto por el cual una entidad de acreditación aprobada en términos de la Ley Federal sobre Metrología y Normalización abrogada por la Ley de Infraestructura de la Calidad, que reconoce la competencia técnica y confiabilidad de organismos de certificación para evaluar la conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad aplicable.
ADHERIDO	Responsable que, de manera voluntaria, desarrolla o se obliga a observar un esquema de mejores prácticas.
AUDITORÍA VOLUNTARIA	Proceso sistemático, independiente y documentado, iniciado por solicitud de un responsable al Instituto, enfocado a evaluar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados por los responsables para el tratamiento de datos personales, para la obtención de evidencia que permita determinar su conformidad con las disposiciones previstas en la Ley General y demás normativa aplicable.
CERTIFICACIÓN	Procedimiento llevado a cabo por un organismo de certificación para evaluar la conformidad de un esquema de mejores prácticas o sistemas de gestión y su implementación, así como productos y servicios tecnológicos de tratamiento de datos personales, con relación a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás normatividad que de ella derive.
CERTIFICADO	Documento expedido por un organismo de certificación acreditado y reconocido por el INAI, mediante el cual se hace constar la certificación en materia de mejores prácticas en la protección de datos personales del sector público.
CONFORMIDAD	Cumplimiento de algún requisito previsto en el esquema de mejores prácticas.
ENCARGADO	La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.
ENTIDAD DE ACREDITACIÓN	Persona moral autorizada para acreditar organismos de certificación en materia de protección de datos personales de conformidad con la Ley Federal sobre Metrología y Normalización.

EVALUACIÓN DE COMPETENCIA	Procedimiento mediante el cual se examinan las competencias de un servidor público en materia de protección de datos personales.
LEY GENERAL	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
LEY DE INFRAESTRUCTURA DE LA CALIDAD	Ley que abroga a la Ley Federal sobre Metrología y Normalización.
LINEAMIENTOS GENERALES	Lineamientos Generales de Protección de Datos Personales para el Sector Público.
INSTITUTO O INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
ORGANISMO DE CERTIFICACIÓN	Persona moral que tiene por objeto realizar funciones de certificación en materia de mejores prácticas en la protección de datos personales del sector público.
PARÁMETROS	Parámetros de esquemas de mejores prácticas en materia de protección de datos personales en el sector público.
REGISTRO	Registro de Esquemas de Mejores Prácticas del Instituto.
REGLAS DE OPERACIÓN O REGLAS	Reglas de Operación del Registro de Esquemas de Mejores Prácticas del Instituto.
RESPONSABLE	Los sujetos obligados a que se refiere el artículo 1 de la Ley General.
RESPONSABLE COORDINADOR	Responsable que coordina el desarrollo de esquemas de mejores prácticas elaborados en conjunto con otros responsables o encargados.
SECRETARÍA	Secretaría de Economía.
SISTEMA DE GESTIÓN	Sistema de gestión de seguridad de datos personales al que se refieren los artículos 34 de la Ley General y 65 de los Lineamientos.

¿QUÉ SON LAS MEJORES PRÁCTICAS DE PROTECCIÓN DE DATOS PERSONALES?

Las **Mejores Prácticas en materia de protección de datos personales** se enfocan en identificar acciones, reglas, criterios y procedimientos que resultan eficaces para elevar el nivel de protección de datos personales a través de acciones preventivas en la materia.

Permiten a los responsables o encargados demostrar el cumplimiento en materia de protección de datos personales mediante **Esquemas de Mejores Prácticas** en protección de datos personales a los que se refieren los artículos 72 y 73 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), y 119 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos).

Los **Esquemas de Mejores Prácticas** definen aquellas acciones, reglas, criterios y procedimientos que tienen como **finalidad**:

- **Elevar el nivel** de protección de los datos personales en el sector público.
- **Armonizar el tratamiento** de datos personales en un sector específico.
- Facilitar el ejercicio de los derechos de **acceso, rectificación, cancelación, oposición y portabilidad** de datos personales a las personas titulares.
- **Facilitar las transferencias** de datos personales.
- **Complementar** las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales en el sector público.
- **Demostrar ante el Instituto** y otros interesados, el cumplimiento de la normatividad aplicable en materia de protección de datos personales en el sector público.

Los responsables o encargados podrán adoptar o desarrollar **Esquemas de Mejores Prácticas** de manera individual o en acuerdo con otros responsables, encargados u organizaciones que decidan la validación o reconocimiento por parte del Instituto o en su caso Organismos Garantes para su posterior inscripción en el **Registro de Esquemas de Mejores Prácticas (REMP)**[1], previamente deberá cumplir con la normativa correspondiente a los Parámetros de Mejores Prácticas en materia de protección de datos personales del sector público (Parámetros)[2] y las Reglas de Operación del Registro de Esquemas de Mejores Prácticas (Reglas).[3]

Principios que rigen las Mejores Prácticas

Las mejores prácticas se regirán por los siguientes principios:

- **Imparcialidad.** Las validaciones y reconocimientos de los esquemas de mejores prácticas, así como su certificación deberán realizarse de forma tal que se salvaguarde la objetividad e imparcialidad.

- **Responsabilidad.** El responsable y encargado deberán establecer mecanismos que permitan acreditar el cumplimiento de las obligaciones previstas en la Ley General[4] y demás normativa aplicable, así como rendir cuentas sobre el tratamiento de los datos personales en su posesión, al titular, al responsable o encargado, y al Instituto.

1 Para su consulta: https://registro-esquemas.inai.org.mx/
2 Para su consulta: http://www.dof.gob.mx/2019/INAI/ACT-PUB-11-09-2019-07.pdf
3 Para su consulta: http://www.dof.gob.mx/2020/INAI/ACT-PUB-17-06-2020-04.pdf
4 Para su consulta: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

- **Obligatoriedad.** Una vez que se adhiera a un determinado esquema de mejores prácticas, deberá cumplir e implementar las acciones, reglas, criterios y procedimientos establecidos en el mismo.

- **Transparencia.** Las prácticas señaladas en los esquemas adoptados deberán ser transparentes, salvo aquella información que se especifique como confidencial o reservada en términos de la normatividad aplicable.

- **Voluntariedad.** La decisión sobre el desarrollo o la adopción de un esquema de mejores prácticas es de carácter voluntario.

Modalidades de los Esquemas de Mejores Prácticas

El **responsable o encargado** podrá desarrollar o adoptar esquemas de mejores prácticas bajo las siguientes modalidades:

- **Reglas para adaptar la normativa** de datos personales en sectores específicos, validados por el Instituto.

- **Sistemas de gestión validados** por el Instituto.

- **Esquemas de mejores prácticas, sistemas de gestión, y productos o servicios tecnológicos** de tratamiento de datos personales, certificados por un organismo de certificación en materia de mejores prácticas en la protección de datos personales del sector público, los cuales serán reconocidos por el Instituto.

Las modalidades antes mencionadas se desarrollarán a detalle en los siguientes capítulos de esta guía.

Alcance normativo

- **Alcance total.** Cuando abarquen todos los principios, deberes y obligaciones previstos en la Ley General y demás normativa que de ella derive, incluyendo, en su caso, las reglas para adaptar la normativa, entre ellos, los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; los deberes de seguridad y confidencialidad, así como las obligaciones vinculadas a los derechos de los titulares, la relación entre responsable y encargado, las transferencias, las evaluaciones de impacto en la protección de datos personales y el establecimiento de un sistema de gestión de seguridad de datos personales, entre otros.

- **Alcance parcial.** Cuando abarquen todos los principios, deberes y obligaciones previstos en la Ley General y demás normativa que de ellas derive, incluyendo, en su caso, las reglas para adaptar la normativa, entre ellos, los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; los deberes de seguridad y confidencialidad, así como las obligaciones vinculadas a los derechos de los titulares, la relación entre responsable y encargado, las transferencias, las evaluaciones de impacto en la protección de datos personales y el establecimiento de un sistema de gestión de seguridad de datos personales, entre otros.

Alcance material

A su vez, los esquemas de mejores prácticas podrán tener cualquiera de los siguientes alcances materiales:

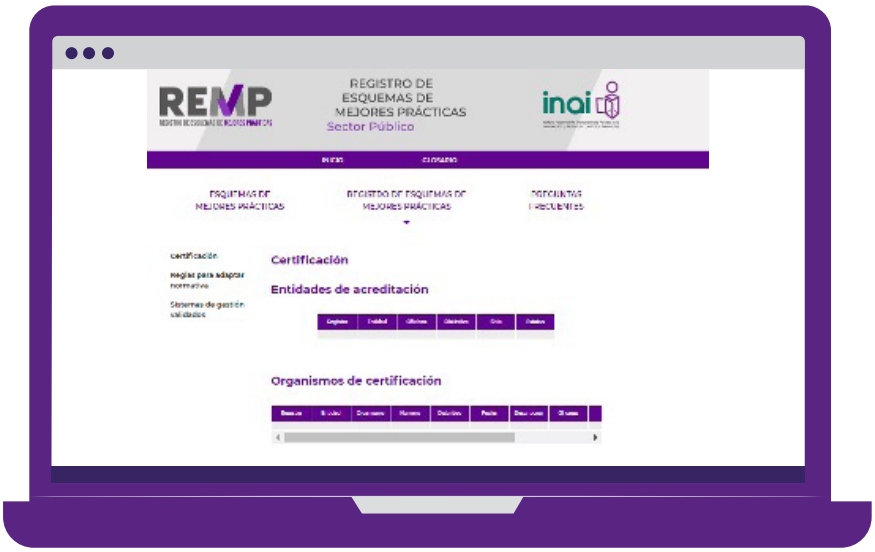
- **Total:** Cuando abarquen todos los procesos de datos personales que realice el responsable o encargado adherido.

- **Parcial:** Cuando abarquen sólo algunos procesos específicos que realice el responsable o encargado adherido.

REGISTRO DE ESQUEMAS DE MEJORES PRÁCTICAS

El Registro de Esquemas de Mejores Prácticas (REMP)[5] permitirá a los interesados conocer a los responsables y encargados que han adoptado **Esquemas de Mejores Prácticas**. A través del REMP se publicará información relacionada con los Esquemas que el Instituto y los Órganos Garantes consideren de interés general y que no se encuentre clasificada en términos de la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública o las legislaciones estatales en la materia.

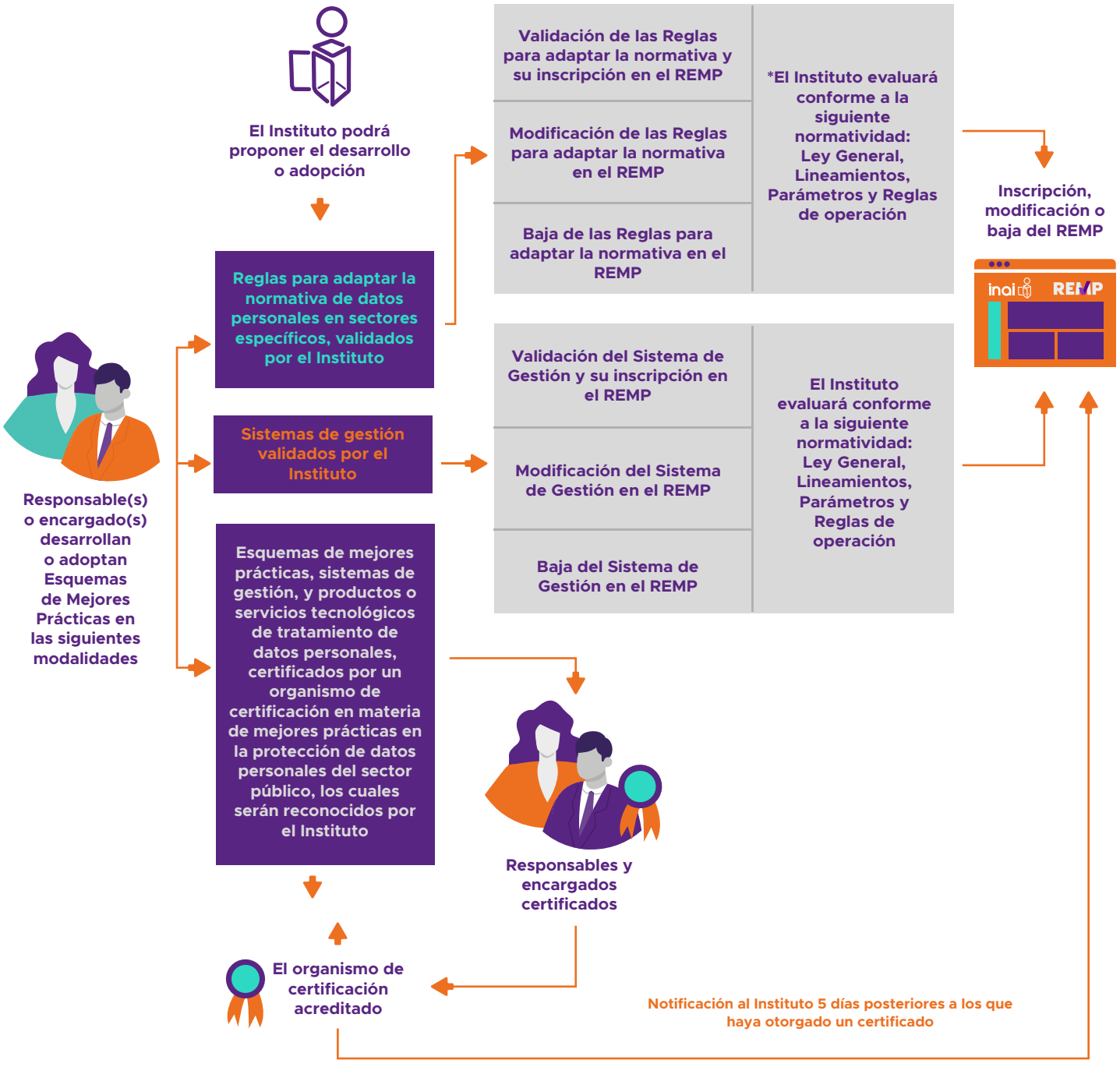
El REMP lo administra el Instituto y se encuentra disponible en https://registro-esquemas.inai.org.mx/; está conformado por tres secciones:



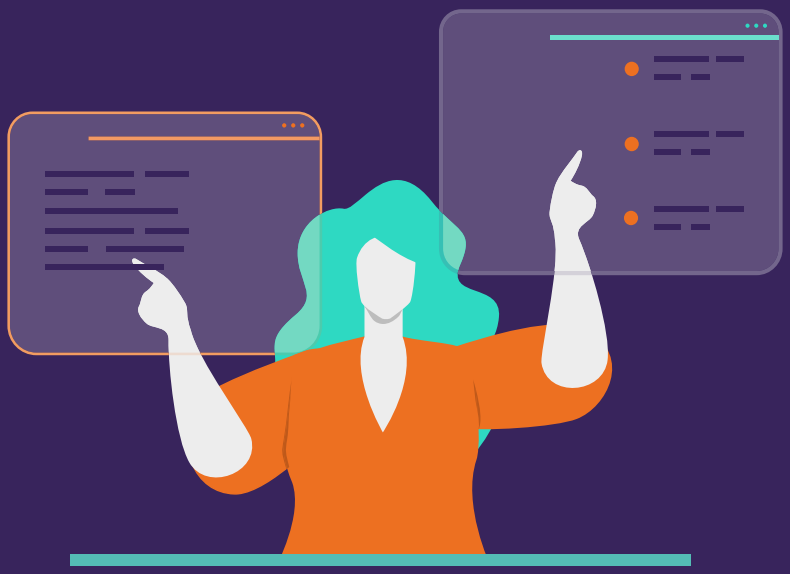
En los posteriores capítulos se desarrollará cada una de las modalidades para la inscripción en el REMP.

5 Para su consulta: https://registro-esquemas.inai.org.mx/

Esquema general para el trámite de Inscripción en el REMP de acuerdo con sus diferentes modalidades.

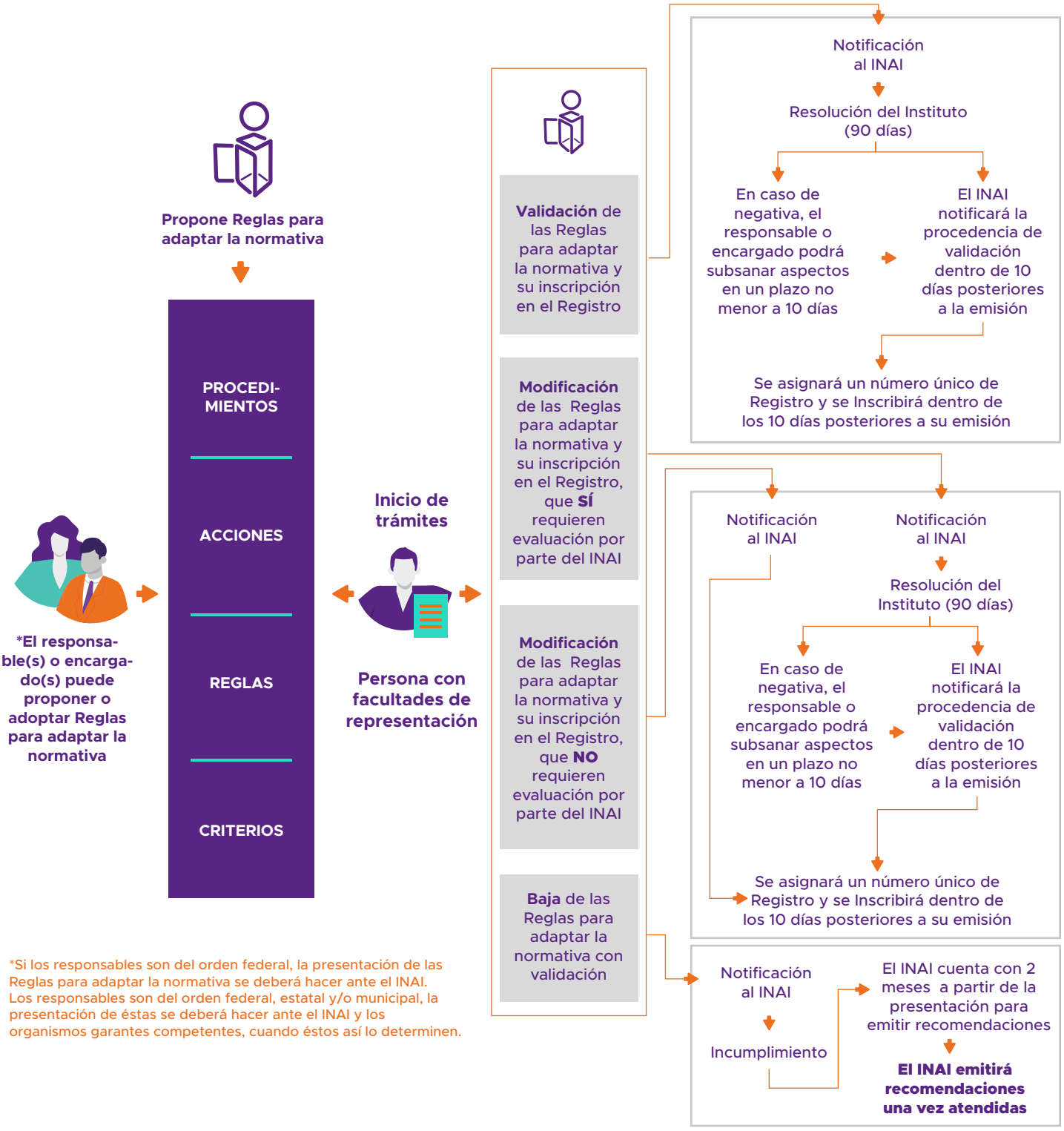


REGLAS PARA ADAPTAR LA NORMATIVA Y SU INSCRIPCIÓN EN EL REGISTRO



REGLAS PARA ADAPTAR LA NORMATIVA DE DATOS PERSONALES EN SECTORES ESPECÍFICOS, VALIDADOS POR EL INSTITUTO

Esquema general del procedimiento para la adopción o implementación de las Reglas para adaptar normativa.

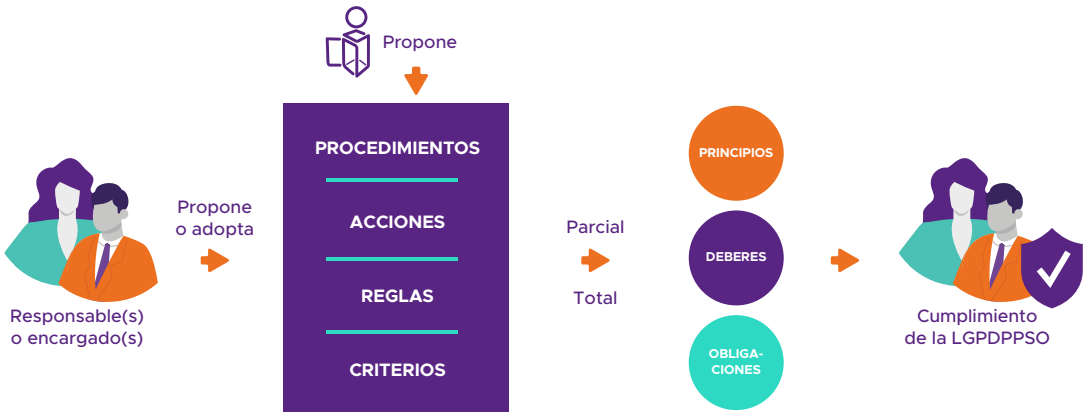


*Si los responsables son del orden federal, la presentación de las Reglas para adaptar la normativa se deberá hacer ante el INAI. Los responsables son del orden federal, estatal y/o municipal, la presentación de éstas se deberá hacer ante el INAI y los organismos garantes competentes, cuando éstos así lo determinen.

Las **Reglas para adaptar normativa**[6] tienen por objetivo establecer reglas, criterios, procedimientos o acciones específicas para mejorar la eficiencia de la implementación de los principios, deberes y obligaciones en materia de Protección de Datos Personales previstos en la Ley General[7] y Leyes estatales en la materia.

Las **Reglas para adaptar normativa** podrán tener un **alcance total** cuando abarquen todos los procesos de datos personales que realice el responsable o encargado, y/o **alcance parcial** cuando abarquen sólo algunos procesos específicos.

El Instituto podrá proponer a los responsables el desarrollo o adopción de **Reglas para adaptar la normativa**, cuando considere que ayudará a mejorar la eficiencia de la aplicación de la norma y podrán desarrollarse a través de códigos de buenas prácticas, modelos en materia de datos personales, programas u otros. A continuación, se muestra de manera general el proceso de adopción o desarrollo:



Procedimiento para solicitar la validación del Instituto y su inscripción en el REMP

Las Reglas para adaptar la normativa que desarrollen o adopten los responsables en términos de los artículos 72 y 73 de la Ley General y del artículo 10 fracción I de los Parámetros, que soliciten la validación del Instituto, así como su inscripción, modificación y baja, deberán ser notificados al Instituto.

6 Para su consulta: https://registro-esquemas.inai.org.mx/?page_id=610

7 Para su consulta: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Trámite de validación de las Reglas para adaptar la normativa y su inscripción en el REMP

Requisitos y procedimientos del trámite de validación de las Reglas para adaptar la normativa y su inscripción en el REMP:

1. **Servidor público con facultades** para realizar el trámite. En caso de que las Reglas para adaptar normativa se hayan desarrollado por dos o más responsables o encargados, la notificación deberá realizarla el responsable coordinador designado previamente por ellos mismos.

2. **Notificar al Instituto** de la existencia de Reglas para adaptar la normativa que soliciten la validación. La notificación deberá contener lo siguiente:

La notificación deberá contener la siguiente información
La denominación de las Reglas para adaptar la normativa.
La denominación de los responsables o el nombre completo, denominación o razón social de los encargados que han decidido adherirse o adoptar las Reglas para adaptar la normativa, al momento de la presentación de la solicitud de validación.
Denominación del responsable coordinador, en caso de Reglas para adaptar la normativa desarrolladas en conjunto por dos o más responsables o encargados, así como la documentación prevista en el artículo 18 de las Reglas.
Objetivo de las Reglas para adaptar la normativa.
Sector al que aplican las Reglas para adaptar la normativa.
La vigencia de las Reglas para adaptar la normativa, en su caso.
Alcance de las Reglas para adaptar la normativa de acuerdo con el artículo 19 de los Parámetros.
Ámbito personal de aplicación, es decir, el tipo o grupo de titulares cuyos datos personales están vinculados con el tratamiento al que aplican las Reglas para adaptar la normativa.
Los requisitos y el procedimiento de adhesión a las Reglas para adaptar la normativa en caso aquellas desarrolladas en conjunto por dos o más responsables o encargados.
Los medios por los cuales se comunicará a los interesados cualquier aspecto relacionado con las Reglas para adaptar la normativa en caso de aquellas desarrolladas en conjunto por dos o más responsables o encarga dos, incluidas las modificaciones o cancelaciones a las mismas.
Documento que contenga el desarrollo de las Reglas para adaptar la normativa que se someten a validación.
Datos de contacto o un medio habilitado con fines de difusión de las Reglas para adaptar la normativa.
El correo electrónico y el domicilio, para oír y recibir notificaciones, de conformidad con el artículo 12 de las Reglas.
La notificación deberá ir acompañada de un dispositivo de almacenamiento electrónico con la información referida anteriormente, salvo que dicha notificación sea realizada a través del sistema informático que, en su caso, habilite el Instituto.

3. **Instituto resolverá** la procedencia de la validación de Reglas para adaptar la normativa y su inscripción en el REMP, en un plazo de 90 días contados a partir de día siguiente a la recepción de la notificación.

4. **Resolución por parte del Instituto**, en caso de negativa el responsable o encargado podrá subsanar aspectos de las Reglas para adaptar la normativa en un plazo no menor a diez días; en caso de que lo requiera, el solicitante podrá solicitar una prórroga que no podrá exceder de treinta días naturales, lo cual deberá presentarse por escrito al Instituto por una sola vez, justificando lo anterior.

5. **El Instituto notificará** al responsable o encargado la procedencia de la validación dentro de los diez días posteriores a la emisión de esta.

6. Cuando el Instituto valide las Reglas para adaptar la normativa con validación en el REMP, se procederá a su **inscripción y publicación en el REMP dentro de los diez días** posteriores a la emisión de esta.

Modificación de las Reglas para adaptar la normativa y su inscripción en el REMP

Las modificaciones a cualquier contenido de las Reglas para adaptar la normativa previstos en el Capítulo IV de los Parámetros y por el artículo 20 de las Reglas, deberán ser notificados al Instituto por las personas previstas para hacer notificaciones en el artículo 17 de las Reglas. Requisitos y procedimientos del trámite de modificación de las Reglas para adaptar la normativa y su inscripción en el REMP:

1. Identificar el tipo de modificación:

    - **Modificaciones que no requieren evaluación por parte del Instituto**. Cuando las modificaciones notificadas al Instituto no afecten de manera sustantiva el contenido de las Reglas, no requerirán de evaluación por parte del Instituto y se realizará la actualización en un plazo de **10 días** en el REMP.

    - **Modificaciones que sí requieren evaluación por parte del Instituto**. La resolución sobre procedencia de la modificación de las Reglas para adaptar la normativa con validación resolverá en el plazo de 90 días para emitir una resolución. En caso de negativa el solicitante podrá subsanar lo solicitado por el Instituto para su acreditación.

2. Servidor público con facultades para realizar la notificación ante el Instituto.

3. Notificar al Instituto de las Reglas para adaptar la normativa que soliciten modificación. La notificación deberá contener lo siguiente:

Requisitos que deberá contener la notificación
El nombre y número único de registro de las Reglas para adaptar la normativa que se modifica.
Las modificaciones propuestas, los motivos de las modificaciones, así como la fecha en que pretenden hacerse efectivas o se hicieron efectivas.

La documentación necesaria para acreditar la modificación, en su caso.
La notificación deberá ir acompañada de un dispositivo de almacenamiento electrónico con la información referida en los numerales anteriores, salvo que dicha notificación sea realizada a través del sistema informático que, en su caso, habilite el Instituto.

Las **modificaciones propuestas** deberán cumplir, en todo momento, con los requisitos establecidos en la Ley, los Lineamientos Generales, los Parámetros, las Reglas y demás normativa aplicable.

Baja de las Reglas para adaptar la normativa y su inscripción en el REMP

En caso de que las Reglas para adaptar la normativa dejen de tener aplicación, de conformidad con los artículos 21, 22 y 23 de los Parámetros, la persona designada para realizar notificaciones al Instituto deberá notificarle este hecho, en un plazo no mayor a diez días posteriores a que se actualice cualquiera de los supuestos en que pueda ser desechado de acuerdo con el artículo 22 de los Parámetros.

Las Reglas podrán ser objeto de baja cuando:

- Así lo **decidan y lo soliciten** quienes hayan presentado el trámite de su validación.
- Haya **concluido su vigencia**, en caso de que ésta sea prevista o en caso contrario, éstas serán de carácter permanente hasta en tanto no se actualice alguna condición prevista en su baja.
- Cuando se determine que **dejaron de cumplir el objetivo** de establecer reglas, criterios, procedimientos o acciones específicos para mejorar la eficiencia de la implementación de los principios, deberes y obligaciones de protección de datos personales previstos en la Ley general y las leyes estatales en la materia, atendiendo a las necesidades o características particulares de un sector.

Requisitos y procedimientos del trámite de baja de las Reglas para adaptar la normativa y su inscripción en el REMP:

1. **Servidor público** con facultades para realizar el trámite ante el Instituto.

2. **Notificación de la terminación de Reglas para adaptar la normativa** con validación. La notificación deberá incluir:

Requisitos del trámite de baja de Reglas para adaptar la normativa con validación
El nombre y número único de registro de las Reglas para adaptar la normativa con validación del cual se solicita la baja.
Los motivos por los que las Reglas para adaptar la normativa dejan de tener aplicación.

Cuando el Instituto observe algún incumplimiento en los términos en que fue emitida la validación de Reglas para adaptar la normativa, se iniciará el procedimiento de baja de las Reglas para adaptar la normativa del REMP. El responsable o encargado podrá subsanar y aportar la documentación que estime procedente ante el Instituto en un plazo de **15 días** contados a partir de la notificación, por su parte el Instituto contará con un plazo de máximo **2 meses** contados a partir de su presentación; este plazo podrá ampliarse por un periodo igual cuando existan razones justificadas y sea notificado al responsable o encargado.

Como consecuencia de la baja de Reglas para adaptar la normativa con validación, el responsable, encargado o responsable coordinador se abstendrán de hacer referencia o publicar dichas Reglas para adaptar la normativa como validadas por el Instituto.

Durante el desarrollo del procedimiento de baja, el Instituto publicará en el REMP[8], que la validación en cuestión se encuentra sujeta a dicho procedimiento. Una vez que el Instituto haya emitido la resolución correspondiente, ésta se publicará en el REMP con sus respectivos cambios.

Las Reglas para adaptar la normativa no eximen a los responsables ni encargados de su obligación de cumplir con lo dispuesto por la Ley General y demás normatividad aplicable.

Los trámites relacionados con la validación, modificación o baja de las Reglas para adaptar la normativa e inscripción en el REMP, que se realicen ante el INAI serán gratuitos y se presentarán por escrito en sus oficinas ubicadas en Avenida Insurgentes Sur, Número 3211, Colonia Insurgentes Cuicuilco, en la Alcaldía Coyoacán, Código Postal 04530, de lunes a jueves de 9:00 a 18:00 horas y viernes de 9:00 a 15:00 horas, o a través de otros medios que el INAI habilite para esos efectos.

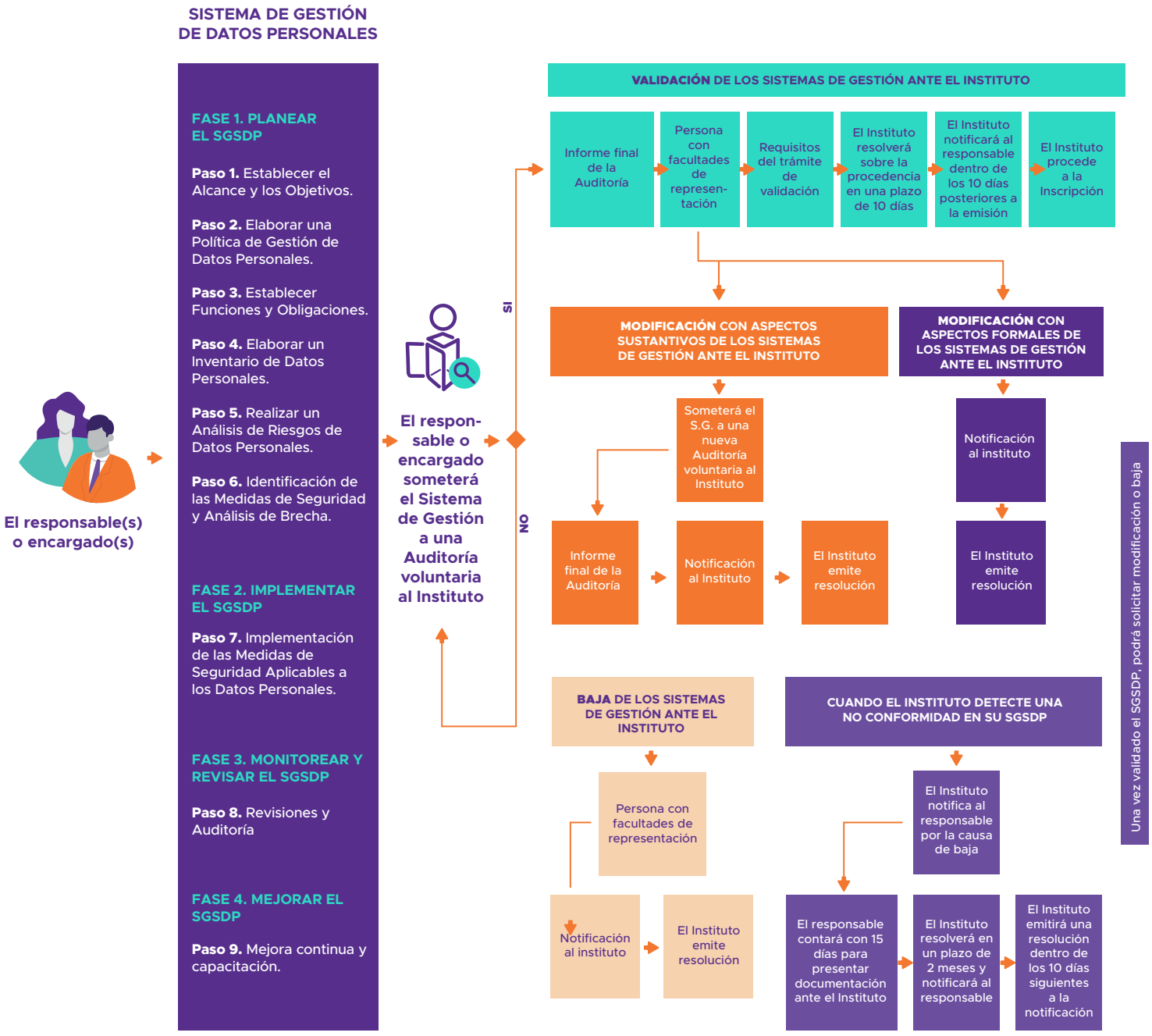
Para más información contacte al **Centro de Atención a la Sociedad** del INAI.

8 Para su consulta en: https://registro-esquemas.inai.org.mx/

SISTEMAS DE GESTIÓN
VALIDADOS POR EL INSTITUTO

SISTEMAS DE GESTIÓN VALIDADOS POR EL INSTITUTO

Diagrama general de los procedimientos para la validación, modificación o baja de los Sistemas de Gestión validados por el Instituto.



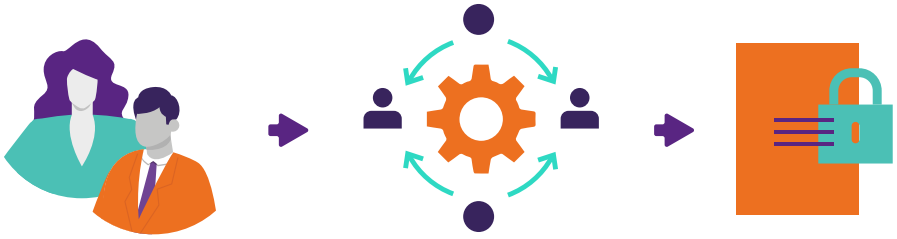
La **Gestión** es un conjunto de actividades coordinadas para dirigir y controlar un proceso o tarea. Un Sistema es un conjunto de elementos mutuamente relacionados o que interactúan por un fin u objetivo. Por lo tanto, un **Sistema de Gestión (SG)** se define como un conjunto de elementos y actividades interrelacionadas para establecer metas y los medios de acción para alcanzarlas.[9]

El **Sistema de Gestión** permite operar, controlar de forma sistemática y transparente sus procesos a fin de lograr con éxito sus actividades, ya que está diseñado para mejorar continuamente el desempeño de las actividades interrelacionadas en los procesos.

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

Un **Sistema de Gestión de Seguridad de Datos Personales (SGSDP)** tiene por objetivo proveer un marco de trabajo para el tratamiento de datos personales que permita mantener vigente y mejorar la protección de datos personales para el cumplimiento de la legislación y fomentar las buenas prácticas.

Es responsabilidad de los **Sujetos Obligados** contar con un **Sistema de Gestión** que contenga todas aquellas actividades que permiten establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en el artículo 34 de la Ley General.



LAS FASES QUE CONTEMPLA EL SGSDP

En caso de las recomendaciones en materia de Seguridad de los Datos Personales, emitidas por el INAI, el sistema de gestión propuesto se basa en el modelo denominado "Planificar-Hacer-Verificar-Actuar" (PHVA).[10]

Las fases del ciclo PHVA considera diferentes pasos y objetivos específicos para el SGSDP que se describen a continuación:

Fase 1. Planear el SGSDP

En la fase de planeación del SGSDP se requiere establecer los objetivos y procesos necesarios para llegar a la meta u obtener los resultados esperados por el responsable, en este caso en particular, la protección y seguridad de los datos personales.

9 Para su consulta: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

10 Ídem

Paso 1. Establecer el Alcance y los Objetivos

El responsable debe definir el alcance y establecer los objetivos del sistema de gestión. A continuación, se muestra un ejemplo de objetivo y alcance:

Objetivo	**¿Qué se quiere lograr?**	Implementar medidas de seguridad de datos personales en la Secretaría del Porvenir
Alcance	**¿A dónde queremos llegar ?**	Implementar las medidas de seguridad al departamento de Recursos Humanos de la Secretaría del Porvenir

Paso 2. Elaborar una Política de Gestión de Datos Personales

Una vez que han sido definidos los alcances y objetivos de la gestión de los datos personales, el responsable directamente deberá emitir e implementar una política de gestión y seguridad que ayude al logro de los objetivos planteados.

La política debe establecer el compromiso de cumplir con la legislación en protección de datos personales por parte de todos los involucrados en el tratamiento, por lo que debe ser comunicada a los mismos, e incluir al menos las siguientes reglas:

Estructura de una política					
¿Qué?		**¿Quién?**	**¿Por qué?**	**¿Cómo?**	**¿Cuándo/ donde?**
¿Qué voy a proteger?		**¿Quién lo va a proteger?**	**¿Cuál es la razón y la acción?**		**¿Cuál es el periodo?**
Activo(s) de información	Activo(s) de Apoyo	Responsable/ Encargado	Identificar la razón del tratamiento	Identificar la acción del tratamiento	Periodo de conservación definido por el responsable
Datos Personales	Bases de datos en formato digital	Personal encargado de TI	Pruebas de seguridad	Auditorías informáticas	Después de 2 años

Paso 3. Establecer Funciones y Obligaciones

El responsable debe determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener el SGSDP.

	Obtención	Uso	Divulgación	Almacenamiento	Bloqueo	Cancelación
Sistema de administración de personal	X	X			X	X
Archivero, expedientes, empleados		X		X		X

Paso 4. Elaborar un Inventario de Datos Personales

Se debe establecer y mantener actualizado un inventario de los sistemas de tratamiento de datos personales que utiliza una organización. Este inventario debe identificar o estar vinculado con la información básica que permita conocer el tipo de tratamiento al que son sometidos los datos personales, la cual se relaciona de manera directa con su flujo o ciclo de vida, considerando:

Paso 5. Realizar un Análisis de Riesgos de Datos Personales

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos los datos personales, el riesgo no se puede erradicar completamente, pero sí se puede minimizar a través de la mejora continua.

El objetivo de esta sección es que los responsables determinen las características del riesgo que mayor impacto puede tener sobre los datos personales que tratan, con el fin de que prioricen y tomen la mejor decisión respecto a los controles más relevantes e inmediatos a implementar.

Activo	Amenaza	Vulnerabilidad	Daño/Impacto	Potencial/ Probabilidad
Expediente de becas (electrónico)	Intrusiones	Servidores sin firewall (cortafuegos)	Borrado permanente de información	Muy probable
Expediente de sanciones (papel)	Incendio	Material susceptible al fuego	Pérdida definitiva de información	Poco probable

Paso 6. Identificación de las Medidas de Seguridad y Análisis de Brecha

Con base en el análisis de riesgos se deberán seleccionar e implementar las medidas de seguridad administrativas, técnicas o físicas que permitan disminuir los riesgos, y podrán ser seleccionadas del listado mostrado en la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales en su Anexo D[11], sobre controles de seguridad.

Dichos controles de seguridad se han agrupado en 10 dominios principales que son:

01	Políticas del SGSDP
02	Cumplimiento legal
03	Estructura organizacional de la seguridad
04	Seguridad física y ambiental
05	Gestión de comunicaciones y operaciones
06	Control de acceso
07	Clasificación y acceso de los activos
08	Seguridad del personal
09	Desarrollo y mantenimiento de sistemas
10	Vulneraciones de seguridad

11 Para su consulta: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Es importante tener claro cuáles son los controles que ya están funcionando en una organización de manera efectiva, con su respectivo nivel de madurez, así como las medidas identificadas como faltantes, para constituir un programa de trabajo que refleje los recursos designados, los responsables, y las fechas compromiso para su implementación.

El **análisis de brecha** consiste en identificar:

- Las medidas de seguridad existentes.
- Las medidas de seguridad existentes que operan correctamente.
- Las medidas de seguridad faltantes.
- Si existen nuevas medidas de seguridad que puedan remplazar a uno o más controles implementados actualmente.

Fase 2. Implementar el SGSDP

En esta fase se **implementan y operan las políticas**, procesos, procedimientos y controles o mecanismos del SGSDP. En el caso que nos ocupa, en esta fase se deberán implementar las medidas de seguridad que hayan resultado aplicables según el análisis de riesgos realizado en la fase de planeación.

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

Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales

En esta fase se deberán implementar las medidas de seguridad que hayan resultado aplicables según el análisis de riesgos realizado en la fase de planeación.

La organización deberá considerar un conjunto de indicadores para identificar de manera oportuna, cualquier cambio en el contexto de la organización y así mantener una visión general de la imagen del riesgo, entre más pronto se realice esta detección, las partes interesadas podrán tomar decisiones más efectivas para proteger los datos personales.

Fase 3. Monitorear y Revisar el SGSDP

En esta fase, se evalúan y miden los resultados de las políticas, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.

Paso 8. Revisiones y Auditoría

Se debe monitorear y revisar el riesgo con sus factores relacionados, es decir, el valor de los activos, las amenazas, vulnerabilidades, el impacto, y la probabilidad de ocurrencia, para identificar en una etapa temprana cualquier cambio en el contexto del alcance y objetivos del SGSDP de la organización y así mantener una visión general de la imagen del riesgo.

Se debe contar con un programa de **Auditoría** para monitorear y revisar la eficacia y eficiencia del SGSDP. Este programa debe planearse, establecerse y mantenerse tomando en cuenta la política de gestión de datos personales. El Instituto pone a disposición de los responsables o encargados las **Auditorías voluntarias** para evaluar el cumplimiento y madurez de los sistemas de gestión implementados.

Fase 4. Mejorar el SGSDP

Paso 9. Mejora continua y capacitación

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.
Programa de capacitación que considere:

- Los requerimientos y actualizaciones del sistema de gestión.
- La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos.
- Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales.
- Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Registros de las capacitaciones impartidas (listas de asistencia, material de la capacitación impartida, evaluaciones de la capacitación, etc.).

DOCUMENTO DE SEGURIDAD

El **responsable** deberá elaborar un **documento de seguridad** que contenga los resultados que previamente se obtuvieron del Sistema de Gestión.

El **documento de seguridad** describe y da cuenta de manera general sobre las medidas de seguridad físicas, técnicas y administrativas adoptadas por los responsables para garantizar la **confidencialidad**, **integridad y disponibilidad** de los datos personales.

De acuerdo con el artículo 35 de la Ley General, el **responsable deberá elaborar un documento de seguridad** y debe contener por lo menos, lo siguiente:

1. El inventario de datos personales y de los sistemas de tratamiento.
2. Las funciones y obligaciones de las personas que traten datos personales.
3. El análisis de riesgos.
4. El análisis de brecha.
5. El plan de trabajo.
6. Los mecanismos de monitoreo y revisión de las medidas de seguridad.
7. El programa general de capacitación.

Actualización del documento de seguridad

De acuerdo con el artículo 36 de la Ley general, el responsable deberá **actualizar el documento de seguridad** cuando ocurran los siguientes eventos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Vulneraciones de seguridad

En caso de **vulneraciones de seguridad** como señala el artículo 37 de la Ley General, el responsable o encargado debe contar con:

- Plan de trabajo de acciones preventivas y correctivas.
- Bitácora de vulnerabilidades

Debe considerarse como vulneraciones de seguridad, en cualquier fase de tratamiento de datos cuando exista:

- La pérdida o destrucción no autorizada.
- El robo, extravío o copia no autorizada.
- El uso, acceso o tratamiento no autorizado.
- El daño, la alteración o modificación no autorizada.

El responsable deberá llevar una bitácora de las vulnerabilidades a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo y las acciones correctivas implementadas de forma inmediata y definitiva.

Así mismo deberá **informar al titular**, y según corresponda al Instituto y a los Organismos garantes de las Entidades Federativas, las vulnerabilidades que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que haya empezado a tomar las acciones para la revisión y conocer el grado de afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

De acuerdo con el artículo 41 de la Ley general, el responsable **deberá informar al titular** al menos lo siguiente:

- La naturaleza del incidente.
- Los datos personales comprometidos.
- Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.
- Las acciones correctivas realizadas de forma inmediata.
- Los medios donde puede obtener más información al respecto.

El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase de tratamiento de los datos personales guarden confidencialidad respecto a éstos, aún después de finalizar su relación con el mismo. Deberá establecer medidas de seguridad físicas, técnicas y administrativas.

Medidas de Seguridad Físicas

Son aquellas acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Por ejemplo: cámaras de seguridad, controles de acceso, seguridad perimetral, etc.

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.

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.

El INAI pone a tu disposición las siguientes guías que sirven de apoyo para la implementación del SGSDP, así como el documento orientador.

- Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales.
- Programa de Protección de Datos Personales.

VALIDACIÓN DE LOS SISTEMAS DE GESTIÓN ANTE EL INSTITUTO

Para la **validación de los sistemas de gestión** y su inscripción en el REMP[12] será necesario cumplir con los requisitos previstos en el artículo 25 de los Parámetros, y el artículo 43 de las Reglas. Los responsables o encargados podrán realizar el trámite de validación de los Sistemas de Gestión ante el Instituto de acuerdo con los siguientes pasos:

1. El responsable o encargado deberá someter su Sistema de Gestión y su implementación a una **Auditoría voluntaria** según lo previsto en el artículo 151 de la Ley General, para solicitar al Instituto su validación e inscripción en el REMP.

2. Presentar ante el Instituto una solicitud para la validación de su **Sistema de Gestión**, una vez que haya concluido la Auditoría voluntaria y cuente con el informe final que conste el resultado y el alcance de la Auditoría.

3. **Servidor público** con facultades para realizar la notificación ante el Instituto.

4. **Requisitos del trámite** de validación de los Sistemas de Gestión y su inscripción en el REMP. La solicitud deberá incluir o siguiente:

12 Para su consulta: https://registro-esquemas.inai.org.mx/?page_id=610

Requisitos que deberá contener la solicitud de validación
La denominación del sistema de gestión
La denominación del responsable que presenta la solicitud de validación
El informe final de la auditoría voluntaria en el que conste el resultado y el alcance de la auditoria. Dicho informe deberá tener una fecha de emisión que no exceda los seis meses a la fecha de la presentación de la solicitud;
Datos de contacto o un medio habilitado con fines de difusión del sistema de gestión
El correo electrónico y el domicilio, para oír y recibir notificaciones, de conformidad con el artículo 12 de las Reglas
La notificación deberá ir acompañada de un dispositivo de almacenamiento electrónico con la información referida anteriormente, salvo que dicha notificación sea realizada a través del sistema informático que, en su caso, habilite el Instituto.

5. El Instituto resolverá sobre la procedencia de la validación del sistema de gestión en un plazo de 10 días contados a partir del día siguiente de la recepción de la solicitud de validación.

6. Una vez emitida la resolución sobre la procedencia de validación, el Instituto notificará al responsable dentro de 10 días posteriores a la emisión de la misma.

7. En caso de que la resolución del Instituto valide el sistema de gestión, se asignará un número único de registro y se procederá a su **inscripción y publicación en el REMP, dentro de 10 días** posteriores a la emisión de la misma.

MODIFICACIÓN DE LOS SISTEMAS DE GESTIÓN ANTE EL INSTITUTO

Las modificaciones a cualquier contenido de los Sistemas de Gestión previstos en el Capítulo V de los Parámetros y por el artículo 46 de las Reglas. Los responsables o encargados podrán realizar el trámite de modificación de los Sistemas de Gestión ante el Instituto de acuerdo con los siguientes pasos:

1. Servidor Público con facultades para realizar la notificación ante el Instituto.

2. Requisitos del trámite de modificación de los Sistemas de Gestión y su inscripción en el REMP.

    - **Modificaciones con aspectos formales.** Modificación de forma que no afecten el funcionamiento del sistema de gestión, deberá notificar al Instituto, con los siguientes requisitos:

La notificación deberá contener la siguiente información
El nombre y número único de registro del sistema de gestión que se modifica.

Las modificaciones propuestas, los motivos de las modificaciones, así como la fecha en que pretenden hacerse efectivas o se hicieron efectivas.
La notificación deberá ir acompañada de un dispositivo de almacenamiento electrónico con la información referida anteriormente.

- **Modificaciones con aspectos sustantivos**. Las modificaciones con aspectos sustantivos de sistemas de gestión con validación, deberá someterse a una **Auditoría voluntaria** en el que conste el resultado y el alcance de la modificación.

La notificación deberá contener la siguiente información
El nombre y número único de registro del sistema de gestión que se modifica.
Las modificaciones propuestas, los motivos de las modificaciones, así como la fecha en que pretenden hacerse efectivas o se hicieron efectivas.
La documentación necesaria para acreditar la modificación, consistente en el informe final de la auditoría voluntaria en el que conste el resultado y el alcance de dicha modificación. Dicho informe deberá tener una fecha de emisión que no exceda los tres meses a la fecha de la presentación de la solicitud.
La notificación deberá ir acompañada de un dispositivo de almacenamiento electrónico con la información referida anteriormente.

Cuando el Sistema de Gestión de un responsable haya sido modificado en su funcionamiento, el responsable interesado deberá notificar al Instituto este hecho, así como informarle si someterá el Sistema de Gestión a una **nueva Auditoría voluntaria** para evaluar los efectos del cambio. El Instituto resolverá la solicitud de la modificación del Sistema de Gestión en un plazo de **10 días** y otros **10 días** posteriores a la emisión se procederá a su inscripción y publicación en el REMP.[13]

BAJA DE LOS SISTEMAS DE GESTIÓN ANTE EL INSTITUTO

En caso de que se actualicen cualquiera de los supuestos previstos en el artículo 29 de los Parámetros, causará baja la validación e inscripción en el REMP de un sistema de gestión con validación.

Los Sistemas de Gestión podrán ser objeto de baja del REMP cuando haya dejado de cumplir los objetivos con los que fue validado, además de las siguientes causas:

- Concluya la vigencia de la validación sin haberse renovado.
- El responsable que cuente con un Sistema de Gestión validado y lo solicite al Instituto.
- El Instituto detecte una no conformidad derivado de una nueva auditoría o un incumplimiento normativo derivado de algún procedimiento sustanciado por el Instituto, siempre que este incumplimiento conlleve una **no conformidad** del Sistema de Gestión validado.
- Se extinga el adherido a los tratamientos vinculados al Sistema de Gestión validado.

13 Para su consulta: https://registro-esquemas.inai.org.mx/?page_id=610

- El responsable del Sistema de Gestión con validación dado de baja del Registro se abstendrá de hacer referencia o publicitar dicho sistema de gestión como validado por el Instituto.
- Durante el desarrollo del procedimiento de baja, el Instituto publicará en el REMP que la validación en cuestión se encuentra sujeta a dicho procedimiento. Una vez que el Instituto haya emitido la resolución correspondiente, ésta se publicará en el Registro con sus respectivos efectos.

Los responsables o encargados podrán **realizar el trámite de baja** de los Sistemas de Gestión ante el Instituto de acuerdo con los siguientes pasos:

1. Servidor público con facultades de representación para realizar la notificación ante el Instituto.

2. Requisitos del trámite de baja de los Sistemas de Gestión y su inscripción en el REMP.

Requisitos para el trámite de baja de los sistemas de gestión con validación
El nombre y número único de registro del sistema de gestión con validación del cual se solicita la baja.
Los motivos por los que el sistema de gestión se da de baja del Registro.

Cuando el Instituto detecte una no conformidad

El Instituto iniciará con la notificación por parte del Instituto al responsable, de las causas que estima procedente dar de baja del REMP.

- El responsable contará con un plazo de **quince días** contados a partir del día siguiente de la notificación para manifestar lo que a su derecho convenga y aportar la documentación que estime procedente ante el Instituto.

- Recibidas las manifestaciones y documentación presentadas, el Instituto, en un plazo máximo de **dos meses** contados a partir de que aquéllas sean presentadas, las valorará y resolverá al respecto. Este plazo podrá ampliarse por un periodo igual, cuando existan razones que lo motiven y sea notificado al responsable.

- El Instituto emitirá una resolución dentro de los **diez días** siguientes al que haya recibido alegatos.

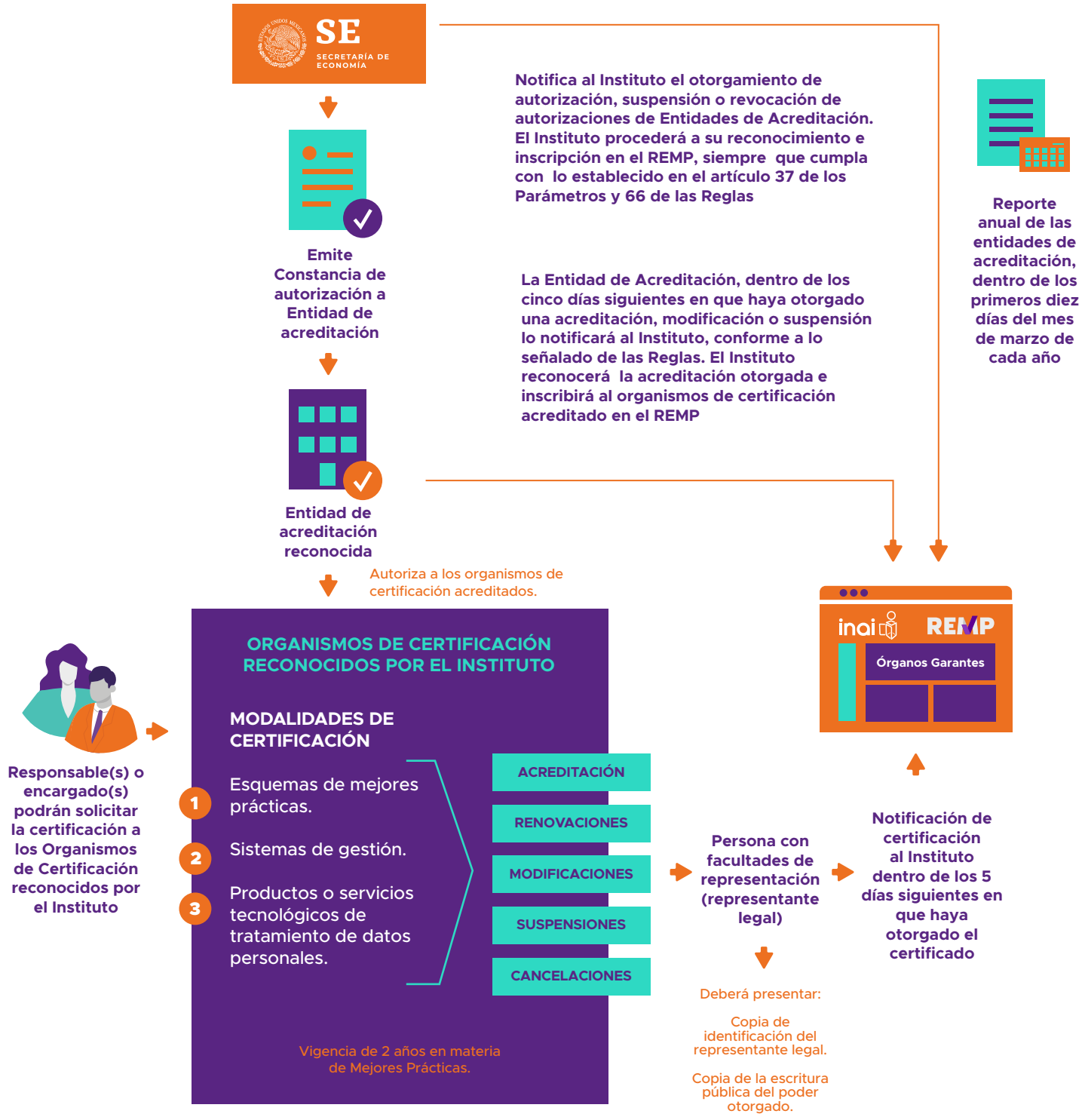
- El responsable del sistema de gestión con validación dado de baja del REMP se abstendrá de hacer referencia o publicitar dicho Sistema de Gestión como validado por el Instituto.

Los trámites relacionados con la validación, modificación o baja de los Sistemas de Gestión que realicen ante el INAI serán gratuitos y se presentarán por escrito en sus oficinas ubicadas en Avenida Insurgentes Sur, Número 3211, Colonia Insurgentes Cuicuilco, en la Alcaldía Coyoacán, Código Postal 04530, de lunes a jueves de 9:00 a 18:00 horas y viernes de 9:00 a 15:00 horas, o a través de otros medios que el INAI habilite para esos efectos.

Para más información contacte al **Centro de Atención a la Sociedad** del INAI.

SISTEMAS DE CERTIFICACIÓN
DE MEJORES PRÁCTICAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

SISTEMAS DE CERTIFICACIÓN EN MATERIA DE MEJORES PRÁCTICAS EN LA PROTECCIÓN DE DATOS PERSONALES DEL SECTOR PÚBLICO Y EL REGISTRO



Los responsables o encargados certificados podrán solicitar a los **organismos de certificación** reconocidos por el Instituto que se encuentren plenamente identificados en el REMP,[14] la Certificación de sus Esquemas de Mejores Prácticas o Sistemas de Gestión, así como los productos y servicios tecnológicos de tratamiento de datos personales.

Reconocimiento

El Instituto y los Órganos Garantes, reconocerán las certificaciones otorgadas por los **organismos de certificación reconocidos por el Instituto**, los cuales se pueden consultar en el REMP.

Organismos de Certificación

Los organismos de certificación deberán notificar al Instituto y a los Órganos Garantes, las renovaciones, modificaciones, suspensiones, restauraciones o cancelaciones de las certificaciones que otorgue al responsable o encargado. Así mismo deberá proporcionar un **certificado** al responsable o encargado que previamente haya cumplido con los requisitos de acuerdo con la normatividad aplicable, además de contener:

- El nombre y el logotipo del organismo de certificación.
- El nombre y número de certificación del responsable o encargado certificado.
- La información de las oficinas y, en su caso, servicios que se encuentren amparados por el certificado.
- La fecha efectiva de otorgamiento del certificado y su vigencia.
- La descripción de los alcances normativo y material de la certificación.
- La declaración de conformidad con la Ley General o las legislaciones estatales en la materia, los Parámetros, así como los que emitan los órganos garantes para tal efecto y demás normatividad aplicable.

Vigencia y renovación

Las certificaciones otorgadas en materia de mejores prácticas en la protección de datos personales del sector público tendrán una vigencia de **dos años**. El interesado podrá solicitar la **renovación** correspondiente ante el **organismo de certificación**, el cual seguirá los procedimientos establecidos.

Notificación al Instituto de certificados otorgados

El organismo de certificación acreditado, dentro de los **cinco días siguientes en que haya otorgado un certificado**, notificará al Instituto dicha certificación, a través de los medios previstos por el artículo 9 de las Reglas, y de conformidad con lo señalado en el artículo 68. La notificación correspondiente deberá ir acompañada de un dispositivo de almacenamiento electrónico con la información referida en el artículo 68 de las Reglas, salvo que dicha notificación sea realizada a través del sistema informático que, en su caso, habilite el Instituto.

14 Para consulta en: https://registro-esquemas.inai.org.mx/?page_id=610

Reconocimiento de las certificaciones otorgadas e inscripción en el REMP

El Instituto reconocerá la certificación otorgada e inscribirá el certificado de dicho responsable o encargado en el REMP, siempre que cumpla con lo previsto en el contenido de las notificaciones, y publicará la información relacionada con la misma, dentro de un plazo de **diez días** contados a partir del día siguiente en que haya sido realizada la notificación del certificado correspondiente, con el objeto de que los interesados conozcan a los responsables y encargados que han adoptado Esquemas de Mejores Prácticas, a través del **REMP de manera pública** considerando lo previsto en el artículo 58 de los Parámetros y artículo 92 de las Reglas.

Requisitos que deberá contener la notificación
Domicilio del organismo de certificación para oír y recibir notificaciones.
El nombre, número de certificación y logotipo de los responsables o encargados certificados.
La información sobre las oficinas que se encuentran amparadas por el certificado en particular.
El vínculo al sitio de Internet del responsable o encargado certificado, en su caso.
La fecha efectiva de otorgamiento del certificado.
Descripción del alcance de la certificación.
El certificado.
El correo electrónico y el domicilio, para oír y recibir notificaciones, de conformidad con el artículo 12 de las Reglas.

Modificaciones de las certificaciones

Para el caso de modificación, suspensión o cancelación a la certificación otorgada, el organismo de certificación acreditado en la materia deberá notificar al Instituto, a través de los medios previstos por el artículo 9 de las Reglas, cualquier modificación, suspensión o cancelación a las certificaciones otorgadas a responsables o encargados, en un plazo de **cinco días** posteriores a la fecha en la que el organismo de certificación resolvió o decidió sobre la misma.

Dicha notificación deberá incluir lo previsto en el artículo 68 de las presente Reglas y deberá ir acompañada de un dispositivo de almacenamiento electrónico con la información señalada, salvo que dicha notificación sea realizada a través del sistema informático que, en su caso, habilite el Instituto.

Efectos del Registro de la notificación de la modificación, suspensión o cancelación a la certificación otorgada

Una vez realizada la notificación al Instituto de modificación a la certificación otorgada a un responsable o encargado, éste hará constar dicho cambio en el REMP, siempre que cumpla con lo previsto en el artículo 68 de las Reglas, y publicará dicha modificación dentro de los

cinco días siguientes a la notificación correspondiente, considerando lo previsto en los artículos 58 los Parámetros y 92 de las Reglas.

Cuando alguna certificación que haya sido suspendida sea restaurada, este hecho se hará constar en el REMP y se publicará la información relacionada con dicha restauración, dentro de los **cinco días** siguientes a que el Instituto tenga conocimiento del hecho por parte del organismo de certificación, considerando lo previsto en los artículos 58 de los Parámetros y 92 de las Reglas.

Actores en el proceso de certificación

Para lograr la **certificación por parte de los responsables o encargados**, previamente los **organismos de certificación** deberán contar con la acreditación de la **entidad de acreditación** reconocida por el Instituto y estas a su vez deberán contar con autorización previa de la Secretaría en los términos previstos por la Ley de Infraestructura de la Calidad.[15]

Entidades de acreditación

El Instituto reconocerá las autorizaciones otorgadas por la Secretaría a las entidades de acreditación a través de su inscripción en el REMP.[16]

La Secretaría deberá notificar al Instituto cuando modifique, suspenda, restaure o revoque la autorización de una entidad de acreditación, lo que deberá hacerse constar en el REMP.

Presentar anualmente ante el Instituto un reporte anual de sus actividades con relación a las acreditaciones en la materia.

15 Para su consulta: https://www.dof.gob.mx/nota_detalle.php?codigo=5596009&fecha=01/07/2020

16 Para su consulta: https://registro-esquemas.inai.org.mx/?page_id=610

Los Organismos de Certificación

El Instituto reconocerá las acreditaciones otorgadas a organismos de certificación a través de si inscripción en el REMP.[17] Será necesario que las **Entidades de Acreditación** notifiquen al Instituto las acreditaciones que otorguen a organismos de certificación, de acuerdo con las Reglas.

Presentar anualmente ante el Instituto un reporte anual de sus actividades con relación a las certificaciones en la materia.

Notificar al Instituto o los órganos garantes, según corresponda atendiendo a la naturaleza federal o local del certificado, el otorgamiento, modificación, suspensión, restauración y cancelación de los certificados que otorgue en la materia.

TRÁMITES RELACIONADOS CON LA INSCRIPCIÓN DE LOS ESQUEMAS DE MEJORES PRÁCTICAS RECONOCIDOS O VALIDADOS POR LOS ORGANISMOS GARANTES

Cuando en términos de lo establecido por el artículo 73 de la Ley General, los Organismos Garantes que hayan reconocido o validado Esquemas de Mejores Prácticas, que decidan solicitar al Instituto su inscripción en el REMP administrado por éste, deberán realizar la notificación dentro de los primeros **tres meses del año**, con la finalidad de que esta inscripción se realice en los siguientes tres meses contados a partir de la notificación realizada.

La solicitud para la inscripción en el REMP de los Esquemas de Mejores Prácticas validados o reconocidos por los Organismos Garantes deberá contener:

- La denominación del esquema.
- Nombre del responsable o encargado a quien aplica el esquema.
- El tipo de esquema.
- Sector al que aplica.
- Alcance normativo del esquema.
- Ámbito personal de aplicación, es decir, el tipo o grupo de titulares cuyos datos personales están vinculados con el tratamiento al que aplica el esquema que se notifica.
- La fecha efectiva del reconocimiento o validación del esquema.
- La constancia o resolución emitida por el Organismo Garante.
- Datos de contacto o un medio habilitado con fines de difusión del esquema.

De la inscripción en el REMP de los reconocimientos o validaciones otorgadas por los Organismos Garantes.

Recibida la notificación a la que se refiere el artículo anterior, el Instituto resolverá la inscripción del Esquema de Mejores Prácticas validado o reconocido por el Organismo Garante, siempre que cumpla con lo previsto en el artículo 90 de las Reglas, y publicará la información relacionada con la misma, dentro de un plazo de diez días contados a partir del día siguiente en que haya sido realizada la notificación del certificado correspondiente, considerando lo previsto en el artículo 58 de los Parámetros y artículo 92 de las Reglas.

17 Para su consulta: https://registro-esquemas.inai.org.mx/?page_id=610

Los trámites relacionados con los Sistemas de Certificación en materia de protección de datos personales, que se realicen ante el INAI serán gratuitos y se presentarán por escrito en sus oficinas ubicadas en Avenida Insurgentes Sur, Número 3211, Colonia Insurgentes Cuicuilco, en la Alcaldía Coyoacán, Código Postal 04530, de lunes a jueves de 9:00 a 18:00 horas y viernes de 9:00 a 15:00 horas, o a través de otros medios que el INAI habilite para esos efectos.

Para más información contacte al **Centro de Atención a la Sociedad** del INAI.

FACILITACIÓN Y ASESORÍA PARA EL SEGUIMIENTO DE TRÁMITES

Esquemas de Mejores Prácticas
spd-remp@inai.org.mx

Auditorías Voluntarias
auditoriasvoluntarias@inai.org.mx

Seguridad de Datos Personales
leticia.zamudio@inai.org.mx

FACILITACIÓN DEL SECTOR PÚBLICO

facilitacion.secpub@inai.org.mx

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales