6 de marzo de 2018

Recomendaciones sobre protección de datos personales contenidos en la Credencial para Votar

Objetivo

Proporcionar recomendaciones a los responsables para el tratamiento de los datos personales contenidos en la Credencial para Votar, a partir de las obligaciones que establece la normatividad que regula el derecho de protección de datos personales en los sectores público y privado.

Justificación

La Credencial para Votar es el documento de identidad personal comúnmente utilizado por los ciudadanos para identificarse ante los sujetos obligados para el ejercicio de derechos, la realización de trámites administrativos[1], la adquisición de un bien o servicio y el acceso a oficinas gubernamentales.

Al 23 de febrero de 2018, la lista nominal, que contiene datos de aquellos ciudadanos que solicitaron su inscripción al padrón y cuentan con su credencial para votar con fotografía vigente, ascendía a un total de 88, 875, 266 ciudadanos.[2]

Ahora bien, la Credencial para Votar es un documento que contiene una serie de datos personales, algunos son proporcionados por los ciudadanos para realizar el trámite de inscripción o actualización del Padrón Electoral en cumplimiento de las disposiciones aplicables, y otros son generados por el Instituto Nacional Electoral (INE). Los datos personales contenidos[3] son:

[1] La calidad de medio de identificación personal para trámites administrativos se reconoce desde el artículo Cuarto Transitorio del Decreto de Reformas de la Ley General de Población, publicado en el Diario Oficial de la Federación el 22 de julio de 1992, disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=4678146&fecha=22/07/1992, fecha de consulta 4 de marzo de 2018.

[2] Información disponible en: http://www.ine.mx/credencial/estadisticas-lista-nominal-padron-electoral/ fecha de consulta 2 de marzo de 2018.

[3] La Ley General de Instituciones y Procedimientos Electorales señala en su artículo 156, numeral 1, que la credencial para votar deberá contener, cuando menos, los siguientes datos del elector:

a) Entidad federativa, municipio y localidad que corresponden al domicilio. En caso de los ciudadanos residentes en el extranjero, el país en el que residen y la entidad federativa de su lugar de nacimiento. Aquellos que nacieron en el extranjero y nunca han vivido en territorio nacional, deberán acreditar la entidad federativa de nacimiento del progenitor mexicano. Cuando ambos progenitores sean mexicanos, señalará la de su elección, en definitiva;
b) Sección electoral en donde deberá votar el ciudadano. En el caso de los ciudadanos residentes en el extranjero no será necesario incluir este requisito;
c) Apellido paterno, apellido materno y nombre completo;
d) Domicilio;
e) Sexo;
f) Edad y año de registro;
g) Firma, huella digital y fotografía del elector;
h) Clave de registro, y
i) Clave Única del Registro de Población.

2. Además tendrá:

a) Espacios necesarios para marcar año y elección de que se trate;
b) Firma impresa del Secretario Ejecutivo del Instituto;
c) Año de emisión;
d) Año en el que expira su vigencia, y
e) En el caso de la que se expida al ciudadano residente en el extranjero, la leyenda “Para Votar desde el Extranjero”.

1. Nombre completo (nombre y apellidos)
2. Sexo
3. Fecha de nacimiento
4. Domicilio[4]
5. Entidad federativa, municipio y localidad que corresponde al domicilio
6. Firma
7. Fotografía
8. Huella dactilar
9. Clave Única de Registro de Población
10. Clave de Elector (la genera el INE)
11. OCR (lo genera el INE)

En ese sentido, dada la generalización del uso de la Credencial para Votar como instrumento de identificación, y la cantidad de datos personales que contiene, es importante que los servidores públicos y responsables que tratan los datos personales contenidos en la credencial para votar conozcan la existencia de obligaciones que derivan de la salvaguarda del derecho humano a la protección de datos personales reconocido desde el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos y materializado a través de la normativa secundaria vigente para el sector público y privado.

Contenido

A continuación se presenta la propuesta de contenido para el documento, a partir de cinco recomendaciones generales para el tratamiento de los datos personales de la Credencial para Votar, dentro de las cuales se da una breve explicación de cada una de las frases utilizadas correlacionándolas con las obligaciones relevantes para el documento, que la normativa en materia de protección de datos personales establece, con la finalidad de facilitar el cumplimiento de éstas y garantizar un debido tratamiento.

#LoTienesQueSaber
Recomendaciones para el debido tratamiento de los datos personales de la Credencial para Votar

Contenido

[4] Por lo que se refiere al domicilio, de conformidad con el artículo 156, numeral 4, de la Ley General de Instituciones y Procedimientos Electorales, los ciudadanos podrán optar entre solicitar que aparezca visible en el formato de su credencial para votar o de manera oculta, conforme a los mecanismos que determine el Consejo General.

A) RECOMENDACIONES

La Credencial para Votar, además de cumplir con su principal finalidad que es ejercer el derecho al voto, es utilizada como documento de identidad, ya que contiene, entre otros, los siguientes datos personales: nombre completo, sexo, fecha de nacimiento, en algunos casos domicilio, entidad federativa, municipio y localidad, firma, fotografía, huella dactilar, Clave Única de Registro de Población, clave de elector, OCR.

En ese sentido, el uso de la Credencial para Votar o de los datos contenidos en ella implica un tratamiento de datos personales y, por tanto, la generación de responsabilidades en cuanto a su protección.

Un uso ilegal o una inadecuada protección de los datos personales contenidos en la Credencial para Votar puede tener consecuencias negativas graves para su titular, como el robo de su identidad y, por tanto, responsabilidades administrativas para los servidores públicos que tienen a su cargo su resguardo.

Es por ello, que en este documento, el INAI y el INE te damos cinco recomendaciones básicas para evitar un mal tratamiento de los datos personales contenidos en la Credencial para Votar.

1. No la pidas si no es necesaria

El primer paso para evitar cualquier tratamiento indebido de datos personales es no solicitarlos si no son necesarios para la finalidad que se persigue.

Si bien es una práctica común solicitar la Credencial para Votar como medio de identificación de las personas, se recomienda analizar si en el trámite en cuestión es necesario que se presente este documento o si es suficiente que el interesado se identifique con otro que contenga menos datos personales.

Ello dependerá de la naturaleza del trámite que se realiza y de la necesidad que exista de verificar con un grado de certeza alto la identidad de las personas. Por ejemplo, para la entrada a un edifico pudiera ser suficiente que el visitante se identifique con la credencial expedida por su centro de trabajo o institución educativa; mientras que para realizar un trámite personal, como la expedición de una constancia laboral o de salud, sea indispensable requerir la acreditación de la identidad a través de la presentación de la Credencial para Votar, cédula profesional o pasaporte, entre otros documentos oficiales.

Por lo que, previo a que se solicite a un titular que proporcione su Credencial para Votar se deberá analizar si realmente es necesario, adecuado y relevante contar con dicha información, atendiendo a las finalidades del tratamiento al que serán sometidos los datos personales.

Toma en cuenta que…
Dentro de los principios que deben observarse en el tratamiento de datos personales se encuentran el principio de proporcionalidad, en virtud del cual se tiene la obligación como responsable de sólo solicitar aquellos datos personales que resulten necesarios adecuados y estrictamente necesarios para el cumplimiento de las finalidades que justifican su tratamiento, así como a realizar esfuerzos razonables para limitar el número de datos personales que soliciten al titular, lo cual se conoce como criterio de minimización.

De manera adicional, el principio de finalidad establece la obligación de tratar los datos personales sólo para las finalidades informadas al titular en el aviso de privacidad, las cuales deberán ser concretas, lícitas, explícitas y legítimas, y para los responsables del sector público deberán estar relacionadas con sus atribuciones normativas. En ese sentido, es importante que, en su caso, en el aviso de privacidad se informe que se tratarán los datos personales contenidos en la Credencial para Votar.

2. Si la tienes que pedir, no te quedes con fotocopia

Ahora bien, en el supuesto de que, una vez hecho el análisis sobre la proporcionalidad de solicitar la Credencial para Votar, se determine que la misma es necesaria según la finalidad de que se trate, se sugiere valorar la posibilidad de no fotocopiarla o reproducirla a través de cualquier medio.

En muchas ocasiones no se requerirá contar con un soporte físico o electrónico de la Credencial para Votar, sino que será suficiente sólo su presentación o registrar algunos de los datos personales contenidos en la misma. Para determinarlo, es importante revisar los documentos y disposiciones que regulan el trámite en cuestión, a fin de verificar el procedimiento que se establece para llevarlo a cabo.

Incluso, resulta conveniente hacer una revisión integral de dichas disposiciones con objeto de analizar si el tratamiento de datos personales que se establece está conforme a la norma o, en su caso, si resulta necesario realizar modificaciones para cumplir con las nuevas obligaciones legales, entre las que se podría encontrar la reducción de los datos personales que se requieren para el trámite.

Tome en cuenta que…
Conservar una fotocopia o una reproducción por otro medio de la Credencial para Votar aumenta el riesgo en el tratamiento, ya que ello facilita un uso inadecuado de la información, como la obtención de datos personales o la reproducción del documento para el robo de identidad o para tener un contacto no autorizado con los titulares a través de la generación de bases de datos para el envío de información de diversa.

3. Si la tienes que fotocopiar o reproducir, resguárdala con medidas de seguridad y confidencialidad adecuadas

Dado que la Credencial para Votar contiene diversos datos personales de su titular, en caso de que sea necesario contar con un soporte físico o electrónico de la misma para realizar el trámite en cuestión, como una fotocopia o fotografía digital, es importante que se establezcan y mantengan medidas de seguridad para su almacenamiento y tratamiento, así como también controles o

mecanismos de confidencialidad, de conformidad con lo previsto en la normativa de protección de datos personales.

Las medidas de seguridad que sean adoptadas deberán considerar, entre otros factores, el riesgo inherente de los datos personales contenidos en la Credencial para Votar, las posibles consecuencias de una vulneración para los titulares y el riesgo por el valor potencial cuantitativo o cualitativo que pudieren tener los datos personales para una tercera persona no autorizada para su posesión.

Toma en cuenta que…
El **deber de seguridad** establece la obligación a los responsables de resguardar la información personal que les proporcionen los titulares bajo medidas de seguridad adecuadas, que eviten su pérdida, alteración, destrucción, daño o uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Para dar cumplimiento al deber de seguridad, los responsables están obligados a resguardar los datos personales en bases de datos protegidas con medidas de seguridad administrativas (controles que ayuden a evitar prácticas inadecuadas del personal que pongan en riesgo los datos personales, como por ejemplo, dejar las fotocopias de las Credenciales para Votar al alcance de todos, o compartir contraseñas), físicas (controles aplicados en los espacios físicos e infraestructura que minimicen el robo o acceso no autorizado, como por ejemplo, mantener los espacios debidamente cerrados con los candados suficientes), y técnicas (controles para proteger equipos de cómputo y dispositivos de almacenamiento de virus, malware, entre otros).

Por su parte, el **deber de confidencialidad** impone la obligación a los responsables de establecer controles o mecanismos que tengan por objeto que las personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad de la información personal que le proporcionan los titulares, es decir, que ésta no se difunda o comparta con terceros, salvo que exista consentimiento para ello o alguna obligación normativa.

4. Si ya no es necesaria, suprime los datos personales

Cuando los datos personales que contiene la Credencial para Votar hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron, se deberán eliminar de los archivos o bases de datos, según el procedimiento y medidas que establece la normatividad que regula la protección de los datos personales.

En ese sentido, para cumplir con las obligaciones legales y reducir los riesgos por un inadecuado tratamiento de los datos personales de la Credencial para Votar, se recomienda realizar una revisión exhaustiva de los archivos y bases de datos en los que se reguardan copias o reproducciones de credenciales para votar, a fin de determinar si es necesario o no conservarlas y, en su caso, eliminarlas a la brevedad posible, siguiendo el procedimiento que establece la norma y bajo medidas de destrucción seguras (se recomienda consultar la Guía para el Borrado Seguro de Datos Personales, disponible en el portal de Internet del INAI www.inai.org.mx, o en el vínculo electrónico http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf).

Toma en cuenta que…
En cumplimiento al principio de calidad los responsables tienen la obligación de borrar o eliminar los datos personales de sus bases de datos, cuando éstos hayan dejado de ser necesarios para el cumplimiento de las finalidades para las cuales se hayan obtenido y haya concluido el plazo normativo para su conservación.

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

De manera adicional, los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales deberán ser establecidos y documentados por los responsables, observando los periodos de conservación señalados y considerando la realización de una revisión periódica sobre la necesidad de conservar los datos personales.

Para la supresión de los datos personales se deberán establecer políticas, métodos y técnicas orientadas a la supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima, por lo tanto, deberán tener los siguientes atributos: irreversibilidad, seguridad y confidencialidad y ser favorable al medio ambiente.

5. Mide el riesgo: entre más datos personales trates más obligaciones tendrás que cumplir

El concepto de tratamiento de datos personales es muy amplio, abarca desde su mera obtención y almacenamiento, hasta su transmisión, uso, aprovechamiento, difusión, entre otras acciones.

Cualquier tratamiento de datos personales requiere del cumplimiento de obligaciones legales específicas por parte del responsable, que van desde la puesta a disposición del aviso de privacidad, hasta la implementación de medidas de seguridad técnicas, administrativas y físicas y la reingeniería de procesos con objeto de cumplir con cada uno de los principios y obligaciones que establece la norma.

Asimismo, el responsable está obligado a atender las solicitudes de acceso, corrección, rectificación y cancelación que presenten los titulares con relación a sus datos personales, entre los que se encuentran los contenidos en las fotocopias o reproducciones de su Credencial para Votar.

En ese sentido, con objeto de disminuir riesgos tanto para el titular como para el responsable, la obtención, uso y almacenamiento de datos personales debe realizarse cuando sea estrictamente necesaria, pues de otra forma se estarían adquiriendo obligaciones y riesgos sin justificación o sentido práctico alguno.

Mientras más datos sean objeto de tratamiento, mayores serán las obligaciones para su protección, y aumentará el riesgo de ser acreedor de una sanción o responsabilidad administrativa.

En el caso particular de la Credencial para Votar se debe considerar que la Ley General en Materia de Delitos Electorales prevé una serie de conductas que constituyen delitos y que se relacionan con el uso mal intencionado de la misma, por lo que, deberán ser tratadas con máxima diligencia.

B) PREGUNTAS BÁSICAS PARA VALORAR EL TRATAMIENTO DE DATOS PERSONALES CONTENIDOS EN LAS CREDENCIALES PARA VOTAR

No.	Pregunta	Respuesta	
		Sí	No
1	¿El tratamiento de los datos contenidos en la Credencial para Votar se justifica en finalidades concretas, lícitas, explícitas y legítimas?		
2	¿Los datos personales de la Credencial para Votar se utilizan sólo para las finalidades para las que se obtuvieron y que fueron informadas en el aviso de privacidad?		
3	¿Las finalidades del tratamiento de los datos personales de la credencial para votar están relacionadas con las atribuciones normativas del sujeto obligado?		
4	¿La obtención, uso y/o almacenamiento de los datos, fotocopias o reproducciones de la Credencial para Votar es estrictamente necesario para la finalidad que justifica su tratamiento?		
5	¿Se realizan esfuerzos razonables para limitar el tratamiento de los datos personales contenidos en la credencial para votar al mínimo necesario?		
6	¿Se cuenta con medidas para mantener exactos, completos, correctos y actualizados los datos personales que se obtienen de la Credencial para Votar?		
7	¿Se tienen establecidos plazos adecuados de conservación de los datos personales contenidos en la Credencial para Votar, atendiendo las finalidades para las que se obtuvieron, las disposiciones aplicables en la materia, y los aspectos administrativos, contables, fiscales, jurídicos e históricos?		
8	¿Se establecen y documentan los procedimientos para la conservación y supresión de los datos personales contenidos en la Credencial para Votar?		
9	¿Se prevé la realización de una revisión periódica sobre la necesidad de conservar los datos, fotocopias o reproducciones de las Credenciales para Votar?		
10	¿Se establecen y mantienen medias de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales contenidos en la credencial para votar?		
11	¿En la definición de las medidas de seguridad se toman en cuenta el riesgo inherente, las posibles consecuencias de una vulneración para los titulares, así como el riesgo por el valor cuantitativo o cualitativo que pudieren tener los datos personales tratados para una tercera persona no autorizada para su posesión?		
12	¿Se establecen controles o mecanismos con el objeto de que las personas que intervengan en cualquier fase del tratamiento de los datos personales contenidos en la credencial para votar, guarden confidencialidad respecto de éstos?		
13	¿Se eliminan los datos, fotocopias o reproducciones de la Credencial para Votar por medios seguros y cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades y una vez que haya concluido el plazo de conservación establecido?		

Si en alguna de las preguntas la respuesta fue NO, resulta importante que se reconsidere la conveniencia de obtener y almacenar datos, fotocopias o reproducciones de la Credencial para Votar.

C) GLOSARIO DE TÉRMINOS

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas.

Datos personales: cualquier información relativa a una persona física, que la identifica o hace identificable.

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

INE: Instituto Nacional Electoral.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Normatividad que regula la protección de datos personales: Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento y demás normatividad que deriva de los mismos, para el sector privado; y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Lineamientos Generales de Protección de Datos Personales para el Sector Público y demás normatividad que deriva de los mismos, para el sector público.

Supresión, baja o eliminación: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales, de acuerdo con las medidas de seguridad previamente establecidas por el responsable.

Titular: Es la persona física a quien pertenecen y refieren los datos personales.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

D) INSTRUMENTOS DE FACILITACIÓN

Para mayor información sobre cómo cumplir con las obligaciones en materia de protección de datos personales, se invita a visitar el portal de Internet del INAI, en donde encontrará en la sección de "**Protección de Datos Personales"** diversas guías para orientar el debido tratamiento.

E) DATOS DE CONTACTO INAI

Para mayor información o asesoría sobre el cumplimiento de las obligaciones en materia de protección de datos personales, ponemos a disposición los siguientes canales de comunicación:

a) **Vía telefónica:** Llama al 01-800-835-4324. Tu llamada es gratuita desde cualquier estado de la República, con un horario de atención de lunes a jueves de 9:00 a 18:00 horas, y los viernes de 9:00 a 15:00 horas.
b) **Vía postal:** Puedes escribirnos directamente al Centro de Atención a la Sociedad (CAS) a la siguiente dirección: Insurgentes Sur No. 3211, Col. Insurgentes Cuicuilco, Delegación Coyoacán, C.P. 04530, Ciudad de México.
c) **Vía correo electrónico:** Ponemos a tu disposición la siguiente dirección electrónica: atencion@inai.org.mx
d) **Asesoría personalizada:** Te invitamos a visitar personalmente el CAS, ubicado en Insurgentes Sur No. 3211, Col. Insurgentes Cuicuilco, Delegación Coyoacán, C.P. 04530, Ciudad de México, con un horario de atención de lunes a jueves de 9:00 a 18:00 horas, y los viernes de 9:00 a 15:00 horas.
e) **Página de Internet:** Puedes visitar nuestra página de Internet www.inai.org.mx

F) FUENTES DE INFORMACIÓN

- Decreto de Reformas de la Ley General de Población, publicado en el Diario Oficial de la Federación el 22 de julio de 1992, disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=4678146&fecha=22/07/1992, fecha de consulta 4 de marzo de 2018.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación el 5 de julio de 2010, disponible en https://www.gob.mx/cms/uploads/attachment/file/123648/Ley_Federal_de_Protecci_n_de_Datos_Personales_en_Posesi_n_de_los.pdf, fecha de consulta 6 de marzo de 2018.
- Ley General de Instituciones y Procedimientos Electorales, última reforma publicadas e el Diario Oficial de la Federación el 27 de enero de 2017, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGIPE_270117.pdf, fecha de consulta 4 de marzo de 2018.
- Ley General de Protección de Datos Personales en Posesión de sujetos obligados, publicada en el Diario Oficial de la Federación el 27 de enero de 2017, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf, fecha de consulta 1 de marzo de 2018.
- Ley General en Materia de Delitos Electorales, última reforma publicada en el Diario Oficial de la Federación el 19 de enero de 2018, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGMDE_190118.pdf, fecha de consulta 5 de marzo de 2018.
- Lineamientos Generales de Protección de Datos Personales para el Sector Públicos, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, disponible en: http://diariooficial.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018, fecha de consulta 1 de marzo de 2018.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el Diario Oficial de la Federación el 21 de diciembre de 2011, disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf, fecha de consulta 6 de marzo de 2018.