Av. Lomas de Sotelo 1097 • Col. Lomas de Sotelo • 11200 México, D.F. • Tel. 5395 0777 • Fax 5395 0700
nyce@nyce.org.mx • www.nyce.org.mx



# Procedimientos

**"Desarrollo Conceptual del Modelo de Certificación en materia de Protección de Datos Personales, en el marco de la LFPDPPP y demás normatividad aplicable en la materia"**

# Modelo de Certificación en materia de Protección de Datos Personales, en el marco de la LFPDPPP

**A cerca de los procedimientos y su publicación**

Como parte del presente estudio se desarrolló el capítulo V del documento “Parámetros de autorregulación”, mismo que define los Requisitos, Facultados, Obligaciones y Procedimientos que deben llevar a cabo cada uno de los distintos participantes del esquema, mostrados en el diagrama anterior.

En el presente documento se detallan los procedimientos que deberán seguirse, tanto para la labores de Certificación como de Acreditación, los cuales fueron definidos en los Parámetros de Autorregulación. Estos procedimientos serán un lineamiento base de actuación para los diferentes participantes, sin embargo es conveniente que no sean publicado por la autoridad, de forma que el esquema tenga flexibilidad suficiente para operar en los distintos sectores, industrias y tamaños de empresas que se prevé, por lo anterior, después de que se aprueben y acrediten a las organizaciones correspondientes, éstas deberán desarrollar sus procedimientos, en apego a lo descrito en la Ley, el Reglamento y los Parámetros de Autorregulación, antes de iniciar sus operaciones.

**Acerca de los costos del modelo**

Uno de los objetivos de la autorregulación y por lo tanto del modelo es hacer accesible a la mayoría de los responsables algún esquema de autorregulación y certificación, si bien será necesario establecer un esquema de costos por los servicios de acreditación y certificación, tanto de personas como de empresas, estos costos deberán ser publicados y sometidos a la autorización de la autoridad, de forma que no excedan los límites establecidos.

## PROCEDIMIENTO DE CERTIFICACIÓN

### 1. Información a disposición pública

El organismo de certificación deberá poner a disposición pública lo siguiente:

- **I.** Información detallada acerca de los procesos de evaluación y certificación, incluidas las condiciones para otorgar, mantener, ampliar, reducir, suspender, restaurar y revocar la certificación;
- **II.** Documentos de referencia que contengan los requisitos para la certificación, incluidos los requisitos técnicos específicos para cada certificación;
- **III.** Información general de las tarifas, en su caso;
- **IV.** Información sobre los procedimientos para la recepción y tratamiento de quejas y apelaciones, y
- **V.** Información sobre sus actividades y las limitaciones declaradas bajo las cuales opera.

### 2. Requisitos para solicitar la certificación

El organismo de certificación deberá requerir al solicitante lo siguiente:

- **I.** Características generales: razón o denominación social, domicilios y los recursos humanos y técnicos con los que cuenta;
- **II.** Información general que incluya sus estatutos y actividades, así como su pertenencia a otras organizaciones, en su caso;
- **III.** Alcance de la certificación que se solicita;
- **IV.** Compromiso de cumplir con los requisitos para la certificación y con las demás obligaciones que se le imponen a las organizaciones certificadas, y
- **V.** Descripción de los procesos y servicios que presta, y un listado de los métodos o procedimientos para los cuales busca la certificación, en caso que disponga de ellos.

### 3. Subcontratación

Si fuese necesaria la subcontratación, el organismo de certificación debe:

- **I.** Tener una política en la que se describan las condiciones bajo las cuales puede tener lugar una subcontratación;
- **II.** Asumir la responsabilidad de las actividades de certificación subcontratadas;
- **III.** Asumir la responsabilidad exclusiva para otorgar, mantener, ampliar, reducir, suspender, restaurar o retirar la certificación;
- **IV.** Asegurar que el subcontratado, y en su caso su personal, es competente y cumple con el presente procedimiento y
- **V.** Asegurar que el subcontratado mantenga la confidencialidad de la información.

### 4. Preparación de la evaluación

Antes de que se dé inicio a cualquier evaluación por parte del organismo de certificación se deberá cumplir con lo siguiente:

- **I.** El organismo de certificación deberá designar formalmente a un equipo de evaluación que conste de un número adecuado de evaluadores para cada alcance específico que en su conjunto deberá:
  - a) Tener el conocimiento apropiado para cumplir con las finalidades de la certificación, y

b) Efectuar una evaluación confiable de la competencia de la organización solicitante.

**II.** Asegurarse que los miembros del equipo actúen de forma imparcial, y

**III.** Para las evaluaciones iniciales, además de la visita a la oficina principal, se debe visitar todas las demás instalaciones de la organización solicitante en donde se desarrolle alguna actividad clave de la certificación que está solicitando.

## 5. Evaluación in situ

Cuando el organismo de certificación requiera realizar la evaluación en las instalaciones del solicitante, deberá observar lo siguiente:

**I.** El equipo de evaluación comenzará con la evaluación in situ con una reunión de apertura en la cual se defina claramente el propósito de la evaluación así como los criterios de certificación, y

**II.** El equipo de evaluación debe ser testigo del desempeño de un número representativo del personal de la organización solicitante para asegurar la competencia.

## 6. Hallazgos e informe de evaluación

El equipo de evaluación debe analizar toda la información y evidencia pertinente recopilada durante la revisión de los documentos, registros y la evaluación *in situ.* El análisis debe ser suficiente para permitir al equipo de evaluación determinar el grado de competencia con que cuenta la organización solicitante.

El equipo de evaluación debe apegarse a lo siguiente:

**I.** Antes de abandonar las instalaciones de la organización debe tener lugar una reunión entre el equipo de evaluación y la organización. Se deberá poner a consideración de la organización un informe por escrito, sobre los resultados de la evaluación cuyos contenidos serán:

a. competencia,
b. cumplimiento con los Parámetros,
c. identificación de los incumplimientos, en su caso;

**II.** Debe invitarse a la organización a responder el informe de evaluación y describir las acciones específicas tomadas o que se planifican tomar dentro de un tiempo determinado para la resolución de cualquier incumplimiento identificado, y

**III.** La información que los evaluadores proporcionen a quienes toman las decisiones de certificación, debe incluir como mínimo lo siguiente:

a) La identificación única de la organización solicitante;
b) Las fechas de evaluación in situ;
c) El nombre de los evaluadores involucrados en la evaluación;
d) La identificación única de las instalaciones evaluadas;
e) El alcance propuesto de la certificación que fue evaluado, y
f) El informe de evaluación.

## 7. Toma de la decisión.

Antes de tomar la decisión, el organismo de certificación deberá asegurarse de que la información es adecuada para decidir si se han cumplido los Requisitos para solicitar la certificación descritos en el presente procedimiento.

El organismo de certificación debe proporcionar un certificado a la organización certificada, mismo que deberá contener:

**I.** La identificación y el logotipo del organismo de certificación;
**II.** La identificación única de la organización certificada;
**III.** Oficinas que se encuentran amparadas por el certificado;
**IV.** El número de certificación único de la organización certificada;
**V.** La fecha efectiva de otorgamiento de la certificación, y
**VI.** Descripción del alcance de la certificación.

## 8. Vigilancia

Para mantener la certificación, el organismo de certificación debe llevar a cabo evaluaciones periódicas de vigilancia *in situ,* u otras actividades de vigilancia, al menos en intervalos anuales para mantener el cumplimiento continuo por parte de las organizaciones certificadas.

## 9. Vigencia y Renovación de la certificación

Las certificaciones otorgadas en materia de protección de datos personales, tendrán una vigencia de tres años. Al término de la vigencia, el interesado deberá presentar la solicitud de renovación correspondiente ante el organismo de certificación, el cual evaluará la pertinencia de concederla de acuerdo con los procedimientos de verificación y auditoria establecidos para tal efecto.

## 10. Suspensión de la certificación y restauración

Serán causas de suspensión de la certificación cuando:

**I.** Existan incumplimientos parciales o fuera de tiempo de los requisitos de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, el Reglamento de esta Ley o los parámetros de autorregulación;
**II.** Cuando el Instituto haya girado apercibimiento al responsable certificado y en tanto no se subsanen las causas del mismo, y
**III.** Otras causas señaladas por el Instituto.

Una vez que se hayan subsanado en su totalidad las causas que dieron origen a la suspensión, la certificación deberá ser restaurada en un máximo de 2 días hábiles.

## 11. Revocación del certificado

Serán causas de revocación del certificado cuando:

**I.** Exista falsedad en la información presentada en la solicitud o en los reportes posteriores;
**II.** No dar cumplimiento a las observaciones realizadas durante los procedimientos de certificación;
**III.** Que el Instituto haya sancionado al responsable certificado, y
**IV.** Otras causas graves señaladas por el Instituto.

Las organizaciones certificadas, después de haber sido notificadas, tendrán el término de cinco días hábiles para manifestar lo que a su derecho convenga al organismo de certificación. Concluido dicho término sin que se justifique su actuación, se procederá a la cancelación.

El organismo de certificación debe notificar a la organización certificada que la cancelación de la certificación conlleva la prohibición de hacer cualquier alusión a la certificación, así como la de utilizar cualquier tipo de información o símbolo referente a la misma.

**12. Tipos de Certificados**

El organismo de certificación, cuando represente a un sector de la industria, podrá emitir certificaciones específicas para dicho sector, considerando las particularidades del funcionamiento del sector, así como la legislación aplicable.

**13. Alcance de la certificación**

La certificación podrá realizarse respecto a ciertos tratamientos o a la totalidad de tratamientos que efectúe el responsable.

**14. Suspensión de la certificación**

**15. Cancelación de la certificación**

El organismo de certificación deberá cancelar la certificación de las organizaciones certificadas, cuando éstas:

**I.** Se haga constar que la organización incumple con la Ley Federal de Protección de Datos Personales en Posesión de Particulares o su Reglamento de manera dolosa;

**II.** Renuncien expresamente a la certificación;

**III.** No hayan subsanado las causas que dieron efecto a una suspensión dentro de los veinte días hábiles posteriores al inicio de la misma, o

## PROCEDIMIENTO DE ACREDITACIÓN DE CERTIFICADORES

### 1. Información a disposición pública

La entidad de acreditación deberá poner a disposición pública lo siguiente:

**I.** Información detallada acerca de los procesos de evaluación y acreditación, incluidas las condiciones para otorgar, mantener, ampliar, reducir, suspender, restaurar y revocar la acreditación;
**II.** Documentos de referencia que contengan los requisitos para la acreditación, incluidos los requisitos técnicos específicos para cada sector de acreditación;
**III.** En su caso, información general de las tarifas;
**IV.** Una descripción de los derechos y las obligaciones de los organismos de certificación;
**V.** Información sobre los procedimientos para la recepción y tratamiento de quejas y apelaciones , e
**VI.** Información sobre sus actividades y las limitaciones declaradas bajo las cuales opera.

### 2. Requisitos para solicitar la acreditación de certificadores

La entidad de acreditación deberá requerir al organismo de certificación solicitante lo siguiente:

**I.** Características generales: razón o denominación social, domicilios y los recursos humanos y técnicos con los que cuenta;
**II.** Información general sobre el certificador que incluya sus estatutos y actividades, así como su pertenencia a otras organizaciones, en su caso;
**III.** Alcance de la acreditación que se solicita;
**IV.** Compromiso de cumplir con los requisitos para la acreditación y con las demás obligaciones que se le imponen a los certificadores, y
**V.** Descripción de los servicios de certificación que prestará, así como un listado de los métodos o procedimientos para los cuales busca la acreditación.

### 3. Subcontratación

Si fuese necesaria la subcontratación, la entidad de acreditación debe:

**I.** Tener una política en la que se describan las condiciones bajo las cuales puede tener lugar una subcontratación;
**II.** Asumir la responsabilidad de las evaluaciones subcontratadas;
**III.** Asumir la responsabilidad exclusiva para otorgar, mantener, ampliar, reducir, suspender, restaurar o retirar la acreditación;
**IV.** Asegurar que el subcontratado, y en su caso su personal, es competente y cumple con el presente procedimiento, y
**V.** Asegurar que el subcontratado mantenga la confidencialidad de la información.

### 4. Preparación de la evaluación

Antes de que se dé inicio a cualquier evaluación por parte de la entidad de acreditación se deberá cumplir con lo siguiente:

**I.** La entidad de acreditación deberá designar formalmente a un equipo de evaluación que conste de un número adecuado de evaluadores para cada alcance específico que en su conjunto deberá:

a) Tener el conocimiento apropiado para cumplir con las finalidades de la acreditación, y
b) Efectuar una evaluación confiable de la competencia del organismo de certificación.

**II.** Asegurarse que los miembros del equipo actúen de forma imparcial, y

**III.** Para las evaluaciones iniciales, además de la visita a la oficina principal, se debe visitar todas las demás instalaciones del organismo de certificación solicitante en donde se desarrolle alguna actividad clave de la acreditación que está solicitando.

## 5. Evaluación in situ

Cuando la entidad de acreditación requiera realizar la evaluación en las instalaciones del solicitante, deberá observar lo siguiente:

**I.** El equipo de evaluación comenzará con la evaluación in situ con una reunión de apertura en la cual se defina claramente el propósito de la evaluación así como los criterios de acreditación, y

**II.** El equipo de evaluación debe ser testigo del desempeño de un número representativo del personal del organismo de certificación para asegurar la competencia.

## 6. Hallazgos e informe de evaluación

El equipo de evaluación debe analizar toda la información y evidencia pertinente recopilada durante la revisión de los documentos, registros y la evaluación *in situ.* El análisis debe ser suficiente para permitir al equipo de evaluación determinar el grado de competencia con que cuenta el organismo de certificación solicitante.

El equipo de evaluación debe apegarse a lo siguiente:

**I.** Antes de abandonar las instalaciones del organismo de certificación debe tener lugar una reunión entre el equipo de evaluación y el organismo. Se deberá poner a consideración del organismo de certificación un informe por escrito, sobre los resultados de la evaluación cuyos contenidos serán:
   a. competencia,
   b. cumplimiento con los Parámetros,
   c. identificación de los incumplimientos, en su caso;

**II.** Debe invitarse al organismo de certificación a responder el informe de evaluación y describir las acciones específicas tomadas o que se planifican tomar dentro de un tiempo determinado para la resolución de cualquier incumplimiento identificado, y

**III.** La información que los evaluadores proporcionen a quienes toman las decisiones de acreditación, debe incluir como mínimo lo siguiente:
   a) La identificación única del organismo de certificación;
   b) Las fechas de evaluación in situ;
   c) El nombre de los evaluadores involucrados en la evaluación;
   d) La identificación única de las instalaciones evaluadas;
   e) El alcance propuesto de la acreditación que fue evaluado, y
   f) El informe de evaluación.

## 7. Toma de la decisión.

Antes de tomar la decisión, la entidad de acreditación deberá asegurarse de que la información es adecuada para decidir si se han cumplido los Requisitos para solicitar la acreditación de certificadores descritos en el presente procedimiento.

La entidad de acreditación debe proporcionar un certificado de acreditación al organismo de certificación acreditado, mismo que deberá contener:

**I.** La identificación y el logotipo de la entidad de acreditación;
**II.** La identificación única del organismo de certificación acreditado;
**III.** Oficinas que se encuentran amparadas por el certificado de acreditación;
**IV.** El número de acreditación único del organismo de certificación acreditado;
**V.** La fecha efectiva de otorgamiento de la acreditación, y
**VI.** Descripción del alcance de la acreditación.

## 8. Vigilancia

Para mantener la acreditación, la entidad de acreditación debe llevar a cabo evaluaciones periódicas de vigilancia *in situ,* u otras actividades de vigilancia, al menos en intervalos anuales para mantener el cumplimiento continuo por parte de los organismos de certificación.

## 9. Suspensión de la acreditación y restauración

La entidad de acreditación deberá suspender la acreditación de los organismos de certificación, cuando éstos:

**I.** No proporcionen a la entidad de acreditación en forma oportuna y completa los informes que le sean requeridos respecto a su funcionamiento y operación;
**II.** Impidan u obstaculicen las funciones de verificación y vigilancia de la entidad de acreditación;
**III.** Disminuyan los recursos o la capacidad para emitir certificados al menos por un mes;
**IV.** Emitan documentos donde se hagan constar los resultados de la certificación con información o datos erróneos de manera negligente; o
**V.** No hayan cubierto las cuotas de acreditación, en su caso.

Una vez que se hayan subsanado en su totalidad las causas que dieron origen a la suspensión, la acreditación deberá ser restaurada en un máximo de 2 días hábiles.

## 10. Cancelación de la acreditación

La entidad de acreditación deberá cancelar la acreditación de los organismos de certificación, cuando éstos:

**I.** Emitan documentos donde se hagan constar los resultados de la certificación con información o datos falsos de manera dolosa;
**II.** Nieguen reiterada o injustificadamente el servicio que se les solicite;
**III.** Renuncien expresamente a la acreditación concedida para operar;
**IV.** Se disminuyan los recursos o la capacidad para emitir certificados por más de tres meses consecutivos;
**V.** No hayan subsanado las causas que dieron efecto a una suspensión dentro de los veinte días hábiles posteriores al inicio de la misma, o

**VI.** Cuando se violen las disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, el Reglamento de esta Ley o el presente procedimiento.

Los organismos de certificación, después de haber sido notificados, tendrán el término de cinco días hábiles para manifestar lo que a su derecho convenga a la entidad de acreditación. Concluido dicho término sin que se justifique su actuación, se procederá a la cancelación.

La entidad de acreditación debe notificar al organismo de certificación que la cancelación de la acreditación conlleva la prohibición de ejercer las actividades de certificación y de hacer cualquier alusión a la acreditación, así como la de utilizar cualquier tipo de información o símbolo referente a la misma.

## PROCEDIMIENTO DE AUDITORÍA INTERNA DEL ORGANISMO DE CERTIFICACIÓN

### 1. Programa de auditoría interna

El organismo de certificación deberá elaborar un programa de auditoría interna en el cual debe tomar en consideración la importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías internas anteriores.

Las auditorías internas se deben realizar una o varias de tal forma que al menos una vez al año se cubra con la totalidad de los elementos que se establecen en la norma NMX-EC-065-IMNC-2000, *Requisitos generales para organismos que operan sistemas de certificación de producto* o a la norma que la sustituya.

### 2. Realización de auditoría interna

El organismo de certificación debe asegurarse de que:

**VI.** las auditorías internas son realizadas por personas que tengan conocimientos de certificación de producto, de auditoría y de la norma NMX-EC-065-IMNC-2000, *Requisitos generales para organismos que operan sistemas de certificación de producto* o a la norma que la sustituya;

**VII.** las auditorías internas son realizadas por personas que no auditan su propio trabajo;

**VIII.** el personal responsable del área auditada sea informado del resultado de la auditoría;

**IX.** cualquier acción necesaria sea realizada de manera oportuna y apropiada;

**X.** cualquier oportunidad de mejora sea identificada y comunicada

### 3. Cierre de hallazgos

Los hallazgos de la auditoría deben ser atendidos de acuerdo con el impacto hacia el sistema de gestión del organismo de certificación.

En algunas ocasiones, las auditorías internas se realizan con un alcance acotado exclusivamente para dar seguimiento a las acciones para atender no conformidades detectadas previamente.

## PROCEDIMIENTO PARA LA ATENCIÓN DE SOLICITUDES DE CERTIFICACIÓN

### 1. Recepción de la solicitud

El organismo de certificación debe utilizar un formato de solicitud que le permita obtener todos los elementos necesarios para realizar la certificación.

El organismo de certificación deberá desarrollar la solicitud de servicios, a menos que el IFAI o la Secretaría de Economía le indique el formato de solicitud a utilizar.

La recepción de la solicitud sólo se debe realizar si la organización solicitante ha cubierto todos lodos requisitos para la certificación.

### 2. Revisión de la solicitud

Se debe dejar evidencia de la revisión de la solicitud, de que todos los requisitos para la certificación fueron cubiertos.

En caso de que no se hayan cubiertos todos los requisitos para la certificación, se le hará llegar a la organización solicitante una relación detallada de los requisitos no cubiertos.

### 3. Aprobación de la solicitud

Una vez que el solicitante ha cubiertos todos los requisitos para la certificación, se procederá a liberar la solicitud de servicios para que inicie la etapa de evaluación documental.

## PROCEDIMIENTO PARA LA EVALUACIÓN DOCUMENTAL

### 1. Evaluación documental

En esta etapa se revisa documentalmente que el solicitante de certificación cumple con los requisitos para la certificación por medio de un plan de evaluación, el cual puede ser genérico y aplicable para cada una de las solicitudes de certificación.

La evaluación documental se realiza preferentemente por personal diferente a quien realizó la atención de la solicitud.

Si se encuentra algún incumplimiento que inhiba que el proceso de certificación continúe, se le debe hacer llegar rápidamente al solicitante, una descripción detallada de los requisitos por cubrir y el plazo para recibir la información adicional.

### 2. Informe de evaluación documental

De la evaluación documental se debe elaborar un informe en el cual se hace mención a las desviaciones existentes y el plazo máximo para subsanarlas, de lo contrario, la solicitud de certificación se deberá cancelar.

Una vez que se cubrieron todos los requisitos de la evaluación documental, se le debe hacer llegar a la organización solicitante un informe final, y si se detectan incumplimientos, se puede hacer llegar un informe preliminar para notificar tales desviaciones.