INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO

GERENCIA DE CAPITAL HUMANO

POSGRADOS

"Recomendaciones jurídicas para las instituciones financieras en el tratamiento de las huellas dactilares de sus usuarios en el proceso de verificación de la identificación en las sucursales de México"

REPORTE ANALÍTICO DE EXPERIENCIA LABORAL

Que para obtener el grado de MAESTRA en Derecho de las Tecnologías de la Información y Comunicación

Presenta:

ANA GARCÍA ALCÁNTARA

Asesor:

MTRA. EVELYN TÉLLEZ CARVAJAL

Ciudad de México, julio, 2016.

INFOTEC
POSGRADOS

C4

Asignación de fecha de lectura pública

Ciudad de México, 15 de julio de 2016

La Gerencia de Capital Humano hace constar que el proyecto terminal titulado:

"Recomendaciones jurídicas para el tratamiento de las huellas dactilares de los usuarios de instituciones financieras en la verificación de identificación en sucursales en México"

Desarrollada por el alumno:
Nombre: Ana García Alcántara

Desarrollado bajo la asesoría de:
Mtra. Evelyn Téllez Carvajal

Ha sido revisado y aprobado por los profesores investigadores:

Dr. Alberto Enrique Nava Garcés
Dr. Federico César Lefranc Weegan
Dra. Olivia Andrea Mendoza Enríquez

Quienes han depositado en estas gerencias en su oportunidad sus reflexiones y comentarios que han sido atendidos e integrados en su totalidad por el alumno a la nueva versión escrita del proyecto integrado revisado; siendo corroborados por los mismos revisores, quienes emitieron sus votos aprobatorios por separado que obran en el expediente de investigación correspondiente.

Por lo cual, se expide la presente autorización para la impresión del proyecto terminal al que se ha hecho mención.

Finalmente se designan las 11:30 hrs., del 19 de julio de 2016, para llevar a cabo la lectura pública del trabajo descrito, en el Aula Magna de esta institución.

Vo. Bo.

Encargada de Despacho de la Gerencia de Capital Humano

Mtra. Patricia Ávila Muñoz

*** Anexar la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.**

C.c.p.: Olivia Arambarri Reyna, Responsable de Administración Escolar.

Tabla de contenido

Anexos

Índice de Ilustraciones

Índice de Abreviaturas

INE	Instituto Nacional Electoral
INAI	Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos
UNAM	Universidad Nacional de México
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Reglamento a la Ley	Reglamento a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Servicio de Verificación	Servicio de Verificación de Datos de la Credencial para Votar que el INE proporciona a entes públicos o privados.
El Proyecto	Al proyecto de BBVA Bancomer consiste en la implementación del Servicio de Verificación para verificar la identidad de sus usuarios por medio del cotejo de las huellas dactilares de aquéllos y el registro de huellas dactilares del INE.
Dictamen 3/2012	El Dictamen 3/2012 sobre la evolución de las tecnologías biométricas 00720/12/ES WP 193elaborado por el Grupo de Trabajo del Artículo 29, adoptado el 27 de abril de 2012.
Anexo Único	Anexo Único “Documento completo – Opinión técnica sobre el servicio de verificación de Datos de la Credencial para Votar”, emitido por el INAI, el cual contiene las recomendaciones realizadas por ese Instituto al INE.
Resumen Ejecutivo	Resumen Ejecutivo de la “Opinión técnica sobre el servicio de verificación de Datos de la Credencial para Votar”, extracto del Anexo Único emitido por el INAI.

Introducción

Derivado de mi práctica jurídica como abogada de temas de tecnología, a inicios de 2015 tuve la oportunidad de laborar en la institución financiera BBVA Bancomer, en donde se me comunicó la posibilidad de que dicho banco adoptara un nuevo proyecto al interior de la institución para evitar la suplantación de la identidad de sus clientes y usuarios.

Dicho proyecto consistiría en que BBVA Bancomer adoptaría el Servicio de Verificación que actualmente opera el Instituto Nacional Electoral (INE) con algunas instituciones públicas y privadas, para poder verificar la identidad de sus clientes o usuarios bancarios utilizando sus huellas dactilares, mediante el cotejo de las mismas con las huellas dactilares que el INE tiene registradas en su base de datos.

Es importante mencionar que, en la actualidad, además de BBVA Bancomer, diversas instituciones financieras están trabajando con el INE para la adopción del sistema de cotejo de las huellas dactilares de los usuarios de la banca por medio del Servicio de Verificación, toda vez que la suplantación de identidad de los mismos ha aumentado en los últimos años.

No obstante las ventajas que el proyecto representa para las instituciones financieras, no ha sido implementado por completo debido a que su desarrollo requiere del estudio previo de diversos aspectos tanto técnicos como legales, a efecto de evitar que su operación conlleve incumplimientos legales imputables a las instituciones adoptantes del sistema, especialmente en materia bancaria y de protección de datos personales.

Ahora bien, además de la experiencia y conocimientos adquiridos en el sector bancario privado, actualmente desempeño mi labor profesional como abogada en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en la Coordinación de Protección de Datos Personales, lo que me permite conocer de primera mano el criterio y la postura interna de este Instituto en

relación con diversos temas en materia de privacidad, como lo es el tratamiento de datos biométricos tanto en el sector público como en el privado.

Así, con la experiencia y conocimientos adquiridos con motivo de mi práctica profesional, así como del estudio de la Maestría en Derecho de las Tecnologías de la Información y Comunicación con la especialidad en Datos Personales Digitales en INFOTEC, y sin que ello implique ventilar en ningún momento información confidencial de ninguna de las instituciones mencionadas, el presente trabajo se constituye como una guía o un manual de recomendaciones legales, aplicable a las instituciones bancarias privadas en México que pretendan adoptar el Sistema de Verificación del INE para identificar a sus clientes por medio de sus huellas dactilares, sin ser óbice que, en algunos casos, se toman como referencia aspectos específicos de BBVA Bancomer, por ejemplo, el Aviso de Privacidad de esta institución, pero sin perder de vista que esta guía tiene como objeto alertar al gremio de la banca privada en general, respecto a las obligaciones jurídicas que deben observar en su carácter de responsables del tratamiento de las huellas de sus clientes y, por ende, que al apegarse a las recomendaciones correspondientes que se abordan en este trabajo, el proyecto pueda ser implementando y operado en estricto apego a derecho.

CAPÍTULO I

Sistema de Verificación de identidad de las instituciones financieras y el INE.

CAPÍTULO I Sistema de Verificación de identidad de las instituciones financieras y el INE.

En México, algunas instituciones financieras como Banamex,[1] Santander[2] y Bancomer, están trabajando en conjunto con el Instituto Nacional Electoral, (en adelante INE) en la creación de un sistema de identificación biométrica para validar la identidad de sus clientes haciendo uso de las huellas dactilares de éstos. Las huellas dactilares de los clientes de las instituciones bancarias se pretende que sean cotejadas en tiempo real contra la base de huellas dactilares con que cuenta el INE en virtud del trámite que realizan los ciudadanos para obtener la credencial de elector, ya que en dicho trámite actualmente, (si el ciudadano no se opone), se capturan por medio de un dispositivo electrónico sus diez huellas dactilares.

El objeto de este sistema biométrico que se le conoce como Servicio de Verificación de Datos de la Credencial para Votar, (el cual en lo sucesivo se denominará como "el Proyecto") es que las instituciones financieras puedan validar la autenticidad de la credencial de elector con la que se pretendan identificar las personas (clientes o no clientes de la institución financiera) que acudan a las sucursales bancarias y evitar así la suplantación de la identidad de sus legítimos clientes, pues en diversas ocasiones los defraudadores se presentan a dichas sucursales a realizar operaciones con credenciales de elector apócrifas para allegarse de los recursos de la persona suplantada.

---

[1] "Instituciones bancarias adoptarán el uso de huella digital", *Informador.mx*, s.f.
Recuperado de: *http://www.informador.com.mx/economia/2015/579756/6/instituciones-bancarias-adoptaran-el-uso-de-huella-digital.htm*
Fecha de consulta: 23 de abril de 2015.

[2] Leyva, Jeanette, "Estalla polémica por prueba piloto de INE-Banamex", *El Financiero*, 06 de marzo de 2015.
Recuperado de: *http://www.elfinanciero.com.mx/economia/estalla-polemica-por-prueba-piloto-de-ine-banamex.html*
Fecha de consulta: 23 de abril de 2015.

Esta suplantación de identidad a través de la credencial de elector se realiza generalmente de dos formas:

1. Los defraudadores elaboran credenciales de elector falsas con los datos de la persona a suplantar pero con la fotografía del defraudador.

2. Los defraudadores que poseen cierto parecido físico con el titular de la credencial utilizan la credencial de elector que han robado de su titular o que éste último perdió, para hacerse pasar por éste.

A la fecha las instituciones financieras no cuentan con un medio eficaz para verificar la autenticidad de las credenciales de elector que se les son presentadas como medio de identificación.

Por lo anterior, el Servicio de Verificación de Datos de la Credencial para Votar tiene como objetivo lo siguiente:[3]

> "a) Verificar la vigencia y coincidencia de los datos de la Credencial para Votar (CPV) que presenten los ciudadanos para identificarse ante una institución pública o privada, respecto de la información almacenada en la base de datos del Padrón Electoral.
>
> b) Autenticar las huellas dactilares del ciudadano que se identifique con una Credencial para Votar, mediante la correlación gráfica de las marcas dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en la base de datos con lo almacenado en el Padrón Electoral."

---

[3] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, (INAI), Coordinación de Protección de Datos Personales. Dirección General de Autorregulación Dirección General de Normatividad, Consulta y Atención Regional Mayo de 2015*, Anexo Único Documento completo Opinión técnica sobre el Servicio de Verificación de Datos de la Credencial para Votar*, p. 2.

Para el caso de la huella digital, el Instituto realizará la confrontación de la información proporcionada por la institución, con la que se tiene registrada en la base de datos del Padrón Electoral mediante el uso estándar de minucias dactilares para el intercambio de datos denominado INCITS 378[4], que consiste en un método de comparación de la información de huellas dactilares a partir de minucias, que da como respuesta un porcentaje de similitud de acuerdo al mismo estándar."

La funcionalidad del Proyecto se puede representar de la siguiente forma:

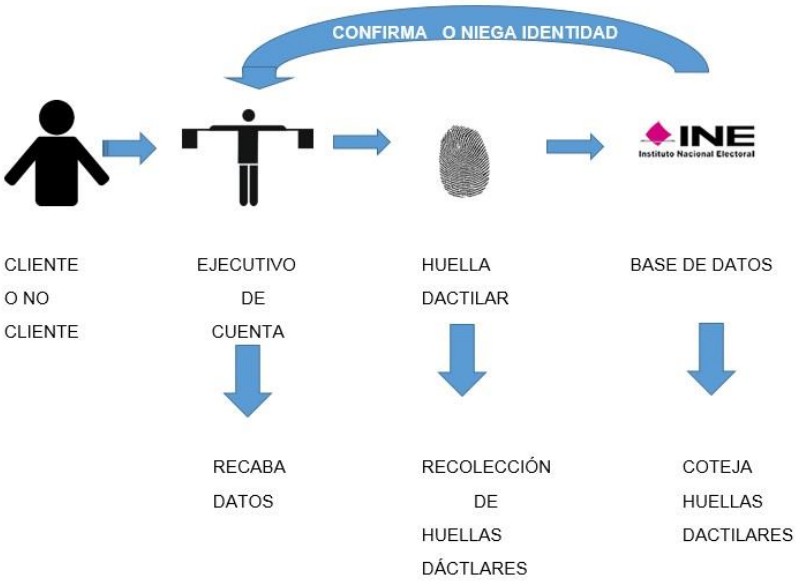


Ilustración 1. Funcionalidad del "Proyecto".

[4] El estándar *ANSI-INCITS 378-2004* fue creado en 2004 por la ANSI, el cual establece criterios para representar e intercambiar la información de las huellas dactilares a través del uso de minucias. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas.
Más información sobre el estándar ANSI-INCITS 378-2004:
http://www.incits.org o en Jain, Anil K. y *et. al*., *Handbook of Biometrics,* Estados Unidos, Springer, 2008, p. 472.

De acuerdo con el Senado de la República, el Instituto Electoral del Distrito Federal y algunos medios de información nacionales, la verificación de la identidad de los clientes contemplaría los siguientes puntos:[5]

Ilustración 2. Intervención del INE para validar la identidad de los usuarios de la banca.

Imagen tomada de "El Financiero"[6]

Sobre esto, el consejero presidente de la Comisión de Fiscalización del INE, Benito Nacif Hernández señaló que:

> "Esta iniciativa responde a un problema muy real y muy grave que requiere atención de las instituciones públicas, que es el problema de robo y de fraudes de identidad, afecta particularmente a las instituciones financieras tanto públicas como privadas. Hemos hablado y hemos firmado convenios también con diversas instituciones como al INFONAVIT, EL (sic) IMSS, además de las instituciones bancarias, la principal ha sido BANAMEX, pero también BANCOMER y otras más están interesadas, porque son víctimas de fraude

[5]Véase Leyva, Jeanette, "Cotejarían con INE identidad en banca", *El Financiero*, periódico de circulación nacional, 05 de marzo de 2015, México, p.4.
[6]*Idem.*

de identidad en la tramitación de créditos principalmente o en el cobro de documentos. Y el número de fraudes que se tienen por el uso de documentos de identificación falsos, incluyendo la propia credencial que es susceptible a falsificación, hay falsificaciones muy burdas y este es un remedio para ese problema".[7]

No obstante lo beneficios del Servicio de Verificación, este Proyecto, ha causado polémica pues algunos especialistas en datos personales consideran que podría ser violatorio de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.[8]

Debido a esto, el INE solicitó la opinión del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, (en adelante INAI), respecto del Servicio de Verificación, por lo que en mayo de 2015 el INAI emitió los siguientes documentos para orientar la operación del INE en dicho Proyecto:

- Anexo Único "Documento completo – Opinión técnica sobre el servicio de verificación de Datos de la Credencial para Votar", el cual se adjunta al presente estudio como **Anexo 1**, en lo sucesivo "Anexo Único".
- Resumen Ejecutivo "Opinión técnica sobre el servicio de verificación de Datos de la Credencial para Votar", el cual se adjunta al presente estudio como **Anexo 2**, en lo sucesivo "Resumen Ejecutivo".

---

[7] Rubio, Francisco, "INE no otorgará el padrón electoral a los bancos: Consejero", *Noticias MVS*, 5 de marzo de 2015.
Recuperado de: *http://www.noticiasmvs.com/#!/noticias/ine-no-otorgara-el-padron-electoral-a-los-bancos-consejero-196.html*
Fecha de consulta: 24 de abril de 2015.

[8] Leyva, Jeanette, "Genera polémica el programa piloto de verificación de huella", *El Financiero*, periódico de circulación nacional, 06 de marzo de 2015, México, p. 5.
Recuperado de: *http://www.especialistas.com.mx/saiweb/viewer.aspx?file=4ejBjxeato5yStCGOR9vKiIC8Sxf8ALQOHbzs@@Lw8jRZmMaxT84kdkY8X0QgHF3tDwXNo7crMtdB0u/MgAfnYQ==&opcion=0&encrip=1*
Fecha de consulta: 24 de abril de 2015.

Para la emisión de la opinión contenida en el Resumen Ejecutivo, el INE remitió al INAI los modelos de Convenio de apoyo y colaboración para instituciones privadas que el INE pretende suscribir con las instituciones con las que opere el Servicio de Verificación, así como el Anexo Técnico del INE, integrante del Convenio de Apoyo y Colaboración, los cuales se adjuntan al presente como **Anexo 3** y **6** respectivamente para futuras referencias.

Sin embargo, es importante señalar que a la fecha no existen recomendaciones oficiales por parte de INAI para las instituciones financieras respecto a la implementación u operación del Servicio de Verificación.

En virtud de lo anterior, en este trabajo se analizarán los aspectos técnicos y legales que conlleva el tratamiento de huellas dactilares en sistemas automatizados como es el caso del Proyecto, además se realizarán las recomendaciones legales pertinentes para que la implementación y operación del Servicio de Verificación por parte de cualquier institución de crédito sean llevadas a cabo en apego a la normativa en materia de datos personales, financiera y demás aplicable en México. En este caso en concreto a efecto de evitar posibles sanciones de las autoridades de privacidad y bancarias, las cuales podrían representar un quebranto económico para la institución financiera así como un desprestigio de la institución frente a sus clientes.

CAPÍTULO II

¿Qué son los datos biométricos?

CAPÍTULO II ¿Qué son los datos biométricos?

Para realizar las recomendaciones legales oportunas en la adopción del Servicio de Verificación por parte de las instituciones financieras, es necesario entender la naturaleza de los datos biométricos, en especial de las huellas dactilares. En este capítulo II se explica qué son los datos biométricos, sus características y otros aspectos importantes para la elaboración de las recomendaciones pertinentes.

Todos los seres humanos tenemos características morfológicas únicas que nos diferencian de los demás como la forma de la cara, la geometría de algunas partes de nuestro cuerpo como las manos, nuestros ojos y, tal vez la más conocida es la huella digital o dactilar. Todos estos rasgos son conocidos como datos biométricos.[9]

De acuerdo con el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas[10] elaborado por el Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, creado en virtud del artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo,[11] los datos biométricos son aquellas propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad.

---

[9] Tolosa Borja, César y Giz Bueno, Álvaro, *Sistema Biométricos*, España, Universidad de Castilla-La Mancha, 2009-2010. Recuperado de:
http://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf
Fecha de consulta: 27 de enero de 2015.

[10] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas 00720/12/ES WP 193, Grupo de Trabajo del Artículo 29, adoptado el 27 de abril de 2012.
Recuperado de: *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*
Fecha de consulta: 26 de julio de 2014.

[11] También conocido como Grupo de Trabajo del Artículo 29.

El término “biometría” y datos “biométricos” provienen del latín *bios*, vida, y *metria*, medidas, por tanto, los datos biométricos constituyen información referente a las medidas y características tanto fisiológicas como morfológicas de los seres vivos a través de técnicas manuales o automatizadas.[12]

La biometría también ha sido considerada como una técnica automatizada que a través de características físicas y pautas de comportamiento identifica y verifica la identidad de las personas, animales y objetos.[13]

En la biometría se distinguen dos grupos de registros biométricos: los fisiológicos o morfológicos y, por otra parte, los conductuales. Los primeros, fisiológicos o morfológicos, serían aquellos que hacen referencia a rasgos o cualidades físicas inalterables y presentes en todas las personas que se traducen en patrones fijos, como son: huella dactilar, geometría de la mano, características del iris, patrones vasculares de la retina, mano, etcétera, mientras que los biométricos conductuales son aquellos que se soportan sobre características de la conducta del ser humano tales como pulsaciones del teclado, dinámica de la firma, etcétera.[14]

El uso de los datos biométricos para la identificación y autenticación de las personas ha cobrado auge en los últimos años en múltiples áreas, por ejemplo, la investigación de delitos, el control del acceso a lugares restringidos, el registro de asistencia y puntualidad de empleados.

Algunos datos biométricos son:

- Huellas dactilares
- Geometría de la mano

---

[12] Dictamen 3/2012 *op. cit*., nota 10.
[13] Hopkins, Richard, “An Introduction to Biometrics and Large Scale Civilian Identification”, *International Review of Law*, Computers and Tecnology, núm. 13, pp. 337-363.
[14] Bueno De Mata, Federico, *Biometría: el uso de las TICS como medio de identificar presuntos autores de hechos delictivos*, México, UNAM- Instituto de Investigaciones Jurídicas UNAM, s/f, p. 132. Recuperado de: *http://biblio.juridicas.unam.mx/libros/6/2940/9.pdf*
Fecha de consulta: 26 de marzo de 2016

- Análisis del iris
- Análisis de retina
- Venas del dorso de la mano
- Rasgos faciales
- Patrón de voz
- Firma manuscrita
- Dinámica de tecleo
- Cadencia del paso al caminar
- Análisis gestual
- Análisis del ADN

De acuerdo con el informe de actividades del 2007 de la Comisión Nacional de Informática y Libertades de Francia,[15]la recolección de datos biométricos es un aspecto de preocupación, toda vez que algunos datos biométricos pueden ser recabados y utilizados sin que el interesado se dé cuenta, ya que todos vamos dejando involuntariamente un rastro de nuestro cuerpo, aunque sea ínfimo, del cual se puede extraer el código ADN. Lo mismo sucede con las huellas dactilares, de las que también vamos dejando un rastro, más o menos fácil de procesar, en nuestra vida cotidiana.[16]

Por tal razón, esta Comisión indicó que la biometría requiere de medidas de seguridad especiales para garantizar la protección de las personas afectadas.

Por su parte, en 2003, el Grupo de Trabajo del Artículo 29 emitió el "Documento de trabajo sobre biometría" donde señala la siguiente inquietud: "Una utilización amplia y sin control de la biometría es preocupante desde el punto de vista de la

---

[15] Agencia Española de Protección de Datos: Proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. Informe 368/2006.

- Tratamiento de la huella digital de los trabajadores.
- Resolución de archivo de actuaciones. Expediente Nº: E/00016/2007

Recuperado de: *http://www.agpd.es/portalwebAGPD/index-ides-idphp.php*
Fecha de consulta: 27 de septiembre de 2014.

[16] Artículo escrito por el grupo de abogados denominado Information Law Group conformado principalmente por Blackmer, Scott; Gotshall, Justine, Nolan. Heather, Rubin, Jaime, entre otros, "Russia Amends Federal Data Protection Law, Privacy Enforcement on the Rise", en la página electrónica de *Information Law Group*, publicado el 19 de Julio de 2011. Recuperado de *http://www.infolawgroup.com/2011/07/articles/international-2/russia-amends-federal-data-protection-law-privacy-enforcement-on-the-rise/*
Fecha de consulta: 27 de abril de 2015.

protección de los derechos y libertades fundamentales de las personas. Este tipo de datos es de una naturaleza especial, ya que tienen que ver con las características comportamentales y fisiológicas de una persona y pueden permitir su identificación inequívoca (...) No obstante, la identificación única depende de diversos factores como las dimensiones de la base de datos y el tipo de información biométrica".[17]

En ese contexto, el tema de la privacidad en el tratamiento de datos biométricos ha sido de preocupación desde hace tiempo principalmente por lo siguiente:

- La tecnología biométrica puede ser percibida como deshumanizante y como una amenaza a la privacidad de las personas. En el caso de los biométricos de autenticación, éstos son vistos como un serio problema ya que las características biométricas de un individuo pueden revelar información sobre su estado de salud o algún otro tipo de información sensible, por ejemplo, el estudio de la retina puede revelar información sobre diabetes o hipertensión en el individuo[18] lo que puede conllevar discriminación para la persona.
- Cuando un dato biométrico es registrado en un sistema, la información contenida en él puede ser usada para fines distintos a los cuales se recabó pues en ningún sistema es fácil asegurar que los datos biométricos solo serán usados para los fines por los cuales se recabaron originalmente.
- El uso cotidiano de datos biométricos en distintas tecnologías puede provocar que el público se insensibilice ante los efectos que pueda tener el tratamiento para la vida cotidiana, por ejemplo, el uso de la biometría en las bibliotecas escolares puede hacer que los niños sean menos conscientes de los riesgos

---

[17] Documento de trabajo sobre biometría 12168/02/ES WP 80, Grupo de Trabajo del Artículo 29, adoptado el 1 de agosto de 2003, p. 2.
Recuperado de: *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_es.pdf*
Fecha de consulta: 18 de mayo de 2016.
[18] Bolle, Ruud M. y *et. al*., *Guide to Biometrics,* Estados Unidos, Springer, 2004, p. 223.

relativos a la protección de datos que pueden tener consecuencias para ellos en una etapa posterior de su vida.[19]

- Los datos biométricos pueden ser considerados datos sensibles. Dependiendo del diseño de los sistemas biométricos, éstos pueden revelar mucha o poca información personal. La clasificación de datos biométricos como "sensibles" estará determinada por las circunstancias específicas, pero compartir datos biométricos con el objetivo de identificar y/o verificar a los individuos es información personal sensible.[20]
- Algunos datos biométricos pueden ser falsificados, por ejemplo, las huellas dactilares, y ser utilizados para suplantar la identidad de sus titulares.[21]

Por lo anterior, la protección de los datos biométricos resulta de vital importancia, ya que si un sistema biométrico no es protegido adecuadamente, éste puede facilitar la obtención de información personal sensible del individuo o acarrear daños materiales o personales para éste, por ejemplo, si un atacante roba la base de datos de un sistema de reconocimiento facial en el cual se almacenan fotografías, se podría inferir la raza de cada uno de los usuarios, lo que podría ser causa de

---

[19] Documento de trabajo sobre biometría 12168/02/ES WP 80…, *op*. *cit.,* nota 17.
[20] Villanueva, Ernesto y Díaz Vannesa, *Derecho de las nuevas tecnologías (en el siglo xx derecho informático),* México, Oxford University Press, 2015, pp. 43 y 46.
[21] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas 00720/12/ES WP193, *op. cit.*, nota 10, p.23.
Algunas noticias e información relevantes relacionadas con este punto:
1. "Falsificación de huellas dactilares en control de acceso", *Cybertronics Security*, 2014.
Recuperado de: *https://www.youtube.com/watch?v=S2cp5j8sgN8*
Fecha de consulta: 16 de enero de 2016.
2. Chong Magallanes, Jahtziri, "Detienen a servidor público del IMSS por falsificar huellas digitales para checar asistencias", *Noticias MVS*, 20 de agosto de 2012.
Recuperado de: *http://www.noticiasmvs.com/#!/noticias/detienen-a-servidor-publico-del-imss-por-falsificar-huellas-digitales-para-checar-asistencias-535*
Fecha de consulta: 16 de enero de 2016.
3. "Clonan huellas digitales: modalidad permitiría pasar sistemas de seguridad biométricos", *Buenos Días Perú*, 08 de abril de 2015.
Recuperado de: *https://www.youtube.com/watch?v=0cIcjwBDXHs y http://panamericana.pe/buenosdiasperu/locales/179775-clonan-huellas-digitales-mafia-suplantaba-postulantes-universidad*
Fecha de consulta: 18 de enero de 2016.

discriminación u otras acciones,[22] o si una persona falsificar las huellas de otra podría tener acceso a lugares, bienes o derechos indebidamente perjudicando al titular de las huellas.

No obstante lo anterior, actualmente no existe un tratado o convención internacional que regule el tratamiento de datos biométricos automatizados, y por ello la regulación depende de cada uno de los países que utilicen este tipo de datos y tecnología, que generalmente recae en las leyes sobre privacidad y datos personales que contemplan la sistematización de la información de cada país.[23]

En México a la fecha no se cuenta con regulación especial que proteja a los datos biométricos.

1. Sistemas biométricos

Un sistema biométrico es un método automático de identificación y verificación de un individuo utilizando características físicas y de comportamiento precisas. Las características básicas que un sistema biométrico para identificación personal debe cumplir son: desempeño, aceptabilidad y fiabilidad. Las cuales apuntan a la obtención de un sistema biométrico con utilidad práctica.[24]

Los sistemas biométricos tienen dos objetivos: el primero es para identificar, es decir, reconocer al individuo, por lo que su funcionamiento está basado en utilizar un dato y compararlo con una lista o base de datos (comparación 1:N). El segundo

---

[22]Rojas González, Isai y Sánchez Pérez, Gabriel, "Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I", *Revista de Seguridad y Defensa Digital: Cultura de prevención para ti*, UNAM, México, número 13, revista bimestral, 2012.
Recuperado de: *http://revista.seguridad.unam.mx/numero-14/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-p*
Fecha de consulta: 13 de junio de 2014.
[23]Véase Bueno De Mata, Federico, *Biometría: el uso de las TICS como medio de identificar presuntos autores de hechos delictivos, op. cit.,* nota 14.
[24] "Bases teóricas y sistemas biométricos", *Revista Red y Seguridad*, UNAM, México, s/n, Recuperado de: *http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/caracteristicassistema.html*
Fecha de consulta: 28 de abril de 2016.

es para autenticar, es decir, verificar la identidad del individuo, por ello su funcionamiento está basado en la utilización de un dato comparándolo con el mismo dato almacenado previamente (comparación 1:1).[25]

El objetivo de los sistemas biométricos es la identificación (reconocimiento) o la autenticación (verificación) de los individuos basada en algunas características fisiológicas o morfológicas. Se debe considerar que para el desarrollo de sistemas biométricos es fundamental distinguir precisamente su objetivo. Esto es, si el sistema biométrico será utilizado para identificar o autenticar, puesto que el reconocimiento y la verificación son actividades totalmente diferentes y para ello algunas características fisiológicas son más apropiadas para la identificación y otras son mejor para la autenticación.[26]

La autenticación responde a la pregunta ¿soy quien pretendo ser? El sistema certifica la identidad de la persona mediante el tratamiento de datos biométricos referidos a la persona que pregunta y toma una decisión sí/no (comparación 1:1). La identificación responde a la pregunta quién soy El sistema reconoce a la persona que pregunta distinguiéndola de otras personas, cuyos datos biométricos también están almacenados. En ese caso, el sistema toma una decisión 1 entre n, y responde que la persona que pregunta es X.[27]

Por otra parte, es importante hacer mención que ningún sistema biométrico puede dar respuestas 100% precisas. Esto se debe a la calidad del sistema, de la muestra, la temperatura, la iluminación, etcétera.

De acuerdo con el "Dictamen 3/2012 sobre la evolución de las tecnologías biométricas", los medidores de evaluación de rendimiento más utilizados son la Tasa

---

[25] Díaz, Vanessa, "Sistemas biométricos en materia criminal: un estudio comparado", en *Revista IUS,* Instituto de Ciencias Jurídicas de Puebla, núm. 31, año VII, México, enero-junio, pp. 28-47

[26]Bueno De Mata, Federico, *Biometría: el uso de las TICS como medio de identificar presuntos autores de hechos delictivos, op. cit.,*nota 14.

[27]Documento de trabajo sobre biometría 12168/02/ES WP 80, p. 3…, *op. cit.* nota 17.

de Falsa Aceptación y la Tasa de Falso Rechazo, y pueden adaptarse al sistema que se utilice.[28]

- La Tasa de Falsa Aceptación (False Acceptance Rate o FAR) es la probabilidad de que un sistema biométrico identifique incorrectamente a un individuo o no rechace aun impostor. Mide el porcentaje de entradas inválidas aceptadas incorrectamente. También se conoce como tasa de falso positivo.
- La Tasa de Falso Rechazo (False Rejection Rate o FRR) es la probabilidad de que el sistema arroje un falso rechazo; esto se produce cuando no se establece la correspondencia entre una persona y su propia plantilla biométrica. También es se conoce como tasa de falso negativo.

El mismo Dictamen señala que lo siguiente:

> "…con una configuración y ajuste adecuados, los errores críticos de los sistemas biométricos pueden minimizarse al nivel permitido para su uso operativo reduciendo los riesgos de evaluaciones incorrectas. Un sistema perfecto tendrá un FAR y FRR igual a cero, pero más comúnmente, guarda una correlación negativa: el aumento de FAR suele reducir el nivel del FRR.
>
> Al evaluar si es aceptable la precisión de un determinado sistema biométrico, es importante evaluar la finalidad del tratamiento, la FAR y la FRR, así como el tamaño de la población.
>
> Además, para evaluar la precisión de un sistema biométrico también podrá tenerse en cuenta la capacidad para detectar una muestra viva, por ejemplo, las impresiones dactilares latentes pueden copiarse y utilizarse para crear

[28]Dictamen 3/2012 sobre la evolución de las tecnologías biométricas 00720/12/ES WP193, *op. cit.* nota 10, pp. 6 y 7.

dedos falsos. Un lector de huellas dactilares no deberá caer en la trampa de realizar una identificación positiva en tal situación."[29]

2. Huellas dactilares

Como ya se mencionó, la huella dactilar es un dato biométrico al ser una característica física única que distingue a todos los seres humanos. La ciencia que se encarga de su estudio se conoce como Dactiloscopia, que viene de los vocablos griegos daktilos (dedos) y skopein (examen o estudio).Este nombre fue inventado por el doctor Francisco Latzina en sustitución al nombre dado por Sir Francis Galtón (Icnofalangometría) en 1892.[30]

De acuerdo con la Universidad Nacional Autónoma de México, todos los sistemas dactiloscópicos se basan en tres principios fundamentales:[31]

- Perennidad: Gracias al fisiólogo checo Juan Evangelista Purkinje se sabe que las huellas dactilares se manifiestan a partir del sexto mes del desarrollo del embrión y que están presentes a lo largo de toda la vida de los seres humanos y hasta la descomposición del cadáver.
- Inmutabilidad: Las huellas dactilares no se ven afectadas en sus características por el desarrollo físico de los individuos ni por enfermedades de ningún tipo y en caso de que llegase a presentarse un desgaste involuntario (por ejemplo una herida o quemadura), el tejido epidérmico que la conforma es capaz de regenerase tomando su forma original en un periodo de 15 días.
- Diversidad Infinita: Las huellas dactilares son únicas e irrepetibles, cada ser humano posee huellas dactilares con características individuales. Es un error

---

[29] *Idem*.
[30] "Clasificación de los sistemas biométricos", *Revista Red y Seguridad*, UNAM, México, s/n, Recuperado de: *http://redyseguridad.fi-p.unam.mx/Proyectos/biometria/clasificacionsistemas/recohuella.html*
Fecha de consulta: 21 de diciembre de 2015.
[31] *Idem*.

común pensar que los gemelos idénticos no cumplen con este principio, sin embargo las huellas dactilares no se desarrollan debido a un proceso genético sino a un proceso aleatorio por lo que no existe ningún tipo de correlación entre gemelos idénticos o individuos de una misma familia.

No obstante lo anterior, existen casos en los que las personas tienen heridas en la yema de sus dedos o sufrieron alguna patología en la piel y algunos sistemas dactilares no serían capaces de reconocer sus huellas; es por ello que normalmente existe una fracción de personas en las que no es posible utilizar la identificación biométrica dactilar[32]. Bajo este entendido, resulta importante analizar la conveniencia de sujetar el acceso a un derecho del titular de las huella a la lectura y reconocimiento del sistema.

Por otro lado, como ya se mencionó anteriormente, la seguridad y protección de los registros de las huellas dactilares, así como de los demás datos biométricos, es sumamente importante. De acuerdo con la UNAM, una huella dactilar reconstruida a partir de la plantilla de minucias[33]tiene un resultado positivo en más del 90% de los casos, y que este tipo de reconstrucciones son más frecuentes de lo que se podría suponer.[34]

---

[32] Vildjiounaite, Elena, "Soft biometrics—combining body weight and fat measurements with fingerprint biometrics", *Pattern Recognition Letters*, vol.27, 1 de abril 2006, p. 325.
Recuperado de: *www.elsevier.com/locate/patrec*
Fecha de la consulta: 15 de octubre de 2014.

[33] Remolina Angarita, Nelson, "Sistemas de identificación biométrica y protección de datos personales: ni "tecnofobia", ni "tecnofascinación", pero sí "tecnoreflexión", *Ámbito Jurídico.com*, 16 de noviembre de 2011.
Recuperado de: *http://www.ambitojuridico.com/BancoConocimiento/N/noti-111116-06_sistemas_de_identificacion_biometrica_y_proteccion_de_datos_pe/noti-111116-06_sistemas_de_identificacion_biometrica_y_proteccion_de_datos_pe.asp*
Fecha de consulta: 27 de abril de 2015.

[34] Comité consultivo de la Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal (T-PD), 2005.
Recuperado de
http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/informe-principios-convencion-108.pdf.
Fecha de consulta: 26 de julio de 2014.

Esto indica que se pueden identificar a personas o falsificar identidades mediante el uso de huellas dactilares que sean obtenidas exitosamente, en su forma original, incluso desde una base de datos de plantillas de minucias.

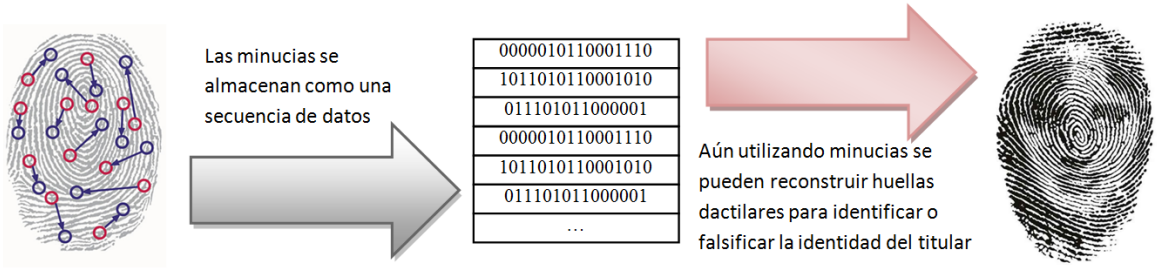


Ilustración 3. Reconstrucción de una huella dactilar a partir de su minucia.

Imagen tomada de: Sánchez Pérez, Gabriel y Rojas González, Isai."Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I"[35]

Lo anterior, nos confirma dos cosas: ningún sistema biométrico es 100% seguro para evitar la suplantación de identidad de las personas y que el manejo incorrecto de los datos biométricos, en este caso las huellas dactilares puede acarrear riesgos graves para el titular de las huellas.

Actualmente en nuestro país no se cuenta con normas o recomendaciones por parte de las autoridades para la protección de las huellas dactilares.

3. Estándares biométricos

Para poder obtener un diseño interoperable, abierto y estandarizado de un sistema biométrico, un factor crítico es la especificación técnica de estándares.[36]

---

[35]Rojas González, Isai y Sánchez Pérez, Gabriel, "Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I", *op.cit.*, nota 22.
[36]Jain, Anil K. y *et. al*., *Handbook of Biometrics,* Estados Unidos, Springer, 2008, p. 471.
Texto original:

De acuerdo con la Facultad de Ingeniería de la UNAM, un estándar es un conjunto de reglas que deben cumplir los productos, procedimientos o investigaciones que afirmen ser compatibles con el mismo producto. Los estándares ofrecen muchos beneficios, reduciendo las diferencias entre los productos y generando un ambiente de estabilidad, madurez y calidad en beneficio de consumidores e inversores.[37]

La carencia de estándares biométricos a nivel industrial ha dificultado el desarrollo de algunos tipos de sistemas biométricos y el crecimiento de este sector industrial,[38] por lo que en los últimos años ha habido una preocupación creciente por parte de lasorganizaciones regulatorias respecto a elaborar estándares relativos aluso de técnicas biométricas.[39]

3.1 Principales organismos de estandarización

A nivel internacional encontramos los siguientes organismos coordinadores de actividades de estandarización biométrica, con más de 60 estándares en desarrollo:

- Subcomité 37 (SC37) del Joint Technical Committee on Information Technology (JTC1) del International Organization for Standardization (ISO), lo cual se resume como ISO/IEC JTC1/SC37.
- Comité Técnico M1 del International Committee for Information Technology Standards (INCITS), organismoacreditado por el American National Standards Institute (ANSI).

"For an interoperable, open, standars-based system design, one critical factor is the precise technical specification of standars."

[37]"Estándares biométricos", *Revista Red y Seguridad*, UNAM, México, s/n. Recuperado de: *http://redyseguridad.fi-p.unam.mx/proyectos/biometria/estandares/estandar.html*
Fecha de consulta: 18 de abril de 2016

[38]*Idem.*

[39] Ortega García, Javier y *et. al*, Biometría y Seguridad, Universidad Autónoma de Madrid, España, 2008, p. 65. Recuperado de: *http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/09/CUADERNO-N%C2%BA-3.pdf*
Fecha de consulta: 18 de abril de 2016

- Information Technology Laboratory (ITL) [55] del Instituto Nacional de Estándares y Tecnología americano (NIST), contribuidor importante a las actividades de estandarización de losorganismos anteriores.

Existen además otros organismos internacionales impulsando iniciativas en materias biométricas tales como el Biometrics Consortium (BC), el International Biometrics Group (IBG), la Biometrics Management Office del Departamento de Defensa americano (DoD) o el European Biometrics Forum (EBF). A nivel nacional, Asociación Mexicana de Biometría e Identidad (AMBI) y organismos nacionales de normalización o la Secretaría de Economía para la creación de Normas Oficiales de acuerdo Ley Federal sobre Metrología y Normalización.

3.2 Estándares utilizados en huellas dactilares

Actualmente, existen varios estándares que son utilizados en soluciones biométricas, tanto para el almacenamiento de información biométrica como para el intercambio de datos entre sistemas. Las principales instituciones internacionales que han aportado a la definición de estos estándares son la American National Standards Institute (ANSI) y la International Organization for Standardization (ISO).[40]

Los estándares para huellas dactilares definidos por estos organismos son los siguientes:[41]

---

[40] Crisaldo, Robert y *et. al*, "Un enfoque de integración entre fprint y SourceAFIS", *Universidad Nacional de Asunción*, Paraguay, s/f.
Recuperado de: *http://www.pol.una.py/cia/sites/default/files/files/Integracion_Fprint_SourceAFIS.pdf*
Fecha de consulta: 18 de abril de 2016.
[41] *Idem.*

Estándares ANSI:

- ANSI/INCITS 381-2004. Formato imágenes de huellas dactilares.
- ANSI/INCITS 377-2004. Formato de información biométrica de huellas dactilares.
- ANSI-INCITS 378-2004. Formato de minucias de huellas dactilares.
- ANSI NIST ITL 1-2007. Formato de información biométrica de huellas dactilares, faciales, cicatrices, marcas y tatuajes.

Estándares ISO:

- ISO/IEC 19794-2. Formato de minucias de huellas dactilares.
- ISO/IEC FCD 19794-3. Formato de información biométrica de huellas dactilares.
- ISO/IEC 19794-4. Formato de imágenes de huellas dactilares.

CAPÍTULO III

Uso de los datos biométricos en el sistema financiero, especialmente las huellas dactilares

CAPÍTULO III Uso de los datos biométricos en el sistema financiero, especialmente las huellas dactilares

No obstante los riesgos que implican el uso de datos biométricos señalados en el capítulo II anterior, la eficacia potencial de la biometría la hace especialmente interesante en determinadas áreas, en las que ya se empiezan a emplear algunos sistemas biométricos,[42] por ejemplo en la banca electrónica, la cual ha sido una de las áreas que mayor crecimiento ha tenido en los últimos años y la que más ha influido en el desarrollo de nuevos sistemas de seguridad, hasta el punto de que este sector pretende reducir los precios de venta de los dispositivos de reconocimiento biométrico para que las computadora de los clientes cuenten con sensores de presión y velocidad de tecleo o webcams con reconocimiento facial que permitan la identificación biométrica de los usuarios.[43]

La principal ventaja que ofrecen tanto la banca electrónica como el comercio electrónico es la posibilidad de acceder a los servicios a través de cualquier computadora o dispositivo que cuente con acceso a Internet. De esta forma el uso de tecnología biométrica ofrece la seguridad tanto a la empresa como al individuo de que la operación que se realice a través de Internet es llevada a cabo de manera confiable.[44]

En relación con el uso de la biometría en el sistema financiero, los últimos datos del sector bancario a nivel mundial apuntan que un 70% de los bancos negocia

---

[42] Tolosa Borja, César y Giz Bueno, Álvaro, "Sistema Biométricos", *op. cit*., nota 9.
[43] Más información sobre el uso de los beneficios de la biometría en la banca se puede consultar en: *http://bbvaopen4u.com/es/actualidad/como-la-biometrica-y-la-geolocalizacion-pueden-beneficiar-la-banca-online.* Fecha de consulta: 20 de diciembre de 2015.
[44] "Fundamentos de Biometría", *Facultad de Ingeniería- Biometría Informática*, UNAM, s.f. Recuperado de:
http://redyseguridad.fi-p.unam.mx/Proyectos/biometria/
Fecha de consulta: 27 de abril de 2015.

proyectos para poner en marcha cajeros más seguros, con mejores medidas antifraudes como los sistemas biométricos.[45]

El principal objetivo del uso de la biometría en los bancos es reemplazar las contraseñas[46] para brindar mayor seguridad a las operaciones de los clientes. Su aplicación puede ayudar a disminuir los ataques de *skimming*[47] (clonación de tarjetas de crédito y débito) y de *surfing*[48](lectura del PIN mientras se teclea, bien mirando directamente o con cámaras de video).

La validación de la identidad de los clientes al momento de realizar pagos utilizando sistemas biométricos tiene las siguientes beneficios: se obtiene una mejor prueba de identidad, un mayor nivel de comodidad para el cliente y el ahorro de costes,[49] ya que las transacciones o procesos de autenticación biométricos son más rápidos y fidedignos en comparación con la verificación de identidad convencional que utilizan símbolos, como son los números de identificación personal (NIP), contraseñas, firmas, etcétera.

---

[45]Viterbo, Pedro, "Los bancos incrementan la seguridad con la biometría" en *Revista Dintel Alta Dirección*, recuperado de *http://www.revistadintel.es/Revista/Numeros/Numero1/Seguridad/Publica/Viterbo.pdf*

[46] Cornejo, Valentino T., "Detrás de la huella", *Revista Istmo Liderazgo con Valores,* edición 277, 2014. Recuperado de:
http://istmo.mx/2005/03/detras_de_la_huella/
Fecha de consulta: 23 de septiembre de 2014.

[47] Rivero, Mario y Gottschalk, Franz, "Los Ataques de Skimming en Cajeros Automáticos y Cómo Prevenirlos", *VISA*, 26 de febrero de 2014, p. 5.
Recuperado de: *http://usa.visa.com/download/merchants/Webinar-Preventing-ATM-Skimming-Spanish-021914.pdf*
Fecha de consulta 19 de abril de 2015.

[48] Espinosa Madrigal, Carmina Cecilia, "Robo de Identidad y Consecuencias Sociales", Documento de Trabajo, Coordinación de Seguridad de la Información, UNAM-CERT, 16 de junio de 2011.
Recuperado de: *http://www.seguridad.unam.mx/documento/?id=16*
Fecha de consulta 19 de abril de 2015.

[49]Véase Kelkboomc, Emile y *et. al*., "Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure", *Revista Electronic Commerce Research and Applications*, 2011, Países Bajos.
Recuperado de*: http://www.jeroenbreebaart.com/papers/ecra/ecra2011.pdf*
Fecha de consulta: 22 de enero de 2015.

Por lo anterior, en distintas partes del mundo se han instalado distintos sistemas biométricos para realizar pagos, por ejemplo, en 2005 Japón introdujo el reconocimiento de huellas dactilares y venas de la palma de la mano en una amplia gama de cajeros automáticos para aminorar los retiros de efectivo no autorizados; en Singapur, el Citibank lanzó un nuevo servicio de pago con huella digital para la autenticación de los clientes de tarjetas de crédito, instalado en nueve establecimientos comerciales tales como tiendas de música y de tecnología, clubes, restaurantes y cines;[50] en Estados Unidos, Apple Pay, el nuevo sistema de pagos móviles para el iPhone 6 y iPhone 6 Plus, permite realizar pagos poniendo la huella digital de sus usuarios en estos dispositivos celulares.[51]

Las economías emergentes también han aplicado la biometría en sus sistemas de pago, por ejemplo, en México Banco Azteca hasta 2007 había registrado las huellas de aproximadamente ocho millones de sus clientes para su autenticación en diversos dispositivos de pago. Algunos proyectos similares han sido desarrollados en la India, en el Medio Oriente, Brasil y otros lugares. A pesar de estos pequeños éxitos, la autenticación biométrica aún no ha sido adoptada a gran escala en las terminales puntos de venta (POS) ni en cajeros automáticos (ATM´s) debido a los

---

[50] *Idem.*
En el original se lee:
"A large amount of trials and fully operational systems have been installed for biometric payment. For example, Japan has introduced finger and palm vein recognition (Ogata, 2009) in a wide range of ATMs in 2005 to counter their substantial problem of unauthorized cash withdrawals (Jones, 2006). The USbased company Pay by Touch enabled customers to pay for goods with a swipe of their finger (Boyle, 2006; Williams, 2008). In Singapore, Citibank launched a new fingerprint authentication payment service for credit card customers, installed in 9 merchant locations such as music and IT stores, clubs, restaurants and cinemas (Tan, 2009). In The Netherlands, supermarket chain Albert Heijn together with payment processing company Equens initiated a trial for fingerprintbased payment authentication (van Hooren, 2009). Also in emerging economies, biometrics have found their way into payment systems", p. 1 Traducción libre.

[51] O'Toole, James, "¿Cómo funciona Apple Pay?", *CNN Expansión*, Estados Unidos, 20 de octubre de 2014.
Recuperado de: *http://www.cnnexpansion.com/tecnologia/2014/10/20/como-funciona-apple-pay*
Fecha de consulta 19 de abril de 2015.

desafíos que representan el tema de la protección de los datos biométricos y la privacidad de los titulares de las huellas.[52]

De acuerdo con Deloitte,[53] la tecnología biométrica ha encontrado una de sus mejores aplicaciones, como herramienta de inclusión financiera.

Un ejemplo de esto es MasterCard, quien ha sido empresa pionera en el uso de los medios biométricos para la banca en el mundo y ha ejecutado con algunos gobiernos sus diferentes usos, logrando que en algunos países dejaran de emitir cheques para el pago de ayudas sociales que resultaba muy caro y poco eficiente, almacenando los datos de los beneficiarios en un chip, la transacción era segura y que el dinero llegaría a la persona correcta.[54]

Mediante un "kit" o paquete integrado por una computadora móvil, un lector de huella digital, un codificador de tarjeta de débito, un micrófono para detectar huella de voz, una cámara y una impresora, MasterCard busca incrementar la afiliación mediante tarjetas de débito que también funcionan como identificación a los programas sociales.[55]

---

[52] Kelkboomc, Emile y *et. al*.,"Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure"… *op. cit*., nota 49.
Texto original:
The Mexico-based Banco Azteca registered the fingerprints of about 8 million customers in 2007 for payment authentication (Jones, 2007). Similar roll-out plans for financial applications have been revealed for the Indian subcontinent, the middle east, Brazil, and others (see International Biometric Group 2005, McIntosch 2009, for an overview). Despite these relatively small-scale successes, biometric authentication has not yet been adopted by large-scale point-of-sale (PoS) and automated teller machine (ATM) systems such as EMV (Europay, Mastercard, VISA (EMVCo) 2008). This could in part be the result of the major challenges that are associated with the adoption of biometrics, such as the proper protection of biometric data for security and privacy reasons" p. 1. Traducción libre.
[53] Zamora, Angélica, "Seguridad biométrica: La banca del futuro", *Revista Summa*, s/n, 7 de febrero de 2014. Recuperado de: *http://www.deloitte.com/view/es_HN/hn/prensa/deloitte-en-medios/bdb1700b56c14410VgnVCM3000003456f70aRCRD.htm*
Fecha de consulta: 23 de julio de 2014.
[54]*Idem.*
[55] Sánchez Onofre, Julio, "Banca fija su mirada en la tecnología biométrica", *El Economista*, 30 de septiembre de 2013.
Recuperado de: *http://eleconomista.com.mx/tecnociencia/2013/09/30/banca-fija-su-mirada-tecnologia-biometrica*

La autenticación de pagos mediante huellas digitales es una tendencia que está cambiando la forma en que compramos y también es una alternativa para aumentar la seguridad y evitar la clonación de tarjetas.[56]

Fecha de consulta: 26de julio de 2014.

[56] Martínez, Ana, "Pagos con huella digital revolucionan e-commerce", *El Financiero*, 15 de abril de 2014.
Recuperado de: *http://www.elfinanciero.com.mx/tech/pagos-con-huella-digital-revolucionan-e-commerce.html*
Fecha de consulta: 23 de abril de 2015.

CAPÍTULO IV

Recomendaciones para que las instituciones bancarias privadas que traten huellas dactilares de sus clientes no infrinjan la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

CAPÍTULO IV Recomendaciones para que las instituciones bancarias privadas que traten huellas dactilares de sus clientes no infrinjan la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

1. Antecedentes de la Protección de datos personales en México

Los primeros esbozos y aproximaciones al derecho a la protección de datos personales en México devienen del reconocimiento del derecho fundamental a la vida privada y familiar.[57]

En diversos convenios internacionales, especialmente los que versan sobre derechos humanos, se ha reconocido a los individuos el derecho a que su vida privada sea respetada y que solo terceros autorizados puedan tener acceso a la información de la persona que ésta misma esté dispuesta a consentir.

Algunos de los principales instrumentos internacionales que consideran el derecho a la privacidad son:

1. La Declaración Universal de los Derechos del Hombre, en el artículo 12 establece el derecho de la persona a no ser objeto de injerencias en su vida privada y familiar, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra tales injerencias o ataques.[58]

---

[57]Peschard Mariscal, Jaqueline, "El Derecho Fundamental a la Protección de Datos Personales en México", en Pinar Mañas, José Luis y Ornelas Núñez, Lina (coords.), *La Protección de Datos Personales en México*, México, Tirant Lo Blanch, 2013, p. 22

[58] La Declaración Universal de los Derechos del Hombre es un documento que sirve como antecedente histórico para el derecho a la privacidad y la protección de los datos personales, pero no es vinculante para el Estado mexicano, como lo señala la siguiente tesis de la SCJN:
Época: Décima Época, Registro: 2006533, Instancia: Primera Sala, Tipo de Tesis: Aislada, Fuente: Gaceta del Semanario Judicial de la Federación, Libro 6, Mayo de 2014, Tomo I, Materia(s): Constitucional, Tesis: 1a. CCXVI/2014 (10a.), Página: 539.
DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS. SUS DISPOSICIONES, INVOCADAS AISLADAMENTE, NO PUEDEN SERVIR DE PARÁMETRO PARA DETERMINAR LA VALIDEZ DE LAS NORMAS DEL ORDEN JURÍDICO MEXICANO, AL NO CONSTITUIR UN

2. El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, señala que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
3. La Convención Americana sobre derechos humanos, en su artículo 11 apartado 2 establece que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

TRATADO INTERNACIONAL CELEBRADO POR EL EJECUTIVO FEDERAL Y APROBADO POR EL SENADO DE LA REPÚBLICA.
La Primera Sala de la Suprema Corte de Justicia de la Nación, en la tesis 1a. CXCVI/2013 (10a.),1 sostuvo que de la interpretación sistemática del artículo 133 de la Constitución Política de los Estados Unidos Mexicanos, en relación con el numeral 4o. de la Ley sobre la Celebración de Tratados, se advierte que son de observancia obligatoria para todas las autoridades del país los derechos humanos reconocidos tanto en la Constitución como en los tratados internacionales, suscritos y ratificados por nuestro país, al ser normas de la unidad del Estado Federal. De ahí que, no obstante la importancia histórica y política de la Declaración Universal de los Derechos Humanos, aprobada y proclamada por la Asamblea General de la Organización de las Naciones Unidas en su Resolución 217 A (III), de 10 de diciembre de 1948, y de que sus principios han sido fuente de inspiración e incorporados a tratados universales y regionales para la protección de los derechos humanos, se concluye que sus disposiciones, invocadas aisladamente, no pueden servir de parámetro para determinar la validez de las normas del orden jurídico mexicano, al no constituir un tratado internacional celebrado por el Ejecutivo Federal y aprobado por el Senado de la República en términos de los artículos 89, fracción X, y 76, fracción I, de la Constitución Federal; lo anterior, sin perjuicio de que una norma internacional de derechos humanos vinculante para el Estado Mexicano pueda ser interpretada a la luz de los principios de la Declaración Universal de los Derechos Humanos, esto es, los principios consagrados en ésta pueden ser invocados por los tribunales para interpretar los derechos humanos reconocidos en los tratados internacionales incorporados a nuestro sistema jurídico.
Amparo directo en revisión 4102/2013. BQM Laboratorios, S.A. de C.V. 2 de abril de 2014. Cinco votos de los Ministros Arturo Zaldívar Lelo de Larrea, José Ramón Cossío Díaz, Alfredo Gutiérrez Ortiz Mena, Olga Sánchez Cordero de García Villegas y Jorge Mario Pardo Rebolledo. Ponente: Olga Sánchez Cordero de García Villegas. Secretario: Ricardo Manuel Martínez Estrada.
La tesis aislada 1a. CXCVI/2013 (10a.) citada, aparece publicada en el Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro XXI, Tomo 1, junio de 2013, página 602, con el rubro: "DERECHOS HUMANOS. LOS TRATADOS INTERNACIONALES VINCULADOS CON ÉSTOS SON DE OBSERVANCIA OBLIGATORIA PARA TODAS LAS AUTORIDADES DEL PAÍS, PREVIAMENTE A LA REFORMA CONSTITUCIONAL PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 10 DE JUNIO DE 2011."
Esta tesis se publicó el viernes 30 de mayo de 2014 a las 10:40 horas en el Semanario Judicial de la Federación.

En atención a los instrumentos anteriores y en virtud de la adhesión de nuestro país a los dos últimos dos[59], México contrajo la obligación de proteger el derecho a la privacidad en su territorio.

Sin embargo, a pesar de que en México la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada el 11 de julio de 2002 en el Diario Oficial de la Federación, ya preveía regulación en materia de datos personales, solo regulabala protección de los datos personales en posesión de órganos y entidades públicas federales.

Por lo anterior, fue necesario reformar la Constitución Política de los Estados Unidos Mexicanos para reconocer el derecho a la protección de datos personales como un nuevo derecho fundamental que dotara al titular de los datos personales de una serie de facultades necesarias enfocadas a disponer y controlar el uso que se le da a la misma ante entes privados, también conocido como el derecho a la "autodeterminación informativa".[60]

Así, el 1 de junio de 2009 fue publicada la reforma del artículo 16 constitucional en la cual se agregó un segundo párrafo a este artículo para establecer lo siguiente:

> "Artículo 16. ….
>
> …toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de

---

[59]Fechas adhesión de México: al Pacto Internacional de Derechos Civiles y Políticos, México se adhirió el 24 de marzo de 1981, y a la Convención Americana sobre derechos humanos, el 24 de marzo de 1981, consultables en:
http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D47.pdf
http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D1BIS.pdf
Fecha de consulta: 04 de mayo de 2016.

[60] Peschard Mariscal, Jaqueline, "El Derecho Fundamental a la Protección de Datos Personales en México", en Pinar Mañas, José Luis y Ornelas Núñez, Lina (coords.), *La Protección de Datos Personales en México*, México, Tirant Lo Blanch, 2013, p. 23.

excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".

Lo anterior, se traduce en la actualidad en que el titular de los datos cuenta con facultades para dar o no su consentimiento para el tratamiento de sus datos, para conocer que su información personal está siendo tratada y los propósitos o motivos de dicho tratamiento, o bien, para acceder, rectificar o cancelar los datos en un momento posterior.[61]

De igual forma fue reformado el artículo 73 constitucional el 30 de abril de 2009, dotando de facultades al Congreso Federal para legislar en materia de protección de datos personales en posesión de los particulares.

2. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

La aprobación de las reformas constitucionales mencionadas dieron las bases necesarias para la emisión de una ley que regulara el tratamiento de datos personales en posesión del *sector privado:* la LFPDPP, publicada en el DOF el 5 de julio de 2010.

Posteriormente, en atención a que el artículo 2 transitorio de la LFPDPP señalaba que el Ejecutivo Federal expediría el reglamento de esta Ley, el 21 de diciembre de 2011fue publicado en el DOF el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en lo sucesivo "Reglamento a la Ley", el cual entró en vigor al día siguiente de su publicación.

---

[61]Peschard Mariscal, Jaqueline, "El Derecho Fundamental a la Protección de Datos Personales en México", en Pinar Mañas, José Luis y Ornelas Núñez, Lina (coords.), *La Protección de Datos Personales en México*, México, Tirant Lo Blanch, 2013, p. 23

La LFPDPPP tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular el tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas, siendo de observancia obligatoria en toda la República Mexicana.[62]

De acuerdo con la LFPDPPP, los sujetos regulados por la misma son todas aquellas personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables,[63] y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

A dichos sujetos obligados la LPDPPP los denomina “responsables” del tratamiento de los datos, y a la persona física a quien corresponden los datos personales como “titular” de los datos.

Por otra parte, la LFPDPPP establece dos figuras más para las personas que tienen contacto con datos personales, las cuales son definidas por la ley como sigue:[64]

---

[62]Véase Ornelas Núnez, Lina, “Características del modelo de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento”, en Pinar Mañas, José Luis y Ornelas Núnez, Lina (coords.), *ídem*, p. 117.

[63] Los supuestos en los que no es aplicable la LFPDPPP a las Sociedades de Información Crediticia son aquellas actividades señaladas en la Ley para Regular las Sociedades de Información Crediticia, es decir, cuando éstas prestan los servicios de recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales, así como de operaciones crediticias y otras de naturaleza análoga que dichas personas mantengan con Entidades Financieras, Empresas Comerciales o las Sofomes E.N.R., (artículo 5º de la Ley para Regular las Sociedades de Información Crediticia), pues dicha ley contiene obligaciones y regulación especial en materia de protección de datos personales para dichas sociedades.

[64] Artículo 3º de la LFPDPPP, fracciones IX y XVI respectivamente.

“Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable”.

“Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos”.

Asimismo, la ley establece que por “tratamiento” se deberá entender a éste como “la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales”.

Por lo anterior, la LFPDPPP resulta aplicable a la materia del presente trabajo de investigación en virtud de que:

1. Los datos biométricos son datos personales de acuerdo con la definición del artículo 3, fracción V de la LFPDPPP, pues como se menciona en capítulos anteriores, los datos biométricos no cambian con el tiempo y son únicos para cada persona permitiendo la identificación de los titulares de los mismos y resultan ser datos que recabarán las instituciones financieras.
2. Las entidades financieras tratarán las huellas dactilares (datos biométricos) de sus clientes en virtud de la obtención, uso y almacenamiento que harán de las huellas que corroborarán con el sistema de captación de huellas que está en poder del INE.

Así la LFPDPP es aplicable a este tipo de instituciones y es importante señalar que derivado de lo anterior surgen diversas obligaciones para los responsables del tratamiento de datos personales en dichas instituciones, teniendo como principales obligaciones la observancia de los principios establecidos en la ley en el tratamiento de los datos y el respeto a los derechos de acceso, rectificación, oposición y cancelación de los datos, así como el deber de seguridad y confidencialidad de los datos.

Ahora bien, considerando que el “Proyecto” de identificación de los clientes bancarios por medio de sus huellas dactilares resulta un tratamiento de datos personales llevado a cabo por las instituciones Bancarias y a quienes les es aplicable la LFPDPPP, a continuación se emiten las siguientes recomendaciones para el cumplimiento de las obligaciones que les impone la LFPDPPP al caso en concreto:

3. Principios de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

El derecho a la protección de los datos personales se regula a través de ocho principios, los cuales se traducen en obligaciones concretas para los responsables del tratamiento. Estos principios son: licitud, lealtad, consentimiento, información, proporcionalidad, finalidad, calidad y responsabilidad, como se muestra en la siguiente figura.[65]

[65] Artículo 6º de la LFPDPPP: “Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.”

Ilustración 4. Principios de la LFPDPPP

Imagen tomada de la "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"[66].

De acuerdo con el artículo 6 de la LFPDPPP, los responsables en el tratamiento de datos personales deberán observar los principios anteriores; en caso contrario, la ley establece una sanción por concepto de multa que considera de 100 a 160 días de salario mínimo vigente en el Distrito Federal[67] aplicable a los responsables que incumplan con los mismos.

---

[66]Instituto Federal de Acceso a la Información y Protección de Datos, 2014, consultable *http://inicio.inai.org.mx/SitePages/ifai.aspx*, fecha de consulta: 17 de octubre de 2015.

[67] La LFPDPPP señala:

Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:

…

IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;

Artículo 64.- Las infracciones a la presente Ley serán sancionadas por el Instituto con:

…

II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior…

En atención a lo anterior, a continuación se explican brevemente cada uno de los principios y se emiten las recomendaciones específicas al Proyecto para su cumplimiento.

3.1 Licitud

De acuerdo con la LFPDPPP y el Reglamento a la Ley, el principio de licitud obliga al responsable del tratamiento a que:

a) Los datos personales sean recabados y tratados de manera lícita conforme a las disposiciones establecidas en la LFPDPPP y demás normativa aplicable (artículo 6 de la LFPDPPP).[68]

b) El tratamiento de los datos personales sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional (artículo 11 del Reglamento a la Ley).[69]

Al respecto, el Convenio de apoyo y colaboración para instituciones privadas que celebrará con INE (**Anexo 3**), señala en su cláusula sexta lo siguiente:

"SEXTA.- Las obligaciones de ambas partes son las siguientes:

[...]

d) Proteger los datos personales de los ciudadanos conforme a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, el Código Federal de Instituciones y Procedimientos Electorales, el Reglamento del Instituto Federal Electoral en Materia de

---

[68]**Artículo 7.- Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.**
[...]
[Énfasis añadido]

[69]**Principio de licitud**
Artículo 10.El principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.

Transparencia y Acceso a la Información Pública y los Lineamientos para Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores en el ámbito de competencia de cada una de estas instituciones."

Si bien la cláusula anterior considera a la LFPDPPP como una norma aplicable, no hace mención al Reglamento a la Ley ni otras disposiciones en materia de datos personales que le pudieran ser aplicables al caso en concreto, por lo que se sugiere que esta cláusula sea modificada para quedar de la siguiente forma:

"d) Proteger los datos personales de los ciudadanos conforme a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, ***su Reglamento,*** *el Código Federal de Instituciones y Procedimientos Electorales, el Reglamento del Instituto Federal Electoral en Materia de Transparencia y Acceso a la Información Pública y los Lineamientos para Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores* ***y la demás normativa aplicable tanto para el sector público como privado en materia de datos personales*** *en el ámbito de competencia de cada una de estas instituciones."*

Además de la modificación de la cláusula anterior, ¿cómo pueden las instituciones financieras cumplir con el principio de licitud?

En el caso del Proyecto se recomienda realizar las siguientes acciones:

1. Revisar que los datos se traten conforme a la LFPDPPP, su Reglamento y demás normativa aplicable (la forma del cumplimiento señala en este capítulo).
2. Determinar la normativa del sector bancario y comercial como se indica en los siguientes apartados que adicionalmente regula el tratamiento de datos personales realizado por instituciones bancarias (se señala más adelante en el capítulo 5).
3. Incluir cláusulas contractuales de datos personales en los contratos u otros instrumentos jurídicos que las instituciones financieras firmen con terceros las cuales prevean la obligación de los terceros de cumplir con este principio, especialmente en los siguientes contratos:

- Si es el caso, en los contratos de prestación de servicios que la institución financiera celebrara con terceros para la contratación de servicios de administración de las bases de datos o del sistema de verificación de huella, o algún servicio similar, y
- En los contratos laborales o en las cartas de confidencialidad que celebre la institución financiera con sus empleados que tuvieran acceso a la base de datos de las huellas dactilares o fueran a intervenir en cualquier proceso del sistema de verificación.

3.2 Legalidad

De acuerdo con el artículo 7 de la LFPDPPP y 44 del Reglamento a la Ley, este principio consisten en que el responsable deberá recabar y tratar los datos personales sin utilizar medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.[70]

Lo anterior implica que el responsable deberá:[71]

---

[70] La LFPDPPP señala:
Artículo 7.- Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.
La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.
En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley.

Por su parte el Reglamento a la LFPDPPP señala:

Artículo 44.- El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, en los términos establecidos en el artículo 7 de la Ley.
No se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales. Existe una actuación fraudulenta o engañosa cuando:
I. Exista dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento;
II. Se vulnere la expectativa razonable de privacidad del titular a la que refiere el artículo 7 de la Ley, o
III. Las finalidades no son las informadas en el Aviso de Privacidad.

[71] "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares", Instituto Federal de Acceso a la Información y Protección de Datos, 2014. Recuperado de: *http://inicio.inai.org.mx/SitePages/ifai.aspx*
Fecha de consulta: 12 de marzo de 2016.

- No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales, y
- Respetar en todo momento la expectativa razonable de privacidad del titular.

Para que la institución financiera cumpla con ello, se recomienda realizar las siguientes acciones:

1. Las Instituciones Financieras que implementen el "Proyecto" deberán adecuar sus avisos de privacidad para prever en estos el tratamiento de las huellas dactilares de los clientes, especialmente la recolección y el uso de éstas (incluyendo el número de huellas a recabar), así como las finalidades de dicho tratamiento.

Para el caso en particular de Bancomer, el Aviso de Privacidad actual[72] de esta institución, el cual se agrega al presente estudio como **Anexo 4**, no prevé el tratamiento de las huellas dactilares como se indica en el apartado del principio de finalidad.

2. Capacitar a los empleados que recabarán las huellas dactilares para que dicha recolección sea llevada a cabo en cumplimiento de la LFPDPPP, así como a la persona o Departamento de Datos Personales designados en términos del artículo 30 de la LFPDPP para que atiendan las solicitudes de ejercicio de derechos ARCO de los titulares respecto de las huellas dactilares recabadas en los términos que se señalan más adelante.
3. Este tratamiento de las huellas dactilares de los clientes deberá preverse en los contratos de productos y servicios bancarios, en los cuales se deberá expresar claramente la finalidad de dicho tratamiento (identificación de los titulares), así como las consecuencias de la cancelación u oposición del

[72] Fecha de consulta del Aviso de Privacidad de Bancomer: 21 de diciembre de 2015, en la página www.bancomer.com.

tratamiento por parte del titular del dato. Para tales efectos ver el apartado de consentimiento.

4. Establecer auditorías internas periódicas para vigilar el cumplimiento de las obligaciones señaladas en este documento, así como crear sanciones al personal que no cumpla con dichas obligaciones.
5. Para el cumplimiento de la expectativa razonable de privacidad del titular, la institución financiera deberá tratar los datos conforme lo acordado e informado al titular, en los términos de la normatividad aplicable y el Aviso de Privacidad.

3.3. Consentimiento

El principio de consentimiento se encuentra establecido en el artículo 8 de la LFPDPPP en el cual se establece la obligación del responsable de recabar el consentimiento del titular de los datos personales para el tratamiento de los mismos, salvo las excepciones previstas en la LFPDPPP.[73]

De lo anterior se colige que el responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales. La solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el Aviso de Privacidad, es decir, el consentimiento

[73] El artículo 8 de la LFPDPPP señala lo siguiente:
"Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.
El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.
Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el Aviso de Privacidad, no manifieste su oposición.
Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley.
El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el Aviso de Privacidad, establecer los mecanismos y procedimientos para ello".

se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.[74]

Respecto a lo que se debe entender por consentimiento en materia de datos personales, el artículo 3, fracción IV de la LFPDPPP señala que aquél es "la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos".

Establecido lo anterior, a continuación se desglosan las obligaciones que la institución financiera deberá observar para el cumplimiento de este principio:

3.3.1 Obtención del consentimiento

Como ya mencionó, los artículos 10 y 37 de la LFPDPPP señalan los casos en los que el responsable estará exceptuado de recabar el consentimiento de los titulares de los datos para su tratamiento.

Bajo ese tenor, el artículo 10, fracción IV de la LFPDPPP señala que el responsable estará exceptuado de obtener el consentimiento del titular para el tratamiento cuando éste: "tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable".

Para que dicha excepción sea aplicable al "Proyecto", los contratos bancarios de adhesión motivo por el cual se van a tratar las huellas dactilares deberán contener, previamente a la recolección o cualquier otro tratamiento de las huellas, una cláusula que indique que el cliente acepta el uso y la recolección de sus huellas para verificar su identidad como condición o requisito para la celebración de operaciones bancarias directamente en la sucursal sobre sus cuentas.

[74]"Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"... *op. cit*. nota 71.

No obstante lo anterior, para la emisión del dictamen del INAI respecto al "Servicio de Verificación", el INE presentó al INAI el modelo de convenio de colaboración que pretendía firmaría con las instituciones privadas con las que opere el Servicio de Verificación, el cual contiene la siguiente cláusula:[75]

> "QUINTA.- Las obligaciones de"_____",[76] son las siguientes:
>
> […]
>
> e) Establecer en los avisos de privacidad que se elaboren de conformidad con la Ley de Protección de Datos Personales en Posesión de los Particulares, la posibilidad de verificación de los datos personales contenidos en la credencial para votar que los ciudadanos proporcionen a"_____".
>
> f) El Aviso de Privacidad, deberá contener un campo en el que se indique si el titular acepta o no, el tratamiento de sus datos personales para el Servicio de Verificación de datos de la Credencial para Votar. Dicho Aviso de Privacidad deber ser complementado con un campo de conformación del consentimiento de titular de los datos en el que expresamente acepte el cotejo de los datos que presenta con los del Servicio de Verificación de datos de la Credencial para Votar.[…]"

Al respecto, el INAI emitió las siguientes recomendaciones:

> "Verificar que, efectivamente, las instituciones privadas a las que se presta el Servicio de Verificación informen en su Aviso de Privacidad sobre esta finalidad del tratamiento de los datos personales…".[77]

---

[75] Anexo Único, p.28.
[76] Los espacios en blanco en esta cláusula se refieren a la institución privada que opere el Servicio de Verificación con el INE.
[77] Resumen Ejecutivo, p. 11.

> “Prever explícitamente en los convenios de apoyo y colaboración para instituciones privadas, la obligación del INE y de la institución, de generar evidencia que permita acreditar transferencias de datos personales de la institución al INE, en cumplimiento a las obligaciones que prevé la LFPDPPP para las transferencias, incluyendo: i) si dichas transferencias son informadas por la institución a los titulares; ii) si el tratamiento de los datos personales para el Servicio de Verificación fue consentido y, en ese sentido, la transferencia de datos personales de la institución al INE, y ii) la entrega de los avisos de privacidad de las instituciones privadas al INE”.[78] (Énfasis añadido).

Por lo anterior, la recomendación para la obtención del consentimiento de las personas clientes de las instituciones financieras, a fin de recabar las huellas dactilares para su tratamiento, debe realizarse previo a su recolección, no obstante de que la obtención del consentimiento está exceptuado para el “Proyecto” como se explicó en párrafos anteriores.

3.3.2 *Tipo de consentimiento*

El artículo 8 de la ley señala que el consentimiento para el tratamiento de los datos personales podrá ser otorgado por sus titulares de forma tácita o expresa.

El consentimiento tácito para el tratamiento de los datos se entenderá que ha sido otorgado por el titular de los datos cuando habiéndose puesto a disposición éste el Aviso de Privacidad respectivo, no manifiesta su oposición al tratamiento de sus datos.

El consentimiento expreso será, de acuerdo con la propia LFPDPP, cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o

[78] *Ibidem*, p. 16.

por cualquier otra tecnología, o por signos inequívocos y será necesario otorgarlo de esta forma cuando el responsable pretender tratar los siguientes tipos de datos:

1. En los casos en que lo exija una ley o reglamento
2. Datos Financieros
3. Datos Patrimoniales
4. En los casos en que los solicite el responsable para acreditar el mismo
5. Lo acuerden así el titular y el responsable

Para el caso que nos ocupa, es importante hacer mención que la Cámara de Diputados en 2013 aprobó por unanimidad la propuesta de reforma al artículo 3º de la LFPDPPP para integrar en la definición de datos sensibles a los datos de identificación biométrica.79

En la exposición de motivos, los diputados señalaron que en virtud de la evolución tecnológica, las empresas están solicitando con mayor frecuencia los datos biométricos de sus usuarios, los cuales no han sido incluidos en el marco jurídico vigente.

Debido a que actualmente en el Congreso de la Unión se encuentra en análisis la propuesta de "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados" emitida por el INAI, y dado el antecedente del párrafo anterior (la intención de los legisladores de considerar a los datos de identificación biométrica como datos sensibles), se recomienda que el consentimiento de los clientes se recabe por escrito y con firma del titular de los datos, como a continuación se especifica:

---

[79]Proyecto de Decreto presentado por los diputados Arely Madrid Tovilla y Manuel Añorve Baños, turnado a la Cámara de Senadores que puede ser consultado en la Gaceta Parlamentaria, en el número 3890-IV, martes 22 de octubre de 2013 en la página *http://gaceta.diputados.gob.mx/Gaceta/62/2013/oct/20131022-IV.html*
Fecha de última consulta 8 de julio de 2015.

- Mediante la firma del Aviso de Privacidad que contenga la información necesaria para el tratamiento de las huellas, de acuerdo a lo señalado en el principio de información que más adelante se detalla, y con antelación a la recolección de las huellas dactilares del cliente.

Lo anterior tomando en consideración que actualmente no existe certeza de las reformas que en la materia serán aprobadas en la nueva "Ley General de Protección de Datos Personales", que posteriormente puedan ser tomadas en consideración para la actualización de la LFPDPPP; por ende, de manera preventiva, y para dar cumplimiento de lo establecido en los artículos 9 de la LFPDPPP y 17 del Reglamento a la Ley que establecen que el responsable deberá recabar el consentimiento del titular de manera expresa y por escrito tratándose de datos sensibles, y el artículo 20 del mismo Reglamento que señala que la carga de la prueba del consentimiento recae en todos los casos en el responsable del tratamiento, es que se recomienda la obtención del consentimiento por escrito.

Con lo anterior, también se daría cumplimiento al artículo 31 del Reglamento a la Ley que señala que para "demostrar la puesta a disposición del Aviso de Privacidad en cumplimiento al principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable".

3.3.3 *Negación del servicio bancario derivada de la negativa del cliente para el tratamiento de sus huellas dactilares*

En caso de que el cliente no quisiera firmar el Aviso de Privacidad, ni permitiera la recolección de sus huellas dactilares, o posteriormente, manifestara su oposición para el tratamiento de estos datos, siempre que el contrato bancario aplicable estipule la obligación del cliente de permitir la recolección de sus huellas y consentir el tratamiento como condición para la prestación de los servicios bancarios contratados en las sucursales de la institución financiera, ésta última podrá negar la prestación de dichos servicios por virtud del artículo 1949 del Código Civil Federal que establece que "la facultad de resolver las obligaciones se entiende implícita en

las recíprocas, para el caso de que uno de los obligados no cumpliere lo que le incumbe".

Lo anterior, quiere decir que si el cliente ha firmado el contrato de prestación de servicios bancarios con la cláusula que lo obliga a consentir el tratamiento de sus huellas dactilares para la prestación de esos mismos servicios y no cumpliera con esta obligación, la institución financiera no estaría obligada a prestar los servicios contratados, salvo que exista un caso fortuito o de fuerza mayor que no le permitiera al cliente cumplir con dicha obligación (como la falta de uno sus los dedos, la imposibilidad del sistema de escanear sus huellas por desgaste de éstas, etcétera).

Respecto a los contratos bancarios comentados es importante establecer que existen dos tipos de personas: los clientes (personas que ya cuentan con un producto o servicio contratado con la institución financiera) y los no clientes o usuarios (personas que se presentan a la sucursal por primera vez a contratar un producto o servicio).

Para que la obligación del consentimiento del tratamiento de las huellas sea vinculante para ambos tipos de personas, se recomienda que la institución financiera realice lo siguiente:

- Para el caso de los no clientes, ésta deberá proporcionar al cliente el contrato que corresponda, el cual contenga en ese momento la cláusula de consentimiento del tratamiento de las huellas como condición para la prestación de los servicios bancarios en sucursal.
- Para las personas que a la fecha de implementación del "Proyecto" ya sean clientes de algún producto o servicio con la institución, ésta deberá modificar los contratos respectivos a efecto de incluir la condición mencionada, registrar el cambio en el Registro de Contratos de Adhesión de CONDUSEF y dar aviso de este cambio a los clientes con 30 días naturales de anticipación a la fecha en que pretendan iniciar la operación del Servicio de Verificación con los clientes de acuerdo con los artículos 2 y 17 de las Disposiciones de carácter general en

materia de transparencia aplicables a las instituciones de crédito y sociedades financieras de objeto múltiple, entidades reguladas.[80]

---

[80]DISPOSICIONES DE CARÁCTER GENERAL EN MATERIA DE TRANSPARENCIA APLICABLES A LAS INSTITUCIONES DE CRÉDITO Y SOCIEDADES FINANCIERAS DE OBJETO MÚLTIPLE, ENTIDADES REGULADAS.
CAPÍTULO I. DISPOSICIONES COMUNES
Artículo 2. Para los efectos de las presentes Disposiciones, en singular o plural, se entiende por:
…
V. Contrato de Adhesión: Al documento elaborado unilateralmente por las Instituciones Financieras para establecer en formatos uniformes los términos y condiciones aplicables a la celebración de una o más operaciones pasivas, activas o de servicios que lleven a cabo con los Usuarios, en el entendido de que estos últimos no podrán negociar dichos términos y condiciones;
CAPÍTULO II. DE LOS CONTRATOS DE ADHESIÓN

SECCIÓN I. DISPOSICIONES COMUNES
Artículo 3. Se consideran operaciones masivas y, por tanto, serán las únicas sujetas a lo previsto en este Capítulo, las que se realizan mediante los siguientes tipos de Contratos de Adhesión que documenten operaciones que no excedan de novecientas mil UDI, al momento de celebrar el contrato:

I. Las aperturas de créditos en cuenta corriente, denominadas en moneda nacional, otorgadas a personas físicas o morales vinculadas o no a tarjetas de crédito o a cualquier otro Medio de Disposición que permita ejercer el crédito;
II. Las líneas de crédito que se otorguen de manera sucesiva o en serie y utilicen alguna tarjeta plástica u otro Medio de Disposición como medio de identificación de los Usuarios, o bien, para la disposición de los recursos;
III. Los créditos garantizados a la vivienda;
IV. Las aperturas de Créditos al Consumo;
V. El arrendamiento financiero con opción terminal de compra;
VI. Los depósitos de dinero a la vista, tanto de personas físicas como morales con o sin chequera, con o sin tarjeta de débito;
VII. Las operaciones pasivas distintas a las previstas en la fracción anterior, a las cuales les es aplicable la GAT nominal y real;
VIII. El crédito de habilitación o avío;
IX. El crédito refaccionario;
X. El crédito simple a personas morales;
XI. Las operaciones de factoraje financiero, y
XII. Las operaciones de banca electrónica.

Artículo 17. Para modificar los Contratos de Adhesión, las Instituciones Financieras deben dar aviso a los Usuarios, con treinta días naturales de anticipación, a través del estado de cuenta o de cualquier medio cierto pactado en dichos contratos. En el caso de que exista más de un producto o servicio ofertado en conjunto en beneficio del Usuario relacionado entre sí, deben notificar de todos los cambios que sufran los productos o servicios pertenecientes al mismo.

Tratándose de modificaciones a los Contratos de Adhesión relativos a Créditos Garantizados a la Vivienda y créditos con plazo fijo de vencimiento, las Instituciones Financieras deben contar con el consentimiento expreso del Usuario y formalizarlas conforme a las disposiciones legales aplicables.

Es importante señalar que con la implementación del esquema anterior, la institución de crédito no le está negando al cliente totalmente el acceso a los recursos de sus cuentas, pues el cliente conservaría la opción de realizar operaciones por otros medios, por ejemplo, mediante el uso de cajeros automáticos, el uso de tarjetas bancarias en terminales punto de venta o por medio de la banca electrónica.

3.4. Información

El principio de información, según explica el Dictamen de la LFPDPPP, se concreta en un derecho para el titular de los datos personales, en cuanto a que a través del Aviso de Privacidad el responsable le informa de los términos a los que se sujeta el tratamiento de sus datos personales y, en su caso, recaba el consentimiento necesario. Por tanto, es también una obligación del responsable.[81]

Dicho principio se encuentra regulado en el artículo 15 de la LFPDPPP que señala que "el responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del Aviso de Privacidad", señalando la propia ley en su artículo 16 los elementos mínimos que deberá contener el aviso.[82]

En cuanto a la puesta a disposición del titular del aviso, la LFPDPPP señala que:

---

[81] Ornelas Núñez, Lina, "Los principios de la protección de datos personales", en Pinar Mañas, José Luis y Ornelas Núnez, Lina (coords.), *La Protección de Datos Personales en México,* México, Tirant Lo Blanch, 2013, p. 72.

[82] Artículo 16.- El Aviso de Privacidad deberá contener, al menos, la siguiente información:
I. La identidad y domicilio del responsable que los recaba;
II. Las finalidades del tratamiento de datos;
III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
V. En su caso, las transferencias de datos que se efectúen, y
VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al Aviso de Privacidad, de conformidad con lo previsto en esta Ley.
En el caso de datos personales sensibles, el Aviso de Privacidad deberá señalar expresamente que se trata de este tipo de datos.

Si los datos fueron obtenidos directamente de su titular:	
1. De manera personal	El aviso se deberá poner a disposición del titular: En el momento en que se recaben los datos, salvo que el responsable lo hubiera facilitado con anterioridad (art. 17, fracción I de la LFPDPPP).
2. Por cualquier medio electrónico	El aviso se deberá poner a disposición del titular: De manera inmediata al menos con la identidad del responsable y los mecanismos para que el titular conozca el Aviso de Privacidad.
Si los datos fueron obtenidos indirectamente del titular:	
Y los datos serán: -Tratados para una finalidad prevista en la transferencia consentida, u -Obtenidos de una fuente de acceso público.	El aviso se deberá poner a disposición del titular: En el primer contacto que se tenga con el titular.
Y el responsable pretenda utilizar los datos personales para una finalidad distinta a la consentida, es decir, tenga lugar un cambio de la finalidad.	El aviso se deberá poner a disposición del titular: Previo al aprovechamiento de los datos personales (art. 29, fracción II del Reglamento):

Fuente: Elaboración propia con datos obtenidos de la "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares", Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, México, 2014, *op. cit.* 72.

No obstante que la obtención del consentimiento del cliente para el tratamiento de las huellas dactilares en el "Proyecto" podría recabarse en un medio distinto al Aviso de Privacidad, es obligación del responsable poner a disposición de los titulares de los datos el Aviso de Privacidad.

Respecto a lo anterior, el "Anexo Único" emitido por el INAI señala que el INE deberá observar la siguiente obligación: "*Verificar que, efectivamente, las instituciones privadas a las que preste el Servicio de Verificación informen en su*

Aviso de Privacidad sobre esta finalidad del tratamiento de los datos personales…".[83] (Énfasis añadido).

Asimismo, respecto a las transferencias de las huellas que tendrán lugar de la institución financiera al INE, en el "Anexo Único" el INAI realizó la siguiente recomendación:

> "*Prever explícitamente en los convenios de apoyo y colaboración para instituciones privadas que la institución incluya en su Aviso de Privacidad la transferencia de datos personales que realiza al INE en el marco del Servicio de Verificación*, de conformidad con lo previsto en el artículo 16, fracción V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares."[84] (Énfasis añadido).

En el caso específico de Bancomer, el actual Aviso de Privacidad de la institución no cuenta con la información necesaria para el cumplimiento del principio de información con relación al "Proyecto"[85], en tal virtud, dicho aviso deberá ser modificado *previo a la implementación del*"*Proyecto*" a efecto de prever la siguiente información faltante:

a) Que las huellas dactilares serán sometidas a tratamiento por parte de la institución financiera.
b) Las finalidades del tratamiento de las huellas dactilares.
c) Que las finalidades del tratamiento de las huellas dactilares son finalidades necesarias y que dan origen a la relación jurídica entre el cliente y la institución financiera.

No es óbice recalcar que dicha modificación deberá realizarse en términos sencillos, con la información necesaria, en lenguaje claro y comprensible, y con una

---

[83] Resumen Ejecutivo**,** p. 11.
[84] *Ibidem*, p. 16.
[85] Véase Anexo 4.

estructura y diseño que facilite su entendimiento para dar cumplimiento al artículo 24 del Reglamento a la Ley.

Para el caso de Bancomer, se recomienda la inserción de la propuesta de texto en el Aviso de Privacidad actual de Bancomer que se adjunta al presente trabajo como **Anexo 5**.

3.5. Calidad

Los artículos 11 de la LFPDPPP y 36 del Reglamento a la Ley señalan que el responsable debe adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las siguientes características:[86]

- **Exactos:** Los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles. Por ejemplo, un tarjetahabiente o cliente bancario cuenta con un saldo en su tarjeta de crédito por "x" cantidad y en los estados de cuenta aparecen otro saldo que no corresponde a los movimientos realizados por el cliente.
- **Completos:** Los datos personales están completos cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular. Por ejemplo, cuando un cliente de la banca designa beneficiarios de sus cuentas para el caso de su fallecimiento, dicha designación deberá constar en el expediente del cliente en el banco.
- **Pertinentes:** Los datos personales son pertinentes cuando corresponden efectivamente al titular. Por ejemplo, los datos del adeudo son pertinentes cuando corresponden al deudor y no a una homonimia.
- **Actualizados:** Los datos están actualizados cuando están al día y corresponden a la situación real del titular. Por ejemplo, el número telefónico

[86]"Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"... *op. cit*. nota 71, pp. 58 y 59.

que se tiene registrado en la base de datos está actualizado cuando, efectivamente, corresponde al titular con el que está vinculado.

- **Correctos:** Los datos personales son correctos cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados.

Lo anterior, tienen como objeto que no sea alterada la veracidad de la información y que el titular se vea afectado por dicha situación.

Debido a que el titular de los datos es quien proporcionará las huellas dactilares, la institución financiera contaría con la presunción legal de que los datos cumplen con las características señaladas, en tanto el titular del dato no manifieste y acredite lo contrario, o bien el responsable cuente con evidencia de lo contrario (artículo 36 del Reglamento a la Ley).

Por lo antes dicho, para el cumplimiento de este principio, las imágenes de las huellas dactilares deberán ser capturadas por la institución financiera de manera fiel a su original y que éstas deberán ser asociadas a su titular, ya de la correcta captura y asociación dependerá que el cliente pueda ser identificado cada vez que acuda a una sucursal bancaria, y que por el contrario, no sea identificado como si fuera otro cliente por una mala asociación de las huellas (falso positivo), o que no se le pueda identificar como el titular de sus propias cuentas, o incluso, como ningún cliente del banco (falso negativo) y por ende no se le permita realizar operaciones en la sucursal.

Finalmente para mantener actualizados las huellas dactilares de los clientes se recomienda:

- Realizar revisiones periódicas de la base de datos de huellas dactilares para verificar que los datos estén actualizados (altas, bajas y rectificaciones).

- Adoptar las medidas técnicas necesarias para garantizar que se rectifiquen los datos personales que fueran inexactos de oficio, así como cancelar aquellos que por derecho corresponda en apego a los plazos y la forma se señalan en el apartado de los derechos de rectificación y cancelación, respectivamente.
- Adicionalmente, el sistema biométrico deberá ser diseñado de manera que permita la rectificación del dato en caso de que éste se haya capturado o asociado de manera incorrecta, y que genere la evidencia correspondiente de la actualización o rectificación y cancelación de los datos cuando tengan lugar dichas acciones.

Sobre este punto se ahondará más adelante en el apartado delos derechos de rectificación y cancelación.

- Asimismo, en caso de que la institución contrate los servicios de un encargado para el tratamiento de las huellas, se deberá informar a los encargados sobre las correcciones o actualizaciones de estos datos que tengan lugar, a fin de que realicen lo conducente en la base de datos que manejen.

Plazo de conservación de los datos

De acuerdo con el artículo 36 del Reglamento a la Ley, la conservación de los datos personales deberá observar lo siguiente:

- Los plazos de conservación de los datos personales no deberán aquellos plazos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento.
- Dichos plazos deberán atender las disposiciones aplicables a la materia de que se trate, y
- Dichos plazos deberán tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

Asimismo, dicho precepto establece que “una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos en su posesión previo bloqueo de los mismos, para su posterior supresión”.[87]

Entonces se tiene que el plazo de conservación es igual a:

Plazo de conservación=		
Tiempo requerido para llevar a cabo las finalidades del tratamiento	+ Plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables	+ Periodo de bloqueo

Fuente: Elaboración propia con datos obtenidos dela “Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares”, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, México, 2014, *op. cit.* 72.

Por lo anterior, se analizarán los requisitos anteriores para determinar el plazo total de conservación aplicable al “Proyecto”:

1. *Tiempo requerido para llevar a cabo las finalidades del tratamiento*

Como ya se ha mencionado, la finalidad del tratamiento de las huellas es la verificación de la identidad de los clientes en sucursales de la institución financiera, por esta razón, las huellas deben ser conservadas, en primer lugar, por todo el tiempo que dure la relación contractual con el cliente, es decir, mientras el cliente mantenga vigente algún producto o servicio con la institución en cuyo contrato se haya pactado el tratamiento de las huellas.

Una vez terminada la relación contractual con el cliente, se deben computar los siguientes plazos adicionales que se indican.

[87] Artículo 36 del Reglamento de la LFPDPPP.

2*. Plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables*

Sobre este punto, existen diversas disposiciones aplicables al caso que determinan plazos en los que la institución debe conservar la información.

El primer plazo legal de conservación es el establecido por el artículo 49 del Código de Comercio como a continuación se lee:

> "*Los comerciantes están obligados a conservar por un plazo mínimo de diez años* los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen *contratos, convenios o compromisos que den nacimiento a derechos y obligaciones*". (Énfasis añadido).

Lo anterior resulta aplicable, en virtud de que, a pesar de que las huellas dactilares no serán utilizadas en el "Proyecto" como un factor de autenticación biométrico para la manifestación del consentimiento a que se refiere las Disposiciones de carácter general aplicables a las instituciones de crédito (Circula Única de Bancos), es decir, las huellas dactilares no harán las veces de firma electrónica, el uso de las huellas en el "Proyecto" sí formará parte la operación que las instituciones financieras realicen con sus clientes en sus cuentas, pues con ellas las instituciones verificarán la identidad de la persona a la que posteriormente permitirán el acceso a las cuentas como el titular de las mismas; luego entonces, dicha identificación del cliente sí forma parte de la operación bancaria, es decir, del "contrato, convenio o compromiso" que da lugar a derechos y obligaciones entre la institución y el cliente que menciona el artículo 49 del Código de Comercio, y por lo tanto, toda la información que constituye el contrato, convenio o compromiso desde

la identificación del cliente hasta la culminación de la operación bancaria de que se trate debe ser conservada por un periodo de 10 años.[88]

Por su parte, la 59ª regla de Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito observa lo siguiente:

> "59ª.- …
>
> *Los datos y documentos que integran los expedientes de identificación de Clientes deberán ser conservados durante toda la vigencia de la cuenta o contrato y, una vez que estos concluyan, por un periodo no menor a diez años contado a partir de dicha conclusión*. Asimismo, aquellos datos y documentos que deben recabarse de los Usuarios, deberán ser conservados por el periodo antes referido contado a partir de la fecha en que el Usuario lleve a cabo la Operación de que se trate.
>
> Para tal efecto, las Entidades cumplirán con los criterios que conforme a la Ley, haya dictado o autorice la Comisión, en materia de microfilmación, grabación, conservación y destrucción de documentos". (Énfasis añadido).

Al ser las huellas un dato para identificar al cliente, de lo anterior se desprende que dichos datos deben ser conservados por un periodo de 10 años para el cumplimiento de la disposición arriba citada.

---

[88] Hay que recordar que una institución financiera es un comerciante de acuerdo con la definición del artículo 3º fracción II del Código de Comercio se reputan comerciantes a las sociedades constituidas con arreglo a las leyes mercantiles, en admiculación con el artículo 75, fracción XIV del mismo Código que señala que la ley reputa a las operaciones de bancos como actos de comercio.

Entonces, en virtud de lo establecido por los artículos citados en este punto, resulta que las huellas dactilares deben ser conservadas por un periodo legal y jurídico de 10 años.[89]

3. *Periodo de bloqueo*

Respecto al periodo de bloqueo, el artículo 37 de la LFPDPPP establece que:

> "Artículo 37. …
>
> *Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario*, el responsable deberá proceder a la *cancelación* de los datos en su posesión *previo bloqueo* de los mismos, *para su posterior supresión*". (Énfasis añadido).

De acuerdo con señalado con el INAI, el bloqueo es la acción que tiene por objeto impedir el tratamiento de los datos personales para cualquier finalidad, con excepción de su almacenamiento y acceso para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, hasta el plazo de prescripción correspondiente. Concluido dicho periodo se deberá proceder a la supresión de los datos.[90]

Asimismo, el artículo 1047 del Código de Comercio señala que:

---

[89] No se hace especial mención de los plazos de conservación prescritos en las disposiciones fiscales, administrativas y contables referidas en la LFPDPPP en virtud de que dichos plazos son menores a los mencionados en este punto (de 10 años), *e.g*. el Código Fiscal de la Federación un plazo de conservación de 5 años.

[90] "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"... *op. cit*. nota 71, p. 60.

> “En todos los casos en que el presente Código no establezca para la prescripción un plazo más corto, la prescripción ordinaria en materia comercial se completará por el transcurso de diez años”.

En atención a que no se pueden prever todas las acciones legales que un cliente pudiera interponer en contra de la institución financiera en materia mercantil por virtud de la celebración de operaciones en sucursal en la que formaría parte el uso de la huella dactilar como ya se mencionó, la información relacionada con cada una de las operaciones realizadas (contratación de productos y servicios, ejecución de transacciones, etcétera) debe ser conservada por el plazo en que dichas acciones aún no prescriban para contar con los elementos necesarios para la defensa jurídica de la institución ante una eventual demanda en materia mercantil.[91]

Por lo anterior se concluye que el **periodo de bloqueo** de las huellas dactilares una vez concluida la relación contractual con el cliente (una vez cumplida la finalidad del tratamiento), debe ser por 10 años.

Durante dicho periodo, la institución no podrá tratar las huellas, salvo para almacenarlas y acceder a estas para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, hasta el plazo de prescripción correspondiente.[92]

Para lo anterior, se debe establecer mecanismos y procedimientos para evitar que los datos personales se traten durante el periodo de bloqueo.

En resumen, de los puntos 1, 2 y 3 tenemos lo siguiente:

---

[91] Existen otras disposiciones legales que en materia fiscal, administrativa, laboral y penal, establecen plazos de conservación de la información generada, sin embargo, por tratarse de plazos menores a los señalados en las disposiciones de anteriores no se consideran en este estudio para del cómputo del plazo de conservación.

[92] “Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares”... *op. cit*. nota 71, p. 60.

Plazo de conservación=		
Tiempo requerido para llevar a cabo las finalidades del tratamiento	+ Plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables	+ Periodo de bloqueo (almacenamiento y acceso para determinar posibles responsabilidades en relación con el tratamiento de los datos personales)
Indefinido	**10 años**	**10 años**[93]
Plazo de conservación = **10 años contados a partir de la terminación de la relación jurídica con el cliente (una vez cumplida la finalidad del tratamiento)**		

Fuente: Elaboración propia con datos obtenidos dela "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares", Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, México, 2014, *op. cit.*72.

En conclusión, como se señala en el cuadro, el plazo de conservación de las huellas que debe observar la institución financiera comprenderá el tiempo que dure la relación contractual con el cliente y 10 años adicionales una vez terminada la relación contractual con el cliente.

Para la prueba del cumplimiento de los plazos de conservación los artículos 38 y 39 del Reglamento a la Ley señalan que el responsable debe establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales, por lo que se deberán implementar las medidas técnicas necesarias en el sistema biométrico o en la base de datos de las huellas para crear evidencia necesaria para la comprobación de la conservación, bloqueo y supresión de estos datos ante la autoridad supervisora en la materia (INAI) o los clientes que lo soliciten.

[93] En este caso el periodo de conservación es igual al plazo legal de conservación por lo que no incrementa los diez años de conservación ya establecidos en el plazo legal.

4. Eliminación de los datos una vez transcurrido el plazo de conservación

Una vez terminada la relación contractual con el cliente y fenecido el periodo de bloqueo y el plazo legal que se han señalado en el punto anterior (10 años después de terminada la relación), la institución financiera deberá proceder a la eliminación o supresión las huellas respectivas en su base de datos.

Para esto, la institución deberá documentar la supresión de los datos como se señala en el punto anterior por lo que se recomienda lo siguiente:

1. Establecer por escrito los procedimientos para la conservación, bloqueo y supresión de los datos personales.
2. Contar con el documento que establezca los procedimientos de conservación, bloqueo y supresión de los datos personales.
3. Elaborar bitácoras o cualquier otro documento en el que se acredite la fecha de bloqueo o supresión de los datos personales, y la información relevante con relación a dichas acciones.

3.6 Finalidad

De acuerdo con los artículos 12 de la LFPDPP y 40 de su Reglamento, el principio de finalidad consiste en que los datos no pueden ser utilizados para finalidades distintas a aquellas para los que fueron recabados, es decir, los datos personales que el responsable haya recabado del titular sólo podrán ser tratados para las finalidades previstas en el Aviso de Privacidad.

Dichas finalidades del aviso deberán ser determinadas como lo impone el artículo 40 del Reglamento, el cual señala que "*la finalidad o las finalidades establecidas en el Aviso de Privacidad deberán ser determinadas*, lo cual se logra cuando con claridad, sin lugar a confusión y de manera objetiva se especifica *para qué objeto serán tratados los datos personales*". (Énfasis añadido).

Respecto a la finalidad del Servicio de Verificación, el Acuerdo del Consejo General del Instituto Nacional Electoral, por el que se aprueba la implementación del Servicio de Verificación de los datos de la Credencial para Votar, que servirá para garantizar el derecho de protección de datos de los ciudadanos, contenidos en el Padrón Electoral[94], publicado en el Diario Oficial de la Federación el 12 de abril de 2016, señala en su "al poner en marcha el Servicio de Verificación de los datos de la Credencial para Votar, se pretende que las diferentes instituciones públicas y privadas, así como las asociaciones civiles que lo soliciten envíen en tiempo real a este Instituto los datos de las credenciales que los ciudadanos presenten al momento de identificarse, con la finalidad de que se verifique o niegue la correspondencia con los datos del registro que obre en la base de datos del Padrón Electoral, sin que esto implique que el Instituto Nacional Electoral deba proporcionar información confidencial a esas instituciones"

De igual forma, de acuerdo con el Anexo Único (**Anexo 1**) señala que la finalidad del tratamiento de las huellas dactilares para la institución financiera en este servicio es la verificación de la identidad de los clientes como lo describe a continuación:[95]

> "Para el caso que nos ocupa y a partir de los documentos que proporcionó el INE, se identifica que el Servicio de Verificación tiene fundamentalmente las siguientes finalidades:
> (…)
>
> • Autenticar las huellas dactilares del ciudadano que se identifique con una credencial para votar, mediante la correlación gráfica de las marcas

[94] Recuperado de: *http://dof.gob.mx/nota_detalle.php?codigo=5432730&fecha=12/04/2016* Fecha de consulta: 23 de abril de 2016.
[95] Anexo Único, p. 31.

dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en el Padrón Electoral".

Al respecto es importante precisar que el principio de finalidad está estrechamente relacionado con los principios de calidad (ya que los datos deben ser pertinentes, correctos y actualizados para los fines para los cuales fueron recabados), consentimiento (toda vez que el consentimiento del titular se obtendrá en atención a las finalidades indicadas en el Aviso de Privacidad) e información (ya que previo al tratamiento se deben informar las finalidades del mismo)[96], por lo tanto, para poder cumplir con el principio de finalidad es preciso que se cumplir también con las recomendaciones realizadas respecto a los otros 3 principios en los apartados anteriores y subsecuentes.

Por lo anterior, se recomienda que el Aviso de Privacidad de la institución financiera señale explícitamente como una de las finalidades del tratamiento de las huellas dactilares el señalado en el principio de información y en el modelo de Aviso de Privacidad que se muestra como **Anexo 5**.

Por otra parte, es importante destacar que de acuerdo con el artículo 41 del Reglamento a la Ley el responsable deberá *identificar y distinguir en el Aviso de Privacidad entre las finalidades que dieron origen y son necesarias para la relación jurídica entre el responsable y el titular, de aquéllas que no lo son*.

Aunado a lo anterior, el Anexo de Buenas prácticas en el Aviso de Privacidad de Lineamientos del Aviso de Privacidad, emitidos por el otrora IFAI, señala lo siguiente:

"**Buenas prácticas en el listado de datos personales**

Segundo. Como buena práctica, el Aviso de Privacidad podrá *distinguir* entre los *datos personales que son necesarios para las finalidades que*

[96] Ornelas Núnez, Lina, "Los principios de la protección de datos personales", *op. cit.,* nota 81, p. 79.

dan origen a la relación jurídica entre el responsable y el titular, *de aquéllos que serán tratados para finalidades secundarias o accesorias*, así como asociar el tipo de dato personal o categoría con la finalidad para la cual se tratará.

Asimismo, el Aviso de Privacidad podrá informar sobre las fuentes a través de las cuales el responsable obtiene los datos personales que tratará, así como precisar por cada fuente qué datos personales obtiene de éstas". (Énfasis añadido).

Bajo esa tesitura, el INAI ha expresado que existen dos tipos de finalidades en el tratamiento de datos personales: (i) aquéllas que dan origen y son necesarias para la relación jurídica entre el titular y el responsable, a las cuales el INAI identifica como **primarias**, y (ii) todas las demás que no cumplan con esta condición, a las que el mismo organismo llama **secundarias o accesorias.**[97]

Por lo anterior, podemos afirmar que en el "Proyecto":

1. Las finalidades primarias y secundarias del tratamiento de las huellas deben estar previstas en el Aviso de Privacidad y se debe hacer distinción entre unas y otras en el aviso. De acuerdo al objeto de "Proyecto", las finalidades del tratamiento de las huellas dactilares de los clientes serán:

Finalidades Primarias	Finalidades Secundarias
El tratamiento de las huellas para verificar la identidad de los usuarios o clientes y el cotejo de sus huellas con el INE.	No existen finalidades secundarias.

[97]"Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"... *op. cit*. nota 71, p. 52.

Esta distinción resulta importante pues el artículo 42 del Reglamento señala que "*el titular de los datos personales puede negar o revocar su consentimiento*, así como *oponerse para el tratamiento* de sus datos personales *para las finalidades secundarias*, sin que ello tenga como consecuencia la conclusión del tratamiento para las finalidades primarias". (Énfasis añadido).

Como se mencionó en el punto del consentimiento, en caso de que el cliente o titular del dato solicitara la cancelación o se opusiera al tratamiento de sus huellas dactilares, la institución financiera podrá terminar la relación jurídica con el cliente en los términos y con las condiciones señaladas en dicho apartado.

Por lo antes expuesto, además de las recomendaciones vertidas en los párrafos anteriores de este apartado, se realizan las siguientes para el cumplimiento del principio de finalidad en el "Proyecto":

Las huellas dactilares solo podrán ser utilizadas por la institución financiera para la verificación de la identidad de sus clientes en los términos del Aviso de Privacidad.

Si posteriormente, las instituciones financieras pretendieran utilizar las huellas para finalidades distintas, por ejemplo, como firma electrónica, estas instituciones deberán recabar nuevamente el consentimiento de los clientes por escrito de conformidad con el artículo 9 de la LFPDPPP y el artículo15 del Reglamento a la Ley.

3.7 Proporcionalidad

Como lo señala el artículo 6 de la LFPDPPP´, los responsables del tratamiento de los datos personales deberán observar el principio de proporcionalidad, entre otros.

Así, el artículo 45 del Reglamento a la Ley señala que "*sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido*". (Énfasis añadido).

En el Anexo Único emitido por el INAI, respecto al principio de proporcionalidad este instituto señaló:[98]

> "Ahora bien, el INE propone los siguientes datos obligatorios para efectuar las consultas en el Servicio de Verificación de datos de la credencial para votar:
> - Número OCR.
> - Número CIC (Código de Identificación de Credencial).
>
> Por otra parte, se mencionan como datos opcionales para ser confrontados y verificados por el INE en caso de que sean proporcionados por las instituciones públicas y privadas los siguientes:
> - Apellido paterno.
> - Apellido materno.
> - Nombre(s).
> - Año de registro.
> - Número de emisión de la credencial para votar.
> - Clave de elector.
> - Clave Única de Registro de Población (CURP).
> - *Huellas dactilares de los dedos índices de la mano derecha e izquierda*." (Énfasis añadido)

Respecto al número de huellas dactilares que señaló serían tratadas el INE (2), el INAI calificó lo siguiente:[99]

> "Las huellas dactilares de los dedos índices *se consideran proporcionales* para dar cumplimiento a la finalidad relacionada con verificar la coincidencia de los datos de la credencial para votar con el extracto del Padrón Electoral, mediante la correlación gráfica de las marcas dactilares capturadas al momento de presentar la credencial

[98] Anexo Único, p. 34.
[99] *Ibidem*, p. 35.

con aquellas que se encuentran almacenadas en la base de datos del Padrón Electoral.

No obstante, es importante tener en cuenta que el registro de huellas dactilares puede potencialmente representar la información más confiable para la comprobación de la identidad de una persona. Esto sin omitir mencionar que, las circunstancias en las que se recaban las huellas dactilares y los mecanismos que se emplean para recabarlas deben procurar garantizar fiabilidad alta en la autenticación de la identidad de los individuos". (Énfasis añadido).

Por lo anterior, se recomienda las instituciones financieras minimicen el número de huellas dactilares recabadas a sus clientes al número de huellas que el INE requiera a estas instituciones para el funcionamiento del Servicio de Verificación, es decir, las de los dos dedos índices, ya que si las instituciones financieras recabaran las huellas dactilares de los otros dedos en virtud de la implementación del "Proyecto" podrían vulnerar el principio de proporcionalidad, pues las huellas adicionales que recabarán ya no serían necesarias, adecuadas ni relevantes para la función del Servicio de Verificación con el INE.

3.8 Responsabilidad

Para el cumplimiento del principio de responsabilidad señalado en los artículos 6 y 14 de la LFPDPPP y 47 del Reglamento a la Ley, es necesario que las instituciones financieras:

1. En caso de que remitan los datos a un tercero como encargado de los mismos, deberán celebrar un contrato de prestación de servicios con el encargado con los requisitos que señalan los artículos 51, 54 y 55 del Reglamento.
2. Cumplir con los requisitos que señala el artículo 48 del Reglamento a la Ley que a continuación se transcribe:

Medidas para el principio de responsabilidad
Artículo 48. En términos del artículo 14 de la Ley, el responsable deberá adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.
Entre las medidas que podrá adoptar el responsable se encuentran por lo menos las siguientes:
I. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable;
II. Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;
III. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad;
IV. Destinar recursos para la instrumentación de los programas y políticas de privacidad;
V. Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos;
VI. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran;
VII. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;
VIII. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento;
IX. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el presente Reglamento, o
X. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

4. Deberes de la LFPDPPP

Además de los ocho principios antes mencionados, la protección de datos personales se basa en dos deberes: el de confidencialidad y el de seguridad, los cuales se traducen en obligaciones concretas para el responsable. A continuación se desglosan dichos deberes y las recomendaciones para su cumplimiento en el "Proyecto":

4.1 Deber de confidencialidad

El deber de confidencialidad consiste en la obligación de guardar secrecía respecto de los datos personales que se tratan y evitar su difusión, distribución o comercialización no autorizada, así como establecer medidas necesarias para evitar su transmisión o acceso no autorizado.

Al respecto, el artículo 21 de la LFPDPPP y artículo 9, último párrafo del Reglamento a la Ley establecen que el responsable del tratamiento de los datos personales está obligado a observar el deber de confidencialidad conforme a lo siguiente:

> "Artículo 21.- El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.
>
> Artículo 9.- De acuerdo con lo previsto en el artículo 6 de la Ley, los responsables deben cumplir con los siguientes principios rectores de la protección de datos personales:
>
> […]
>
> Asimismo, el responsable deberá observar los deberes de seguridad y confidencialidad a que se refieren los artículos 19 y 21 de la Ley."

De igual forma, el artículo 50 del Reglamento a la Ley establece la obligación del encargado del tratamiento observe el deber de confidencialidad:

> "El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:
>
> …

IV. Guardar confidencialidad respecto de los datos personales tratados […]".

Por otra parte, como es bien sabido, muchas instituciones financieras están contratando y haciendo uso de los servicios de cómputo en la nube ofrecidos por compañías especializadas en estos servicios. Sobre el uso de estos servicios, el Reglamento a la Ley señala:

> "Artículo 52. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:
>
> I. Cumpla, al menos, con lo siguiente:
>
> […]
>
> d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio […]".

De lo dicho hasta ahora, el INAI resumen las obligaciones que el responsable del tratamiento de los datos personales (sea un miembro de la institución bancaria o bien un tercero autorizado) tiene respecto a este deber:[100]

> 1) Guardar confidencialidad en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con el titular, y;

[100]"Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"... *op. cit*. nota 71, p. 70.

2) Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste.

Adicional a lo anterior, el deber de confidencialidad en materia de datos personales también converge con el deber de confidencialidad que prevé el artículo 142 de la Ley de Instituciones de Crédito, también conocido como secreto bancario o fiduciario, que a la letra señala:

> “Artículo 142.- La información y documentación relativa a las operaciones y servicios a que se refiere el artículo 46 de la presente Ley, tendrá carácter confidencial, por lo que las instituciones de crédito, en protección del derecho a la privacidad de sus clientes y usuarios que en este artículo se establece, en ningún caso podrán dar noticias o información de los depósitos, operaciones o servicios, incluyendo los previstos en la fracción XV del citado artículo 46, sino al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a sus representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio.
>
> Como excepción a lo dispuesto por el párrafo anterior, las instituciones de crédito estarán obligadas a dar las noticias o información a que se refiere dicho párrafo, cuando lo solicite la autoridad judicial en virtud de providencia dictada en juicio en el que el titular o, en su caso, el fideicomitente, fideicomisario, fiduciario, comitente, comisionista, mandante o mandatario sea parte o acusado. Para los efectos del presente párrafo, la autoridad judicial podrá formular su solicitud directamente a la institución de crédito, o a través de la Comisión Nacional Bancaria y de Valores”.

Es importante señalar que el artículo anterior dispone que no será considerada como violación a la obligación de confidencialidad o secreto bancario, cuando las instituciones de crédito exhiban o compartan información a las autoridades competentes cuando se realice a petición de estas últimas y en el ámbito de sus facultades correspondientes.

Por otra parte, el artículo 106, fracción XX de la Ley de Instituciones de Crédito establece la prohibición de las instituciones de crédito para compartir la información de sus clientes sin su consentimiento y sin un fundamento legal aplicable:

> **“**A las *instituciones de crédito* les estará *prohibido*:
>
> …
>
> **XX.** *Proporcionar, para cualquier fin*, incluyendo la comercialización de productos o servicios, *la información que obtengan con motivo de la celebración de operaciones con sus clientes, salvo que cuenten con el consentimiento expreso del cliente respectivo*, el cual deberá constar en una sección especial dentro de la documentación a través de la cual se contrate una operación o servicio con una institución de crédito, y siempre que dicho consentimiento sea adicional al normalmente requerido por la institución para la celebración de la operación o servicio solicitado. En ningún caso, el otorgamiento de dicho consentimiento será condición para la contratación de dicha operación o servicio, …”.

Al respecto, el Anexo Único del INAI, señala que en virtud del “Proyecto”, las instituciones financieras realizarían una transferencia de datos al INE cada vez que la institución financiera solicitara la validación del INE respecto de la credencial de elector que un usuario de éstapresentareen sus oficinas o sucursales para identificarse, así como de las huellas dactilares del mismo usuario para corroborar su identidad.

En tal caso, y en atención a la prohibición del artículo 106 de la Ley de Instituciones de Crédito, se reitera la recomendación de prever en el Aviso de Privacidad la transferencia de datos que llevará a cabo la institución financiera al INE para la ejecución del “Proyecto” al INE. No es necesario recabar el consentimiento del titular para dicha transferencia pues en el caso del “Proyecto” se actualizan las excepciones previstas en las fracciones IV y VII del artículo 16 de la LFPDPPP como se explicará más adelante en el apartado “Transferencias de datos personales entre el INE y la institución financiera”.

De acuerdo con el Anexo Único del INAI, los datos de las credenciales de elector y las huellas de los clientes que el INE recibiría de las instituciones de crédito para ser verificados y confrontados por el INE son:

- Apellido paterno
- Apellido materno
- Nombre(s)
- Año de registro
- Número de emisión
- Clave de elector
- CURP
- Huella de dedo índice de la mano derecha, […]
- Huella de dedo índice de la mano izquierda, […]

Por lo anterior, se reitera la conveniencia de incluir en el Aviso de Privacidad de la institución financiera los datos que serán transferidos al INE en virtud del “Proyecto” y se recomiendan las siguientes acciones para el cumplimiento del deber de confidencialidad:

Recomendaciones para el cumplimiento del deber de confidencialidad

1. Establecer procedimientos para evitar fuga de información o el acceso indebido a los datos personales.

Dentro de este punto, se recomienda firmar con los empleados bancarios que vayan a tener contacto con las huellas dactilares o que vayan a participar en el tratamiento, una carta de confidencialidad donde se estipulen las obligaciones de secrecía que dicho personal deberá observar durante el tiempo que dure la relación laboral con la institución financiera y por 10 años más una vez finalizada la misma.

2. Capacitar al personal para que conozca sus obligaciones con relación al tratamiento de datos personales.

3. Prever sanciones al interior de la institución para los empleados que incumplan este deber.

4. Incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas de confidencialidad y para que quienes tengan acceso a los datos personales en posesión del responsable cumplan con esta obligación de confidencialidad.

Para esto, el contrato de prestación de servicios que se celebre con el tercero deberá contener una cláusula de confidencialidad que indique que el tercero está obligado a guardar confidencialidad de los datos personales tratados en virtud del “Proyecto”, con fundamento en la LFPDPPP y en el artículo 142 de la Ley de Instituciones de Crédito (secreto bancario), por el tiempo que dure la relación contractual y durante 10 años una vez terminada la misma.

Esta misma obligación deberá ser estipulada en el convenio de colaboración que celebren la institución financiera y el INE.

5. Realizar verificaciones o supervisiones periódicas al trabajo realizado por los encargados que sean contratados, a fin de verificar que se cumplan con sus obligaciones en torno a la protección de los datos personales.

6. Comunicar el Aviso de Privacidad de la institución financiera al INE con el fin de informar a este tercero las finalidades del tratamiento de las huellas dactilares acordadas entre el cliente bancario y la institución financiera.

7. Documentar y generar evidencia de las medidas adoptadas para garantizar la confidencialidad de los datos personales tratados en el “Proyecto”.

4.2 Deber de seguridad

El artículo 19 de la LFPDPPP establece la obligación para los responsables de implementar y mantener medidas de seguridad administrativas, técnicas y físicas para una adecuada protección de los datos personales que se traten, a efecto de evitar que los datos sufran daños, pérdidas, alteraciones, destrucción o sean objeto del uso, acceso o tratamiento no autorizado.[101]

En ese sentido, el responsable deberá implementar las medidas de seguridad atendiendo lo que establece la LFPDPPP, su Reglamento y las disposiciones específicas que regulen el sector de la actividad que realice el responsable, siempre que éstas contemplen una protección mayor para el titular que las dispuestas en la LFPDPPP y su Reglamento y las cuales no podrán ser menores a aquéllas que los responsables y encargados tengan para el manejo de suinformación.[102]

4.2.1 Factores a considerar para determinar las medidas de seguridad

De acuerdo con el artículo 60 del Reglamento a la Ley, para determinar qué medidas de seguridad deben ser implementadas en el “Proyecto”, las instituciones financieras deberán tomar en cuenta los siguientes factores:[103]

---

[101] *Ibidem,* p. 72.
[102] *Idem.*
[103] *Idem.*

Ilustración 5. Factores para determinar las medidas de seguridad.

Imagen tomada de: "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares".[104]

Adicionalmente, y de manera potestativa, las instituciones financieras procurarán tomar en cuenta los siguientes elementos:

> "I. El número de titulares;
> II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;
> III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y
> IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable".

Para mayor claridad, los factores anteriores se explican a continuación:[105]

> **I. El riesgo inherente por tipo de dato personal.** El riesgo es igual a la amenaza por la vulnerabilidad, por lo que es necesario realizar un análisis de riesgos.

---

[104] *Idem*.
[105] Carrillo D´Herrera, Juan Carlos, "¿Qué pide el reglamento de la Ley?", *Revista de Seguridad y Defensa Digital: Cultura de prevención para ti*, UNAM, México, número 13, revista bimestral, 2012. Recuperado de: *http://revista.seguridad.unam.mx/numero-13/que-pide-el-reglamento-de-la-ley* Fecha de consulta: 26 de abril de 2016.

II. La sensibilidad de los datos personales tratados. La sensibilidad derivada de la misma Ley y definida en datos personales y datos personales sensibles, requiere que hagamos una clasificación de información para determinar la sensibilidad de los datos.

III. El desarrollo tecnológico. El estado actual de la tecnología, si no es conocido, deberá ser analizado con profundidad y relacionado con la sensibilidad de los datos, es decir no solo será conocer el desarrollo tecnológico general del responsable si no por el tipo de sensibilidad de los datos personales que se manejan.

IV. Las posibles consecuencias de una vulneración para los titulares. Históricamente, las organizaciones han valuado la información por el impacto que tiene al interior de la organización, bajo esta legislación, se debe valorar el costo de los datos personales.

V. El número de titulares. Es el volumen de datos personales que maneja el responsable, básicamente de los clientes (personas físicas) y de los empleados.

VI. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento. Este es uno de los requerimientos más complejos, ya que por distintos reportes del Ponemon Institute se sabe que más del 85% de las empresas sufren al menos una vulneración a la seguridad al año, pero esto no se conoce o se decide ocultar. En el estado de California en los Estados Unidos existe desde 2003 una legislación únicamente para vulneraciones a la seguridad (California Senate Bill 1386) y que nos puede ayudar mucho en el manejo de estas situaciones.

VII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión. Este punto nos pide que el

análisis que hagamos de los datos personales no debe ser únicamente en su volumen sino en el riesgo de la reputación de los titulares afectados.

VIII. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares no exime del cumplimiento de otras legislaciones, por el contrario, suma a las variables de riesgo y cumplimiento dichas leyes o regulaciones, como pueden ser las solicitadas por el IMSS, SAT, INFONAVIT, etcétera.

4.2.2 Acciones para la seguridad de los datos

Las acciones que el responsable deberá observar para el cumplimiento del deber de seguridad, de conformidad con el artículo 61 del Reglamento a la Ley, son las que se enlistan a continua, las cuales se encuentran divididas como si se aplicarán a un proyecto específico para su mejor comprensión:[106]

- Clasificación de la información

  1. Elaborar un inventario de datos personales y de los sistemas de tratamiento.

  2. Determinar las funciones y obligaciones de las personas que traten datos personales.

  3. Realizar un registro de los medios de almacenamiento de los datos personales.

- PIA (Privacy Impact Analysis)

[106] *Idem*.

4. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.

5. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva.

- Plan estratégico de mejora

6. Realizar el análisis de brecha que consiste en: la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.

7. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.

- Auditoría y capacitación

8. Llevar a cabo revisiones o auditorías.

9. Capacitar al personal que efectúe el tratamiento.

Asimismo, el artículo 61 de referencia obliga al responsable a contar con una relación de las medidas de seguridad derivadas de los puntos anteriores.

4.2.3 Actualización de medidas de seguridad

Las medidas de seguridad del responsable, en este caso, las instituciones financieras, se deberán actualizar cuando ocurra cualquiera de los siguientes eventos (artículo 62 del Reglamento a la Ley):

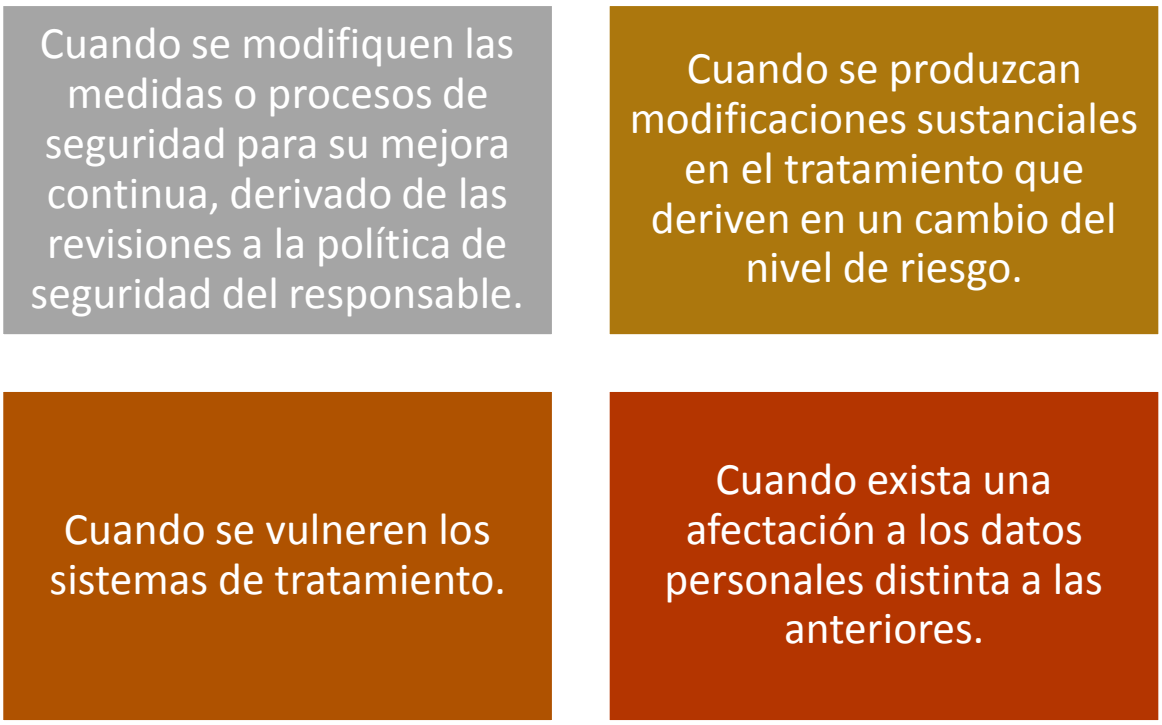


Ilustración 6. Causales para actualizar las medidas de seguridad.

Si se están tratando datos personales sensibles, los responsables deberán revisar, y en su caso, actualizar las relaciones correspondientes una vez al año.

4.2.4 Vulneraciones a la seguridad

Se consideran vulneraciones a la seguridad de los datos personales ocurridas en cualquier fase del tratamiento, las siguientes:[107]

[107] "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"... *op. cit*. nota 71, p. 74

Ilustración 7. Vulneración a la seguridad de los datos (LFPDPPP y su Reglamento)

Imagen tomada de Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares".[108]

¿Qué hacer en caso de una vulneración de seguridad?

Al respecto, el artículo 64 del Reglamento a la Ley establece que "el responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes."

Para lo anterior, la institución financiera deberá informar al titular o cliente lo siguiente (artículo 65 del Reglamento a la Ley):

- La naturaleza del incidente;

[108] *Ibidem*, p. 74.

- 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, y
- Los medios donde puede obtener más información al respecto.

4.2.5 Medidas correctivas

Cuando ocurra una vulneración a los datos personales que trate el responsable, el Reglamento a la Ley (artículo 66) establece que el responsable deberá analizar y corregir las medidas de seguridad correspondientes a efecto de que no se repitan.

Recomendaciones para el deber de seguridad

Por lo anteriormente expuesto, se recomienda a las instituciones financieras realizar las siguientes acciones sobre el “Proyecto” para el cumplimiento del deber de seguridad:

1. Establecer y mantener las medidas de seguridad administrativas, físicas y técnicas.

2. No adoptar medidas de seguridad menores a aquéllas que mantengan para el manejo de su propia información;

3. Tomar en cuenta el riesgo inherente por tipo de dato personal de que se trate, las posibles consecuencias para los titulares derivadas de una vulneración, la sensibilidad de los datos personales tratados y el desarrollo tecnológico;

4. Considerar las acciones que establece el artículo 61 del Reglamento de la LFPDPPP pata la implementación y mantenimiento de las medidas de seguridad;

5. Actualizar las medidas de seguridad implementadas, cuando así se requiera, según los criterios antes descritos;

6. Notificar a los titulares de los datos personales que se tratan sobre las vulneraciones de seguridad que se presenten, con la información y en el momento antes señalado.

7. Llevar a cabo las acciones correctivas que sean necesarias.

Para determinar las medidas de seguridad mínimas que la institución deberá implementar para el cumplimiento de este deber, se recomienda analizar en conjunto con las áreas de seguridad lógica, prevención de fraudes, seguridad informática o cualquier otra área interna de la institución financiera similar que atienda los asuntos relacionados con la seguridad de la información, los siguientes documentos emitidos por el INAI:

1. Recomendaciones en materia de Seguridad de Datos Personales.[109]

2. Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales.[110]

3. Metodología de Análisis de Riesgo BAA.[111]

---

[109] Recuperado de:
http://inicio.ifai.org.mx/MarcoNormativoDocumentos/RECOMENDACIONES%20EN%20MATERIA%20DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf
Fecha de consulta: 06 de diciembre de 2015.
[110] Recuperado de:
http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementacion_SGSDP_marzo2014.pdf
Fecha de consulta: 06 de diciembre de 2015.
[111] Recuperado de:
http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Riesgo_BAA_marzo2014.pdf
Fecha de consulta: 06 de diciembre de 2015.

4. Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en Materia de Seguridad de Datos Personales.[112]

A pesar de que estos documentos no son vinculantes para los responsables del tratamiento de datos, sirven a los responsables como una guía o manual orientativo para la correcta implementación de medidas de seguridad para cada caso en concreto, además de que en caso de ocurriera una vulneración, el INAI tomará en cuenta la implementación de las recomendaciones contenidas en estos documentos para efectos de atenuar la sanción que pudiera aplicarle al responsable por dicha vulneración.

5. Transferencias de datos personales entre el INE y la institución financiera

De acuerdo con el profesor Guillermo Tenorio, la salvaguarda de los datos a través de mecanismos jurídicos que protejan los derechos de acceso, rectificación, cancelación y oposición estaría incompleta sino se hiciera hincapié en una debida protección de los mismos derechos cuando el responsable transfiere los datos del titular a un tercero, quien debiera asegurar el mismo tratamiento que el primer responsable ha dado a los mismos sea nacional o sea un tercero extranjero el que los maneje. A ello se le ha denominado como transferencia de los datos.[113]

De acuerdo con el artículo 3, fracción XIX de la LFPDPPP la transferencia es "toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento".

---

[112] Recuperado de:
http://inicio.ifai.org.mx/DocumentosdeInteres/Tabla_Equivalencia_Funcional_2014.pdf.
Fecha de consulta: 06 de diciembre de 2015.
[113] Tenorio Cueto, Guillermo A., "Análisis crítico de la protección de datos en México", *Los datos personales en México, perspectivas y retos de su manejo en posesión de los particulares,* Ed. Porrúa, México, 2012, p. 65.

Conforme a la definición de tratamiento prevista por la LFPDPPP, la transferencia es un tratamiento de datos personales *per se*.[114]

Por su parte, el artículo 67 del Reglamento a la Ley señala:

> "La transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, *realizada a persona distinta del titular, del responsable o del encargado*".(Énfasis añadido).

Bajo ese tenor, la transferencia es la comunicación de datos personales a otro responsable. Este segundo responsable es el denominado "tercero" que señala el artículo 3º, fracción XVI:[115]"Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos".

Lo anterior conlleva que el "tercero", al igual que el primer responsable, tendrá capacidad para decidir sobre el tratamiento de los datos personales,[116] siendo esto relevante a efecto de distinguirlo de la remisión de datos personales (transmisión de datos entre el responsable y el encargado). En otras palabras, la transferencia de datos personales siempre se efectúa entre dos responsables, pero para efectos de la ley y de este trabajo, se seguirán utilizando los términos de "responsable" y "tercero" para evitar confusiones.

Establecido lo anterior, es importante mencionar que la LFPDPPP y el Reglamento establecen una serie de obligaciones tanto para el responsable como para el "tercero".

---

[114] Recuerde que el tratamiento es definido como "la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, ***transferencia*** o disposición de datos personales."
[115] Ver definición de "tercero" en la pág. 73.
[116] Recio Gayo, Miguel, "Las transferencias nacional e internacional de datos personales", en Piñar Mañas, José Luis y Ornelas Núñez, Lina (coords.), *La Protección de Datos Personales en México*, México, Tirant Lo Blanch, 2013, p. 212.

De acuerdo con los artículos 16, fracción V, 36 y 37 de la LFPDPPP y el artículo 68 del Reglamento, establecen una serie de condiciones para que el responsable pueda realizar una transferencia de datos en general que se pueden resumir de la siguiente manera:

1. El responsable deberá informar al titular en el Aviso de Privacidad correspondiente lo siguiente: que la transferencia se podrá realizar, a quién se transferirán los datos y para qué fines. Asimismo, en caso de requerirse, el Aviso de Privacidad deberá contener una cláusula para que el titular consienta o no la transferencia;

2. El titular deberá haber otorgado su consentimiento para que la transferencia se realice, *salvo los casos de excepción previstos en el artículo 37 de la LFPDPPP, y*

3. El objeto de la transferencia se deberá limitar a la finalidad y condiciones informadas en el Aviso de Privacidad, y que hayan sido consentidas por el titular, en su caso.

Los casos de excepción que prevé el artículo 37 de la LFPDPPP son los siguientes:

> "Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:
>
> I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
>
> II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
>
> III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;

IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y

VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular". (Énfasis añadido).

Al respecto es de observarse que las fracciones IV y VII anteriores son aplicables para el caso del "Proyecto", por lo siguiente:

- La fracción IV es aplicable debido a que las huellas con las que se ostente un nuevo cliente en la sucursal bancaria para abrir una cuenta o celebrar un contrato con la institución serían transferidas al INE con el fin de cotejar la información que el INE tenga relacionada entre los datos de la credencial de elector y las huellas dactilares que se traten, es decir, en interés del titular de los datos de la credencial del INE, pues con ello se evitaría la suplantación de la identidad de la persona en caso de que se tratara de un defraudador con una credencial de elector falsa.

- La fracción VII resulta aplicable una vez que el titular de las huellas es cliente de la institución, es decir, cuando con posterioridad a la apertura de una cuenta o celebración del primer contrato bancario de servicios con la institución, el cliente solicita en la sucursal bancaria la celebración de una operación relacionada con sus productos o cuentas contratados, por ejemplo, una transferencia de fondos, la emisión de una chequera o de una tarjeta adicional, etcétera, y la institución

financiera debe identificarlo conforme a lo pactado en el contrato bancario o de servicios celebrado entre las partes.[117]

Lo anterior, resulta aplicable no obstante la prohibición establecida en el artículo 106, fracción XX de la Ley de Instituciones de Crédito que a la letra señala:

"A las *instituciones de crédito* les estará *prohibido*:

…

XX. *Proporcionar*, para cualquier fin, incluyendo la comercialización de productos o servicios, *la información que obtengan con motivo de la celebración de operaciones con sus clientes, salvo que cuenten con el consentimiento expreso del cliente respectivo*, el cual deberá constar en una sección especial dentro de la documentación a través de la cual se contrate una operación o servicio con una institución de crédito, y siempre que dicho consentimiento sea adicional al normalmente requerido por la institución para la celebración de la operación o servicio solicitado. *En ningún caso, el otorgamiento de dicho consentimiento será condición para la contratación de dicha operación o servicio*, […]". (Énfasis añadido).

Lo anterior, no se contrapone con las excepciones del artículo 37 aplicables mencionadas, puesto que el artículo 106 lo que pretende regular es la transmisión de la información de los clientes a terceros que no estén involucrados con la prestación de servicios original o que dio motivo a la recolección de los datos (un encargado o un tercero autorizado para el

[117] Ver apartado 3.3.3 "Negación del servicio bancario derivada de la negativa del cliente para el tratamiento de sus huellas dactilares" donde se detallan los aspectos jurídicos relacionados con el contrato bancario celebrado entre el cliente/titular del dato y la institución financiera y la inclusión de la cláusula del consentimiento para el tratamiento de las huellas en los contratos bancarios de las personas que a la fecha de la implementación del "Proyecto" ya fueran clientes de la institución.

tratamiento de los datos), es decir, con personas ajenas a la prestación del producto o servicio bancario contratado y cuyo objetivo sea lucrar con la información del cliente para fines distintos al producto o servicio contratado con la institución, por ejemplo, la creación de perfiles del cliente y el envío de información al cliente de publicidad de los servicios del tercero.

Adicionalmente, las Disposiciones de carácter general en materia de transparencia aplicables a las instituciones de crédito y sociedades financieras de objeto múltiple, entidades reguladas señalan expresamente que el uso de los datos personales de los clientes o usuarios deberán atenderse conforme a lo previsto en la LFPDPPP como se indica:[118]

> Artículo 10. Las Instituciones Financieras se abstendrán de utilizar, con fines mercadotécnicos o publicitarios, la información de los Usuarios que estén inscritos en el REUS, a menos que éstos les hubiesen otorgado su autorización para tales efectos, con posterioridad a su inscripción en el mismo.
>
> *En cualquier caso, para el uso de datos personales, las Instituciones Financieras estarán a lo previsto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. (Énfasis añadido).

Por otra parte, el Reglamento en sus artículos 71 al 73 señala los requisitos a los que deberán adherirse el tercero o "receptor" de los datos y el responsable en caso de una **transferencia de datos nacional**, como la que tendrá lugar en el "Proyecto":

> 1. Para realizar una transferencia de datos personales dentro del territorio nacional será necesario que el responsable cumpla con lo previsto en los artículos 36 de la Ley y 68 del presente Reglamento.

[118] Además hay que tomar en cuenta que la Ley más especializada en el caso en concreto (tratamiento de datos personales en el Proyecto) es la LFDPPP, por lo tanto su aplicación es preferente a la Ley de Instituciones de Crédito en este caso.

2. El receptor de los datos o “tercero” deberá tratar los datos personales conforme a lo convenido en el Aviso de Privacidad que le comunique el responsable transferente.

3. La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.

Hay que destacar que en el “Proyecto” la transmisión de datos (huellas dactilares) que realizará la institución financiera al INE para la verificación de la identidad del cliente o titular de las huellas será realizada entre dos responsables, ya que que el INE no tratará los datos como encargado (por cuenta de la institución financiera), sino en colaboración con ésta última, tal y como lo señala el Anexo Único del INAI:

“…cualquier comunicación, difusión o distribución de datos personales entre el INE y la institución, en tanto los dos son responsables del tratamiento de datos personales, es considerada como una transferencia de datos personales.

Ahora bien, de acuerdo con lo descrito en las secciones anteriores, en el Servicio de Verificación existe transferencia de datos personales *de la institución pública o privada hacia el INE*, cuando la primera comunica al INE los datos de las credenciales para votar que presentan los ciudadanos que realizan trámites antes éstas, a fin de que dicho instituto verifique la vigencia y validez de los datos proporcionados, de conformidad con la información que obra en la base

de datos del Servicio de Verificación, la cual se integra a partir del Padrón Electoral".[119] (Énfasis añadido).

Recomendaciones para la transferencia de datos que realizará la institución financiera al INE:

1. Informar al titular de las huellas dactilares (y de los datos de la credencial de elector) la existencia de la transferencia de sus datos en el Aviso de Privacidad.

No es necesario recabar el consentimiento del titular de las huellas para la transferencia de datos al INE, ya que es aplicable la excepción prevista en las fracciones IV y VII del artículo 37 de la LFPDPPP, pues como ya se mencionó, el tratamiento de las huellas nacería como una obligación contractual pactada en el contrato bancario del servicio que se trate a cargo de la institución financiera y el titular de la huella.

3. La institución financiera deberá comunicar al INE el Aviso de Privacidad por medio del cual dio a conocer al titular de las huellas las condiciones a las cuales el titular sujetó el tratamiento de sus datos personales.

6. Derechos ARCO en el "Proyecto"

En particular, la Ley otorga a los titulares de los datos personales el derecho a acceder, rectificar y cancelar su información personal en posesión de terceros, así como a oponerse a su uso.[120]

La Constitución Política de los Estados Unidos Mexicanos reconoce como tal esos derechos en el artículo 16 que señala que toda persona tiene derecho al

---

[119] *Ibidem*, p. 95.
[120] Guía Práctica para ejercer el derecho a la protección de los datos personales, IFAI, México, s/f, p.7.
Recuperado de: *http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf*
Fecha de consulta: 08 de diciembre de 2015.

acceso, rectificación, cancelación y oposición del tratamiento de nuestros datos personales en los términos que fije la ley. A estos se les conoce como derechos ARCO.

Al respecto, el artículo 22 de la LFPDPPPP señala:

> Artículo 22.- Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

Por ende, los responsables del tratamiento de datos personales están obligados a respetar dichos derechos.

Al respecto, cabe mencionar que la creación de bases biométricas son excepciones o limitaciones al derecho de la privacidad y protección de datos personales de los individuos cuyos datos están contenidos en estas bases de datos. Además debe garantizarse el pleno ejercicio de los derechos de acceso, rectificación, cancelación y oposición de procesar la información biométrica. La implementación de sistemas biométricos debe equilibrar y conciliar, por un lado, los intereses individuales tales como los derechos humanos y libertades públicas, y, por el otro, los intereses públicos, como la defensa y seguridad pública.[121]

[121]Véase Díaz, Vanessa, "El ejercicio de los derechos arco ante el flujo transfronterizo de información biométrica", *Derecho y TIC, vertientes actuales,* UNAM, México, 2016, p. 121.
Recuperado de: *http://biblio.juridicas.unam.mx/libros/libro.htm?l=4065*
Fecha de consulta: 11 de diciembre de 2015.

Para lo anterior y el cumplimiento de la normativa nacional respecto a los derechos ARCO, a continuación se enuncian cada uno de estos derechos y las recomendaciones para su correcta observancia en la implementación del “Proyecto”.

6.1 Derecho de Acceso

Los titulares de los datos personales tienen derecho de acceder a su información personal que esté en posesión de terceros, a fin de conocer cuál es y el estado en que se encuentra, es decir, si es correcta y actualizada, o para conocer para qué fines se utiliza. Asimismo, a través del ejercicio del derecho de acceso, se pueden conocer las características generales del uso al que están sometidos los datos personales.[122]

De acuerdo con el artículo 33 de la LFPDPPP, si el cliente realiza una solicitud de acceso a la institución financiera que haya recabado sus huellas dactilares, la institución deberá cumplir con esta obligación poniendo a disposición del titular los datos solicitados, ya sea en sitio, mediante copia simple, documento electrónico u otro medio informado en el Aviso de Privacidad.

Por lo anterior, la institución financiera responsable del tratamiento deberá restructurar el departamento de datos personales para que éste cuente con las herramientas técnicas para que la institución pueda dar acceso a los clientes a sus huellas dactilares registradas:

1. En las oficinas o sucursales bancarias que señale la institución en el Aviso de Privacidad (en sitio).
2. Mediante una copia impresa de las huellas dactilares del cliente.
3. Poniendo a disposición del cliente las huellas registradas en documento electrónico, es decir, por medios magnéticos, ópticos, sonoros, visuales u

[122] “Guía Práctica para ejercer el derecho a la protección de los datos personales”, *op. cit*., nota 120, p.8.

holográficos, por ejemplo, por correo electrónico previamente designado por el cliente o en una memoria externa, o

4. A través de cualquier otra tecnología de la información distinta a las enumeradas en el número anterior y que se encuentre prevista en el Aviso de Privacidad de conformidad con el artículo 102 del Reglamento a la LFPDPPP.

Si el Aviso de Privacidad de la institución no contemplara el uso de las huellas dactilares, como ya se mencionó anteriormente, antes de la implementación del "Proyecto", la institución deberá modificar su Aviso de Privacidad a efecto de incorporar este tratamiento y notificar a los titulares de los datos el cambio del aviso por el medio y bajo el procedimiento indicados en el mismo, tal como lo obliga el artículo 16 fracción VI de la LFPDPPP.

Sin perjuicio de los numerales 1 al 4 anteriores, la institución financiera podrá acordar con sus clientes otros medios de reproducción de las huellas distintas a los medios pactados en el Aviso de Privacidad.

En todos los casos, se deberá recabar el consentimiento del cliente sobre la forma de disposición o entrega de los datos, así como acuse de recibo una vez puestos a disposición a efecto de que la institución cuente con la prueba idónea de la atención al derecho de acceso del cliente.

Sin perjuicio de lo anterior, el acceso a las huellas dactilares por parte del titular de éstas deberá cumplir con lo dispuesto por los artículos 29, 32, 33, 34 y 35 de la LFPDPPP y 101 y 102 del Reglamento a la Ley.

6.2 Derecho de Rectificación

El artículo 24 de la LFPDPPP establece que el titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incorrectos.

Lo anterior significa que los titulares de los datos personales tienen derecho a rectificar su información personal, cuando ésta resulte ser incompleta o inexacta. En

otras palabras, el titular de los datos puede solicitar a quien utilice sus datos personales (al responsable) que los corrija cuando los mismos resulten ser incorrectos o desactualizados o inexactos.[123]

En caso de que el titular de las huellas dactilares solicite a la institución financiera la rectificación de estos datos, la rectificación procedería solo en los siguientes casos:

1. Cuando las huellas dactilares capturadas y asociadas a un cliente determinado por error de la institución fueran asociadas a otra persona distinta del cliente/titular de los datos, es decir, cuando se presente un falso positivo en el sistema biométrico.
2. Cuando la imagen de las huellas dactilares hubieran sido capturadas de manera ineficiente que el cliente no pudiera ser identificado como titular de las huellas y por ende de sus respectivas cuentas, es decir, cuando se presente un falso negativo en el sistema biométrico.
3. Cuando el cliente o titular de los datos sufra una lesión en los dedos de manera que le impidiera identificarse por medio de sus huellas dactilares.

De lo anterior, es importante señalar que las huellas dactilares no cambian con el tiempo como otros datos personales tales como el domicilio, el nombre, o los beneficiarios de las cuentas bancarias de una persona. Es por ello que solo en las causales 1 a 3 anteriores procedería el derecho a la rectificación.

Para efectos de la causal 3, en virtud de que ésta conlleva la imposibilidad del cliente a utilizar sus huellas dactilares como medio de identificación, ya sea a causa de un accidente o por el desgaste de las huellas por el uso de sustancias abrasivas, etcétera, en este caso la institución financiera deberá dar de baja las huellas del cliente o alertar en el sistema biométrico esta situación, a efecto de eliminar este

[123] *Idem*.

requisito de identificación biométrica en sucursal a dicho cliente, pues lo contrario podría conllevar a discriminación del cliente por parte de la institución como lo señala a continuación el artículo 47, fracción VI de las Disposiciones de carácter general en materia de transparencia aplicables a las instituciones de crédito y sociedades financieras de objeto múltiple, entidades reguladas:

> "Se consideran actividades que se apartan de las sanas prácticas y usos relativos al ofrecimiento y comercialización de las operaciones y servicios financieros por parte de las Instituciones Financieras:
>
> VI. Negar a los Usuarios la atención o contratación de operaciones o servicios financieros, por razones de género, raza, etnia, discapacidad física, preferencias sexuales, creencias religiosas, o por cualquier otro tipo de discriminación, salvo por causas que afecten la seguridad del personal de las Instituciones Financieras, clientes o instalaciones, o bien, cuando la negativa de que se trate se funde en disposiciones expresamente previstas en la normativa aplicable;"

La solicitud de rectificación que presente el cliente deberá contener los requisitos establecidos en los artículos 29 y 31 de la LFPDPPP y los artículos 103 y 104 del Reglamento a la LFPDPPP.

De igual forma, el procedimiento de atención a dicha solicitud deberá llevarse a cabo en los términos y plazos que establecen los artículos 25, 28, 30, 32 y 34 de la LFPDPPP, así como los artículos 87 al 93, 95 al 98 y 100 del Reglamento a la Ley.

6.3 Derecho de Cancelación

> "Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales.
>
> La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.
> Una vez cancelado el dato se dará aviso a su titular.

> Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también".

Lo anterior significa que los titulares de los datos personales podrán solicitar que se cancelen, es decir, se eliminen sus datos personales cuando consideren que no están siendo utilizados o tratados conforme a las obligaciones y deberes que tiene el responsable y que se encuentran contenidos tanto en la LFPDPPP como en su Reglamento.[124]

6.4 Derecho de Oposición

El último de los denominados derechos ARCO es el de oposición. Dicho derecho consiste en una acción de negativa respecto al manejo de los datos para determinados fines como pueden ser publicidad, investigación de mercado o encuestas de opinión.[125]

A diferencia de la cancelación, en el mismo no se busca una supresión de los datos proporcionados, por el contrario, se consiente en proporcionarlos, pero se limita u opone el titular al tratamiento para fines específicos.[126]

Al respecto el artículo 27 de la LFPDPPP "el titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular".

Lo anterior conlleva que el derecho de oposición queda ceñido a un bloqueo en el tratamiento de los datos, es decir, que una vez solicitada la oposición el

---

[124] *Idem.*
[125] Bertelsen Repetto, Raúl, "Tratamientos de datos personales y protección de la vida privada", *Cuadernos de extensión jurídica*, núm. 5, Universidad de los Andes, Santiago de Chile, 2001.
[126] Tenorio Cueto, Guillermo A., "Análisis crítico de la protección de datos en México", *op. cit.* nota 113, p. 64.

responsable debe mantenerlos en ese estado de esfera de protección de la cual hablamos cuando nos referimos al bloqueo de datos, y los mismos permanecer así por el tiempo que el titular estime. No serán cancelados pues la naturaleza de la oposición, según la ley, es impedir el tratamiento.[127]

Respecto a los casos en que procede la ejecución de este derecho, el Reglamento a la Ley establece lo siguiente:

> "**Oposición del tratamiento para finalidades distintas**
>
> **Artículo 42.***El titular podrá negar* o revocar su consentimiento, así como *oponerse para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular*, sin que ello tenga como consecuencia la conclusión del tratamiento para estas últimas finalidades."
>
> **"Derecho de oposición**
>
> **Artículo 109.** En términos del artículo 27 de la Ley, *el titular podrá*, en todo momento, *oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo cuando*:
>
> I. *Exista causa legítima y su situación específica así lo requiera*, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular, o
>
> II. *Requiera manifestar su oposición* para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento *para fines específicos*.
>
> *No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable*."

De lo anterior, se desprende que en el caso del "Proyecto", el derecho de oposición solo procedería en cuando las huellas se utilizarán para fines distintos al

---

[127]*Idem.*

“Proyecto”, es decir, para fines que no tengan que ver con la verificación de la identidad del cliente. Cabe mencionar que las huellas dactilares no serían utilizadas para finalidades secundarias como la prospección comercial o publicidad de acuerdo con la información contenida en el Resumen Ejecutivo ni en el Anexo Único emitidos por el INAI, pues la única finalidad del tratamiento en el “Proyecto”, como ya se mencionó, es la verificación de la identidad de los titulares del dato.

Adicional a lo anterior, en virtud de que verificar la identificación del cliente estaría pactada como una obligación a cargo de la institución financiera en el contrato de servicios bancarios que el cliente tenga celebrado, esto actualiza el supuesto señalado en el último párrafo del artículo 109 del Reglamento a la Ley que menciona que “*no procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable*”, por lo que las causales para la procedencia del derecho de oposición mencionadas en las fracciones del artículo 109 del Reglamento no serían aplicables en el “Proyecto”, pues el tratamiento de las huellas para verificar la identidad del cliente sería considerada una obligación contractual (legal) a cargo del responsable (la institución financiera) de acuerdo con el contrato bancario celebrado.

6.5 Consideraciones generales para el cumplimiento de los derechos ARCO

1. Cabe recordar que los medios para ejercer los Derechos ARCO sobre los datos personales en general, incluyendo las huellas dactilares, deberán estar previstos en el Aviso de Privacidad de la institución financiera.

En caso de establecerse un medio o procedimiento distinto para la atención de estos derechos respecto a las huellas dactilares, es necesario señalarlo expresamente en el Aviso.

2. Los procesos y requisitos para la tramitación de solicitudes de ejercicio de Derechos Arco son los mismos que ya se encuentran establecidos en la LFPDPPP

y el Reglamento a la Ley, y que las instituciones ya deben tener establecidos para la atención estas solicitudes respecto a datos personales generales.

2. No se omite señalar que para el análisis y recomendaciones se tomó en cuenta que actualmente las instituciones financieras ya deben contar a la fecha con un encargado o departamento de datos personales para la atención y ejercicio de Derechos Arco por parte de los titulares de los datos personales en general, por ello solo se emitieron las recomendaciones adicionales para el ejercicio de Derechos ARCO sobre las huellas dactilares.

CAPÍTULO V

Recomendaciones para el cumplimento de las disposiciones financieras aplicables

CAPÍTULO V Recomendaciones para el cumplimento de las disposiciones financieras aplicables

1. Facultades del INE para prestar el Servicio de Verificación

Si bien es cierto la facultad del INE para celebrar el convenio de apoyo y colaboración para la operación del Servicio de Verificación con las instituciones financieras no es materia de la legislación bancaria, es importante analizar este punto, pues la certeza jurídica que debe tener una persona moral que celebra un convenio generador de obligaciones (en este caso Bancomer y las demás instituciones financieras que pretendan operar el Servicio de Verificación) depende, entre otras cosas, de la capacidad jurídica que tuviere la otra parte del convenio.

Conforme a la opinión emitida por el INAI en el Anexo Único, señala que a pesar de que aparentemente el INE no cuenta con una base legal que prevea la facultad para utilizar los datos personales de los ciudadanos contenidos en el Padrón Electoral, el INAI no resolverá sobre las facultades del INE, pues a su vez este Instituto no cuenta con las facultades para determinar dicha situación.

Por lo anterior, se recomienda a las instituciones financieras que previo al inicio de operaciones del Servicio de Verificación, celebren el convenio con el INE pactándose en éste que el INE cuenta con las facultades necesarias para llevar a cabo el “Proyecto” (el Servicio de Verificación), y en caso contrario, el INE se comprometerá al pago de daños y perjuicios a las instituciones financieras por el daño que sufrieran dichas instituciones por la falta de facultades del INE para celebrar el convenio o ejecutar el “Proyecto”.

2. Facultades de las instituciones financieras para el tratamiento de las huellas dactilares de los clientes como segundo medio de identificación

De acuerdo con el artículo 52 de la Ley de Instituciones de Crédito (LIC), estas instituciones tienen la facultad de emplear medios electrónicos o tecnologías de

cualquier tipo para la prestación de los servicios que sus clientes tengan contratados con dichas instituciones, siempre que se encuentren pactados en los contratos de servicios o productos, como se señala a continuación:

> "Las instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, y establecerán en los contratos respectivos las bases para determinar lo siguiente:
>
> I. Las operaciones y servicios cuya prestación se pacte;
>
> II. Los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y
>
> III. Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate".

Por su parte el artículo 77 de la LIC señala la obligación de las instituciones de crédito de prestar sus servicios de manera segura:

> "Las instituciones de crédito prestarán los servicios previstos en el artículo 46 de esta Ley, de conformidad con las disposiciones legales y administrativas aplicables, y con apego a las sanas prácticas que propicien la seguridad de esas operaciones y procuren la adecuada atención a los usuarios de tales servicios".

Los artículos 98 y 115 de la LIC señalan que las instituciones deberán identificar a sus clientes para la realización de operaciones bancarias:

> "Artículo 98.- …
> Las instituciones de crédito estarán obligadas a recabar los datos de su clientela, relativos a su identificación y domicilio, de conformidad con las disposiciones que al efecto dicte la Comisión Nacional Bancaria.

Artículo 115.- la Secretaría de Hacienda y Crédito Público en las citadas disposiciones de carácter general emitirá los lineamientos sobre el procedimiento y criterios que las instituciones de crédito deberán observar respecto de:

…

b. La información y documentación que dichas instituciones deban recabar para la apertura de cuentas o celebración de contratos relativos a las operaciones y servicios que ellas presten y que acredite plenamente la identidad de sus clientes;".

Luego, las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito señala que las instituciones (entidades) financieras deberán integrar y conservar un expediente de identificación del cliente previo a la apertura de una cuenta o celebración de contrato para realizar operaciones de cualquier tipo, que contenga *al menos* los siguientes datos y documentos:

4ª.- …
I. Respecto del Cliente que sea persona física y que declare a la Entidad de que se trate ser de nacionalidad mexicana o de nacionalidad extranjera en condiciones de estancia de residente temporal o residente permanente en términos de la Ley de Migración, el expediente de identificación respectivo deberá quedar integrado de la siguiente forma:
a) Deberá contener asentados los siguientes datos:
• apellido paterno, apellido materno y nombre(s) sin abreviaturas;
• género;
• fecha de nacimiento;
• entidad federativa de nacimiento;
• país de nacimiento;
• nacionalidad;
• ocupación, profesión, actividad o giro del negocio al que se dedique el Cliente;
• domicilio particular en su lugar de residencia (compuesto por nombre de la calle, avenida o vía de que se trate, debidamente especificada; número exterior y, en su caso, interior; colonia o urbanización; delegación, municipio o demarcación política similar que corresponda, en su caso; ciudad o población, entidad federativa, estado, provincia, departamento o demarcación política similar que corresponda, en su caso; código postal y país);

• números de teléfono en que se pueda localizar;
• correo electrónico, en su caso;
• Clave Única de Registro de Población, clave del Registro Federal de Contribuyentes (con homoclave), número de identificación fiscal y/o equivalente, así como el país o países que los asignaron, cuando disponga de ellos, y
• número de serie de la Firma Electrónica Avanzada, cuando cuente con ella.
…
b) Asimismo, cada Entidad deberá recabar, incluir y conservar en el expediente de identificación respectivo copia simple de, al menos, los siguientes documentos relativos a la persona física de que se trate:
(i) Identificación personal, que deberá ser, en todo caso, un documento original oficial emitido por autoridad competente, vigente a la fecha de su presentación, que contenga la fotografía, firma y, en su caso, domicilio del propio Cliente.

Del inciso a) de la disposición anterior se infiere que las instituciones podrán recabar los datos de identificación que se mencionan, *sin perjuicio de otros datos adicionales que la institución pudiera recabar con la finalidad de identificar y conocer a su cliente*.

Cabe mencionar además que el inciso b) obliga a las instituciones a verificar que la identificación oficial que presente el cliente se encuentre vigente. Bajo este punto, las instituciones justifican verificar la validez y vigencia de la credencial de elector que el cliente presenta como identificación oficial con el cotejo de huellas dactilares que tiene el INE por medio del Servicio de Verificación.

Por lo anterior, se concluye que las instituciones financieras cuentan con facultades para solicitar a sus clientes sus huellas dactilares para validar su identidad, siempre que así lo hayan pactado en sus contratos de productos o servicios bancarios.

Asimismo, ante la práctica de negar el servicio bancario, las Disposiciones de carácter general en materia de transparencia aplicables a las instituciones de crédito

y sociedades financieras de objeto múltiple, entidades reguladas[128], emitidas por la CONDUSEF señalan lo siguiente:

> CAPÍTULO VII. DE LAS ACTIVIDADES QUE SE APARTAN DE LAS SANAS PRÁCTICAS Y USOSRELATIVOS AL OFRECIMIENTO Y COMERCIALIZACIÓN DE LAS OPERACIONES Y SERVICIOS FINANCIEROS
>
> Artículo 47. Se consideran actividades que se apartan de las sanas prácticas y usos relativos al ofrecimiento y comercialización de las operaciones y servicios financieros por parte de las Instituciones Financieras:
> […]
> VI. Negar a los Usuarios la atención o contratación de operaciones o servicios financieros, por razones de género, raza, etnia, discapacidad física, preferencias sexuales, creencias religiosas, o por cualquier otro tipo de discriminación, *salvo por causas que afecten la seguridad del personal de las Instituciones Financieras, clientes o instalaciones, o bien*, cuando la negativa de que se trate se funde en disposiciones expresamente previstas en la normativa aplicable;

De lo anterior, podemos apuntar que la negativa de la prestación del servicio bancario por parte de las instituciones financieras en caso de que los clientes bancarios o usuarios se negarán a proporcionar sus huellas dactilares para corroborar su identidad en las sucursales bancarias, no constituye una práctica discriminatoria[129] de acuerdo con el artículo 47 anterior, pues como se señaló en el apartado 3.3.3 “Negación del servicio bancario derivada de la negativa del cliente para el tratamiento de sus huellas dactilares”, la institución de crédito no le estaría negando a sus clientes de manera categórica el acceso a los recursos de sus cuentas, sino solo les estaría negando el acceso u operación de las mismas en sucursales, conservando el cliente la opción de operar sus cuentas por los otros

[128] Disponibles en*: http://www.dof.gob.mx/nota_detalle.php?codigo=5403316&fecha=11/08/2015* Fecha de consulta: 28 de abril de 2016.
[129] Salvo los casos en que el cliente esté impedido físicamente para identificarse usando sus huellas dactilares. Ver apartado del Derecho de Rectificación.

medios que las instituciones deben tener habilitados por ley, tales como, las tarjetas bancarias o la banca electrónica (cajeros, terminales punto de venta, banca por internet, entre otros), además de que el objeto de la verificación es la prevención de la suplantación de la identidad de los clientes o usuarios, o en otras palabras, el tratamiento de las huellas se realizaría para evitar que la seguridad de las personas sea afectada como lo refiere el artículo en cita.

No obstante lo anterior, es importante recordar que en caso de que el cliente solicitara revocar su consentimiento para el tratamiento de sus huellas dactilares, o el ejercicio de sus derechos de cancelación u oposición, la institución financiera deberá permitir el ejercicio de dichos derechos, pues a pesar de que las partes hubieran pactado el uso de las huellas para la prestación del servicio en el contrato bancario correspondiente, de acuerdo con la Tercera, fracción I, inciso a de las Disposiciones de carácter general en materia de cláusulas abusivas contenidas en los contratos de adhesión, emitidas por CONDUSEF, las instituciones no podrán pactar la renuncia de un derecho del cliente, como en este caso los derechosde cancelación y oposición al tratamiento de sus datos tutelados por la LFPDPPP, ya que si bien es cierto que las huellas serán utilizadas para un fin legítimo como lo es verificar la identidad de los clientes y prevenir suplantaciones, también lo es que las huellas dactilares no son el único medio por el cual una institución puede validar dicha identidad, pues en caso de que la credencial de elector o cualquier otra identificación que presentara el cliente no fuera suficiente para verificar con certeza que la persona es quien dice ser, la institución podría valerse de otros datos no biométricos para verificar la identidad de la persona, por ejemplo, solicitando otra identificación o realizando preguntas con respuestas secretas previamente designadas por el cliente.

CAPÍTULO VI

Recomendaciones adicionales derivados del Dictamen sobre la evolución de las tecnologías biométricas WP193

CAPÍTULO VI Recomendaciones adicionales derivados del Dictamen sobre la evolución de las tecnologías biométricas WP193

En el capítulo V anterior se han señalado las recomendaciones para el cumplimiento de la ley mexicana en materia de datos personales. De lo anterior, es de percatarse que en la legislación mexicana no se prevé regulación especial para la protección de los datos biométricos o para las huellas dactilares en específico.

Sobre la protección de datos personales en general es importante mencionar que éste un derecho que se ha extendido a diversas partes del mundo en los últimos años y por ello diversos organismos internacionales y autoridades de otros países han emitido instrumentos jurídicos en la materia.

Hablando de derecho internacional público, es importante mencionar que esta rama del derecho adscribe significancia jurídica a los instrumentos jurídicos internacional a partir de su forma: por una parte se encuentran los tratados internacionales que establecen obligaciones internacionales (normas vinculantes o *hard law*) y, por la otra, los instrumentos no vinculantes que no establecen dichas obligaciones (derecho blando o *soft law*).[130]

Así, existen diversos documentos internacionales en materia de datos personales, algunos obligatorios para México y otros de soft law[131]. Los instrumentos de soft law, no obstante que su observancia no es obligatoria o vinculante para México, es decir, no generan la obligación de aplicar su contenido en el interior del territorio mexicano, enriquecen la práctica de la protección de datos personales en

---

[130] "Tipología de Instrumentos Internacionales", Comisión Económica para América Latina y el Caribe, Organización de las Naciones Unidas, Perú, 2013, p. 7. Recuperado de: *http://www.cepal.org/rio20/noticias/noticias/1/50791/2013-861_PR10_Tipologia_instrumentos.pdf* Fecha de consulta: 28 de abril de 2016.

[131] Al respecto es importante señalar que para que un tratado o instrumento internacional sea de observancia obligatoria en México, dicho documento deberá ser aprobado por el Senado de la República y ratificado por el presidente de la República. Asimismo, el documento debe ser promulgado y publicado en el *Diario Oficial de la Federación* para darle plena eficacia jurídica como lo establece la Ley sobre la Celebración de Tratados, consultable en: *http://www.diputados.gob.mx/LeyesBiblio/pdf/216.pdf*
Fecha de consulta: 28 de abril de 2016.

el país. Algunos ejemplos de instrumentos internacionales o extranjeros con recomendaciones para la mejor práctica de la protección de datos personales son: las “Directrices relativas a la protección de la intimidady de la circulación transfronteriza de datos personales” de la OCDE (Organización para la Cooperación y el Desarrollo Económicos) de 1980, el “Marco de privacidad” de APEC (Asia-Pacific Economic Cooperation) de 1999, la “Propuesta de Principios de la OEA (Organización de los Estados Americanos) sobre Privacidad y la Protección de Datos Personales”, la “Directiva 95/46/CE del Parlamento Europeo y del Consejo,de 24 de octubre de 1995, relativa a la protección de las personasfísicas en lo que respecta al tratamiento de datos personalesy a la libre circulación de esos datos”, así como los dictámenes y documentos de trabajo del Grupo de Trabajo del Articulo 29 de la Unión Europea (en adelante UE).

Además de los instrumentos señalados, existen muchas otras recomendaciones internacionales para la protección de datos personales[132], sin embargo, dentro de ese basto número de instrumentos solo algunos contemplan recomendaciones o regulación para brindar especial protección a los datos biométricos.

Algunos de los instrumentos extranjeros que abordan tanto los aspectos jurídicos como los tecnológicos del tratamiento de este tipo de datos son los documentos emitidos por el Grupo de Trabajo del Artículo 29 de la Comisión Europea: el “Dictamen sobre la evolución de las tecnologías biométricas WP193”, adoptado en la Unión Europea el 27 de abril de 2012, y el “Documento de trabajo sobre biometría WP80”, adoptado 01 de agosto de 2003, los cuales contienen

[132] Para más información de otros instrumentos internacionales en materia de protección de datos personales, consultar: *Compendio de Protección de Datos Personales*, México, IFAI, 2010. Recuperado de: *http://inicio.ifai.org.mx/Publicaciones/CompendioProteccionde Datos8.pdf* Fecha de consulta: 29 de abril de 2016.

recomendaciones específicas para el tratamiento de los datos biométricos para la UE.

Estos documentos son derivados de la Directiva 95/46/CE, norma que, junto con la jurisprudencia del Tribunal de Justicia dictada sobre la materia, ha influido decisivamente en el desarrollo a nivel europeo y mundial del derecho a la privacidad y en particular del derecho a la protección de datos[133] y en cuya interpretación ha tenido protagonismo el Grupo del Artículo 29 de la Directiva o "Art. 29 Working Party", así denominado por haber sido creado por mandato del artículo 29 de la Directiva95/46/CE, teniendo como una de sus funciones el formular recomendaciones sobre asuntos relacionados con la protección de las personas en la Unión Europea (UE).[134]

Así, vista la falta de normas o recomendaciones especiales para la protección de datos biométricos en México, los documentos de trabajo sobre biometría de la UE sirven como "guía de buenas prácticas" para el tratamiento de los datos biométricos en México, pues como lo señala la siguiente tesis de la SCJN,[135] "el soft law" puede

---

[133] Piñar Mañas, José Luis, "¿Existe privacidad", *Compendio de Protección de Datos Personales*, México, IFAI, 2010, p.29.
Recuperado de: *http://inicio.ifai.org.mx/Publicaciones/CompendioProteccionde Datos8.pdf*
Fecha de consulta: 16 de febrero de 2016.

[134] Artículos 29, numeral 1 y 30, numeral 3 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.
Recuperado de: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML*
Fecha de consulta: 16 de febrero de 2016.

[135] Publicada en el Semanario Judicial de la Federación del viernes 25 de abril de 2014 a las 9:32 horas y en su Gaceta, Décima Época, Libro 5, Tomo I, abril de 2014, página 202, registro digital 2006224, de título y subtítulo: "DERECHOS HUMANOS CONTENIDOS EN LA CONSTITUCIÓN Y EN LOS TRATADOS INTERNACIONALES. CONSTITUYEN EL PARÁMETRO DE CONTROL DE REGULARIDAD CONSTITUCIONAL, PERO CUANDO EN LA CONSTITUCIÓN HAYA UNA RESTRICCIÓN EXPRESA AL EJERCICIO DE AQUÉLLOS, SE DEBE ESTAR A LO QUE ESTABLECE EL TEXTO CONSTITUCIONAL."
Esta tesis se publicó el viernes 13 de marzo de 2015 a las 9:00 horas en el Semanario Judicial de la Federación.

fungir como punto de referencia o guía para la aplicación del derecho y el respeto a los derechos humanos, en este caso, el de la privacidad.

Época: Décima Época

Registro: 2008663

Instancia: Tribunales Colegiados de Circuito

Tipo de Tesis: Aislada

Fuente: Gaceta del Semanario Judicial de la Federación

Libro 16, Marzo de 2015, Tomo III

Materia(s): Constitucional

Tesis: XXVII.3o.6 CS (10a.)

Página: 2507

"SOFT LAW". LOS CRITERIOS Y DIRECTRICES DESARROLLADOS POR ÓRGANOS INTERNACIONALES ENCARGADOS DE LA PROMOCIÓN Y PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES SON ÚTILES PARA QUE LOS ESTADOS, EN LO INDIVIDUAL, GUÍEN LA PRÁCTICA Y MEJORAMIENTO DE SUS INSTITUCIONES ENCARGADAS DE VIGILAR, PROMOVER Y GARANTIZAR EL APEGO IRRESTRICTO A LOS DERECHOS HUMANOS.

De conformidad con el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos y su alcance protector en materia de derechos humanos, los agentes del Estado Mexicano no sólo deben observar la normativa internacional de carácter obligatorio y la jurisprudencia interamericana, sino que en virtud de las máximas de universalidad y progresividad que también contempla, debe admitirse el

desarrollo de principios y prácticas del derecho internacional de carácter no vinculante previstos en instrumentos, declaraciones, proclamas, normas uniformes, directrices y recomendaciones aceptados por la mayoría de los Estados. Dichos principios son identificados por la doctrina como "soft law" -en inglés-, cuya traducción corresponde a ley suave, normas ligeras, dúctiles o blandas y es empleado dado (i) el sentido de falta de eficacia obligatoria y (ii) en oposición al "hard law" o derecho duro o positivo. Ahora bien, con independencia de la obligatoriedad que revistan, *su contenido puede ser útil para que los Estados, en lo individual, guíen la práctica y mejoramiento de sus instituciones encargadas de vigilar, promover y garantizar el apego irrestricto a los derechos humanos. Sin que ello implique desconocer la observancia primigenia del orden jurídico nacional, ni el principio de subsidiariedad de las normas supranacionales, según el cual, la protección internacional de los derechos humanos es aplicable después de agotada la tutela interna* y, sólo en su defecto, debe acudirse a aquélla, pues más allá de que la Constitución Federal y los tratados no se relacionen en términos jerárquicos, según definió el Máximo Tribunal del País en la jurisprudencia P./J. 20/2014 (10a.)(*), la consulta de directrices no vinculantes sólo reporta efectos prácticos derivados de la experiencia acogida por órganos internacionales encargados de la promoción y protección de los derechos fundamentales.

TERCER TRIBUNAL COLEGIADO DEL VIGÉSIMO SÉPTIMO CIRCUITO.

Amparo en revisión 215/2014. 16 de octubre de 2014. Unanimidad de votos. Ponente: Livia Lizbeth Larumbe Radilla. Secretario: José Francisco Aguilar Ballesteros. (Énfasis añadido).

Asimismo, resulta importante recordar que entre México y la UE existen diversas relaciones comerciales en las que puede haber intercambio de todo tipo de datos personales, motivo por el cual la UE eventualmente requerirá a México que cumpla con un nivel de protección de datos personales igual al de la UE, por lo que la aplicación de las recomendaciones de protección de datos de la UE que no se contrapongan a lo dispuesto por la norma mexicana pueden crear esquemas comerciales y legales favorecedores para México.

Por lo anterior, a continuación se estudiarán las recomendaciones del Dictamen 3/2012 aplicables al caso que nos ocupa y no redundantes con las recomendaciones para el cumplimiento de la LFPDPP y su Reglamento realizadas en el capítulo V anterior, para su aplicación en el "Proyecto" como mejores prácticas, o en su caso, para ampliar la justificación de la legalidad del tratamiento de las huellas dactilares realizada en los capítulos anteriores.[136]

1. Recomendaciones del Dictamen 3/2012 aplicables al "Proyecto"

1.1 Proporcionalidad

Sobre este principio, el Dictamen 3/2012 señala lo siguiente:

> "Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente *si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión* a la luz de las características específicas de la tecnología biométrica que

[136] No se hace mención específica de las recomendaciones del "Documento de trabajo sobre biometría WP80", pues las recomendaciones de este documento aplicables al caso que se estudia en este trabajo son las mismas que las del Dictamen 3/2012 que se mencionan en este capítulo.

se va a utilizar[137]. Un tercer aspecto a ponderar es si *la pérdida de intimidad resultante es proporcional a los beneficios esperados*. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar *la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado".*[138]

Al respecto, es importante mencionar que a diferencia de la Unión Europea, en México no existe un documento similar que proporcione a los responsables pautas para determinar si la proporcionalidad del tratamiento de los datos biométricos que realizara un sistema biométrico es la adecuada o no; por tal motivo a continuación se analizarán los 4 factores que el Dictamen 3/2012 como apoyo para el cumplimiento del principio de proporcionalidad en el "Proyecto":

Factor a considerar para determinar la proporcionalidad del tratamiento (Dictamen 3/2012)	**Análisis del factor:**
1. ¿Considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable*?*	En este punto es importante considerar que el sistema de verificación del INE ha sido diseñado por dicho instituto, por lo que el número de huellas dactilares que recabe la institución financiera al cliente o titular del dato será en función al requerimiento de dicho sistema.

[137] La biometría se utilizará para la identificación o verificación: un identificador biométrico puede considerarse técnicamente idóneo para la una y no para la otra (por ejemplo, las tecnologías caracterizadas por unas bajas tasas de rechazo deberán tener prioridad en los sistemas destinados a utilizarse con fines de identificación a efectos de la aplicación de la ley).
[138] Por ejemplo las tarjetas inteligentes u otros métodos que no recojan o centralicen datos biométricos para fines de autenticación.

¿La probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión?	Como se mencionó en el capítulo I, uno de las funciones del Servicio de Verificación es autenticar las huellas dactilares del ciudadano que se identifique con una Credencial para Votar, mediante la correlación gráfica de las marcas dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en la base de datos con lo almacenado en el Padrón Electoral. Con esto, las instituciones financieras estarán en posibilidad de comprobar que la persona que pretende realizar alguna contratación u operación en sucursales bancarias es en realidad la persona que dice ser, y no se trata de un defraudador, que con una Credencial para Votar falsa o robada, pretenda realizar operaciones ilícitas en las sucursales bancarias de la institución de que se trate. En virtud de que actualmente, no existe otro medio para verificar que la Credencial para Votar de esa persona es auténtica, más que el Servicio de Verificación del INE, es que se infiere que el sistema o el “Proyecto” resulta

	eficaz para evitar el robo o suplantación de identidad en las oficinas bancarias.
La pérdida de intimidad resultante es proporcional a los beneficios esperados.	Como se mencionó en el Capítulo I, el objeto del "Proyecto" es verificar la identidad de los clientes o usuarios de la banca para evitar que terceros suplanten su identidad con credenciales falsas, a partir de la autenticación con el INE de las huellas dactilares del individuo que se presentare a la sucursal bancaria. De lo anterior, se puede apreciar que la finalidad de este tratamiento resulta en beneficio del cliente o usuario de la banca así como de la institución financiera de que se trate, toda vez que al evitarse la suplantación de identidad por medio del "Proyecto" se estarían evitando daños y perjuicios tanto al cliente o usuario como a la institución financiera por el acceso indebido a recursos o la celebración de operaciones por parte de los defraudadores a nombre de otra persona. Este beneficio se maximiza cuando se trata de un nuevo cliente del banco, es decir, de aquella persona que se presenta en una sucursal bancaria para

	abrir una cuenta o celebrar una operación por primera vez y por lo tanto hasta ese momento el banco no cuenta con ningún expediente de identificación previo de esa persona, ya que en este la corroboración de las huellas dactilares es el único medio del cual dispone hoy en día una institución financiera para poder verificar que esa persona que aún no es su cliente y exhibe una credencial para votar para identificarse es en realidad quien dice ser y no se trata de una identificación falsa. Por lo anterior, se concluye que el "Proyecto" cumple con este punto del principio de proporcionalidad.
Considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado.	Sobre este punto, se debe de tomar en consideración que actualmente no existe ningún medio distinto al Servicio de Verificación del INE para que las instituciones financieras pueda corroborar la originalidad de la credencial para votar ni la identidad de las personas que se presentara en una sucursal bancaria. Actualmente, la credencial para votar es, con este nuevo sistema, la única identificación oficial cuya originalidad puede ser corroborada

	utilizando los datos biométricos de las personas, pues otras credenciales oficiales, tales como la cartilla, el pasaporte o la cédula profesional, a la fecha no cuentan con algún mecanismo similar que permita su validación con el grado de efectividad del Sistema de Verificación del INE. Por lo anterior, se considera que a la fecha no existe un medio menos invasivo que permita a las instituciones financieras verificar la originalidad de las credenciales de elector que las personas presenten en sucursales bancarias al momento de celebrar una operación financiera.

Una vez analizado los puntos y factores anteriores, se infiere queel “Proyecto” cumple con el principio de proporcionalidad que señala el Dictamen 3/2012 para el tratamiento de dato biométricos.

1.2 Precisión

El documento observa lo siguiente:

> “Los datos biométricos tratados deberán ser exactos y pertinentes en proporción a la finalidad para la que fueron recogidos. Estos datos deberán ser exactos en la recogida y al establecer el vínculo entre la persona y los datos biométricos. La exactitud en el registro es también importante para prevenir la usurpación de identidad”.

Al respecto, en el “Proyecto” al recabarse las huellas dactilares de cada cliente se estarán asociando las mismas con su nombre y su número de cliente, contrato, tarjeta bancaria, etcétera. Por esto, es importante seleccionar el sistema biométrico más exacto y con menor tasa de error que permita la correcta asociación de la persona con la huella. Igual importancia tiene el trabajo de desarrollo del empleado bancario que “enrole” a la persona en el sistema biométrico.

Para lo anterior se recomienda verificar con el área técnica interna de la institución financiera que el sistema biométrico que se vaya a adquirir permita la correcta asociación de las huellas. De igual forma, se recomienda la capacitación de empleados de la red de sucursales que llevarán a cabo el enrolamiento.

1.3 Minimización de datos

No obstante que la legislación de datos personales mexicana prevé este principio en el artículo 46 del Reglamento a la Ley, el cual señala: “El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.”, el Dictamen señala al respecto para el cumplimiento de este principio en el tratamiento de datos biométricos lo siguiente:

> “Puede surgir una dificultad específica por cuanto los datos biométricos a menudo contienen más información de la necesaria para las funciones de búsqueda de correspondencias. El responsable del tratamiento deberá aplicar el principio de *minimización de datos*. En primer lugar, esto significa que solo deberá tratarse, transmitirse o almacenarse la información necesaria, no toda la información disponible. En segundo lugar, el responsable del tratamiento deberá garantizar que la configuración por defecto promueva la protección de datos, sin tener que tomar medidas al efecto”. (Énfasis añadido).

No obstante que el número de datos recabados para verificar la identidad de una persona depende del sistema biométrico adquirido o en uso, como ya se mencionó en el apartado del principio de proporcionalidad, en virtud de que el diseño del sistema del servicio de verificación del INE funcionará solo con las huellas de los dos dedos índice, la institución financiera deberá evitar recabar huellas dactilares adicionales pues se podría considerar los datos serían excesivos para la finalidad por la cual se están recabando.

Por lo anterior, se sostiene la recomendación de que el sistema biométrico de la institución sea diseñado para recolectar solo las huellas de los dedos índices de cada mano.

2. Recomendaciones sobre el "Motivo Legítimo"

El Dictamen, al igual que la normatividad mexicana, señala que el tratamiento de los datos biométricos debe basarse en "motivos legítimos".

Esto compagina con el principio de finalidad de la LFPDPPP antes explicado, el cual se consigna que "el tratamiento únicamente deberá ser llevado a cabo en el ámbito de finalidades determinadas, explícitas y legítimas relacionadas con la actividad del responsable"[139].

El Dictamen el tratamiento de los datos biométricos deberá basarse en uno de los motivos legítimos previstos en el artículo 7 de la Directiva 95/46/CE.

Por lo anterior, a continuación se citan las recomendaciones sobre este rubro del Dictamen aplicables al "Proyecto":

---

[139] Dictamen de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, p. 32, Recuperado de:
http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf
Fecha de consulta: 16 de febrero de 2016.

2.1 Consentimiento

Respecto al consentimiento para el tratamiento de datos biométricos, el Dictamen señala:

> "…el consentimiento debe ser una manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan. Debe quedar claro que este consentimiento no puede obtenerse libremente haciendo si se hace obligatoria la aceptación de los términos y condiciones generales, ni mediante posibilidades de exclusión voluntaria. Además, el consentimiento debe ser revocable. […]
>
> En muchos casos en los que se tratan datos biométricos, *sin una alternativa válida como una contraseña o una tarjeta de banda magnética, el consentimiento no puede ser otorgado libremente*. […]". (Énfasis añadido).

En el caso del "Proyecto", la utilización de las datos biométricos (huellas dactilares) para la verificación de la identidad de los clientes y no otro medio de autenticación como NIP´s o tarjetas es necesario pues las personas que se presenten por primera vez a una sucursal bancaria no tienen una contraseña o tarjeta para autenticarse. Las huellas dactilares u otros datos biométricos son los únicos datos que una persona lleva consigo que permite que su identidad pueda ser cotejada con la identidad registrada en otra base de datos (en este caso la base del INE).

Para los persona que ya son clientes de la institución y que ya cuenten con una contraseña o NIP que pueda ser utilizada en sucursales como medio de autenticación, se recomienda que una vez superada la comprobación de la identidad del cliente en el primer contacto (cuando aún no es cliente de la institución), se permita al cliente elegir entre continuar con la autenticación por medio de sus huellas cada vez que acuda a una sucursal a realizar una operación o autenticarse por medio del NIP o contraseña designado.

En caso de que el cliente opte por ser autenticado con la contraseña o NIP, las huellas dactilares que se utilizaron en el primer contacto deben conservarse por el periodo mencionado en el principio de calidad, por ser información integrante de la contratación, no obstante que no se vayan a utilizar en eventos posteriores como medio de autenticación.

2.2 Contrato

Respecto a que le tratamiento de los datos biométricos se justifique al amparo un contrato, especialmente de prestación de servicios, el documento señala lo siguiente:

> "El tratamiento de datos personales puede ser necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado. Sin embargo, cabe señalar que esto se aplica, en general, solo cuando se prestan servicios biométricos puros. Esta base jurídica no se puede utilizar para legitimar un servicio secundario consistente en registrar a una persona en un sistema biométrico. Si tal servicio puede separarse del servicio principal, el contrato por el servicio principal no puede legitimar el tratamiento de datos biométricos. Los datos personales no son bienes que puedan intercambiarse por un servicio, por lo que los contratos que prevean o que ofrezcan un servicio solo bajo la condición de que una persona consienta el tratamiento de sus datos biométricos para otro servicio no puede servir de base jurídica para dicho tratamiento".

De lo anterior se puede interpretar que el condicionamiento de la prestación del servicio bancario al consentimiento del cliente del tratamiento de sus huellas dactilares es ilegitimo. Sin embargo, de acuerdo con el punto 2.4 siguiente, el condicionamiento del servicio a la verificación de la identidad por medio de biométricos encuentra su justificación por ser una actividad en interés legítimo del responsable del tratamiento como se detalla en dicho apartado.

2.3 Obligación jurídica

Sobre este motivo legítimo, el Dictamen señala:

> "Otra base jurídica para el tratamiento de datos personales es que este sea necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del mismo. Es el caso, por ejemplo, en algunos países alexpedir o utilizar los pasaportes[140]y los visados[141]."

Al respecto, es importante mencionar que las instituciones financieras solo están obligadas por ley a recabar de sus clientes para su identificación los datos señalados en las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito señalados el apartado "Facultades de las instituciones financieras para el tratamiento de las huellas dactilares de los clientes como segundo medio de identificación" en cuyo listado no se encuentran las huellas dactilares, de lo que resulta que la recolección de las huellas dactilares no es una obligación jurídica a la que se encuentren sujetas estas instituciones.

---

[140] Las impresiones dactilares se han integrado en los pasaportes, en cumplimiento de lo dispuesto en el Reglamento UE nº 2252/2004 del Consejo, de 13 de diciembre de 2004, y en los permisos de residencia, de conformidad con lo dispuesto en el Reglamento UE nº 1030/2002 del Consejo, de 13 de junio de 2002.

[141] El registro de identificadores biométricos en el Sistema de Información de Visados (VIS) fue creado por el Reglamento (CE) nº 767/2008, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS). Véase también el Dictamen n° 3/2007 sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica la Instrucción consular común dirigida a las misiones diplomáticas y oficinas consulares de carrera en relación con la introducción de datos biométricos y se incluyen disposiciones sobre la organización de la recepción y la tramitación de las solicitudes de visado [COM (2006) 269 final]. WP134, Dictamen 2/2005 sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros [COM (2004) 835 final] WP 110; Dictamen 7/2004 sobre la inclusión de elementos biométricos en los permisos de residencia y visados teniendo en cuenta la creación del Sistema de Información de Visados (VIS) WP 96.

Por lo anterior, las instituciones financieras no podrían justificar el tratamiento de las huellas dactilares bajo este motivo señalado por el Dictamen.

2.4 Interés legítimo perseguido por el responsable del tratamiento

Como tercer motivo legítimo el Dictamen señala el "interés legítimo perseguido por el responsable del tratamiento", respecto del cual plantea lo siguiente:

> "…el tratamiento de datos biométricos también puede justificarse cuando sea «necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.
>
> Esto significa que hay casos en que la utilización de los sistemas biométricos es del interés legítimo del responsable del tratamiento de los datos. Este interés, no obstante, *solo es legítimo cuando el responsable del tratamiento puede demostrar que su interés prevalece objetivamente sobre el derecho de los interesados a no estar registrados en un sistema biométrico*. Por ejemplo, cuando la seguridad de zonas de riesgo elevado debe garantizarse específicamente mediante un mecanismo que pueda verificar con precisión si las personas tienen derecho de acceso a estas zonas, la utilización de un sistema biométrico puede ser del interés legítimo del responsable del tratamiento de datos". (Énfasis añadido).

Al respecto, es importante mencionar que el tratamiento de las huellas dactilares en el "Proyecto" se realizará con el objeto de reforzar el proceso de verificación de identidad de sus clientes, a efecto de evitar el acceso o la operación de las cuentas bancarias de un cliente a un tercero no autorizado, como es el caso de los defraudadores, pues de esto se podría derivar controversias judiciales entre el cliente y la institución, las cuales generarían gastos y costas en los procesos judiciales para las instituciones, pérdidas económicas por los reembolsos que tendrá que realizar a los usuarios cuyas procesos judiciales o administrativos prosperen, así como el eventual desprestigio en la reputación de la institución en caso de que la suplantación

de identidad y el engaño a los ejecutivos de sus sucursales se convirtiera en una práctica habitual, y actualmente no existe un medio alternativo menos invasivo para verificar la originalidad de la credencial para votar al momento en que el cliente o el usuario se presentara en sucursal. Por lo anterior, se concluye que el tratamiento de datos biométricos del “Proyecto” redunda en un interés legítimo de las instituciones financieras, lo cual es un motivo legítimo para el tratamiento de las huellas dactilares.

3. Tratamiento automatizado

Como ya se mencionó en los apartados de “Facultades de las instituciones financieras para el tratamiento de las huellas dactilares de los clientes como segundo medio de identificación” y “Derecho de Rectificación”, el “Proyecto” debe tener mecanismos alternos para la identificación de los clientes en caso de que el sistema de identificación biométrica no pueda identificar correctamente a un cliente a efecto de evitar discriminación por la negación del servicio bancario.

Al respecto, el Dictamen señala lo siguiente:

> “Cuando se utilicen sistemas basados en el tratamiento de datos biométricos, deberá prestarse especial atención a las posibles consecuencias discriminatorias para las personas rechazadas por el sistema. Además, con el fin de proteger el derecho del individuo a no estar sujeto a una medida que le afecte sobre la base exclusivamente de un tratamiento automatizado de los datos, deberán introducirse garantías adecuadas, tales como intervenciones humanas, soluciones o mecanismos que otorguen al interesado la posibilidad de defender su punto de vista.”

Por lo anterior, para evitar que un tratamiento automatizado de datos biométricos vulnere los derechos de los clientes o los titulares de los datos, es

necesario que en la sucursal bancaria tenga previstas intervenciones humanas que puedan aplicar un mecanismo alternativo para identificar a las personas que sean rechazadas por el sistema.

4. Seguridad de los datos

En este rubro, si bien es cierto que la LFPDPPP y el Reglamento a la Ley consignan la obligación de establecer medidas de seguridad a los datos personales en su posesión, no pasa desapercibido la siguiente recomendación del documento mencionado:

> "Los datos recogidos y almacenados deberán estar debidamente asegurados. Los diseñadores de los sistemas deberán colaborar con expertos en seguridad a fin de garantizar que las vulnerabilidades en materia de seguridad se aborden adecuadamente, especialmente si los sistemas existentes se migran a internet."

Por lo anterior, se reitera la conveniencia de diseñar el sistema biométrico para el "Proyecto" en conjunto con el área interna de seguridad informática (o áreas análogas) y el área jurídica especializada en protección de datos personales.

5. Garantías para personas con necesidades especiales

Las personas mayores de edad, incapaces y/o cuyas huellas dactilares no pueden ser registradas o reconocidas pueden ser objeto de vulneración a sus derechos.

Al respecto, el documento recomienda lo siguiente:

> “Deberán establecerse garantías contra los riesgos de discriminación o estigmatización de las personas por razón de su edad o su incapacidad para registrarse”.

Por lo anterior, se reitera la recomendación del punto 3.Tratamiento automatizado.

6. Datos sensibles

Este tema ya ha sido abordado en apartados anteriores, sin embargo, no se omite señalar la recomendación que el Dictamen señala al respecto:[142]

> “Algunos datos biométricos pueden considerarse sensibles en el sentido del artículo 8 de la Directiva 95/46/CE[143] y, en particular, los

---

[142]Dictamen 3/2012 sobre la evolución de las tecnologías biométricas 00720/12/ES WP193, *op.cit.,* nota 10, p. 17.

[143] Artículo 8 Tratamiento de categorías especiales de datos
1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.
2. Lo dispuesto en el apartado 1 no se aplicará cuando:
a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o
b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o
c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o
d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o
e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.
3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas

datos que revelen el origen racial o étnico o los datos relativos a la salud…Con objeto de evaluar la sensibilidad de los datos tratados por un sistema biométrico, también deberá tenerse en cuenta el contexto del tratamiento".

"Tratamiento de datos sensibles: según algunos estudios, las huellas dactilares pueden revelar información étnica de la persona".[144]

Una de las fuentes que cita el Dictamen para sostener la afirmación anterior es la página de internet http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm, página especializada en el estudio de las huellas dactilares, la cual señala que a partir del tipo de arcos y bucles con que cuente una huella dactilar se puede determinar origen étnico del titular del dato.

Por lo anterior, se sostiene la recomendación señalada en el apartado del principio de consentimiento respecto a considerar a las huellas dactilares como datos

---

establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.
4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.
5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.
Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.
6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.
7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

[144]Dictamen 3/2012 sobre la evolución de las tecnologías biométricas 00720/12/ES WP193, *op. cit.* nota 10, p. 22.
El dictamen cita, como referencia a esta afirmación, las siguientes páginas de internet: *http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm* y *http://www.crimescene-investigator.net/fingerprintpatterns.html*

personales sensibles, y en consecuencia, realizar el tratamiento conforme a lo que dispone la LFPDPPP para este tipo de datos.

7. Otras recomendaciones específicas del Dictamen

Por último, el dictamen 3/2012 señala los siguientes problemas detectados en el uso de tecnologías que traten impresiones dactilares, los cuales se transcriben a efecto de tenerlos en cuenta para el diseño del sistema biométrico del "Proyecto" en concordancia con las recomendaciones anteriormente señaladas:

> "Existen problemas de protección de datos relacionados con el uso de las impresiones dactilares que pueden describirse brevemente de la manera siguiente:
> • Precisión: aunque las impresiones dactilares presentan un alto índice de precisión, esto puede fallar debido a limitaciones relacionadas con la información (baja calidad de los datos o proceso de adquisición no consistente) o la representación (rasgos seleccionados o calidad de los algoritmos de extracción). Esto puede dar lugar a falsos rechazos o a falsas correspondencias.
> • Impacto: la irreversibilidad del proceso puede reducir la posibilidad de un individuo para ejercer sus derechos o invalidar las decisiones adoptadas basándose en una identificación falsa. El confiar en la precisión de la toma de huellas dactilares puede hacer más difícil rectificar los posibles errores, dando lugar a consecuencias de gran envergadura para los individuos. Esto debe tenerse en cuenta al evaluar la proporcionalidad del tratamiento en relación con la decisión específica que deba adoptarse sobre la base de las impresiones dactilares. Debe también mencionarse que la falta de medidas de seguridad puede dar lugar a la usurpación de identidad, que puede tener un fuerte impacto para el individuo.
> • Vinculación: las impresiones dactilares proporcionan posibilidades de uso indebido, ya que los datos pueden estar vinculados con otras bases de datos. Esta posibilidad de vincularse con otras bases de datos puede dar lugar a usos no compatibles con los fines originales. Existen algunas técnicas, como la biometría convertible o la codificación biométrica, que pueden utilizarse para reducir el riesgo.
> • Tratamiento de datos sensibles: según algunos estudios, las imágenes de huellas dactilares pueden revelar información étnica de la persona[145].

[145] *http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm* y http://www.crimescene-investigator.net/fingerprintpatterns.html.

• Fin o fines ulteriores del tratamiento: el almacenamiento central de datos, especialmente en las grandes bases de datos, implica riesgos asociados a la seguridad de los datos, la vinculación y la desvirtuación de funciones. Esto permite, en ausencia de garantías, el uso de las impresiones dactilares para fines diferentes de los que justificaron originalmente el tratamiento.
• Consentimiento y transparencia: el consentimiento es una cuestión esencial en el uso de las impresiones dactilares para usos distintos de los policiales. Las impresiones dactilares pueden ser copiadas fácilmente de las impresiones dactilares latentes e incluso fotografías, sin conocimiento del individuo. Otras cuestiones relativas al consentimiento son las relacionadas con la obtención del consentimiento de los menores y el papel de los padres a este respecto (por ejemplo, para tomar las huellas dactilares en las escuelas), así como la validez del consentimiento para proporcionar las impresiones dactilares en un contexto laboral.
• Revocabilidad: los datos de impresiones dactilares son muy estables con el tiempo y deben considerarse irrevocables. Una plantilla de impresión dactilar podrá ser revocada con determinadas condiciones.
• Protección anti-suplantación: las impresiones dactilares pueden ser fácilmente recogidas debido a las múltiples huellas que deja una persona. Además, las impresiones dactilares falsas pueden utilizarse con muchos sistemas y sensores, especialmente cuando tales sistemas no incluyen medidas específicas antisuplantación.
El éxito de un ataque depende en gran medida del tipo de sensor (óptico, capacitivo, etcétera) y del material utilizado por el atacante".

CAPÍTULO VII

Costos de implementación de las recomendaciones de este estudio

CAPÍTULO VII Costos de implementación de las recomendaciones de este estudio

1. Costos por asesoría legal

Para la implementación de estas recomendaciones y el cumplimiento de la LFPDPPP la institución financiera puede contratar los servicios jurídicos de una consultora especialista en la materia.

Para determinar el costo de la implementación de las recomendaciones de este trabajo, se ha consultado a un despacho jurídico con especialidad de datos personales el monto de honorarios que cobraría por la prestación de los servicios necesarios para la implementación de estas recomendaciones para poder tomar una base, siendo dicha cotización la siguiente:[146]

Servicios jurídicos necesarios para la implementación de las recomendaciones	Cotización de honorarios
a. Corrección del Aviso de Privacidad y política de privacidad. b. Revisión del convenio con INE (transferencias). c. Acciones al interior de laorganización. I. Carta responsiva de los empleados que tenga contacto con las huellas. II. Cláusulas contractuales. III. Capacitación general. IV. Material de difusión.	$200,000 (doscientos mil pesos 00/100 M.N.)

[146] Honorarios consultados al despacho jurídico Hernández, Narváez, Yáñez y Asociados, S.C. el 12 de febrero de 2016, *http://www.hny.mx/*

2. Costos por consultoría técnica

Para la ejecución de las recomendaciones en materia de seguridad vertidas anteriormente es necesario apoyarse de los servicios profesionales de un especialista en materia de seguridad de la información. De acuerdo con el Anexo Técnico del INE, el cual forma parte integrante del Convenio de Apoyo y Colaboración del INE con las instituciones particulares (Anexo 3) y se adjunta al presente como **Anexo 6**, el flujo de la información y la operación del Sistema de Verificación es el siguiente:

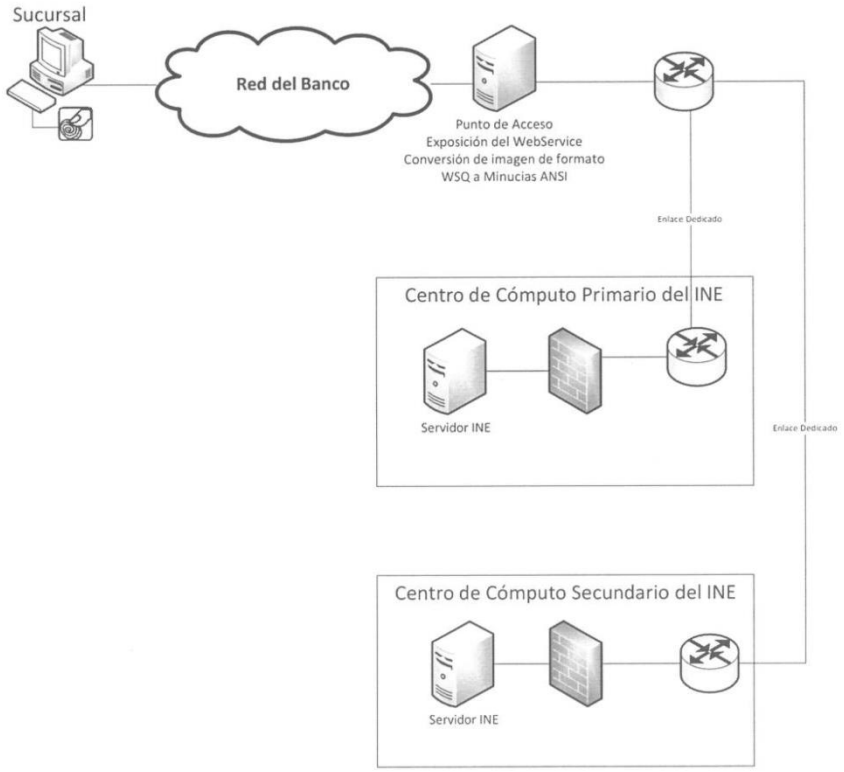


Ilustración 8. Arquitectura general de la solución con Portal de Verificación en la red del INE.

Imagen tomada del Anexo Técnico del INE (Anexo 6)

Para poder determinar una aproximación del costo que significaría para la institución financiera la aplicación de medidas de seguridad generales para que el

sistema brinde la protección técnica necesaria para los datos utilizados se tomará en cuenta la siguiente cotización:[147]

Cotización I (Únicamente con centro de cómputo primario)

Rubro	Componente	Características	Costo estimado en MXP[148]
Punto de acceso	Consultoría implementación de aplicativo	300 horas requeridas para la implementación de aplicación para conexión con el "web service" del INE.	$240,000.00
	Licencia de software para aplicación	Herramientas para desarrollo de aplicaciones (SDK) del lector BioMini/UF300 (Linux)	$13,110.00
	Lector de Huella Digital	Escáner dactilar compacto de altas prestaciones, certificado FIPS 201 Normas de formato NIST certificados interoperables plantilla / imagen (ISO19794-2/ISO19794-4/ANSI-378) Compresión de imagen estándar (WSQ)	$17.860.00[149]
Centro de datos	Cortafuegos	Cisco ASA 5510 Adaptive Security Appliance with AIP SSM-10 (chassis, software, 250 VPN peers, 4 Fast Ethernet interfaces, Triple Data Encryption Standard/Advanced Encryption Standard [3DES/AES])	$24,926.67
	Servidor	2 Servidores de procesamiento: • 2 procesadores Hexacore a 2.8 GHz. • 128 GB en RAM. • 500GB de Disco Duro a 15000 RPM en Raid 1. • 6 interfaces de 1000 • 2 interfaces independientes de fibra canal (HBA) • Fuentes redundantes	$1,182,002.00

[147] Cotización proporcionada por el Lic. en Informática Oscar Adrián Sánchez, egresado de MDTIC de INFOTEC.
[148] Incluye costo de fletes, importación e IVA calculado el 19 de febrero de 2016.
[149] Se cotizan 10 unidades.

		• Chasis tipo rack (incluir rieles de montaje para gabinete de 19 pulgadas). • Sistema operativo Linux, con virtualización activa y soporte técnico durante la vigencia del convenio.[150]	
		Instalación.	$11,791.00
	Almacenamiento	PowerVault NX400, Intel®Xeon®E5-2403v2, 1.8GHz, 8GB Mem 3 Teras	$90,589.00
Enlace dedicado	Servicio de internet dedicado	El servicio Internet Dedicado permite conectar la red de la institución de una manera directa a un puerto dedicado de la red mundial de Internet, a través de un enlace privado y exclusivo de última milla.[151]	$108,000.00
		Gran total:	1,688,278.67 Por tres años de servicios

[150] La cotización del servicio incluye soporte durante tres años.
[151] Costos calculados por 3 años de servicio.

Cotización 2 (Con los dos centros de cómputo)

Rubro	Componente	Características	Costo estimado en MXP[152]
Punto de acceso	Consultoría implementación de aplicativo	300 horas requeridas para la implementación de aplicación para conexión con el "web service" del INE.	$240,000.00
	Licencia de software para aplicación	Herramientas para desarrollo de aplicaciones (SDK) del lector BioMini/UF300 (Linux	$13,110.00
	Lector de Huella Digital	Escáner dactilar compacto de altas prestaciones, certificado FIPS 201 Normas de formato NIST certificados interoperables plantilla / imagen (ISO19794-2/ISO19794-4/ANSI-378) Compresión de imagen estándar (WSQ)	$17.860.00[153]
Centro de datos primario y secundario	Cortafuegos	2 Cisco ASA 5510 Adaptive Security Appliance with AIP SSM-10 (chassis, software, 250 VPN peers, 4 Fast Ethernet interfaces, Triple Data Encryption Standard/Advanced Encryption Standard [3DES/AES])	$49,853.34
	Servidor	4 Servidores de procesamiento: • 2 procesadores Hexacore a 2.8 GHz. • 128 GB en RAM. • 500GB de Disco Duro a 15000 RPM en Raid 1. • 6 interfaces de 1000 • 2 interfaces independientes de fibra canal (HBA) • Fuentes redundantes • Chasis tipo rack (incluir rieles de montaje para gabinete de 19 pulgadas). • Sistema operativo Linux, con virtualización activa y	$2,364,004.00

[152] Incluye costo de fletes, importación e IVA calculado el 19 de febrero de 2016.
[153] Se cotizan 10 unidades.

		soporte técnico durante la vigencia del convenio.[154]	
		2 Instalaciones.	$23,582.00
	Almacenamiento	2 PowerVault NX400, Intel®Xeon®E5-2403v2, 1.8GHz, 8GB Mem 3 Teras	$181,178.00
Enlace dedicado	Servicio de Internet dedicado	2 servicios de Internet Dedicado que permitan conectar la red de la institución de una manera directa a un puerto dedicado de la red mundial de Internet, a través de un enlace privado y exclusivo de última milla.[155]	$216,000.00
		Gran total:	3,105,587.34

[154] La cotización del servicio incluye soporte durante tres años.
[155] Costos calculados por 3 años de servicio.

Conclusiones

Primera. Cumplimiento de la ley de protección de datos.

Las huellas dactilares que se utilizarán en el “Proyecto” son datos personales de acuerdo a la LFPDPPP, como se explicó en este trabajo, por ende, a los responsables del tratamiento de estas huellas les aplica la normatividad mexicana en materia de datos personales.

Ahora bien, los datos biométricos al ser perenes, inmutables, únicos e irrepetibles para cada persona, son datos con una naturaleza distinta a otro tipo de datos personales, pues los biométricos a diferencia de otro tipo de datos, como la dirección de una persona o su teléfono, no pueden ser modificados si llegaran a caer en manos de terceros no autorizados. Ante esto, se considera que los datos biométricos requieren protección adicional y adecuada a su naturaleza, sin embargo, en la legislación mexicana en materia de datos personalesno se cuenta actualmente con regulación o recomendaciones de la autoridad especiales para el tratamiento de datos biométricos, incluyendo a las huellas dactilares.

Actualmente en la LFPDPPP solo se contempla protección especial para los datos sensibles, sin embargo, a pesar de que los datos biométricos poseen una naturaleza más sensible que otro tipo de datos, no se pueden considerar como datos sensibles de *facto* de acuerdo a la definición actual de datos sensibles de la LFPDPPP, para que gozaran de aquella protección adicional de la ley.

No obstante lo anterior, en virtud de que el término “datos de identificación biométrica” fue integrado en la definición de “datos sensibles” en el Proyecto de reforma del artículo 3, fracción VI de la LFPDPPP mencionada en este estudio, además de que diversas fuentes y autores concuerdan en considerar a los datos biométricos como datos sensibles, en este trabajo se recomienda que el tratamiento de las huellas dactilares en el “Proyecto” se realice en apego a la normativa mexicana de datos personales como si se trataran de datos sensibles.

Así, siendo las huellas dactilares datos personales, cuyo tratamiento se recomienda como el de los datos sensibles, que no cuentan con regulación ni recomendaciones oficiales para su tratamiento, se realizan las recomendaciones de este trabajo como una guía para las instituciones financieras para la implementación y operación del “Proyecto” a efecto de que este sistema cumpla con la normatividad en materia de datos personales y mejores prácticas aplicables al caso.

El seguimiento de las recomendaciones deberá realizarse con apoyo de profesionales del derecho y técnicos especializados en protección de datos personales y biometría.

Segunda. Cumplimiento de la ley desde el diseño.

Si bien es cierto la LFPDPPPP no señala como obligación de los responsables adoptar sistemas biométricos de determinadas características, también lo es que dicha ley y su Reglamento contienen obligaciones generales en materia de seguridad que los responsables deben cumplir, por lo que para prevenir violaciones a la seguridad de las huellas dactilares de los usuarios bancarios es recomendable apostar por la implementación de sistemas biométricos de calidad y medidas de seguridad adecuadas al interior de la institución financiera de que se trate, esto es, ante las diferentes tecnologías existentes en el mercado, se debe dar preferencia a aquellas que ofrezcan mayor fiabilidad y seguridad de los datos.

Por esto, la implementación del sistema biométrico del “Proyecto” al interior de la institución financiera se debe realizar en conjunto con profesionales especialistas en seguridad de la información.

Dada la falta de recomendaciones por parte del INAI y de la regulación de los datos biométricos en la ley, y toda vez que las recomendaciones de la UE son instrumentos orientativos emitidos por un conjunto de países con años con delantera en la regulación y estudio de la protección de datos personales en comparación con

México, es que se exhorta a analizar las recomendaciones de la UE mencionadas o las que pudieran ser aplicables al “Proyecto” de acuerdo al diseño final del sistema.

Tercera. Alternativa para los rechazos o fallos del sistema.

A pesar de que la implementación del “Proyecto” conlleva beneficios para los usuarios de la banca (evitar fraudes y suplantaciones), es necesario por las razones expuestas en el cuerpo de este estudio, implementar en paralelo un medio secundario para identificar inequívocamente a los usuarios en caso de que el sistema de identificación de huellas dactilares no reconozca al usuario o tuviera alguna falla. Esto para evitar controversias jurídicas con los clientes y usuarios ante la eventual negativa del servicio al no ser identificados por el sistema.

Cuarta. Más vale prevenir que lamentar.

La implementación de las recomendaciones aquí vertidas no solo pueden prevenir a la institución financiera un quebranto millonario por las posibles multas que el INAI pudiera fincar en su contra por incumplimientos a la LFPDPPP, sino que también le permite crear en sus clientes confiablidad respecto al manejo de su información personal lo que puede generar fidelidad comercial.

Bibliografía

JAIN, ANIL K. y *et. al*., *Handbook of Biometrics,* Estados Unidos, Springer, 2008, p. 471.

ORNELAS NÚNEZ, Lina, “Características del modelo de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento”, en PINAR MAÑAS, José Luis y ORNELAS NÚNEZ, Lina (coords.), *La Protección de Datos Personales en México,* México, Tirant Lo Blanch, 2013, p. 117.

ORNELAS NÚÑEZ, Lina, “Los principios de la protección de datos personales”, en PINAR MAÑAS, José Luis y ORNELAS NÚNEZ, Lina (coords.), *La Protección de Datos Personales en México,* México, Tirant Lo Blanch, 2013, p. 72.

PESCHARD MARISCAL, Jaqueline, “El Derecho Fundamental a la Protección de Datos Personales en México”, en PINAR MAÑAS, José Luis y ORNELAS NÚÑEZ, Lina (coords.), *La Protección de Datos Personales en México*, México, Tirant Lo Blanch, 2013, pp. 22 y 23.

RECIO GAYO, Miguel, “Las transferencias nacional e internacional de datos personales”, en PIÑAR MAÑAS, José Luis y ORNELAS NÚÑEZ, Lina (coords.), *La Protección de Datos Personales en México*, México, Tirant Lo Blanch, 2013, p. 212.

TENORIO CUETO, Guillermo A., “Análisis crítico de la protección de datos en México”, *Los datos personales en México, perspectivas y retos de su manejo en posesión de los particulares,* Ed. Porrúa, México, 2012, p. 65.

VILLANUEVA, Ernesto y DÍAZ, Vannesa, *Derecho de las nuevas tecnologías (en el siglo xx derecho informático),* México, Oxford University Press, 2015, pp. 43 y 46.

Legislación

Acuerdo del Consejo General del Instituto Nacional Electoral, por el que se aprueba la implementación del Servicio de Verificación de los datos de la Credencial para Votar, que servirá para garantizar el derecho de protección de datos de los ciudadanos, contenidos en el Padrón Electoral, 2016, México.

Código Civil Federal, 1928, México.

Código de Comercio, 1889, México.

Constitución Política de los Estados Unidos Mexicanos, 1917, México.

Convención Americana sobre Derechos Humanos “Pacto de San José”, 1969.

Declaración Universal de los Derechos del Hombre, 1948.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, 1995, Unión Europea.

Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito, 2009, México.

Disposiciones de carácter general en materia de transparencia aplicables a las instituciones de crédito y sociedades financieras de objeto múltiple, entidades reguladas, 2014, México.

Ley de Instituciones de Crédito, 1990, México.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, con comentarios de Alberto Enrique Nava Garcés, Porrúa, 2011.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2002, México.

Ley sobre la Celebración de Tratados, 1992, México.

Pacto Internacional de Derechos Civiles y Políticos, 1966.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2011, México.

Jurisprudencia

Tesis P./J. 20/2014 (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. I, abril de 2014, p. 202.

Tesis: 1a. CCXVI/2014 (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima Época, t. I, mayo de 2014, p. 539.

Hemerografía

LEYVA, Jeanette, “Cotejarían con INE identidad en banca”, *El Financiero*, periódico de circulación nacional, 05 de marzo de 2015, México, p.4.

LEYVA, Jeanette, “Genera polémica el programa piloto de verificación de huella”, *El Financiero*, periódico de circulación nacional, 06 de marzo de 2015, México, p. 5.

HOPKINS, Richard, “An Introduction to Biometrics and Large Scale Civilian Identification”, *International Review of Law*, Computers and Tecnology, núm. 13, pp. 337-363.

DÍAZ, Vanessa, “Sistemas biométricos en materia criminal: un estudio comparado”, en *Revista IUS,* Instituto de Ciencias Jurídicas de Puebla, núm. 31, año VII, México, enero-junio, pp. 28-47

BERTELSEN REPETTO, Raúl, “Tratamientos de datos personales y protección de la vida privada”, *Cuadernos de extensión jurídica*, núm. 5, Universidad de los Andes, Santiago de Chile, 2001.

Fuentes electrónicas

“Agencia Española de Protección de Datos: Proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. Informe 368/2006”. Recuperado de: *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/calidad/common/pdfs/2006-0368_Proporcionalidad-del-tratamiento-de-la-huella-dactilar-de-alumnos-de-un-colegio.pdf*

"Bases teóricas y sistemas biométricos", *Revista Red y Seguridad*, UNAM, México, s/n, Recuperado de: *http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/caracteristicassistema.html*

BLACKMER, Scott y *et. al.,* "Russia Amends Federal Data Protection Law, Privacy Enforcement on the Rise", *Information Law Group*, 19 de Julio de 2011. Recuperado de: *http://www.infolawgroup.com/2011/07/articles/international-2/russia-amends-federal-data-protection-law-privacy-enforcement-on-the-rise/*

BUENO DE MATA, Federico, *Biometría: el uso de las TICS como medio de identificar presuntos autores de hechos delictivos*, México, UNAM- Instituto de Investigaciones Jurídicas UNAM, s/f, p. 132. Recuperado de: *http://biblio.juridicas.unam.mx/libros/6/2940/9.pdf*

CHONG MAGALLANES, Jahtziri, "Detienen a servidor público del IMSS por falsificar huellas digitales para checar asistencias", *Noticias MVS*, 20 de agosto de 2012. Recuperado de: *http://www.noticiasmvs.com/#!/noticias/detienen-a-servidor-publico-del-imss-por-falsificar-huellas-digitales-para-checar-asistencias-535*

"Clasificación de los sistemas biométricos", *Revista Red y Seguridad*, UNAM, México, s/n. Recuperado de: *http://redyseguridad.fi-p.unam.mx/Proyectos/biometria/clasificacionsistemas/recohuella.html*

"Clonan huellas digitales: modalidad permitiría pasar sistemas de seguridad biométricos", *Buenos Días Perú*, 08 de abril de 2015. Recuperado de: *https://www.youtube.com/watch?v=0cIcjwBDXHs y http://panamericana.pe/buenosdiasperu/locales/179775-clonan-huellas-digitales-mafia-suplantaba-postulantes-universidad*

"Comité consultivo de la Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal (T-PD)", 2005. Recuperado de: *http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/informe-principios-convencion-108.pdf*.

CORNEJO, Valentino T., "Detrás de la huella", *Revista Istmo Liderazgo con Valores,* edición 277, 2014. Recuperado de: *http://istmo.mx/2005/03/detras_de_la_huella/*

CRISALDO, Robert y *et. al*, "Un enfoque de integración entre fprint y SourceAFIS", *Universidad Nacional de Asunción*, Paraguay, s/f. Recuperado de: *http://www.pol.una.py/cia/sites/default/files/files/Integracion_Fprint_SourceAFIS.pdf*

DÍAZ, Vanessa, "El ejercicio de los derechos arco ante el flujo transfronterizo de información biométrica", *Derecho y TIC, vertientes actuales,* UNAM, México, 2016, p. 121. Recuperado de: *http://biblio.juridicas.unam.mx/libros/libro.htm?l=4065*

Dictamen 3/2012 sobre la evolución de las tecnologías biométricas 00720/12/ES WP 193, adoptado el 27 de abril de 2012 por el Grupo de Trabajo sobre Protección de Datos del Artículo 29 de la Directiva 95/46/CE. Recuperado de: *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm*

"Dictamen de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares", p. 32, Recuperado de: *http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf*

Documento de trabajo sobre biometría 12168/02/ES WP 80, adoptado el 1 de agosto de 2003 por el Grupo de Trabajo sobre Protección de Datos del Artículo 29 de la Directiva 95/46/CE. Recuperado de: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_es.pdf

ESPINOSA MADRIGAL, Carmina Cecilia, "Robo de Identidad y Consecuencias Sociales", Documento de Trabajo, Coordinación de Seguridad de la Información, UNAM-CERT, 16 de junio de 2011. Recuperado de: *http://www.seguridad.unam.mx/documento/?id=16*

"Estándares biométricos", *Revista Red y Seguridad*, UNAM, México, s/n. Recuperado de: *http://redyseguridad.fi-p.unam.mx/proyectos/biometria/estandares/estandar.html*

"Falsificación de huellas dactilares en control de acceso", *Cybertronics Security*, 2014. Recuperado de: *https://www.youtube.com/watch?v=S2cp5j8sgN8*

"Fundamentos de Biometría", *Facultad de Ingeniería- Biometría Informática*, UNAM, s/f. Recuperado de: *http://redyseguridad.fi-p.unam.mx/Proyectos/biometria/*

"Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares", Instituto Federal de Acceso a la Información y Protección de Datos, 2014. Recuperado de: *http://inicio.inai.org.mx/SitePages/ifai.aspx*

"Guía Práctica para la atención de las solicitudes de ejercicio de los Derechos ARCO", Instituto Federal de Acceso a la Información y Protección de Datos, s/f. Recuperado de: *http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf*

http://www.crimescene-investigator.net/fingerprintpatterns.html

http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm

"Instituciones bancarias adoptarán el uso de huella digital", *Informador.mx*, s.f. Recuperado de: *http://www.informador.com.mx/economia/2015/579756/6/instituciones-bancarias-adoptaran-el-uso-de-huella-digital.htm*

KELKBOOMC, Emile y *et. al*., “Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure”, *Revista Electronic Commerce Research and Applications*, 2011, Países Bajos. Recuperado de*: http://www.jeroenbreebaart.com/papers/ecra/ecra2011.pdf*

LEYVA, Jeanette, “Estalla polémica por prueba piloto de INE-Banamex”, *El Financiero*, 06 de marzo de 2015. Recuperado de: *http://www.elfinanciero.com.mx/economia/estalla-polemica-por-prueba-piloto-de-ine-banamex.html*

MARTÍNEZ, Ana, “Pagos con huella digital revolucionan e-commerce”, *El Financiero*, 15 de abril de 2014. Recuperado de: *http://www.elfinanciero.com.mx/tech/pagos-con-huella-digital-revolucionan-e-commerce.html*

ORTEGA GARCÍA, Javier y *et. al*, Biometría y Seguridad, Universidad Autónoma de Madrid, España, 2008, p. 65. Recuperado de: *http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/09/CUADERNO-N%C2%BA-3.pdf*

O’TOOLE, James, “¿Cómo funciona Apple Pay?”, *CNN Expansión*, Estados Unidos, 20 de octubre de 2014. Recuperado de: *http://www.cnnexpansion.com/tecnologia/2014/10/20/como-funciona-apple-pay*

PIÑAR MAÑAS, José Luis, “¿Existe la privacidad”, *Compendio de Protección de Datos Personales*, México, IFAI, 2010, p.29. Recuperado de: *http://inicio.ifai.org.mx/Publicaciones/CompendioProteccionde Datos8.pdf*

“Proyecto de decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados”. Recuperado de: *http://gaceta.diputados.gob.mx/PDF/63/2016/may/20160503-I.pdf.*

“Proyecto de Decreto que reforma el artículo 3o. y adiciona un párrafo al 8o. de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares”, Gaceta Parlamentaria Cámara de Diputados, año XVI, número 3890-IV, martes 22 de octubre de 2013. Recuperado de: *http://gaceta.diputados.gob.mx/Gaceta/62/2013/oct/20131022-IV.html*

RIVERO, Mario y GOTTSCHALK, Franz, “Los Ataques de Skimming en Cajeros Automáticos y Cómo Prevenirlos”, *VISA*, 26 de febrero de 2014, p. 5. Recuperado de: *http://usa.visa.com/download/merchants/Webinar-Preventing-ATM-Skimming-Spanish-021914.pdf*

REMOLINA ANGARITA, Nelson, “Sistemas de identificación biométrica y protección de datos personales: ni “tecnofobia”, ni “tecnofascinación”, pero sí “tecnoreflexión”, *Ámbito Jurídico.com*, 16 de noviembre de 2011. Recuperado de: *http://www.ambitojuridico.com/BancoConocimiento/N/noti-111116-06_sistemas_de_identificacion_biometrica_y_proteccion_de_datos_pe/noti-*

111116-06_sistemas_de_identificacion_biometrica_y_proteccion_de_datos_pe.asp

ROJAS GONZÁLEZ, Isai y SÁNCHEZ PÉREZ, Gabriel, "Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I", *Revista de Seguridad y Defensa Digital: Cultura de prevención para ti*, UNAM, México, número 13, revista bimestral, 2012. Recuperado de: *http://revista.seguridad.unam.mx/numero-14/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-p*

RUBIO, Francisco, "INE no otorgará el padrón electoral a los bancos: Consejero", *Noticias MVS*, 5 de marzo de 2015. Recuperado de: *http://www.noticiasmvs.com/#!/noticias/ine-no-otorgara-el-padron-electoral-a-los-bancos-consejero-196.html*

SÁNCHEZ ONOFRE, Julio, "Banca fija su mirada en la tecnología biométrica", *El Economista*, 30 de septiembre de 2013. Recuperado de: *http://eleconomista.com.mx/tecnociencia/2013/09/30/banca-fija-su-mirada-tecnologia-biometrica*

"Tipología de Instrumentos Internacionales", Comisión Económica para América Latina y el Caribe, Organización de las Naciones Unidas, Perú, 2013, p. 7. Recuperado de: *http://www.cepal.org/rio20/noticias/noticias/1/50791/2013-861_PR10_Tipologia_instrumentos.pdf*

TOLOSA BORJA, César y GIZ BUENO, Álvaro, *Sistema Biométricos*, España, Universidad de Castilla-La Mancha, 2009-2010. Recuperado de: *http://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf*

VILDJIOUNAITE, Elena, "Soft biometrics—combining body weight and fat measurements with fingerprint biometrics", *Pattern Recognition Letters*, vol. 27, 1 de abril 2006, p. 325. Recuperado de: *www.elsevier.com/locate/patrec*

VITERBO, Pedro, "Los bancos incrementan la seguridad con la biometría" en *Revista Dintel Alta Dirección, s/n.* Recuperado de: *http://www.revistadintel.es/Revista/Numeros/Numero1/Seguridad/Publica/Viterbo.pdf*

ZAMORA, Angélica, "Seguridad biométrica: La banca del futuro", *Revista Summa*, s/n, 7 de febrero de 2014. Recuperado de: *http://www.deloitte.com/view/es_HN/hn/prensa/deloitte-en-medios/bdb1700b56c14410VgnVCM3000003456f70aRCRD.htm*

Anexo 1.

Anexo Único “Documento completo – Opinión técnica sobre el servicio de verificación de Datos de la Credencial para Votar”, emitido por el INAI.

CONACYT
Consejo Nacional de Ciencia y Tecnología

INFOTEC

Coordinación de Protección de Datos Personales
Dirección General de Autorregulación
Dirección General de Normatividad, Consulta y Atención Regional
Mayo de 2015

Anexo Único

Documento completo

Opinión técnica sobre el Servicio de Verificación de Datos de la Credencial para Votar

Contenido

I. Glosario

Anexo Técnico 3.2	Anexo Técnico del Convenio de apoyo y colaboración entre el Instituto Nacional Electoral "EL INE" y "LA INSTITUCIÓN" Versión 3.2, mediante oficio INE/DERFE/356/2015.
CPEUM	Constitución Política de los Estados Unidos Mexicanos.
Derechos ARCO	Derechos de acceso, rectificación, cancelación y oposición.
DERFE	Dirección Ejecutiva del Registro Federal de Electores.
INAI o Instituto	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos.
INE	Instituto Nacional Electoral.
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
LFTAIPG	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
LGIPE	Ley General de Instituciones y Procedimientos Electorales.
LGP	Ley General de Población.
LOAPF	Ley Orgánica de la Administración Pública Federal.
Lineamientos ARCO	Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores.
Manifestación de datos personales	Manifestación de protección de datos personales recabados por el Registro Federal de Electores.
Recomendaciones	Recomendaciones en materia de Seguridad de Datos Personales.
RINEMTAIP	Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública.
RLFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Servicio de Verificación	Servicio de Verificación de Datos de la Credencial para Votar.
SGSDP	Sistema de Gestión de Seguridad de Datos Personales.

II. Descripción general del Servicio de Verificación de Datos de la Credencial para Votar

Con el objeto de dar a conocer al Instituto el alcance, objetivos y operación del Servicio de Verificación el INE manifestó lo siguiente:

> "El Instituto, a través de la Dirección Ejecutiva del Registro Federal de Electores, contempla implementar un servicio de verificación de datos de la Credencial para Votar, para que las instancias públicas y privadas estén en posibilidad de revisar la información concerniente al ciudadano en términos de su vigencia y autenticidad.
>
> **1. Objetivos del servicio**
>
> a) Verificar la vigencia y coincidencia de los datos de la Credencial para Votar (CPV) que presenten los ciudadanos para identificarse ante una institución pública o privada, respecto de la información almacenada en la base de datos del Padrón Electoral. (Esta acción ya se realiza actualmente a través del servicio de consulta permanente de la Lista Nominal de Electores en la página de internet del Instituto).
>
> b) Autenticar las huellas dactilares del ciudadano que se identifique con una Credencial para Votar, mediante la correlación gráfica de las marcas dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en la base de datos con lo almacenado en el Padrón Electoral.
>
> **2. Descripción del servicio**
>
> El servicio consiste en establecer los mecanismos y esquemas de seguridad necesarios de apoyo y colaboración, por los que el Instituto a través de la Dirección Ejecutiva del Registro Federal de Electores, verificará la vigencia de las credenciales para votar que presenten los ciudadanos para identificarse ante instituciones públicas y privadas, cotejando que los datos contenidos en estas Credenciales, coincidan con los que obran en poder del Instituto. Lo anterior conforme a los términos de lo que se asiente dentro de los Anexos Técnicos de los convenios que para el efecto se firmen con las instituciones interesadas.
>
> El Instituto en ningún caso y bajo ningún motivo proporcionará información confidencial de los ciudadanos a través del servicio de verificación de la Credencial para Votar. Tampoco se permitirá el acceso a la información, bases de datos ni sistemas internos de información o de bases de datos del Instituto. Es importante señalar que el servicio únicamente indicará de manera afirmativa o negativa, si la información de las Credenciales para Votar presentadas ante las instituciones en comento, corresponde con la que tiene el Instituto en la base de datos del Padrón Electoral.
>
> El servidor tampoco podrá ser compartido con personas físicas o morales nacionales o extranjeras, sino que será de manera exclusiva para las instituciones que firmen los convenios respectivos.
>
> Para el caso de la huella digital, el Instituto realizará la confrontación de la información proporcionada por la institución, con la que se tiene registrada en la base de datos del Padrón Electoral mediante el uso estándar de minucias dactilares para el intercambio de datos denominado INCITS 378, que consiste en un método de comparación de la información de huellas dactilares a partir de minucias, que da como respuesta un porcentaje de similitud de acuerdo al mismo estándar. Este servicio se hará siempre y cuando la institución interesada

cuente con los equipos e infraestructura tecnológica necesaria para la captación de las huellas dactilares y su envío al Instituto, así como la autorización del ciudadano.

Es importante enfatizar que la verificación de la huella digital no implica la generación de una nueva base de datos, toda vez que no se estaría recabando dicho dato biométrico, sino que únicamente se compararían los datos que componen la huella digital con los que posee el Instituto y se tendría como resultado la coincidencia o no de éstos. En síntesis, si bien este proyecto implica el tratamiento de datos personales que obran en el Registro Federal de Electores, en la implementación de este mecanismo no se recabarían datos, y en consecuencia, no habría una base de datos *espejo*, sino que únicamente se utilizarían para corroborar coincidencias y brindar certeza, no sólo de que la Credencial es vigente, sino de que la persona que se identifica como alguien determinado, efectivamente es quien dice ser. Es de resaltar que en los Convenios de Apoyo y Colaboración que se suscriban para tal efecto, se establecerán de manera clara y puntual, las obligaciones de las partes, entre las cuales se encuentra la antes referida de tal forma que se dé estricto cumplimiento a las mismas y de lo contrario se deberán aplicar las sanciones y medidas necesarias a que haya lugar, como pudiera ser, la suspensión del servicio de verificación.

3. Procedimiento técnico del Servicio de Verificación de Datos de la Credencial para Votar.

Se tiene integrado un proyecto de Convenio de Apoyo y Colaboración, así como los Anexos Técnico y Administrativo-Económico correspondientes para establecer las condiciones y características del Servicio de Verificación de Datos de la Credencial para Votar con las instituciones públicas o privadas interesadas.

En el Anexo Técnico antes referido, se establecen las bases y mecanismos técnicos necesarios para que el Instituto pueda realizar la verificación de los datos de los ciudadanos, contenidos en la Credencial para Votar que soliciten las instituciones, considerando y garantizando la confidencialidad de la información proporcionada por los ciudadanos, así como los recursos tecnológicos y operativos de ambas instituciones.

A continuación se describen de manera general los aspectos más relevantes:

a. Esquema de operación.

Se establece el uso de un Portal de Verificación (*servicio Web*) encargado de recibir las solicitudes de las aplicaciones de consulta desarrolladas por la institución para enviarlas al Servidor de Verificación de Instituto, mismo que devolverá como respuesta la verificación de los datos recibidos respecto a los datos contenidos en la base de datos del Padrón Electoral. La base de datos sobre la cual operarán las consultas de datos, estará conformada con la información necesaria del Sistema Integral de Información del Registro Federal de Electores (SIIRFE), misma que será actualizada diariamente por el Instituto.

Se ha considerado que los datos en la Credencial para Votar que permitirían validar la vigencia del documento, y en su caso, autenticar mediante la huella dactilar que el ciudadano que porta la credencial es el mismo que realizó el trámite ante este Instituto, son los siguientes:

- OCR y/o CIC (Código de Identificación de la Credencial),
- Apellido Paterno,
- Apellido Materno,
- Nombre (s),

- Clave de Elector,
- Año de Registro,
- Número de emisión, y
- Huellas Dactilares de los dedos índices.

El INE proporcionará el servicio *Web* para las consultas de verificación de datos (texto y minucia) proporcionando únicamente como respuesta el estatus de vigencia de la Credencial, un código respecto de la coincidencia o no de los datos y para el caso de la comparación de las minucias de las huellas dactilares, el porcentaje de similitud mediante el uso de la minucia estándar INCITS 378.

La institución deberá proporcionar al Instituto la infraestructura de cómputo necesaria para la operación y administración de las aplicaciones para las consultas de verificación de datos, así como los equipos de seguridad perimetral. Estos equipos estarán ubicados en las instalaciones de este Instituto y serán operados por personal de la Dirección Ejecutiva del Registro Federal de Electores. Las cuotas de recuperación de mantenimiento de la infraestructura de cómputo serán a cargo de la institución interesada en el servicio y para las instituciones privadas se solicitará una cuota mensual de operación del servicio, la cual se establecerá en un Anexo Económico-Administrativo.

b. Infraestructura tecnológica y de comunicaciones.

La institución interesada en el servicio es responsable de contratar la instalación y operación de los enlaces de comunicación dedicados entre la institución y esta autoridad electoral, con el ancho de banda requerido para el adecuado funcionamiento del sistema que soportará las aplicaciones de consulta de verificación. Se establecerán los mecanismos de seguridad para que los datos viajen en modo seguro de la red de la institución y/o Negocios Adicionales hasta la red del Instituto. Los equipos y software requeridos para el aseguramiento de las comunicaciones entre el INE y la institución serán determinadas de forma conjunta y deberán ser provistas por la institución interesada.

c. Mecanismos de seguridad.

Con el propósito de garantizar la confidencialidad de la información, se detallan aspectos de seguridad relacionados con que la información que entregue la institución al INE será utilizada únicamente para la validación de la misma; el acceso al servicio *Web* por parte de la institución será exclusivamente a través de los medios que establezca el INE para el protocolo *Hyper Text Transfer Protocol Secure* (HTTPS); el certificado *SSL* del servidor será proporcionado por el INE; la institución no tendrá acceso a ningún sistema o infraestructura que opere en el INE. El INE mantendrá sincronizados los servidores que soportarán los sistemas a través de un servidor de tiempo vía *Network Time Protocol* (NTP), con el objetivo de identificar las transacciones de acuerdo a la fecha y hora en que éstas se lleven a cabo.

El INE y la institución pública o privada que se trate, establecerán los mecanismos de seguridad y los protocolos de comunicación permitidos y puertos de comunicación a utilizar, tanto para el acceso a los sistemas, como de comunicación entre ambas instituciones. El INE se reserva el derecho de detener los sistemas en caso de que se identifique o existan indicios de un incidente que altere la seguridad o en su defecto que dicho incidente sea crítico.

Se establecerá la conformación de un Comité Técnico integrado por personal del INE y de la institución pública o privada para evaluar periódicamente la operación del servicio y, en su caso, determinar los ajustes que se consideren necesarios para mejorar y garantizar los niveles de servicio, así como mantener y fortalecer los mecanismos de la seguridad de la información.

4. Beneficios

La implementación del servicio de verificación de datos de la Credencial para Votar, otorgará certeza a la prestación de bienes y servicios que otorgan las instituciones públicas y privadas a los ciudadanos, lo cual redundará en un beneficio concreto a la sociedad en general, ya que garantizará la efectiva protección de los datos personales de los ciudadanos como titulares de la información que proporcionan, de manera que se inhiban conductas ilícitas como el robo de identidad.

El mayor beneficio que trae a la sociedad la implementación del Servicio de Verificación de Datos de la Credencial para Votar, será la reducción al máximo de las operaciones con datos falsos o sustraídos a sus titulares, evitando así la vulneración o mal uso de datos personales, y evitando la afectación económica, social y jurídica de los ciudadanos y de las instancias públicas y/o privadas, ante quienes se realizan diversos trámites y solicitudes de servicios.

Lo anterior, tomando en cuenta que el robo de identidad se produce cuando una persona utiliza información personal de una persona física o moral con la intención de efectuar o vincularlo con algún fraude u otro delito.

La identidad la constituyen los datos personales como el nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y de seguridad social; números de tarjeta de crédito y de cuentas bancarias; nombres de usuario y contraseñas; incluyendo información financiera o médica, así como cualquier otro dato que permita identificar a una persona.

El robo de identidad causa serios problemas económicos, pero también afecta severamente la reputación de la víctima. Los efectos negativos en su reputación (historial crediticio, médico o criminal) y las subsecuentes dificultades para restablecer su credibilidad, son cuestiones que afectan la vida del individuo a escala social (pérdida de empleo, expulsión de círculos personales, profesionales o académicos, divorcios o separaciones, litigios legales, entre otras).

De igual forma, el uso de identidad falsa ante las diversas instituciones públicas o privadas, trae como consecuencia altos costos de servicios financieros (altas tasas de interés en tarjetas de crédito, créditos personales, créditos hipotecarios, etc.), incremento en el número de servicios médicos que deben ofrecer las instituciones de seguridad social, incremento en el costo de pólizas de seguros médicos, entre otras problemáticas sociales.

La implantación de un procedimiento que contribuya a reforzar la autenticidad de la actual identificación oficial de los mexicanos impulsa la credibilidad y confianza en las transacciones comerciales de cualquier índole en el País."

III. Esquema de aplicación de la LFTAIPG entre los sujetos obligados

La LFTAIPG se integra por cuatro títulos, el primero relativo a disposiciones comunes para los sujetos obligados, el segundo que refiere al acceso a la información en el Poder Ejecutivo Federal, el tercero que atañe al acceso a la información en los demás sujetos obligados y el cuarto relativo a responsabilidades y sanciones.

El título primero de la LFTAIPG comprende las disposiciones comunes para todos los sujetos obligados. En sus 27 artículos regula diversos aspectos sustantivos en materia de acceso a la información y protección de datos personales. Dichas disposiciones constituyen normas que aplican y obligan por igual a cualquiera de las autoridades, instituciones o entidades públicas reguladas por la LFTAIPG.

Por su parte, el artículo 61 de la LFTAIPG establece que el Poder Legislativo Federal, a través de la Cámara de Senadores, la Cámara de Diputados, la Comisión Permanente y la Auditoría Superior de la Federación; el Poder Judicial de la Federación a través de la Suprema Corte de Justicia de la Nación, del Consejo de la Judicatura Federal y de la Comisión de Administración del Tribunal Federal Electoral; los órganos constitucionales autónomos y los tribunales administrativos, en el ámbito de sus respectivas competencias, establecerán mediante reglamentos o acuerdos de carácter general, los órganos, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información, de conformidad con los principios y plazos establecidos en la misma.

De las disposiciones citadas se advierte que si bien es cierto existen una serie de elementos (órganos, criterios y procedimientos institucionales) que deben ser establecidos mediante reglamentos o acuerdos de carácter general por parte de los sujetos obligados citados en el artículo 61 de la LFTAIPG, también los es que todos los sujetos obligados están constreñidos a observar, entre otras, las disposiciones previstas en el capítulo IV del título primero. El citado capítulo contiene, esencialmente, el régimen al que debe sujetarse todo tratamiento de datos personales en el ámbito público federal, ya que en el mismo se prevén los principios y deberes a observar, así como los derechos con que cuenta todo titular respecto de su información personal para hacer efectivo su derecho fundamental a la protección de datos personales previsto en el artículo 16, segundo párrafo de la CPEUM.

Se estima de relevancia la aclaración antes formulada para efectos de conocer y fijar los alcances que tiene la LFTAIPG en su articulado en función del tipo de sujeto obligado respecto del que se hace el análisis.

Por lo anterior, en el caso específico y particular que es motivo de estudio en el presente documento, a continuación se llevará a cabo un análisis que tiene su punto de partida en lo dispuesto en el título primero, capítulo IV de la LFTAIPG, así como en las disposiciones que reglamenten, desarrollen o complementen el articulado ahí contenido.

IV. Aplicación de la LFTAIPG al INE en materia de datos personales

Los artículos 1 y 3, fracciones II y XIV y 4, fracción III de la LFTAIPG disponen lo que a continuación se indica:

> "**Artículo 1.** La presente Ley es de orden público. Tiene como finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.
>
> **Artículo 3.** Para los efectos de esta Ley se entenderá por:
> […]
>
> **XIV. Sujetos obligados:**
>
> **a)** El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República;
> **b)** El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos;
> **c)** El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;
> **d)** Los órganos constitucionales autónomos;
> **e)** Los tribunales administrativos federales, y
> **f)** Cualquier otro órgano federal.
>
> […]
>
> **Artículo 4.** Son objetivos de esta Ley:
> […]
>
> **III.** Garantizar la protección de los datos personales en posesión de los sujetos obligados;
> […]"

De las disposiciones anteriores, se desprende que la LFTAIPG tiene entre sus objetivos garantizar la protección de los datos personales en posesión del Poder Ejecutivo Federal, Poder Legislativo Federal, Poder Judicial de la Federación, órganos constitucionales autónomos, tribunales administrativos federales y cualquier otro órgano federal.

En términos del artículo 3, fracción XIV, inciso d de la LFTAIPG al INE le resultan aplicables las disposiciones previstas en dicho ordenamiento en lo que respecta al tratamiento de datos personales que lleve a cabo en el diseño, desarrollo, implementación y administración del Sistema de Verificación. Lo anterior, con fundamento en los artículos 41, fracción V, apartado A de la CPEUM y 29 de la LGIPE al ser el INE un organismo público autónomo.

V. Principios y derechos en materia de datos personales

1. Principio de licitud

El principio de licitud, a nivel constitucional, encuentra su fundamento en el principio de legalidad previsto en los artículos 14 y 16 de la CPEUM. Derivado del mismo, todo poder público está sujeto a la ley y, en consecuencia, todo acto suyo debe ser conforme a la misma, bajo pena de invalidez en caso de no cumplirlo.

En el contexto del derecho a la protección de datos personales, el artículo 36 del RINEMTAIP, aprobado en sesión ordinaria del Consejo General del INE el 02 de julio de 2014 mediante el Acuerdo INE/CG70/2014, dispone que en el tratamiento de datos personales que lleven a cabo servidores públicos del INE están obligados a observar, entre otros, el principio de licitud, el cual de acuerdo con los estándares internacionales y nacionales en la materia exige que todo tratamiento de datos personales, por parte de un responsable de carácter público, debe sujetarse a las facultades o atribuciones que la normatividad aplicable les confiera expresamente.

Es importante mencionar que el artículo 36 del RINEMTAIP establece que el Comité de Información del INE emitirá los lineamientos en los que se desarrollen los principios rectores de la protección de datos personales. No obstante, de acuerdo con lo informado por el INE en la reunión celebrada en este Instituto el 27 de febrero de 2015, no se han emitido dichos lineamientos, por lo que no existe documento normativo alguno en el que se detallen las características y alcances del documento mediante el cual se cumplirán los principios que rigen el tratamiento de datos.

En relación con el marco normativo que da sustento a su actuar, el INE manifestó lo siguiente:

> "El marco normativo sobre el que se implementa el "Servicio de Verificación de Datos de la Credencial" de manera expresa se encuentra regulado en el Título VI de los Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores.
>
> No obstante, la atribución para esta verificación tiene su soporte normativo en el marco de las responsabilidades del Instituto Nacional Electoral, a través de la Dirección Ejecutiva del Registro Federal de Electores para la expedición de la Credencial para Votar, así como la naturaleza dual que contiene al ser el instrumento primordial para ejercer el voto, y al mismo tiempo como el medio de identificación vigente más confiable y aceptado.
>
> Dicho marco normativo a continuación se detalla:
>
> - Constitución Política de los Estados Unidos Mexicanos.- Según lo previsto en el artículo 41, base V, Apartado A, el Instituto Nacional Electoral es un organismo público autónomo dotado de personalidad jurídica y patrimonio propio, en cuya integración participan el Poder Legislativo de la Unión, los partidos políticos nacionales y los ciudadanos, en los términos que ordene la ley. En el ejercicio de esta función estatal, la certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad serán principios rectores.
>
>   Por su parte, la citada disposición determina en el Apartado B, inciso a), numeral 3, que a este Instituto le corresponde, en los términos que establecen la Constitución y las leyes, el padrón y la lista de electores.
>
> - Ley General de Instituciones y Procedimientos Electorales.- En el marco de las atribuciones que la ley electoral le confiere a la Dirección Ejecutiva del Registro Federal de Electores, se encuentra la correspondiente a expedir la Credencial para Votar de conformidad con lo dispuesto en su artículo 54, párrafo 1, inciso c).

Por su parte el artículo 136, párrafo 1, establece que los ciudadanos tendrán la obligación de acudir a las oficinas o módulos que determine el Instituto, a fin de solicitar y obtener su Credencial para Votar.

El artículo 156 de la Ley Electoral en su párrafo 5 determina que la Credencial para Votar tendrá una vigencia de 10 años, contados a partir del año de su emisión, a cuyo término el ciudadano deberá solicitar una nueva credencial.

En el mismo sentido el artículo 131, párrafo 2 de la legislación electoral estipula que la Credencial para Votar es el documento indispensable para que los ciudadanos puedan ejercer su derecho de voto.

- Tesis Aislada XV/2011: La Credencial para Votar tiene naturaleza dual e indisoluble, al ser el instrumento primordial para ejercer el voto, y al mismo tiempo, el Medio de Identificación vigente más confiable y aceptado:

  CREDENCIAL PARA VOTAR CON FOTOGRAFÍA. AL PERDER VIGENCIA COMO INSTRUMENTO ELECTORAL, TAMBIÉN LA PIERDE COMO DOCUMENTO DE IDENTIFICACIÓN OFICIAL.- *De la interpretación de los artículos 35, fracciones I y II; 36, fracción I, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 6, párrafo 1, inciso b), y 200 del Código Federal de Instituciones y Procedimientos Electorales, y cuarto transitorio del Decreto expedido el veintidós de julio de mil novecientos noventa y dos, que reforma la Ley General de Población, se desprende que la credencial para votar con fotografía es, esencialmente, el documento oficial necesario para ejercer el derecho al voto el cual, además y en forma accesoria, sirve como medio de identificación oficial. Así, dada su naturaleza dual e indisoluble se concluye que, al perder su vigencia como instrumento electoral, también la pierde como documento de identificación oficial.*

  Cuarta Época:

  Recurso de apelación. SUP-RAP-109/2010.—Actor: Partido de la Revolución Democrática.—Autoridad responsable: Consejo General del Instituto Federal Electoral.—25 de agosto de 2010.—Unanimidad de votos.—Ponente: José Alejandro Luna Ramos.—Secretario: Eugenio Isidro Gerardo Partida Sánchez.
  La Sala Superior en sesión pública celebrada el trece de julio de dos mil once, aprobó por unanimidad de seis votos la tesis que antecede.

  Gaceta de Jurisprudencia y Tesis en materia electoral, Tribunal Electoral del Poder Judicial de la Federación, Año 4, Número 9, 2011, páginas 55 y 56.

De las disposiciones normativas citadas válidamente se arriba a la conclusión que al ser la Dirección Ejecutiva del Registro Federal de Electores, la responsable de expedir la Credencial para Votar, documento que tiene como función ser un medio de identificación para trámites administrativos, puede llevar a cabo la verificación de aquellas que son presentadas ante diversas instituciones públicas y privadas."

En alcance a las manifestaciones anteriores, el INE señaló lo que a continuación se indica:

"De conformidad con lo dispuesto en los artículos 12 y 54 de la Ley General de Instituciones y Procedimientos Electorales, una de las principales atribuciones de la Dirección Ejecutiva del Registro Federal de Electores es formar el Padrón Electoral revisarlo y mantenerlo actualizado permanentemente, conforme a los procedimientos establecidos en el Libro Cuarto de la propia Ley.

Cabe precisar, que el Padrón Electoral consta de la información básica de los varones y mujeres mexicanos mayores de 18 años, que se obtiene a través de la aplicación de la Técnica Censal total o parcial; por la inscripción directa y personal de los ciudadanos y la actualización de sus datos; o mediante la información que proporcionan las autoridades competentes relativas a fallecimientos y a la suspensión de derechos políticos de los ciudadanos, tal y como lo disponen los artículos 128 y 129 de la Ley instrumental en la materia.

Asimismo de conformidad con el artículo 154 de la Ley referida, y con el fin de mantener permanentemente actualizado el Padrón Electoral, la Dirección Ejecutiva del Registro Federal de Electores, recaba de los órganos de las administraciones públicas federales y estatales la información necesaria para registrar todo cambio que lo afecte, es decir:

- La de servidores públicos del Registro Civil quienes deberán informar al Instituto de los fallecimientos de ciudadanos.

- De jueces que dicten resoluciones que detecten la suspensión o pérdida de derechos políticos o la declaración de ausencia o presunción de muerte de un ciudadano así como la rehabilitación de los derechos políticos de los ciudadanos de que se trate.

- La de la Secretaría de Relaciones Exteriores quien deberá dar aviso al Instituto, cuando:

    a) Expida o cancele cartas de naturalización;
    b) Expida certificados de nacionalidad, y
    c) Reciba renuncias a la nacionalidad.

De igual forma a fin de mantener actualizado el Padrón Electoral el Instituto, a través de la Dirección Ejecutiva del Registro Federal de Electores se realiza anualmente una campaña intensa para convocar y orientar a la ciudadanía, a que acudan a incorporarse al Padrón Electoral, independientemente a esta campaña, la ciudadanía también pueden solicitar su inscripción al Padrón Electoral en periodos distintos, pues los ciudadanos también participan en la actualización del Padrón Electoral ya que tienen la obligación de inscribirse en el Registro Federal de Electores e informar a este de su cambio de domicilio dentro de los 30 días siguientes a que este ocurra, de acuerdo con lo dispuesto por los artículos 130, 138 y 142 de la Ley en la materia

Es así que con base en el Padrón Electoral, la Dirección Ejecutiva del Registro Federal de Electores expedirá, en su caso, las Credenciales para Votar; a aquellos ciudadanos que hayan acudido a las oficinas o módulos que determine el Instituto, a fin de solicitar y obtener su Credencial para Votar con fotografía, tal y como lo disponen los artículos 134 y 136 de la Ley en comento, en los términos manifestados desde la propia exposición de motivos, en la que precisa que la Credencial para votar "tiene carácter de documento de identidad ciudadana" con vigencia de 10 años contados a partir del al año de emisión, a cuyo término el ciudadano deberá solicitar una nueva credencial, procedimiento con el cual se actualizará nuevamente las huellas, fotografía, el domicilio y en general los datos de todos aquellos ciudadanos a los que se les venza su credencial.

Por otra parte se debe considerar que la Credencial para Votar es en la actualidad el documento oficial tanto para ejercer el derecho al voto, como el medio de identificación más utilizado por los ciudadanos mexicanos para los diferentes trámites ante instituciones tanto públicas como privadas; lo cual ayuda a que el Registro Federal de Electores dentro de sus actividades permanentes actualice los datos de todos aquellos ciudadanos que requieren identificarse con datos recientes en los diversos trámites que realizan ante las entidades del sector público como del sector privado, lo que redunda en actualización permanente del Padrón Electoral.

De ésta manera la Credencial para Votar tiene una naturaleza dual e indisoluble, que ha sido reconocida por el Tribunal Electoral del Poder Judicial de la Federación en sus resoluciones, tal como se cita en la siguientes Tesis:

Tesis XV/2011
CREDENCIAL PARA VOTAR CON FOTOGRAFÍA. AL PERDER VIGENCIA COMO INSTRUMENTO ELECTORAL, TAMBIÉN LA PIERDE COMO DOCUMENTO DE IDENTIFICACIÓN OFICIAL.- De la interpretación de los artículos 35, fracciones I y II; 36, fracción I, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 6, párrafo 1, inciso b), y 200 del Código Federal de Instituciones y Procedimientos Electorales, y cuarto transitorio del Decreto expedido el veintidós de julio de mil novecientos novena y dos, que reforma la Ley General de Población**, se desprende que la credencial para votar con fotografía es, esencialmente, el documento oficial necesario para ejercer el derecho al voto el cual, además y en forma accesoria, sirve como medio de identificación oficial.** Así, dada su naturaleza dual e indisoluble se concluye que, al perder su vigencia como instrumento electoral, también la pierde como documento de identificación oficial.

Cuarta Época:
Recurso de apelación. SUP-RAP-109/2010.- Actor: Partido de la Revolución Democrática.- Autoridad responsable: Consejo General del Instituto Federal Electoral.- 25 de agosto de 2010.- Unanimidad de votos.- Ponente: José Alejandro Luna Ramos.- Secretario: Eugenio Isidro Gerardo Partida Sánchez.

La Sala Superior en sesión pública celebrada el trece de julio de dos mil once, aprobó por unanimidad de seis votos la tesis que antecede.
Gaceta de Jurisprudencia y Tesis en materia electoral, Tribunal Electoral del Poder Judicial de la Federación, Año 4, Número 9, 2011

El efecto de ser el documento oficial de identificación de los mexicanos, proviene del Decreto por el que se modificó la Ley General de Población, para la instrumentación del Registro Nacional de Ciudadanos el 22 de julio de 1922, ya que en su artículo Cuarto Transitorio, se establece que: **en tanto no se expida la Cédula de Identidad Ciudadana, la Credencial para Votar servirá como medio de identificación personal en trámites administrativos, de acuerdo a los convenios que para tal efecto suscriba la autoridad electoral.**

De esta manera, el Instituto ha celebrado diversos convenios con Instituciones públicas y privadas, a efecto de que la Credencial para Votar pueda ser utilizada por los ciudadanos como medio de identificación, teniendo como referencia que el Instituto desde 1992 y hasta el año 2014, ha celebrado 124 convenios con diversos estados, dependencias e Instituciones públicas y privadas con el objeto de que la Credencial para Votar sea aceptada como medio de identificación, tal como se describen en el anexo adjunto.

Cabe señalar que en el clausulado de dichos convenios se estipula la leyenda mediante la cual se especifica el uso de la credencial como medio de identificación, siempre y cuando sea vigente, que sus datos sean claros y no contenga tachaduras o enmendaduras, de tal manera que los ciudadanos se preocupen en solicitar una nueva credencial ante un deterioro prematuro o la perdida de vigencia, ya que de otra manera no les será aceptada por las instituciones. Este supuesto tiene una nueva repercusión directa en la actualización del Padrón Electoral, ya que la nueva solicitud permite captar y asentar los datos más recientes del ciudadano tanto en el Padrón como en el listado nominal.

Para mayor precisión se transcribe la cláusula referida:

"OCTAVA.- La vigencia de la credencial para votar, con fotografía, será por el periodo comprendido en dicho documento, no siendo válida si presenta tachaduras o enmendaduras o carece de firma, huella digital o fotografía. Las perforaciones realizadas en la misma con motivo de su uso en comicios locales o federales, no se consideran como alteración."
En este sentido, proporcionar a las Instituciones Públicas y Privadas un "Servicio de Verificación de Datos de la Credencial para Votar", previo consentimiento de los ciudadanos y garantizando la seguridad de la información de sus datos personales, contribuye para que la Dirección Ejecutiva del Registro Federal de Electores cumpla con las

> obligaciones impuestas por la Ley, de mantener un Padrón Electoral actualizado, auténtico y confiable, pues como resultado de la verificación de aquellas Credenciales que hayan perdido su vigencia, se extravíen, o sobre las cuales se hacen correcciones de datos de la persona o el domicilio; tiene como consecuencia directa que el ciudadano mantenga actualizada su Inscripción, de tal manera que la verificación de datos entre las instituciones públicas y/o privadas con el Instituto, coadyuva en la actualización permanente del Padrón Electoral."

Conforme a lo planteado en la consulta que motivó la presente opinión técnica, el proyecto tiene por objeto la validación y cotejo de los datos personales contenidos en la credencial para votar a efecto de conocer la autenticidad y/o vigencia de la misma, a partir de información que conforma el Padrón Electoral.

En un ejercicio estrictamente descriptivo, a partir de lo manifestado por el INE respecto del proyecto de referencia, se advierten los siguientes elementos:

1. La solicitud para que se preste el Servicio de Verificación tiene por objeto corroborar la vigencia y coincidencia de los datos de la credencial para votar que presentan los ciudadanos.
2. Los datos personales de las credenciales para votar se verificarían contra los que obran en la base de datos del Padrón Electoral.

En este sentido, a efecto de determinar si el tratamiento de datos personales que llevaría a cabo el INE en el marco del Servicio de Verificación se apega al principio de licitud, resulta necesario analizar a partir de la CPEUM, la LGIPE y la LGP, las siguientes cuestiones:

1) Las atribuciones del INE y la utilización del Padrón Electoral para el Servicio de Verificación.
2) Los alcances de la normativa respecto del uso de la credencial para votar como medio de identificación.

1.1. Las atribuciones del INE y la utilización del Padrón Electoral para el Servicio de Verificación

En el presente apartado se hará un análisis que tiene por objeto revisar el marco normativo constitucional, legal, reglamentario y administrativo para corroborar si el INE está facultado para prestar el Servicio de Verificación y si para tal fin está autorizado para utilizar el Padrón Electoral. El análisis se hará en tal sentido, ya que una cuestión no necesariamente puede llevar a la otra.

1.1.1 Marco constitucional y legal en materia electoral

El artículo 41, fracción V, apartados A y B de la CPEUM señala lo que a continuación se indica:

> "**Artículo 41.** El pueblo ejerce su soberanía por medio de los Poderes de la Unión, en los casos de la competencia de éstos, y por los de los Estados, en lo que toca a sus regímenes interiores, en los términos respectivamente establecidos por la presente Constitución Federal y las particulares de los Estados, las que en ningún caso podrán contravenir las estipulaciones del Pacto Federal.
> […]
>
> **V.** La organización de las elecciones es una función estatal que se realiza a través del Instituto Nacional Electoral y de los organismos públicos locales, en los términos que establece esta Constitución.
>
> **Apartado A.** El Instituto Nacional Electoral es un organismo público autónomo dotado de personalidad jurídica y patrimonio propio, en cuya integración participan el Poder Legislativo de la Unión, los partidos políticos nacionales

y los ciudadanos, en los términos que ordene la ley. En el ejercicio de esta función estatal, la certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad serán principios rectores.

Apartado B. Corresponde al Instituto Nacional Electoral en los términos que establecen esta Constitución y las leyes:

…
3. El padrón y la lista de electores;
…

Los artículos 30, 31 numeral 1, los artículos 32, 54, 126, 127, 128, 130, 133 numerales 1 y 2, los artículos 134, 138 y 154 de la LGIPE prevén lo siguiente:

"**Artículo 30.**
1. Son fines del Instituto:

a) Contribuir al desarrollo de la vida democrática;

b) Preservar el fortalecimiento del régimen de partidos políticos;

c) Integrar el Registro Federal de Electores;

d) Asegurar a los ciudadanos el ejercicio de los derechos político-electorales y vigilar el cumplimiento de sus obligaciones;

e) Garantizar la celebración periódica y pacífica de las elecciones para renovar a los integrantes de los Poderes Legislativo y Ejecutivo de la Unión, así como ejercer las funciones que la Constitución le otorga en los procesos electorales locales;

f) Velar por la autenticidad y efectividad del sufragio;

g) Llevar a cabo la promoción del voto y coadyuvar a la difusión de la educación cívica y la cultura democrática, y

h) Fungir como autoridad única para la administración del tiempo que corresponda al Estado en radio y televisión destinado a los objetivos propios del Instituto, a los de otras autoridades electorales y a garantizar el ejercicio de los derechos que la Constitución otorga a los partidos políticos en la materia.
[…]

Artículo 31.

1. El Instituto es autoridad en la materia electoral, independiente en sus decisiones y funcionamiento y profesional en su desempeño.
[…]

Artículo 32.

1. El Instituto tendrá las siguientes atribuciones:
a) Para los procesos electorales federales y locales:

I. La capacitación electoral;

II. La geografía electoral, que incluirá la determinación de los distritos electorales y su división en secciones electorales, así como la delimitación de las circunscripciones plurinominales y el establecimiento de cabeceras;

III. El padrón y la lista de electores;

IV. La ubicación de las casillas y la designación de los funcionarios de sus mesas directivas;

V. Las reglas, lineamientos, criterios y formatos en materia de resultados preliminares; encuestas o sondeos de opinión; observación electoral; conteos rápidos; impresión de documentos y producción de materiales electorales, y
VI. La fiscalización de los ingresos y egresos de los partidos políticos y candidatos.

b) Para los procesos electorales federales:

I. El registro de los partidos políticos nacionales;

II. El reconocimiento a los derechos y el acceso a las prerrogativas de los partidos políticos nacionales y de los candidatos a cargos de elección popular federal;

III. La preparación de la jornada electoral;

IV. La impresión de documentos y la producción de materiales electorales;

V. Los escrutinios y cómputos en los términos que señale esta Ley;

VI. El cómputo de la elección de Presidente de los Estados Unidos Mexicanos en cada uno de los distritos electorales uninominales;

VII. La declaración de validez y el otorgamiento de constancias en las elecciones de diputados y senadores;

VIII. La educación cívica en procesos electorales federales, y

IX. Las demás que le señale esta Ley y demás disposiciones aplicables.

2. Además de las anteriores, el Instituto, en los términos que establece esta Ley, contará con las siguientes atribuciones:

a) La organización de la elección de los dirigentes de los partidos políticos, cuando éstos lo soliciten y con cargo a sus prerrogativas, en los términos que establezca la Ley;

b) La elección y remoción del Consejero Presidente y los Consejeros Electorales de los Organismos Públicos Locales;

c) Suscribir convenios con órganos del Poder Ejecutivo Federal que establezcan los mecanismos de coordinación y aseguren cooperación en materia de inteligencia financiera;

d) La verificación de los requisitos, así como la organización, desarrollo, cómputo y declaración de resultados de las consultas populares a que se refiere la fracción VIII del artículo 35 de la Constitución;

e) Verificar el porcentaje requerido por la fracción IV del artículo 71 de la Constitución, para la presentación de iniciativas de leyes o decretos por parte de los ciudadanos;

f) Asumir directamente la realización de las actividades propias de la función electoral que corresponde a los Organismos Públicos Locales, en los términos de esta Ley;
g) Delegar las atribuciones a los Organismos Públicos Locales, sin perjuicio de reasumir su ejercicio directo en cualquier momento;

h) Atraer a su conocimiento cualquier asunto de la competencia de los Organismos Públicos Locales, cuando su trascendencia así lo amerite o para sentar un criterio de interpretación;

i) Emitir criterios generales para garantizar el desarrollo de los mecanismos de participación ciudadana previstos en las leyes federales que para tal efecto se emitan, con el fin de que los ciudadanos participen, individual o colectivamente, en las decisiones públicas, y

j) Las demás que le señale esta Ley y demás disposiciones aplicables.

Artículo 54.

1. La Dirección Ejecutiva del Registro Federal de Electores tiene las siguientes atribuciones:

a) Aplicar la técnica censal en forma parcial en el ámbito territorial que determine la Junta General Ejecutiva;

b) Formar el Padrón Electoral;

c) Expedir la credencial para votar según lo dispuesto en el Título Primero del Libro Cuarto de esta Ley;

d) Revisar y actualizar anualmente el Padrón Electoral conforme al procedimiento establecido en el Libro Cuarto de esta Ley;

e) Establecer con las autoridades federales, estatales y municipales la coordinación necesaria, a fin de obtener la información sobre fallecimientos de los ciudadanos, o sobre pérdida, suspensión u obtención de la ciudadanía;

f) Proporcionar a los órganos competentes del Instituto y a los partidos políticos nacionales y candidatos, las listas nominales de electores en los términos de esta Ley;

g) Formular, con base en los estudios que realice, el proyecto de división del territorio nacional en 300 distritos electorales uninominales, así como el de las cinco circunscripciones plurinominales;

h) Mantener actualizada la cartografía electoral del país, clasificada por entidad, distrito electoral federal, distrito electoral local, municipio y sección electoral;

i) Asegurar que las comisiones de vigilancia nacional, estatales y distritales se integren, sesionen y funcionen en los términos previstos por esta Ley;

j) Llevar los libros de registro y asistencia de los representantes de los partidos políticos a las comisiones de vigilancia;

k) Solicitar a las comisiones de vigilancia los estudios y el desahogo de las consultas sobre los asuntos que estime conveniente dentro de la esfera de su competencia;

l) Acordar con el Secretario Ejecutivo del Instituto los asuntos de su competencia;

m) Asistir a las sesiones de la Comisión del Registro Federal de Electores sólo con derecho de voz;

n) Proceder a la verificación del porcentaje de ciudadanos inscritos en la lista nominal de electores requerido para solicitar consulta popular o iniciar leyes o decretos ante el Congreso de la Unión, en términos de lo previsto en las leyes, y

ñ) Las demás que le confiera esta Ley.

2. Para coadyuvar en los trabajos relativos al Padrón Electoral se integrará la Comisión Nacional de Vigilancia, que presidirá el Director Ejecutivo del Registro Federal de Electores, con la participación de los partidos políticos nacionales.

"**Artículo 126.**

1. El Instituto prestará por conducto de la dirección ejecutiva competente y de sus vocalías en las juntas locales y distritales ejecutivas, los servicios inherentes al Registro Federal de Electores.

2. El Registro Federal de Electores es de carácter permanente y de interés público. Tiene por objeto cumplir con lo previsto en el artículo 41 constitucional sobre el Padrón Electoral.

3. Los documentos, datos e informes que los ciudadanos proporcionen al Registro Federal de Electores, en cumplimiento de las obligaciones que les impone la Constitución y esta Ley, serán estrictamente confidenciales y no podrán comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en los que el Instituto fuese parte, para cumplir con las obligaciones previstas por esta Ley, en materia electoral y por la Ley General de Población en lo referente al Registro Nacional Ciudadano o por mandato de juez competente.

4. Los miembros de los Consejos General, locales y distritales, así como de las comisiones de vigilancia, tendrán acceso a la información que conforma el Padrón Electoral, exclusivamente para el cumplimiento de sus funciones y no podrán darla o destinarla a finalidad u objeto distinto al de la revisión del Padrón Electoral y las listas nominales.

Artículo 127.

1. El Registro Federal de Electores será el encargado de mantener actualizado el Padrón Electoral.

Artículo 128.

1. En el Padrón Electoral constará la información básica de los varones y mujeres mexicanos, mayores de 18 años que han presentado la solicitud a que se refiere el párrafo 1 del artículo 135 de esta Ley, agrupados en dos secciones, la de ciudadanos residentes en México y la de ciudadanos residentes en el extranjero."

Artículo 130.

1. Los ciudadanos están obligados a inscribirse en el Registro Federal de Electores y a informar a éste de su cambio de domicilio dentro de los treinta días siguientes a que éste ocurra.

2. Asimismo, los ciudadanos participarán en la formación y actualización del Padrón Electoral en los términos de las normas reglamentarias correspondientes.

Artículo 133.

1. El Instituto se encargará de formar y administrar el padrón electoral y la lista de electores.

2. El Instituto emitirá los lineamientos en los que se establezcan los plazos y términos para el uso del padrón electoral y las listas de electores en los procesos electorales locales.
[…]"

Artículo 134.

1. Con base en el Padrón Electoral, la Dirección Ejecutiva del Registro Federal de Electores expedirá, en su caso, las credenciales para votar.

Artículo 138.

1. A fin de actualizar el Padrón Electoral, el Instituto, a través de la Dirección Ejecutiva del Registro Federal de Electores realizará anualmente, a partir del día 1o. de septiembre y hasta el 15 de diciembre siguiente, una campaña intensa para convocar y orientar a la ciudadanía a cumplir con las obligaciones a que se refieren los dos párrafos siguientes.

2. Durante el periodo de actualización deberán acudir ante las oficinas de la Dirección Ejecutiva del Registro Federal de Electores, en los lugares que ésta determine, para ser incorporados al Padrón Electoral todos aquellos ciudadanos:

a) Que no hubiesen sido incorporados durante la aplicación de la técnica censal total, y
b) Que hubiesen alcanzado la ciudadanía con posterioridad a la aplicación de la técnica censal total.

3. Durante el periodo de actualización también deberán acudir a las oficinas los ciudadanos incorporados en el Padrón Electoral que:

a) No hubieren notificado su cambio de domicilio;
b) Hubieren extraviado su credencial para votar, y
c) Suspendidos en sus derechos políticos hubieren sido rehabilitados.

4. Los ciudadanos al acudir voluntariamente a darse de alta o dar aviso de cambio de domicilio, o bien al ser requeridos por el personal del Instituto durante la aplicación de la técnica censal, tendrán la obligación de señalar el domicilio en que hubieren sido registrados con anterioridad y, en su caso, firmar y poner las huellas dactilares en los documentos para la actualización respectiva.

5. Los partidos políticos nacionales y los medios de comunicación podrán coadyuvar con el Instituto en las tareas de orientación ciudadana.

Artículo 154.

1. A fin de mantener permanentemente actualizado el padrón electoral, la Dirección Ejecutiva del Registro Federal de Electores recabará de los órganos de las administraciones públicas federal y estatal la información necesaria para registrar todo cambio que lo afecte.

2. Los servidores públicos del Registro Civil deberán informar al Instituto de los fallecimientos de ciudadanos, dentro de los diez días siguientes a la fecha de expedición del acta respectiva.

3. Los jueces que dicten resoluciones que decreten la suspensión o pérdida de derechos políticos o la declaración de ausencia o presunción de muerte de un ciudadano así como la rehabilitación de los derechos políticos de los ciudadanos de que se trate, deberán notificarlas al Instituto dentro de los diez días siguientes a la fecha de expedición de la respectiva resolución.

> **4.** La Secretaría de Relaciones Exteriores deberá dar aviso al Instituto, dentro de los diez días siguientes a la fecha en, que:
>
> **a)** Expida o cancele cartas de naturalización;
> **b)** Expida certificados de nacionalidad, y
> **c)** Reciba renuncias a la nacionalidad.
>
> **5.** Las autoridades señaladas en los párrafos anteriores deberán remitir la información respectiva en los días señalados, conforme a los procedimientos y en los formularios que al efecto les sean proporcionados por el Instituto.
>
> **6.** El presidente del Consejo General podrá celebrar convenios de cooperación tendentes a que la información a que se refiere este artículo se proporcione puntualmente."

De las disposiciones citadas destaca que el INE es la autoridad en materia electoral cuyo objetivo es contribuir al desarrollo de la vida democrática, preservar el fortalecimiento del régimen de partidos políticos, integrar el Registro Federal de Electores, asegurar a los ciudadanos el ejercicio de los derechos político-electorales, garantizar la celebración periódica y pacífica de las elecciones para renovar a los integrantes de los Poderes Legislativo y Ejecutivo de la Unión, así como ejercer las funciones que la Constitución Política le otorga en los procesos electorales locales, entre otras.

También se advierte que la DERFE, unidad administrativa adscrita al INE, cuenta con atribuciones para formar, revisar y actualizar anualmente el Padrón Electoral, así como expedir la credencial para votar según lo dispuesto en la LGIPE, por resaltar algunas de sus atribuciones.

De las disposiciones citadas se advierte que el Padrón Electoral es una base de datos en donde se encuentra la información, documentación e imágenes de los ciudadanos mexicanos mayores de 18 años que han solicitado su credencial para votar, destacando que la información que lo conforma no puede destinarse a una finalidad u objeto distinto al de la revisión del Padrón Electoral y las listas nominales.

En este sentido, se advierte que el Padrón Electoral tiene un uso eminentemente electoral, tan es así que el artículo 9 de la LGIPE señala que para el ejercicio del voto los ciudadanos deben, además de los requisitos que fija el artículo 34 constitucional, estar inscritos en el Registro Federal de Electores y contar con la credencial para votar.

Aunado a lo anterior, de conformidad con los artículos 54, 127 y 133 de la LGIPE el INE tiene la obligación de formar y administrar el Padrón Electoral, a través de la DERFE, así como emitir los lineamientos en los que se establezcan los plazos y términos para el uso del Padrón Electoral y las listas de electores en los procesos electorales locales, como es el caso de los lineamientos que resultan aplicables para los años 2014-2015.

En cuanto al Padrón Electoral conviene subrayar que su actualización implica para el INE:

a) Realizar una campaña intensa para convocar y orientar a la ciudadanía para acudir ante las oficinas de la DERFE para ser incorporados al Padrón Electoral todos aquellos ciudadanos que no hubiesen sido incorporados durante la aplicación de la técnica censal total; que hubiesen alcanzado la ciudadanía con posterioridad a la aplicación de la técnica censal total; que no hubieren notificado su cambio de domicilio; que hubieren extraviado su credencial para votar o hayan sido suspendidos en sus derechos políticos o hubieren sido rehabilitados.
b) Recabar de los órganos de las administraciones públicas federal y estatal la información necesaria para registrar todo cambio que lo afecte, tales como del Registro Civil la información sobre los fallecimientos de ciudadanos; de

los jueces las resoluciones que decreten la suspensión o pérdida de derechos políticos o la declaración de ausencia o presunción de muerte de un ciudadano, así como la rehabilitación de los derechos políticos de los ciudadanos de que se trate, o bien, de la Secretaría de Relaciones Exteriores sobre la expedición de cartas de naturalización, certificados de nacionalidad y renuncias a la nacionalidad.

De la lectura de la CPEUM y la LGIPE se advierte la ausencia de alguna disposición que aludiera expresamente a las atribuciones del INE para prestar el Servicio de Verificación y para el uso del Padrón Electoral para dicho Servicio.

1.1.2 Marco normativo constitucional y legal en materia de identidad

Los artículos 4 y 36, fracción I de la CPEUM disponen lo siguiente:

"**Artículo 4°.-**
[…]

Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento.
[…]

"**Artículo 36.-** Son obligaciones del ciudadano de la República:

I. Inscribirse en el catastro de la municipalidad, manifestando la propiedad que el mismo ciudadano tenga, la industria, profesión o trabajo de que subsista; así como también inscribirse en el Registro Nacional de Ciudadanos, en los términos que determinen las leyes.

La organización y el funcionamiento permanente del Registro Nacional de Ciudadanos y la expedición del documento que acredite la ciudadanía mexicana son servicios de interés público, y por tanto, responsabilidad que corresponde al Estado y a los ciudadanos en los términos que establezca la ley.
[…]"

Por su parte, los artículos 85, 86, 88, 97, 98, 101 y 104 de la LGP establecen lo siguiente:

"**Artículo 85.-** La Secretaría de Gobernación tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero.

Artículo 86.- El Registro Nacional de población tiene como finalidad registrar a cada una de las personas que integran la población del país, con los datos que permitan certificar y acreditar fehacientemente su identidad.

Artículo 88.- El Registro Nacional de Ciudadanos se integra con la información certificada de los mexicanos mayores de 18 años, que soliciten su inscripción en los términos establecidos por esta ley y su reglamento.

Artículo 97.- El Registro Nacional de Ciudadanos y la expedición de la Cédula de Identidad Ciudadana son servicios de interés público que presta el Estado, a través de la Secretaría de Gobernación.

Artículo 98.- Los ciudadanos mexicanos tienen la obligación de inscribirse en el Registro Nacional de Ciudadanos y obtener su Cédula de Identidad Ciudadana.

> **Artículo 101.-**La Secretaría de Gobernación podrá verificar los datos relativos a la identidad de las personas, mediante la confrontación de los datos aportados por los ciudadanos con los que consten en los archivos correspondientes de dependencias y entidades de la Administración Pública que, para el ejercicio de sus funciones, tengan establecidos procedimientos de identificación personal.
>
> Las dependencias y entidades que se encuentren en el supuesto anterior estarán obligadas a proporcionar la información que para este efecto solicite la Secretaría de Gobernación.
>
> **Artículo 104.-**La Cédula de Identidad Ciudadana es el documento oficial de identificación, que hace prueba plena sobre los datos de identidad que contiene en relación con su titular."

El artículo 27, fracción XXXVI de la LOAPF señala lo siguiente:

> "**Artículo 27.-** A la Secretaría de Gobernación corresponde el despacho de los siguientes asuntos:
> […]
>
> XXXVI. Formular y conducir la política de población, salvo lo relativo a colonización, asentamientos humanos y turismo, así como manejar el servicio nacional de identificación personal, en términos de las leyes aplicables;
> […]"

De las disposiciones citadas destacan los siguientes elementos, respecto al derecho de identidad, en el marco jurídico mexicano:

a) Toda persona tiene derecho a la identidad, para lo cual es obligación de los ciudadanos mexicanos inscribirse en el Registro Nacional de Ciudadanos.
b) La Secretaría de Gobernación tiene a su cargo el registro y la acreditación fehaciente de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero.
c) El Registro Nacional de Ciudadanos y la expedición de la cédula de identidad ciudadana son servicios de interés público que presta el Estado, a través de la Secretaría de Gobernación.
d) El Registro Nacional de Ciudadanos se integra con la información certificada de los mexicanos mayores de 18 años, mientras que la cédula de identidad ciudadana es el documento oficial de identificación, la cual hace prueba plena sobre los datos de identidad que contiene en relación con su titular.

En este sentido, de acuerdo con el artículo 85 de la LGP, en relación con el artículo 27, fracción XXXVI de la LOAPF, la Secretaría de Gobernación es la autoridad competente para acreditar fehacientemente la identidad de las personas residentes en nuestro país, a través de la expedición de la cédula de identidad ciudadana.

Respecto a la credencial para votar el artículo cuarto transitorio del decreto que reforma y adiciona diversas disposiciones a la Ley General de Población, publicado en el Diario Oficial de la Federación el 22 de julio de 1992, dispone lo siguiente:

> "**CUARTO.-** En el establecimiento del Registro Nacional de Ciudadanos se utilizará la información que proporcionará el Instituto Federal Electoral proveniente del padrón electoral y de la base de datos e imágenes obtenidas con motivo de la expedición y entrega de la credencial para votar con fotografía prevista en el artículo 164 del Código Federal de Instituciones y Procedimientos Electorales. En tanto no se expida la cédula de identidad ciudadana, esta credencial podrá servir como medio de identificación personal en trámites administrativos de acuerdo a los convenios que para tal efecto suscriba la autoridad electoral."

De la disposición transcrita se advierte que hasta en tanto no se expida la cédula de identidad ciudadana, la credencial para votar podrá servir como medio de identificación personal en los trámites administrativos, de acuerdo con los convenios que para tal efecto suscriba el INE. A partir de lo anterior, la credencial para votar se constituye en un documento que permite el ejercicio de determinados derechos político electorales, así como en un documento que puede ser utilizado válidamente como medio de identificación. Esto último, hasta en tanto no se cumpla la condición de expedir la cédula de identidad ciudadana.

De la lectura de la CPEUM y de la LGP, se advierte la ausencia de alguna norma expresa relativa a las facultades del INE para prestar el Servicio de Verificación y para que el Padrón Electoral pudiera ser utilizado para el mencionado Servicio.

1.1.3 Marco normativo reglamentario y administrativo

El artículo 32 numeral 3 del RINEMTAIP prevé de forma expresa lo siguiente:

> "**Artículo 32. Del acceso a datos personales**
> […]
>
> 3. El acceso, rectificación, cancelación y oposición a los datos personales en posesión del Registro Federal de Electores se regirán conforme a los Lineamientos que presente la Comisión del Registro Federal de Electores a la aprobación del Consejo. Esos Lineamientos deberán ajustarse al procedimiento y plazos que establece el presente Reglamento. En estos Lineamientos se deberán prever los mecanismos por medio de los cuales se validen éstos datos a las instancias públicas y privadas que lo requieran y sobre la verificación de la emisión fehaciente de las credenciales para votar por parte del Instituto Nacional Electoral.
> […]"

En relación con lo anterior, el artículo 45 de los Lineamientos ARCO, dispone lo siguiente:

> "**45**. El Instituto por conducto de la Dirección Ejecutiva, a través de la suscripción de convenios de apoyo y colaboración y bajo mecanismos de seguridad, establecerá los procedimientos para verificar los datos personales que soliciten las instancias públicas y privadas, mediante el uso de tecnologías.
>
> Los convenios que se celebren con instancias privadas deberán establecer que los avisos de privacidad que éstas hubiesen elaborado de conformidad con la Ley de Protección de Datos Personales en Posesión de Particulares, incluyan como una posibilidad de tratamiento de datos personales la validación y verificación a que se refiere el presente Capítulo."

En los Lineamientos ARCO, concretamente en el capítulo VI denominado "De la validación o cotejo de datos personales proporcionados por instancias públicas y privadas y verificación de la emisión de la credencial para votar con fotografía", se establece el régimen general a través del cual se llevará a cabo esta validación o cotejo de datos de la credencial para votar, destacando las siguientes reglas:

a) La DERFE está obligada a establecer procedimientos para verificar los datos personales que soliciten las instancias públicas y privadas mediante el uso de tecnologías.
b) La verificación de los datos personales proporcionados por las instancias públicas o privadas se debe circunscribir exclusivamente a su cotejo con los datos personales que obren en el Registro Federal de Electores.
c) El mecanismo de verificación a que se hace referencia no constituye elemento para determinar la autenticidad de la credencial para votar.

Según se observa de la simple lectura, tanto el RINEMTAIP como los Lineamientos ARCO contienen disposiciones que expresamente refieren al Servicio de Verificación. De manera explícita establecen la posibilidad de que el INE preste el Servicio y que lo haga a partir del cotejo de los datos personales que obran en el Registro Federal de Electores.

1.1.4 Consideraciones respecto de las atribuciones del INE y la utilización del Padrón Electoral para el Servicio de Verificación

En materia electoral, en los artículos 41, fracción V, apartados A y B de la CPEUM y 30, 31 numeral 1, 32, 54, 130, 133 numerales 1 y 2, 134, 138 y 154 de la LGIPE se advierte la ausencia, de manera expresa, de alguna referencia que aludiera a las facultades del INE para prestar el Servicio de Verificación y para el uso del Padrón Electoral con motivo de dicho Servicio.

Por lo que refiere a identidad, en los artículos 4 y 36, fracción I de la CPEUM,85, 86, 88, 97, 98, 101 y 104, cuarto transitorio de la LGP y 27, fracción XXXVI de la LOAPF se advierte la ausencia, de manera expresa, de alguna referencia que aludiera a las atribuciones del INE para prestar el Servicio de Verificación y para el uso del Padrón Electoral con motivo de dicho Servicio.

Conforme a lo expuesto, en las disposiciones constitucionales y legales en materia electoral y/o de identidad se advierte la ausencia de manera expresa de una referencia normativa para que el INE preste el Servicio de Verificación y para la utilización del Padrón Electoral para el citado Servicio. Conforme a las manifestaciones del propio INE, el mencionado Servicio de Verificación ocurriría necesariamente en uno de los dos contextos apuntados, electoral o de identidad, por lo que en principio el sustento del actuar del INE al respecto debiera encontrarse en las normas constitucionales o legales electorales o de identidad, o bien, en algún desarrollo reglamentario o administrativo que derive de las mismas.

En donde sí se encontró una referencia expresa respecto al Servicio de Verificación fue en el RINEMTAIP y en los Lineamientos ARCO. Ambos instrumentos normativos contienen disposiciones que expresamente habilitan al INE para prestar el Servicio de Verificación, así como para el uso del Padrón Electoral para el cotejo de los datos, con lo que pareciera cumplirse con el principio de licitud.

Dado que a nivel constitucional o legal, en materia electoral o de identidad, se advierte la ausencia de una referencia expresa para la prestación del Servicio de Verificación, conviene cuestionarse sí el RINEMTAIP y los Lineamientos ARCO dan sustento para que el INE preste el Servicio apuntado válidamente y que lo haga a partir del cotejo de los datos personales que obran en el Registro Federal de Electores.

El RINEMTAIP y los Lineamientos ARCO constituyen un desarrollo que deriva de la LFTAIPG, en términos de lo establecido en el artículo 61. En tal sentido, conviene cuestionarse lo siguiente:

1. Si el RINEMTAIP y los Lineamientos ARCO, que se dio a sí mismo el INE con fundamento en el artículo 61 de la LFTAIPG, pueden suplir la ausencia de una norma constitucional o legal que expresamente refiera al Servicio de Verificación como parte de las facultades del INE.
2. Si el RINEMTAIP y los Lineamientos ARCO constituyen el espacio normativo correcto para establecer las habilitaciones necesarias para que el INE preste el Servicio de Verificación.

¿El RINEMTAIP y los Lineamientos ARCO, que se dio a sí mismo el INE con fundamento en el artículo 61 de la LFTAIPG, pueden suplir la ausencia de una norma constitucional o legal que expresamente refiera al Servicio de Verificación como parte de las facultades del INE?

Desde la óptica del derecho a la protección de datos personales, la habilitación del INE para prestar el Servicio de Verificación así como la autorización para el uso del Padrón Electoral para el mismo, basados en el RINEMTAIP y los Lineamientos ARCO, se considera que es insuficiente para suplir la ausencia de una norma constitucional o legal que expresamente refiera al tema, ya que tanto el RINEMTAIP como los Lineamientos ARCO constituyen normas que tienen por objeto desarrollar elementos a partir de una base legal, cuestión que no puede ser de otro modo en el sistema jurídico mexicano. Es decir, dichos instrumentos no están diseñados o concebidos para prever cuestiones novedosas respecto de lo que una ley prevé.

Lo anterior, deviene de los efectos que provoca el esquema constitucional de división de poderes que establece la CPEUM, que se encuentra erigido a partir de un esquema de pesos y contrapesos que pretende distribuir de manera equilibrada el ejercicio del poder público a cargo del Estado. Así las cosas, de este esquema constitucional deriva el principio de reserva de ley, en virtud del cual se delimita un espacio para que determinados aspectos regulatorios sean directa y exclusivamente desarrollados, con mayor o menor detalle, por el órgano encargado de la función legislativa.

Confirma lo anterior, la tesis jurisprudencial que a continuación se cita:

> "Época: Novena Época
> Registro: 172521
> Instancia: Pleno
> Tipo de Tesis: Jurisprudencia
> Fuente: Semanario Judicial de la Federación y su Gaceta
> Tomo XXV, Mayo de 2007
> Materia(s): Constitucional
> Tesis: P./J. 30/2007
> Página: 1515
>
> FACULTAD REGLAMENTARIA. SUS LÍMITES.
>
> La facultad reglamentaria está limitada por los principios de reserva de ley y de subordinación jerárquica. El primero se presenta cuando una norma constitucional reserva expresamente a la ley la regulación de una determinada materia, por lo que excluye la posibilidad de que los aspectos de esa reserva sean regulados por disposiciones de naturaleza distinta a la ley, esto es, por un lado, el legislador ordinario ha de establecer por sí mismo la regulación de la materia determinada y, por el otro, la materia reservada no puede regularse por otras normas secundarias, en especial el reglamento. El segundo principio, el de jerarquía normativa, consiste en que el ejercicio de la facultad reglamentaria no puede modificar o alterar el contenido de una ley, es decir, los reglamentos tienen como límite natural los alcances de las disposiciones que dan cuerpo y materia a la ley que reglamentan, detallando sus hipótesis y supuestos normativos de aplicación, sin que pueda contener mayores posibilidades o imponga distintas limitantes a las de la propia ley que va a reglamentar. Así, el ejercicio de la facultad reglamentaria debe realizarse única y exclusivamente dentro de la esfera de atribuciones propias del órgano facultado, pues la norma reglamentaria se emite por facultades explícitas o implícitas previstas en la ley o que de ella derivan, siendo precisamente esa zona donde pueden y deben expedirse reglamentos que provean a la exacta observancia de aquélla, por lo que al ser competencia exclusiva de la ley la determinación del qué, quién, dónde y cuándo de una situación jurídica general, hipotética y abstracta, al reglamento de ejecución competerá, por consecuencia, el cómo de esos mismos supuestos jurídicos. En tal virtud, si el reglamento sólo funciona en la zona del cómo, sus disposiciones podrán referirse a las otras preguntas (qué, quién, dónde y cuándo), siempre que éstas ya estén contestadas por la ley; es decir, el reglamento desenvuelve la

> obligatoriedad de un principio ya definido por la ley y, por tanto, no puede ir más allá de ella, ni extenderla a supuestos distintos ni mucho menos contradecirla, sino que sólo debe concretarse a indicar los medios para cumplirla y, además, cuando existe reserva de ley no podrá abordar los aspectos materia de tal disposición.
>
> Acción de inconstitucionalidad 36/2006. Partido Acción Nacional. 23 de noviembre de 2006. Unanimidad de diez votos. Ausente: José de Jesús Gudiño Pelayo. Ponente: Genaro David Góngora Pimentel. Secretarios: Makawi Staines Díaz, Marat Paredes Montiel y Rómulo Amadeo Figueroa Salmorán.
>
> El Tribunal Pleno, el diecisiete de abril en curso, aprobó, con el número 30/2007, la tesis jurisprudencial que antecede. México, Distrito Federal, a diecisiete de abril de dos mil siete."

Ahora bien, el hecho de considerar que las disposiciones del RINEMTAIP y los Lineamientos ARCO sean insuficientes para suplir la ausencia de una norma constitucional o legal que expresamente refiera a las facultades del INE en la materia, así como a la posibilidad de que el Padrón Electoral se use para prestar el Servicio de Verificación, tampoco significa que el INE carezca de facultades para la prestación del mencionado Servicio y que para tal efecto se le imposibilite hacer uso del Padrón Electoral. Para estar en posibilidades de desentrañar si el INE cuenta con las facultades para prestar el Servicio de Verificación y determinar si puede hacer uso del Padrón Electoral para el citado Servicio, sería necesario interpretar los textos constitucionales y/o legales analizados, cuestión para la cual este Instituto se encuentra imposibilitado jurídicamente por carecer de facultades al respecto.

¿El RINEMTAIP y los Lineamientos ARCO constituyen el espacio normativo correcto para establecer las habilitaciones necesarias para que el INE preste el Servicio de Verificación y para ello pueda hacer uso del Padrón Electoral?

En el contexto del derecho a la protección de datos personales, se estima que la temática relativa al Servicio de Verificación desarrollada en el RINEMTAIP y los Lineamientos ARCO es incompatible, en lo sustantivo, con aquella a la que alude el artículo 61 de la LFTAIPG, considerando que las disposiciones específicas relativas al citado Servicio carecen de elementos que tengan por objeto desarrollar cuestiones vinculadas con los órganos, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información o la protección de los datos personales, de conformidad con la LFTAIPG.

Confirma lo anterior, lo expresado por el INE en el sentido de que el Servicio de Verificación tiene como propósito primordial, revisar y mantener actualizado el Padrón Electoral, cuestión que por sí misma explica y confirma que se trata de una regulación que sustantivamente corresponde y, por tanto es propia, de la materia electoral, en todo caso.

En el supuesto de que la temática se ubicase en el contexto de la identidad, la conclusión no cambia, la regulación establecida por el INE sigue refiriendo a aspectos y procesos sustantivamente relacionados con cuestiones distintas a la protección de datos (en este caso identificación), con independencia de la vinculación tangencial que pueda tener con la citada protección de datos personales y otros derechos fundamentales.

El hecho de que el RINEMTAIP y los Lineamientos ARCO no constituyan el espacio normativo correcto para establecer las habilitaciones necesarias para que el INE preste el Servicio de Verificación y la posibilidad de que el Padrón Electoral se use para prestar el Servicio de Verificación, tampoco significa que el INE no posea atribuciones al respecto y que el Padrón Electoral no pueda utilizarse válidamente para prestar el Servicio. Para estar en posibilidades de desentrañar si el INE cuenta con las facultades para prestar el Servicio de Verificación y para determinar si puede hacer uso del Padrón Electoral en tal contexto, sería necesario interpretar los textos constitucionales y/o legales analizados, cuestión para la cual este Instituto se encuentra imposibilitado jurídicamente al no ser la instancia facultada para tal fin.

1.2 Los alcances de la normativa respecto del uso de la credencial para votar como medio de identificación

Conforme a la normativa citada y analizada, no hay lugar a dudas que la credencial para votar puede ser utilizada en su calidad de medio de identificación, conforme a lo establecido expresamente en el artículo cuarto transitorio de la LGP.

El artículo cuarto transitorio expresamente refiere a este atributo de la credencial para votar, al tenor de lo siguiente:

> "**CUARTO.-** En el establecimiento del Registro Nacional de Ciudadanos se utilizará la información que proporcionará el Instituto Federal Electoral proveniente del padrón electoral y de la base de datos e imágenes obtenidas con motivo de la expedición y entrega de la credencial para votar con fotografía prevista en el artículo 164 del Código Federal de Instituciones y Procedimientos Electorales. En tanto no se expida la cédula de identidad ciudadana, esta credencial podrá servir como medio de identificación personal en trámites administrativos de acuerdo a los convenios que para tal efecto suscriba la autoridad electoral."

De acuerdo con lo anterior, para efectos de protección de datos personales, es posible confirmar que uno de los tratamientos para los que está habilitada la credencial para votar es como medio de identificación, siempre que no haya sido expedida la cédula de identidad ciudadana.

En tal sentido, y conforme a las consideraciones anteriores, resulta relevante destacar lo siguiente:

1. Si bien es cierto, el INAI identificó referencia expresa en el RINEMTAIP y los Lineamientos ARCO para que el INE preste el Servicio de Verificación y la posibilidad de que el Padrón Electoral se use para prestar dicho Servicio, también lo es que sería recomendable que dicha referencia se encontrara de manera expresa en sede constitucional o legal.
2. A la ausencia de referencias normativas constitucionales o legales expresas **de ninguna manera se le pretende dar un alcance en el sentido de señalar que el INE carece de facultades para prestar el Servicio de Verificación y que no puede hacer uso del Padrón Electoral** para tal fin.
3. El sentido que se pretende dar, a partir de las consideraciones del presente documento, es que para determinar si el INE está facultado para la prestación del Servicio de Verificación a través del uso del Padrón Electoral **resulta necesario un ejercicio de interpretación.**
4. **El IFAI estaría imposibilitado para realizar cualquier tipo de interpretación**, por menor, simple o evidente que resulte, ya que en cualquier caso ésta impactaría en la fijación de los alcances de las disposiciones legales existentes en materia electoral o de identificación, cuestión que corresponde a instancias diversas conocer, en su caso.

Como se puede advertir, se considera de la mayor importancia que el Servicio de Verificación cuente con una base y fundamento legal que deje claro cuáles son las atribuciones con que cuenta el INE para prestar el Servicio de Verificación mediante el uso del Padrón Electoral, y en ese sentido se precisen puntalmente los alcances de su actuar. Todo ello en beneficio de la seguridad jurídica de los ciudadanos mexicanos.

Establecido lo anterior, y teniendo en cuenta que el INAI advirtió ausencia de **referencias normativas constitucionales y/o legales expresas** relativas al Servicio de Verificación, a continuación se hará un análisis técnico de cada uno de los principios, deberes, derechos y obligaciones en materia de transferencias, sin perjuicio de las consideraciones formuladas en materia de licitud.

El hecho de que el IFAI esté impedido para pronunciarse respecto del principio de licitud, por las razones indicadas, no obsta para analizar y emitir recomendaciones respecto del resto de los principios, deberes, derechos y obligaciones en materia de transferencias, ya que en modo alguno con este análisis se pretende cambiar el sentido de la conclusión obtenida respecto de las facultades del INE para prestar el Servicio de Verificación mediante el uso del Padrón Electoral.

2. Principio del consentimiento

De acuerdo con los estándares internacionales en la materia, por regla general, la causa que legitima o habilita determinado tratamiento de datos personales es el consentimiento o autorización del titular.

En la LFTAIPG el principio del consentimiento se encuentra normado sustantivamente en dos artículos. El artículo 21 establece que los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información. Por su parte, el artículo 22 en su proemio indica que no se requerirá el consentimiento de los individuos para proporcionar los datos personales en los casos que ahí se indica.

En ambos casos, se alude al consentimiento como elemento a partir del cual se habilita el tratamiento de datos personales. En el caso del artículo 21 de la LFTAIPG se establece la necesidad de recabar consentimiento expreso, por escrito o por un medio de autenticación similar cuando se pretenda difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información. En el supuesto del artículo 22 de la misma ley, se señala que salvo las seis hipótesis normativas ahí previstas, se debe recabar el consentimiento de los individuos, en una interpretación *contrario sensu*.

La regla general antes indicada suele presentar excepciones en al ámbito comparado y la normativa federal mexicana para el ámbito público no es la excepción. El artículo 22 de la LFTAIPG dispone lo siguiente:

> "**Artículo 22.** No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:
>
> **I.** (Se deroga).
> **II.** Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
> **III.** Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
> **IV.** Cuando exista una orden judicial;
> **V.** A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y
> **VI.** En los demás casos que establezcan las leyes."

Por su parte, en armonía con los supuestos descritos, el artículo 36 del RINEMTAIP señala que en el tratamiento de datos personales sus servidores públicos están obligados a observar el principio de consentimiento. Es importante señalar que el artículo 36 del RINEMTAIP, establece que el Comité de Información del INE emitirá los lineamientos en los que se desarrollen los principios rectores de la protección de datos personales. Sin embargo, de acuerdo con lo informado por el INE en la reunión celebrada en este Instituto el 27 de febrero de 2015, **no se han emitido dichos lineamientos**, por lo que no existe documento normativo alguno en el que se detallen los mecanismos para cumplir con el principio del consentimiento.

Para el presente análisis, conviene traer a colación las finalidades que motivan el diseño, implementación y operación del Sistema de Verificación, mismas que se advierten de los documentos proporcionados por el INE y que son fundamentalmente las siguientes:

- Verificar la vigencia y coincidencia de los datos de la credencial para votar que presentan los ciudadanos para identificarse ante una institución pública o privada, respecto de la información almacenada en la base de datos del Padrón Electoral.
- Autenticar las huellas dactilares del ciudadano que se identifique con una credencial para votar, mediante la correlación gráfica de las marcas dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en el Padrón Electoral.

Atendiendo al proyecto que nos ocupa y tomando como referencia las disposiciones vigentes que resultan aplicables en la materia, se advierte que en el marco del Servicio de Verificación, el INE estaría obligado a recabar el consentimiento de aquellos titulares cuyos datos de la credencial para votar sean objeto del Servicio, salvo que se actualice alguna de las excepciones previstas en el artículo 22 de la LFTAIPG.

Al respecto, el INE manifestó que en una cláusula del convenio se prevé que la institución privada está obligada a recabar en el aviso de privacidad el consentimiento del ciudadano, al tenor de lo siguiente:

> "En una cláusula del convenio está incorporado que la institución privada está obligada a recabar en el aviso de privacidad el consentimiento del ciudadano respecto de un uso de los datos de su Credencial para Votar para la verificación de los mismos a través del servicio de verificación. Cabe señalar que se va a agregar al sistema de verificación un campo de confirmación del consentimiento del titular a la institución pública o privada."

Lo anterior, se puede corroborar en la cláusula quinta incisos e y f del modelo de convenio de apoyo y colaboración que el INE suscribiría con las instituciones privadas en los siguientes términos:

> "QUINTA.- Las obligaciones de"_____", son las siguientes:
> […]
>
> e) Establecer en los avisos de privacidad que se elaboren de conformidad con la Ley de Protección de Datos Personales en Posesión de los Particulares, la posibilidad de verificación de los datos personales contenidos en la credencial para votar que los ciudadanos proporcionen a"_____".
>
> f) El aviso de privacidad, deberá contener un campo en el que se indique si el titular acepta o no, el tratamiento de sus datos personales para el Servicio de Verificación de datos de la Credencial para Votar. Dicho aviso de privacidad deber ser complementado con un campo de conformación del consentimiento de titular de los datos en el que expresamente acepte el cotejo de los datos que presenta con los del Servicio de Verificación de datos de la Credencial para Votar.
> […]"

A su vez, en el apartado 4.2.3.1, denominado Verificación de datos de la credencial para votar, del Anexo Técnico 3.2 del convenio de colaboración aludido se puede observar, entre los datos de entrada del servicio *web*, un campo obligatorio que refiere a la confirmación del consentimiento del titular de la credencial.

Antes de formular las consideraciones en torno al principio del consentimiento, se aclara que en este apartado no se abordará la procedencia y/o viabilidad de utilizar el aviso de privacidad como mecanismo para recabar el consentimiento, en este apartado no se hará mayor pronunciamiento, ya que el mismo es materia del principio de información.

Asimismo, se aclara que las cuestiones relacionadas con el consentimiento en el contexto de transferencias de datos, con instituciones públicas o privadas, serán abordadas en el apartado de transferencias del presente documento.

En el caso de los modelos de convenios de colaboración que el INE aportó, se identifican mecanismos a través de los cuales las instituciones privadas solicitarían el consentimiento de las personas que deseen ser objeto del Servicio de Verificación.

No obstante, si bien existe la previsión apuntada (la obligación de la institución privada de recabar el consentimiento), el consentimiento constituye una obligación a cargo del INE también, en su calidad de sujeto obligado de la LFTAIPG, y por lo tanto también le correspondería cumplir con esta obligación siempre que no se actualice alguno de los supuestos del artículo 22 de la LFTAIPG.

En tal sentido, en su caso, se considera necesario contar con un mecanismo de obtención del consentimiento, conforme a lo previsto en la LFTAIPG. Lo anterior, con independencia del cumplimiento de los principios y deberes que le corresponda a las instituciones públicas o privadas usuarias del Servicio de Verificación, conforme a la legislación aplicable.

Por lo que hace al sector público, es importante destacar que en el modelo de convenio de colaboración que el INE suscribiría con instituciones públicas se advierte la ausencia de mecanismos para solicitar el consentimiento de las personas que participen en el proceso del Servicio de Verificación. Al respecto, se considera importante se revise, caso por caso, la normativa aplicable y en función de ello se determine la necesidad de obtener el consentimiento y en dicha medida incorporar en los convenios que resulten aplicables la cláusula correspondiente.

Por lo que refiere a la obligación del INE de obtener el consentimiento de las personas que participen en el proceso del Servicio de Verificación, cabe señalar que la misma resulta exigible siempre e independientemente de la naturaleza pública o privada de la institución con quien suscriba el convenio, siempre que no se actualice alguno de los supuestos del artículo 22 de la LFTAIPG.

En virtud de lo anterior, en relación con el principio de consentimiento, el INAI emite las siguientes observaciones y recomendaciones:

1. De acuerdo con lo dispuesto en los artículos 21 y 22 de la LFTAIPG, que la obtención del consentimiento se haga de manera previa al tratamiento de datos personales para el Servicio de Verificación.

2. Que el consentimiento se obtenga de manera:

    a. Libre, sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.
    b. Específica, referido a una o varias finalidades determinadas que justifiquen el tratamiento.
    c. Informada, que el titular tenga conocimiento previo de la existencia y características del tratamiento a que serán sometidos sus datos personales.
    d. Expresa, lo cual se traduce en que la voluntad del titular se manifieste de forma escrita.
    e. Inequívoca, esto es la existencia de elementos que de manera indubitable demuestren su otorgamiento.

3. Que el mecanismo para la obtención del consentimiento procure ser en la mayor medida de lo posible un medio sencillo, gratuito y de fácil acceso para que el titular pueda manifestar su voluntad.

4. Que se prevean las condiciones jurídicas y materiales mínimas para contar con un respaldo suficiente para estar en posibilidades de acreditar, para todos los efectos, que se obtuvo válidamente el consentimiento del ciudadano involucrado por lo que al INE se refiere.

5. Prever en el modelo de convenio de colaboración que el INE que suscriba con instituciones públicas mecanismos para solicitar el consentimiento de las personas que participen en el proceso del Servicio de Verificación previa revisión, caso por caso, de la normativa aplicable, en los casos que resulte procedente.

6. Implementar un mecanismo que permita recabar el consentimiento del titular desde el momento en que acude a obtener la credencial para votar, o bien, actualizar su información personal.

7. Emitir los lineamientos en los que se detallen los diversos principios aplicables en materia de protección de datos personales, como el del consentimiento. Al respecto, se sugiere considerar la inclusión de disposiciones normativas que expresamente señalen los alcances del mismo, así como las obligaciones a observar por parte del INE al respecto.

3. Principio de finalidad

De conformidad con los estándares internacionales, este principio implica que el tratamiento de datos personales que realice un responsable deberá limitarse a cumplir con las finalidades explícitas y legítimas informadas al titular, o bien, para finalidades compatibles con las mismas.

Aunado a los requerimientos anteriores, el tratamiento de datos personales que efectúen específicamente las instancias públicas debe acotarse a las finalidades determinadas, explícitas y legítimas para las cuales fueron obtenidos en función de las atribuciones conferidas a éstas por ministerio de ley.

En este sentido, el artículo 20, fracción II de la LFTAIPG dispone que los sujetos obligados deben tratar los datos personales que posean en relación con los propósitos para los cuales se hayan obtenido.

Por su parte, el artículo 36 RINEMTAIP señala que en el tratamiento de datos personales sus servidores públicos están obligados a observar el principio de finalidad. Es importante señalar que el artículo 36 del RINEMTAIP, establece que el Comité de Información del INE emitirá los lineamientos en los que se desarrollen los principios rectores de la protección de datos personales. Sin embargo, de acuerdo con lo informado por el INE en la reunión celebrada en este Instituto el 27 de febrero de 2015, no se han emitido dichos lineamientos, por lo que no existe documento normativo alguno en el que se detallen los mecanismos para cumplir con el principio de finalidad.

Con base en las consideraciones anteriores, se puede advertir que el principio de finalidad implica el cumplimiento de los siguientes requerimientos:

1. El tratamiento de datos personales que se efectúe responda a finalidades determinadas, explícitas y legítimas.
2. Tratándose de responsables de carácter público, las finalidades que motivan el tratamiento de los datos personales deben ser compatibles con las atribuciones conferidas a éstos por ministerio de ley.

Para el caso que nos ocupa y a partir de los documentos que proporcionó el INE, se identifica que el Servicio de Verificación tiene, fundamentalmente, las siguientes finalidades:

- Verificar la vigencia y coincidencia de los datos de la credencial para votar que presentan los ciudadanos para identificarse ante una institución pública o privada respecto de la información almacenada en la base de datos del Padrón Electoral.
- Autenticar las huellas dactilares del ciudadano que se identifique con una credencial para votar, mediante la correlación gráfica de las marcas dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en el Padrón Electoral.

Al respecto, conviene señalar que las finalidades del Servicio de Verificación resultan ser determinadas y explícitas, sin embargo para conocer si las mismas son compatibles con las atribuciones conferidas al INE se requieren de los elementos a que se hace referencia en el análisis del principio de licitud. Como ya se indicó en el análisis jurídico de dicho principio, este Instituto advirtió la ausencia de elementos jurídicos que le permitan corroborar la existencia de normas constitucionales y/o legales expresas, en materia electoral o de identidad, sobre las facultades del INE mediante el uso del Padrón Electoral para el Servicio de Verificación, cuestión que impacta directamente en el estudio del principio de finalidad, como se puede observar, ya que sin este componente, resulta imposible identificar la compatibilidad de las finalidades del tratamiento con las atribuciones del responsable, en este caso el INE.

Consistentemente con las conclusiones del principio de licitud, **de ninguna manera se pretende señalar que el INE carezca de atribuciones para prestar el Servicio de Verificación mediante el uso del Padrón Electoral y que las finalidades del tratamiento resulten incompatibles con las mismas para prestar dicho Servicio**. **Únicamente se busca dejar claro que para estar en posibilidades de desentrañar si el INE cuenta con las facultades para prestar el Servicio de Verificación mediante el uso del Padrón**, y a partir de ello estar en posibilidades de calificar la compatibilidad de finalidades y atribuciones, **sería necesario interpretar los textos constitucionales y/o legales analizados** en el apartado de licitud, cuestión para la cual este Instituto se encuentra imposibilitado jurídicamente al no ser la instancia facultada para tal fin.

En virtud de lo anterior, en relación con el principio de finalidad, el INAI emite las siguientes observaciones y recomendaciones:

1. De acuerdo con lo dispuesto en el artículo 20, fracción II de la LFTAIPG, cerciorarse que las atribuciones del INE sean compatibles con las finalidades perseguidas a través del Servicio de Verificación, ello por supuesto, una vez se materialice lo indicado en el numeral 1.

2. Emitir los lineamientos en los que se detallen los diversos principios aplicables en materia de protección de datos personales, como el de finalidad. Al respecto, se sugiere considerar la inclusión de disposiciones normativas que expresamente señalen los alcances del mismo, así como las obligaciones a observar por parte del INE al respecto.

4. Principio de proporcionalidad

De acuerdo con los estándares internacionales, el principio de proporcionalidad implica que el responsable trate los datos personales que le resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

Así, el artículo 20, fracción II de la LFTAIPG dispone lo que a continuación se indica:

> "**Artículo 20.** Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:
> […]
>
> **II.** Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
> […]"

Por su parte, el artículo 36 RINEMTAIP es omiso respecto del principio de proporcionalidad, al menos de lo que expresamente se advierte del mismo.

Con base en lo anterior, es pertinente mencionar que conforme a los documentos proporcionados por el INE dicho servicio se bifurca en dos finalidades:

- Verificar la vigencia y coincidencia de los datos de la credencial para votar que presentan los ciudadanos para identificarse ante una institución pública o privada respecto de la información almacenada en la base de datos del Padrón Electoral.
- Autenticar las huellas dactilares del ciudadano que se identifique con una credencial para votar, mediante la correlación gráfica de las marcas dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en el Padrón Electoral.

Adicionalmente, el punto 4.2.3.1 del Anexo Técnico 3.2 del modelo de convenio de apoyo y colaboración que suscribiría el INE con la institución de que se trate establece lo siguiente:

> "**4.2.3.1 Verificación de datos de la Credencial para votar**
>
> La verificación de datos de la Credencial para votar provista por "EL INE" tiene por objeto validar la información (texto y minucias) del ciudadano a partir del número OCR o el CIC (Código de Identificación de la Credencial) ubicados en el reverso de la Credencial para votar a través de un Web Service que puede ser utilizado por aplicaciones desarrolladas por "LA INSTITUCIÓN."

A partir de lo anterior puede apreciarse que existe una diferencia entre la verificación (en sentido amplio) de los datos y municias proporcionados por el ciudadano y la validación de la credencial para votar como documento expedido por el INE, a partir del número OCR o el CIC ubicados al reverso de su credencial para votar.

En este sentido, según se advierte la verificacion sería el procedimiento mediante el cual la información de la credencial para votar que un ciudadano presenta para identificarse ante una institución pública o privada se compara o confronta con el Padrón Electoral, a efecto de determinar la coincidencia o no entre los datos proporcionados y la información almacenada que sirve como referencia para el cotejo.

Ahora bien, como resultado de la comparación o confronta de la información proporcionada por las instituciones públicas y privadas con respecto al Padrón Electoral, el INE valida los datos y, en consecuencia, determina si expidió la credencial para votar.

Caso similar ocurre con las huellas dactilares, donde siempre y cuando resulte positiva la correlación gráfica de las marcas dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en el extracto del Padrón Electoral, éstas se tendrán por validadas o autenticadas.

Las precisiones anteriores son relevantes debido a que mediante la verificación de la información contenida en la credencial para votar, en cuanto a su vigencia y coincidencia con la almacenada en el Padrón Electoral, se pretende comprobar en última instancia que la credencial para votar es un documento confiable como medio de identificación y, por tanto, idónea para acreditar la identidad de una persona física concreta que se pretende identificar con ella.

De esta manera, el análisis del principio de proporcionalidad en el caso concreto debe dirigirse a determinar si los datos requeridos, que serán objeto del Servicio de Verificación, son adecuados, pertinentes y no excesivos para determinar la coincidencia de éstos con los del Padrón Electoral, vigencia y autenticación de la credencial para votar y, como fin último, acreditar la identidad de una persona. Asimismo, el análisis de la proporcionalidad de los datos personales debe tener como parámetro la prueba de la necesidad en su exigencia, así como su idoneidad para lograr el fin propuesto.

En la medida que los datos requeridos sean adecuados, pertinentes y necesarios para comprobar la identidad de una persona, por ejemplo, reduciendo el margen de error que pudiera llevar a rechazar injustificadamente credenciales en trámites administrativos por considerarlas inválidas, cuando sean auténticas y se encuentran vigentes, éstos se considerarán proporcionales en relación con los propósitos que dieron origen al tratamiento.

Ahora bien, el INE propone los siguientes datos obligatorios para efectuar las consultas en el Servicio de Verificación de datos de la credencial para votar:

- Número OCR.
- Número CIC (Código de Identificación de Credencial).

Por otra parte, se mencionan como datos opcionales para ser confrontados y verificados por el INE en caso de que sean proporcionados por las instituciones públicas y privadas los siguientes:

- Apellido paterno.
- Apellido materno.
- Nombre(s).
- Año de registro.
- Número de emisión de la credencial para votar.
- Clave de elector.
- Clave Única de Registro de Población (CURP).
- Huellas dactilares de los dedos índices de la mano derecha e izquierda.

Con base en las anteriores consideraciones, a continuación se procede a realizar un análisis general sobre la proporcionalidad de los datos personales que soliciten las instituciones públicas o privadas para el Servicio de Verificación teniendo en consideración las finalidades identificadas:

Dato	Valoración
Número OCR	El OCR **se considera proporcional** en la medida que es adecuado, pertinente y necesario para dar cumplimiento a la finalidad relacionada con verificar la coincidencia de los datos de la credencial para votar con el extracto del Padrón Electoral. Lo anterior, en consideración a que el OCR está conformado por una serie de dígitos, de los cuales, los primeros 4 refieren al número de sección y el resto a un número consecutivo asignado a cada clave de elector, datos que fueron asignados por el INE, lo cual permitiría validar que la credencial para votar fue expedida por dicho organismo.
Número de CIC	El Código de Identificación de Credencial (CIC) **se considera proporcional** en la medida que es adecuado, pertinente y necesario para dar cumplimiento a la finalidad relacionada con verificar la coincidencia de los datos de la credencial para votar con el extracto del Padrón Electoral. Lo anterior, en virtud de que el CIC es un valor consecutivo que identifica al plástico de la credencial y que se asigna durante su producción.
Nombre Apellido paterno Apellido materno	El nombre y apellidos de una persona física **se consideran proporcionales** en tanto que son adecuados, pertinentes y necesarios para dar cumplimiento a la finalidad relacionada con verificar la coincidencia de los datos de la credencial para votar con el extracto del Padrón Electoral, ya que el nombre completo de las personas físicas puede ubicarse en la categoría de datos de identificación por excelencia, junto con otros datos que permitirían en estricto sentido identificar al individuo entre la colectividad.
Año de registro Número de emisión Clave de elector	El año de registro, número de emisión y la clave de elector **podrían considerarse proporcionales** para dar cumplimiento a la finalidad relacionada con verificar la coincidencia de los datos de la credencial para votar con el extracto del Padrón Electoral, en la medida que de manera conjunta con el número OCR o CIC permitan confirmar que la credencial para votar fue expedida por el INE y que, por tanto, es válida como medio de identificación.
Clave Única de Registro de Población (CURP)	La Clave Única de Registro de Población **se considera proporcional** para dar cumplimiento a la finalidad relacionada con verificar la coincidencia de los datos de la credencial para votar con el extracto del Padrón Electoral. Lo anterior, en consideración a que la validación de la CURP garantizaría que la consulta arroje un resultado veraz y

Dato	Valoración
	confiable, sin posibilidad de homonimias. No obstante lo anterior, se recomienda tener en cuenta que según lo ha establecido el Pleno de este Instituto, en el Criterio 3/10[1], este dato relaciona el nombre de una persona con su fecha de nacimiento y el lugar de nacimiento. En consecuencia, se considera importante tener en cuenta que al requerir la CURP se está teniendo acceso indirectamente a datos adicionales del titular.
Huellas dactilares de los dedos índices	Las huellas dactilares de los dedos índices **se consideran proporcionales** para dar cumplimiento a la finalidad relacionada con verificar la coincidencia de los datos de la credencial para votar con el extracto del Padrón Electoral, mediante la correlación gráfica de las marcas dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en la base de datos del Padrón Electoral. No obstante, es importante tener en cuenta que el registro de huellas dactilares puede potencialmente representar la información más confiable para la comprobación de la identidad de una persona. Esto sin omitir mencionar que, las circunstancias en las que se recaban las huellas dactilares y los mecanismos que se emplean para recabarlas deben procurar garantizar fiabilidad alta en la autenticación de la identidad de los individuos.

En virtud de lo anterior, en relación con el principio de proporcionalidad, el INAI recomienda emitir los lineamientos en los que se detallen los diversos principios aplicables en materia de protección de datos personales, específicamente el principio de proporcionalidad. Al respecto, se sugiere considerar la inclusión de disposiciones normativas que expresamente señalen los alcances de éstos, así como las obligaciones a observar por parte del INE al respecto.

Asimismo, en caso de que el INE amplíe el catálogo de respuestas sobre la coincidencia o no de los datos proporcionados por la institución para la realización del cotejo correspondiente y el porcentaje de similitud de la huella digital, se hacen propias las recomendaciones identificadas con los numerales 6 del deber de confidencialidad y 9 del apartado de transferencias.

[1] Disponible en el siguiente vínculo electrónico: http://inicio.ifai.org.mx/Criterios/03-10%20CURP.pdf y consultado por última vez el 17 de abril de 2015.

5. Principio de información

De conformidad con los estándares internacionales, el principio de información consiste en la obligación de los responsables del tratamiento de datos personales, de informar a los titulares de los datos personales, las características principales del tratamiento al que será sometida su información personal, a través del aviso de privacidad o leyenda de información, entre otras denominaciones.

El aviso de privacidad o leyenda de información tiene como propósito principal establecer y delimitar el alcance, términos y condiciones del tratamiento de los datos personales, a fin de que el titular pueda tomar decisiones informadas con relación a sus datos personales y mantenga el control y disposición de la información que le corresponde.

Asimismo, el aviso de privacidad permite al responsable transparentar el tratamiento o uso que da a los datos personales que están en su posesión, así como los mecanismos que tiene habilitados para que los titulares ejerzan sus derechos con relación a su información personal, lo que, sin duda, fortalece el nivel de confianza del titular con relación a la protección de sus datos.

Con relación a este principio, los artículos 20, fracción III y 23 de la LFTAIPG establecen lo siguiente:

> "**Artículo 20.** Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:
> […]
>
> III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;
> […]
>
> **Artículo 23**. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales."

Por su parte, los artículos 2, 36, párrafo 1 y 38 del RINEMTAIP prevén lo siguiente:

> "**ARTÍCULO 2**
> Del Glosario
> 1. Para los efectos del presente Reglamento, se entenderá por:
> […]
>
> IX. Comité: el Comité de Información;
> […]
>
> XLIII. Órgano Garante: el Órgano Garante de la Transparencia y el Acceso a la Información;
>
> XLIV. Órganos responsables: aquellas unidades administrativas del Instituto señaladas en la Ley, el Reglamento Interior del Instituto Nacional Electoral u otras disposiciones administrativas de carácter general, que en cumplimiento de sus atribuciones puedan tener información bajo su resguardo. De igual modo se consideran órganos responsables a los partidos políticos y agrupaciones políticas nacionales, en términos de la Ley;
> […]
>
> **ARTÍCULO 36**

> Principios de protección de datos personales
> 1. En el tratamiento de datos personales, los servidores públicos del Instituto deberán observar los principios de licitud, calidad de los datos, información al titular, consentimiento, seguridad, confidencialidad y finalidad para la que fueron recabados. Con el propósito de detallar los principios antes aludidos, el Comité emitirá los Lineamientos obligatorios para los órganos que posean datos personales.
> […]
>
> **ARTÍCULO 38**
> Del aviso al Comité y al Órgano Garante
> 1. Los órganos responsables que posean, por cualquier título sistemas de datos personales, deberán hacerlo del conocimiento del Comité y del Órgano Garante. Los órganos responsables mantendrán un listado actualizado de los sistemas de datos personales que posean. El listado se publicará en el portal de internet del Instituto."

A su vez, el numeral 45 de los Lineamientos ARCO señala lo que a continuación se indica:

> "**45.** El Instituto por conducto de la Dirección Ejecutiva, a través de la suscripción de convenios de apoyo y colaboración y bajo mecanismos de seguridad, establecerá los procedimientos para verificar los datos personales que soliciten las instancias públicas y privadas, mediante el uso de tecnologías.
>
> Los convenios que se celebren con instancias privadas deberán establecer que los avisos de privacidad que éstas hubiesen elaborado de conformidad con la Ley de Protección de Datos Personales en Posesión de Particulares, incluyan como una posibilidad de tratamiento de datos personales la validación y verificación a que se refiere el presente Capítulo."

De conformidad con lo anterior, se puede advertir que el principio de información implica las obligaciones siguientes para el INE:

1. Poner a disposición de los titulares el documento en que se establezcan los propósitos del tratamiento de los datos personales, en el momento en que se recaben los datos personales;
2. Hacer del conocimiento del Comité de Información y del Órgano Garante de la Transparencia y el Acceso a la Información, los sistemas de datos personales que posean los órganos responsables, mantener actualizado dicho listado y publicarlo en el portal de Internet del INE, y
3. Establecer en los convenios que celebren con instancias privadas para verificar datos personales de la Credencial para Votar, que los avisos de privacidad de dichas instancias incluyan como finalidad en el tratamiento de los datos personales, la posibilidad de validación y verificación de los datos personales contenidos en la Credencial para Votar.

Ahora bien, es importante señalar que el artículo 36 del RINEMTAIP antes citado, establece que el Comité de Información del INE emitirá los lineamientos en los que se desarrollen los principios rectores de la protección de datos personales. Sin embargo, de acuerdo con lo informado por el INE en la reunión celebrada en este Instituto el 27 de febrero de 2015, no se han emitido dichos lineamientos, por lo que no existe documento normativo alguno en el que se detallen las características y contenidos del documento mediante el cual se cumplirá el principio de información, comúnmente conocido como aviso de privacidad o leyenda de información.

No obstante, de acuerdo con los estándares nacionales e internacionales (entre ellos la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Lineamientos de Protección de Datos Personales, los Estándares Internacionales sobre Protección de Datos Personales y Privacidad, Resolución de Madrid, y la Directiva 95/46/CE del Parlamento Europeo y del Consejo), en general, el aviso de privacidad deberá contener la siguiente información:

1. La identidad y domicilio del responsable que trata los datos personales.
2. Los datos personales que serán sometidos a tratamiento, distinguiendo expresamente aquéllos que son sensibles;
3. Las finalidades del tratamiento.
4. Las facultades del ente público para tratar los datos personales para dichas finalidades.
5. Las transferencias de datos personales que, en su caso, se efectúen; el tercero receptor de los datos personales, y las finalidades de las mismas.
6. Los medios y el procedimiento para ejercer los derechos de acceso, rectificación, cancelación y oposición, y en su caso para revocar el consentimiento.
7. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso.
8. Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

En ese sentido, a partir de las obligaciones identificadas en el marco regulatorio que resulta aplicable al tratamiento de datos personales que realiza el INE y de los estándares nacionales e internacionales antes descritos, a continuación se analizará la forma en que el proyecto de Servicio de Verificación atiende el principio de información, y se emitirán recomendaciones al respecto.

Obligación 1. Poner a disposición de los titulares el documento en que se establezcan los propósitos del tratamiento de los datos personales, en el momento en que se recaben los datos personales.

De conformidad con la información proporcionada por el INE en los diversos documentos presentados ante este Instituto con motivo de la presente opinión técnica, los datos personales que se tratarán en el Servicio de Verificación son aquéllos que se obtienen para la integración del Padrón Electoral, la emisión de credenciales para votar y la incorporación de la lista nominal de electores.

En ese sentido, la leyenda de información que proporciona el INE a los titulares de los datos personales para cumplir con el principio de información, corresponde al tratamiento de datos personales que se realiza para las finalidades antes señaladas, es decir, la integración del Padrón Electoral, la emisión de credenciales para votar y la incorporación de la lista nominal de electores.

Ahora bien, en el oficio INE/DERFE/1108/2014, de fecha 2 de diciembre de 2014, el INE manifestó que la leyenda de información, la cual denominan *Manifestación de protección de datos personales recabados por el Registro Federal de Electores* (en lo sucesivo, la Manifestación), se encuentra disponible en la sección de las características de la credencial para votar de la página de Internet del INE.

Por otra parte, en la reunión celebrada el pasado 27 de febrero, ante pregunta expresa del INAI con relación al momento en que dan a conocer la Manifestación a los titulares, el INE explicó que en el formato de la *Solicitud Individual de Inscripción o Actualización al Padrón Electoral y Recibo de la Credencial,* que llenan los ciudadanos para tramitar su Credencial para Votar, se informa, al final, el vínculo electrónico en el que se puede consultar la Manifestación. Al respecto, dicho formato incluye la siguiente leyenda:

¡IMPORTANTE!
Sólo con la credencial que le entregaremos podrá votar; por eso le recordamos que debe regresar por ella. Así no solo tendrá una nueva credencial, sino que gracias a ella aparecerá en la Lista Nominal de la casilla electoral

donde le corresponda votar.

PROTECCIÓN DE DATOS PERSONALES

El Instituto Nacional Electoral, a través de la Dirección Ejecutiva del Registro Federal de Electores, es responsable del debido uso, tratamiento y protección de los datos de los ciudadanos que se recaban para los trámites de inscripción y actualización en el Padrón Electoral, en términos de la Ley General de Instituciones y Procedimientos Electorales y la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Para mayor información, en la página www.ine.mx podrá consultar la manifestación de protección de datos personales recabados por el Registro Federal de Electores.

Asimismo, en dicha reunión, el INE manifestó que en los módulos en los que se tramitan las Credenciales para Votar hay carteles en los que se explica que dicho Instituto protege los datos personales, pero que los mismos no contienen el texto completo de la Manifestación.

A partir de lo anterior, se advierte que al momento de tramitar la credencial para votar, el INE no pone a disposición de los titulares la Manifestación, sino que los remite a su sitio de Internet en donde la misma se puede consultar.

En cuanto a la forma en que se obtienen los datos personales, en la reunión del 27 de febrero, el INE manifestó lo siguiente, ante pregunta expresa del INAI:

> "**18.** Señalar cuáles son las formas de obtención de los datos personales que se registran en el Padrón Electoral. Es decir, si se obtienen de forma presencial, por Internet, correo electrónico, correo postal, vía telefónica, entre otros.
>
> **RESPUESTA:** Es únicamente presencial en los módulos de atención ciudadana del INE y es mediante el llenado del formato denominado Solicitud Individual de Inscripción o Actualización al Padrón Electoral y Recibo de la Credencial. En el caso de personas incapacitadas para acudir físicamente al módulo, éste se traslada al domicilio y para la inscripción de mexicanos residentes en el extranjero aún no está instrumentado el mecanismo para la obtención de los datos personales.
> […]"

Con relación a lo anterior, en el oficio INE/DERFE/356/2015, de fecha 18 de marzo de 2015, el INE explicó lo siguiente:

> "[…]
>
> El artículo 128 de la Ley General de Instituciones y Procedimientos Electorales, señala que en el Padrón Electoral constará la información básica de los varones y mujeres mexicanos mayores de 18 años que presenten la solicitud individual en que consten firma, huella dactilares y fotografía del ciudadano de acuerdo al artículo 135 de la Ley en cita.
>
> De acuerdo con el artículo 134, con base en el Padrón Electoral, la Dirección Ejecutiva del Registro Federal de Electores expedirá, en su caso, las Credenciales para Votar.
>
> De conformidad a lo establecido por el artículo 136, párrafo 1 de la Ley General de Instituciones y Procedimientos Electorales los ciudadanos tendrán la obligación de acudir a las oficinas o módulos que determine el Instituto, a fin de solicitar y obtener su credencial para votar con fotografía.
>
> El párrafo siguiente establece que para solicitar la Credencial para Votar, el ciudadano deberá identificarse, preferentemente, con documento de identidad expedido por autoridad, o a través de los medios y procedimientos que

> determine la Comisión Nacional de Vigilancia del Registro Federal de Electores. La Dirección Ejecutiva del Registro Federal de Electores conservará copia digitalizada de los documentos presentados.
>
> El párrafo 3 del mismo artículo, requiere que en todos los casos, al solicitar un trámite registral, el interesado deberá asentar su firma y huellas dactilares en el formato respectivo.
>
> El artículo 140 señala que la solicitud de incorporación en el Padrón Electoral se hará en forma individual y deberá contener los datos siguientes; apellido paterno, apellido materno, nombre completo, lugar y fecha de nacimiento, edad y sexo, domicilio actual y tiempo de residencia, ocupación, en su caso número y fecha del certificado de naturalización y firma, huellas dactilares y fotografía del solicitante.
>
> Además, deberán asentarse los datos de entidad federativa, municipio y localidad donde se realice la inscripción, distrito electoral federal y sección electoral correspondiente al domicilio del solicitante y la fecha de solicitud de inscripción. Por lo que efectivamente se puede concluir que la obtención de datos personales es de forma presencial en los Módulos de Atención Ciudadana.
>
> De lo anterior se advierte que los datos se obtienen de forma presencial y personalísima."

Como se puede observar, los datos personales para la integración del Padrón Electoral, la emisión de credenciales para votar y la incorporación de la lista nominal de electores, los obtiene el INE de forma presencial y directamente de su titular.

Ahora bien, de conformidad con lo establecido en el artículo 20, fracción III de la LFTAIPG, el INE tendría que dar a conocer la Manifestación en el momento en que los titulares le proporcionan sus datos personales para tramitar su credencial para votar, sobre todo al considerar que no existe impedimento alguno para ello, pues los datos se obtienen de forma presencial y directamente de los titulares. No obstante, como se señaló anteriormente, el INE remite a los titulares a su portal de Internet para consultar la Manifestación en un momento posterior.

En cuanto al contenido de la Manifestación, como se señaló, el INE publica actualmente en su portal de Internet la *Manifestación de protección de datos personales recabados por el Registro Federal de Electores,* la cual se puede consultar en el siguiente vínculo: http://www.ine.mx/archivos2/portal/credencial/datosPersonales.html/

Por otra parte, en la reunión del 27 de febrero y en el oficio INE/DERFE/356/2015, el INE señaló que emitirá una nueva Manifestación una vez que se implemente el Servicio de Verificación y, al respecto, envió a este Instituto el nuevo texto de la Manifestación.

En cuanto a la Manifestación que el INE utiliza actualmente para el tratamiento de datos personales para la integración del Padrón Electoral, la emisión de credenciales para votar y la incorporación de la lista nominal de electores, la cual se publica en el portal de Internet del INE, se pudo observar que la misma no incluye como una de las finalidades del tratamiento, el Servicio de Verificación. Ahora bien, en cuanto al contenido de información de la nueva Manifestación, la cual se pondrá a disposición de los titulares una vez que se implemente dicho servicio, según lo señalado por el INE, se tiene lo siguiente:

Contenidos de información que se propone incluir en la Manifestación de acuerdo con los estándares nacionales e internacionales	Texto de la Manifestación	Observaciones*
La identidad y domicilio del responsable que trata los datos personales.	El Instituto Nacional Electoral (INE), a través de la Dirección Ejecutiva del Registro Federal de Electores, con	Sin observaciones.

Contenidos de información que se propone incluir en la Manifestación de acuerdo con los estándares nacionales e internacionales	Texto de la Manifestación	Observaciones*
	domicilio en Av. Insurgentes Sur 1561, Col. San José Insurgentes, C.P. 03740, Benito Juárez, México, Distrito Federal, es responsable del uso y protección de los datos de los ciudadanos que se recaban para los trámites de inscripción y actualización al Padrón Electoral para la obtención de la Credencial para Votar, en los Módulos de Atención Ciudadana.	
Los datos personales que serán sometidos a tratamiento, distinguiendo expresamente aquéllos que son sensibles.	4. Datos personales tratados A. El Instituto recabará e incorporará en el Registro Federal de Electores los datos personales que forman parte del Padrón Electoral, que de conformidad con el artículo 140, numeral 1 de la LEGIPE son proporcionados por los ciudadanos para realizar algún trámite de inscripción o actualización al Padrón Electoral, y en consecuencia para la obtención de su Credencial para Votar con Fotografía e incorporación a la Lista Nominal de Electores, siendo los siguientes: 1. Nombre(s) 2. Apellido paterno 3. Apellido materno 4. Sexo 5. Edad 6. Fecha y Lugar de Nacimiento 7. Domicilio 8. Entidad federativa, municipio y localidad que corresponde al domicilio 9. Tiempo de residencia en el domicilio 10. Ocupación 11. Firma 12. Fotografía	• De conformidad con lo establecido en el formato de *Solicitud Individual de Inscripción o Actualización al Padrón Electoral y Recibo de la Credencial,* se observa que se recaban más datos de los señalados en el punto 4 de la Manifestación, entre ellos: gemelo, escolaridad, firma, información contenida en el medio de identificación, comprobante de domicilio y documento de identidad con fotografía que proporcione el ciudadano. • Asimismo, de conformidad con dicho formato, el INE sí recaba datos personales sensibles, en aquellos casos en los que se describa el tipo de discapacidad del ciudadano. En ese sentido, se sugiere verificar el listado de datos personales que realmente se recaban, a fin de informar de manera exacta al respecto en la Manifestación.

Contenidos de información que se propone incluir en la Manifestación de acuerdo con los estándares nacionales e internacionales	Texto de la Manifestación	Observaciones*
	13. Huellas dactilares 14. Clave Única del Registro de Población 15. Número y fecha del certificado de naturalización, en su caso. Asimismo, el Instituto recabará los siguientes datos adicionales, que no forman parte del Padrón Electoral y sus derivados, y son proporcionados por los ciudadanos para realizar algún trámite de inscripción o actualización al Padrón Electoral: 1. Teléfono 2. Correo electrónico B. Los datos personales recabados por el Instituto para su incorporación en el Registro Federal de Electores y que podrán ser sujetos de tratamiento para el Servicio de Verificación de Datos de la Credencial para Votar son los siguientes: 1. Nombre(s) 2. Apellido paterno 3. Apellido materno 4. CIC 5. OCR 6. Clave de elector 7. Año de registro 8. Número de emisión d la credencial de elector 9. Huellas dactilares de los dedos índices 10. Clave Única del Registro de Población 5. Señalamiento expreso de los datos personales sensibles que se traten El Instituto no recaba datos personales	

Contenidos de información que se propone incluir en la Manifestación de acuerdo con los estándares nacionales e internacionales	Texto de la Manifestación	Observaciones*
	sensibles de los ciudadanos, que se refieran a datos ideológicos (posturas ideológicas, religiosas, filosóficas o morales), opiniones políticas, afiliación sindical, estado de salud físico o mental, información genética, vida u orientación sexual, origen étnico o racial.	
Las finalidades del tratamiento.	2. Finalidades del tratamiento Los datos personales que el ciudadano proporciona al Instituto son estrictamente confidenciales y serán tratados conforme a las obligaciones previstas en la Constitución Política de los Estados Unidos Mexicanos, en la Ley General de Instituciones y Procedimientos Electorales (LEGIPE) y en 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, referentes al tratamiento de los datos personales en los trámites de inscripción o actualización al Padrón Electoral, y en consecuencia la obtención de su Credencial para Votar e incorporación a la Lista Nominal de Electores, para ejercer su derecho al voto y contar con un medio de identificación personal. Los datos personales que los ciudadanos proporcionan al Registro Federal de Electores que se citan en el apartado B del numeral 4 de esta manifestación, previo consentimiento de sus titulares, podrán ser susceptibles de tratamiento para el Servicio de Verificación de datos de la Credencial para Votar, con la finalidad de corroborar que los datos de la	En esta Manifestación ya se incluye la finalidad del Servicio de Verificación. No obstante, se recomienda señalar que la falta de consentimiento por parte del ciudadano para que sus datos personales sean utilizados en el Servicio de Verificación, no será motivo para que el INE no tramite su credencial para votar.

Contenidos de información que se propone incluir en la Manifestación de acuerdo con los estándares nacionales e internacionales	Texto de la Manifestación	Observaciones*
	credencial para votar que se presente ante instituciones públicas o privadas para trámites administrativos sean coincidentes con los que obran en este Instituto, aportando con ello elementos que eviten la posible comisión de un ilícito por parte de terceros, respecto de su credencial.	
Las facultades del ente público para tratar los datos personales para dichas finalidades.	En términos de lo dispuesto por los artículos 20, fracción III y 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, así como 32, párrafos 2 y 3, 35 y 36 del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública, así como el Título VI de los Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en posesión de la Dirección Ejecutiva del Registro Federal de Electores, el Instituto Nacional Electoral informa al ciudadano la manifestación de protección de datos personales recabados por el Registro Federal de Electores, en los siguientes términos. […] 2. Finalidades del tratamiento Los datos personales que el ciudadano proporciona al Instituto son estrictamente confidenciales y serán tratados conforme a las obligaciones previstas en la Constitución Política de los Estados Unidos Mexicanos, en la Ley General de Instituciones y Procedimientos Electorales (LEGIPE) y en el artículo Cuarto Transitorio del Decreto de Reformas de la Ley General de Población, publicado en el	Se sugiere hacer referencia a los artículos principales de la Constitución Política de los Estados Unidos Mexicanos, y la Ley General de Instituciones y Procedimientos Electorales que habiliten al INE al tratamiento de los datos personales para las finalidades informadas en la Manifestación, evitando incluir un listado demasiado extenso de artículos y centrándose en los sustantivos.

Contenidos de información que se propone incluir en la Manifestación de acuerdo con los estándares nacionales e internacionales	Texto de la Manifestación	Observaciones*
	Diario Oficial de la Federación el 22 de julio de 1992,	
Las transferencias de datos personales que, en su caso, se efectúen; el tercero receptor de los datos personales, y las finalidades de las mismas.	6. Transferencias de datos personales que en su caso se efectúen Los documentos, datos e informes que los ciudadanos proporcionen al Registro Federal de Electores, en cumplimiento de las obligaciones que les impone la Constitución y la LEGIPE, no podrán comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en que el Instituto Nacional Electoral fuese parte, para cumplir con las obligaciones previstas por la Ley en materia electoral y por la Ley General de Población en lo referente al Registro Nacional Ciudadano o por mandato de juez competente. Los miembros de los Consejos General, Locales y Distritales, así como de las comisiones de vigilancia, tendrán acceso a la información que conforma el Padrón Electoral, exclusivamente para el cumplimiento de sus funciones y no podrán darle o destinarla a finalidad u objeto distinto al de la revisión del padrón electoral y las listas nominales. En el marco del Servicio de Verificación de datos de la Credencial para Votar los datos señalados en el apartado B del numeral 4 de esta manifestación, no serán bajo ninguna circunstancia objeto de transferencia, dado que únicamente se trata de la confronta de datos coincidentes para evitar la posible comisión de un ilícito por parte de terceros. 7. Cláusula que indique si el titular	Sin observaciones.

Contenidos de información que se propone incluir en la Manifestación de acuerdo con los estándares nacionales e internacionales	Texto de la Manifestación	Observaciones*
	acepta o no la transferencia cuando así se requiera No aplica (el LEGIPE y normatividad reglamentaria establecen claramente las condiciones de la transferencia).	
Los medios y el procedimiento para ejercer los derechos de acceso, rectificación, cancelación y oposición, y en su caso para revocar el consentimiento.	3. Mecanismos para que el titular pueda manifestar su negativa para otras finalidades. En los casos en que el Instituto haya recabado datos falsos en el Registro Federal de Electores, ya sea por un error de procesamiento, por un tercero o en forma dolosa, los ciudadanos podrán solicitar el cotejo, corrección y supresión de datos personales del Padrón Electoral. Asimismo, los ciudadanos podrán interponer escritos de queja cuando consideren que algún funcionario u órgano del Instituto, partido político, organismo electoral de entidades federativas, o cualquier sujeto con derecho a tener sus datos personales a través del Registro Federal de Electores, haga un tratamiento diverso a las finalidades establecidas en la Constitución y en la LEGIPE. El Instituto atenderá las solicitudes de cotejo, corrección, supresión y queja de los ciudadanos por el tratamiento de sus datos personales, conforme lo previsto en los Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores. […]	• Se sugiere incluir la información de los apartados 3 y 8 en un solo apartado, para que así se haga referencia a los cuatro derechos: acceso, rectificación, cancelación y oposición. • Se sugiere valorar la eliminación de los apartados 9 y 10, ya que no aplican al caso particular. • Se sugiere incluir el derecho de oposición al que refiere el numeral 33 del Capítulo Segundo de los Lineamientos ARCO. • Se sugiere señalar con precisión los vínculos electrónicos en los que, en su caso, se pueden obtener los formatos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, o donde se pueden presentar las solicitudes; o bien proporcionar los números telefónicos donde se puede obtener mayor información al respecto.

Contenidos de información que se propone incluir en la Manifestación de acuerdo con los estándares nacionales e internacionales	Texto de la Manifestación	Observaciones*
	8. Medios y procedimientos para ejercer los derechos ARCO El ciudadano podrá exigir en todo momento los derechos de acceso y rectificación de sus datos personales que obren en el Registro Federal de Electores, mediante los formatos que se encuentran a su disposición en el Módulo de Atención Ciudadana, en la página de internet del Instituto, en las oficinas de la Dirección Ejecutiva y en las Vocalías Locales y Distritales del Registro Federal de Electores, conforme lo previsto en los Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores. 9. Mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de sus datos personales Está contemplado en la fracción anterior, por lo que se refiere a los datos personales recabados por el Instituto y que no forman parte del Padrón Electoral (cancelación y oposición de datos personales) 10. Opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de sus datos personales No aplica (al tratarse de una obligación de los ciudadanos inscribirse y actualizarse en el Padrón Electoral y	

Contenidos de información que se propone incluir en la Manifestación de acuerdo con los estándares nacionales e internacionales	Texto de la Manifestación	Observaciones*
	toda vez que los datos personales no se dan a conocer salvo las excepciones que la LEGIPE establece.).	
La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso.	11. Uso de cookies, web beacons o cualquier otra tecnología similar o análoga No aplica.	Sin observaciones, en virtud de que los datos no se obtienen por medios remotos.
Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.	12. Procedimientos y medios por los cuales el responsable comunicará a los titulares los cambios en el aviso de privacidad El Instituto informará al ciudadano de manera oportuna cualquier modificación, cambio o actualización derivada de nuevos requerimientos legales que afecten los procedimientos de inscripción y actualización del Padrón Electoral y en consecuencia el tratamiento de sus datos personales, a través de la página de internet www.ine.mx, en los Módulos de Atención Ciudadana y los diversos medios de difusión (radio, televisión, prensa, etc.) de que disponga para ello.	Sin observaciones.

* Estas observaciones se realizan únicamente con base en la información proporcionada por el INE en los documentos presentados para la presente opinión técnica, y en ese sentido no validan que el INE lleve a cabo el tratamiento de datos personales de acuerdo con lo declarado en la Manifestación. Es obligación del INE verificar que la información contenida en la Manifestación esté completa y corresponda con exactitud al tratamiento que realiza.

Ahora bien, como se señaló, el INE dará a conocer esta Manifestación, en la que ya se incluye al Servicio de Verificación como una finalidad más del tratamiento, una vez que dicho servicio se haya implementado. Esto implica que a los titulares cuyos datos personales hayan sido recabados con anterioridad a la implementación del Servicio de Verificación, no se les informó con relación a dicha finalidad, pues como se explicó anteriormente, la Manifestación que utiliza actualmente el INE no la incluye. En ese sentido, se hace necesario que el INE tome medidas necesarias para informar a estos titulares que su información personal que obra en el Padrón Electoral puede ser utilizada para el Servicio de Verificación.

Al respecto, el INE manifestó lo siguiente en la reunión del 27 de febrero:

> "**20.** Señalar si el INE tiene considerado algún procedimiento para dar a conocer a los titulares de los datos personales, cuya información se haya recabado previo a la puesta en operación del Servicio de verificación de datos de la

Credencial para Votar, que sus datos personales contenidos en el Padrón Electoral se utilizarán para la nueva finalidad vinculada con este servicio, y en su caso, describir dicho procedimiento o medidas a implementar para lo anterior.

RESPUESTA: En los convenios precisar que al momento que se haga la compulsa por parte de las instituciones públicas o privadas se hará del conocimiento al ciudadano. El INE va a analizar la utilización de medidas compensatorias como el portal de Internet del INE, spots en medios masivos de información, carteles en los módulos de información. El INE hará el envío de una respuesta más detallada sobre ello."

Lo cual reiteró en el oficio INE/DERFE/356/2015 en los siguientes términos:

"**20.** Señalar si el INE tiene considerado algún procedimiento para dar a conocer a los titulares de los datos personales, cuya información se haya recabado previo a la puesta en operación del Servicio de verificación de datos de la Credencial para Votar, que sus datos personales contenidos en el Padrón Electoral se utilizarán para la nueva finalidad vinculada con este servicio, y en su caso, describir dicho procedimiento o medidas a implementar para lo anterior.

RESPUESTA: El Instituto implementará medidas compensatorias carteles en los Módulos de Atención Ciudadana, difusión en medios de comunicación para hacer del conocimiento a aquellos ciudadanos cuyos datos fueron proporcionados al Registro Federal de Electores, con anterioridad a la implementación del Servicio de Verificación de Datos de la Credencial para Votar."

Como es posible observar, el INE tiene considerado implementar mecanismos para dar a conocer la nueva finalidad o el cambio en la Manifestación a través de medios de comunicación masiva, lo cual se considera adecuado para informar a los titulares cuyos datos personales se hayan recabado antes de la implementación del Servicio de Verificación, esta finalidad.

Obligación 2. Hacer del conocimiento del Comité de Información y del Órgano Garante de la Transparencia y el Acceso a la Información, los sistemas de datos personales que posean los órganos responsables, mantener actualizado dicho listado y publicarlo en el portal de Internet del INE.

Al respecto, en la reunión del 27 de febrero, el INE informó lo siguiente:

"**22.** Informar si se tiene dado de alta ante la instancia correspondiente, el sistema de datos personales denominado "Sistema Integral de Información del Registro Federal de Electores (SIIRFE)", y en su caso, proporcionar a esta Autoridad la cédula descriptiva del sistema de datos personales. Lo anterior, con fundamento en lo dispuesto por el artículo 23 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que a la letra señala lo siguiente:

"Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales".

RESPUESTA: Dentro del listado del INE, se encuentra la descripción del sistema. El SIIRFE está conceptualizado como 8 subsistemas. INE nos hará llegar la descripción de los 8 subsistemas que conforman el SIIRFE, así como el link donde se puede consultar.

Cabe señalar que la base principal que será utilizada para el sistema de verificación será el subsistema SIIRFE-SAP, mismo que también nos harán llegar."

Con relación a lo anterior, en el oficio INE/DERFE/356/2015, el INE precisó lo siguiente:

"**22.** Informar si se tiene dado de alta ante la instancia correspondiente, el sistema de datos personales denominado "Sistema Integral de Información del Registro Federal de Electores (SIIRFE)", y en su caso, proporcionar a esta Autoridad la cédula descriptiva del sistema de datos personales. Lo anterior, con fundamento en lo dispuesto por el artículo 23 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que a la letra señala lo siguiente:

"Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales".

RESPUESTA: Como se señaló en la reunión, el Sistema de Verificación de datos de la Credencial para Votar es independiente al SIIRFE. Está en trámite para su aprobación y publicación la Cédula descriptiva del sistema de datos personales correspondientes a Sistema de Verificación de datos de la Credencial para Votar, la cual se anexa al presente oficio.
[…]"

De conformidad con lo informado por el INE la cédula descriptiva del Sistema de Verificación se encontraba en trámite para su aprobación. Sin embargo, al realizar una consulta al sistema de datos personales del INE, este Instituto encontró que ya se encuentra publicado en el mismo, un sistema denominado "Servicio de Verificación de datos de la Credencial para Votar", en el que se hacen ciertas acotaciones en los rubros relativos a "Fecha de creación" y "Última actualización", relativas a que el servicio se encuentra en fase de desarrollo y pruebas. Lo anterior es posible constatarlo a través del siguiente vínculo:
http://www.ine.mx/archivos3/portal/historico/recursos/IFE-v2/UTSID/UTSID-SistemasdedatospersonalesdelIFE/anexosdatospersonales/Mar-15/SDP_DERFE_2014_39.pdf

Con relación al contenido de la cédula, se observa lo siguiente:

- En el objetivo del sistema no se incluye la finalidad para la cual el INE presta el Servicio de Verificación, misma que fue informada en la reunión del 20 de abril, es decir, para mantener depurado y actualizado el Padrón Electoral.
- En cuanto al tipo de datos, se observa que hay una inconsistencia entre lo señalado en la Manifestación y la cédula descriptiva de sistema de datos personales. Lo anterior, en virtud de que en la Manifestación se hace referencia al CIC y huellas dactilares de los dedos índices, los cuales no se incluyen dentro del apartado de "Tipo de datos" de la cédula referida, y en esta última se describen los siguientes datos adicionales a los contenidos en la Manifestación: RFC, domicilio, folio nacional, año de emisión, localidad, sección, vigencia, edad y sexo.

Obligación 3. Establecer en los convenios que celebren con instancias privadas para verificar datos personales de la credencial para votar, que los avisos de privacidad de dichas instancias incluyan como finalidad en el tratamiento de los datos personales, la posibilidad de validación y verificación de los datos personales contenidos en la credencial para votar.

Al respecto, la cláusula quinta del **convenio de apoyo y colaboración para instituciones privadas,** en su versión del 18 de marzo de 2015, establece lo siguiente:

"QUINTA.- Las obligaciones de "_____", son las siguientes:
[…]
e) Establecer en los avisos de privacidad que se elaboren de conformidad con la Ley de Protección de Datos Personales en Posesión de Particulares, la posibilidad de verificación de los datos personales contenidos en la Credencial para Votar que los ciudadanos proporcionen a "_____".
[…]"

Visto lo anterior, el convenio referido sí tiene previsto que la institución privada incluya en sus avisos de privacidad, como una de las finalidades del tratamiento de los datos personales, la posibilidad de validación y verificación de los datos personales contenidos en la credencial de elector. No obstante, es importante señalar que el nombre correcto de la ley es Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En virtud de lo anterior, en relación con el principio de información, el INAI emite las siguientes observaciones y recomendaciones:

1. De conformidad con lo establecido en el artículo 20, fracción III de la LFTAIPG, el INE deberá dar a conocer la *Manifestación de protección de datos personales recabados por el Registro Federal de Electores* a los titulares de los datos personales al momento en que proporcionan sus datos para la integración del Padrón Electoral, la emisión de credenciales para votar y la incorporación de la lista nominal de electores, y no sólo remitirlos al portal de Internet del INE para conocer el contenido de la Manifestación.

   Es de relevante importancia que se dé a conocer la Manifestación cuando el titular proporciona sus datos personales, y no de manera posterior, pues sólo así se cumplirá con el objetivo del principio de información que, como ya se señaló, se centra en dar a conocer al titular las características principales del tratamiento, a fin de que éste tome decisiones informadas con relación a la entrega de sus datos personales.

   Para ello, será necesario que en los módulos en los que se tramiten las credenciales para votar se cuente con el texto de la Manifestación completo. Es importante señalar que no es necesario que se entregue una copia de la misma a cada titular, sino que es suficiente con que se ponga a su disposición para su lectura, con independencia de que si el titular requiera copia de la misma el INE se la pueda proporcionar o lo invite a obtenerla en versión electrónica a través de su portal de Internet.

   Al respecto se recomienda:

   - La colocación de carteles en los módulos que contengan la Manifestación, o bien la inclusión de esta última en el formato o cédula que se entrega a los titulares cuando tramitan la Credencial para Votar.
   - Capacitar al personal que labora en los mismos para concientizarlos sobre la importancia del cumplimiento de esta obligación.

2. Tomar las medidas necesarias para que la nueva Manifestación, en la que ya se incluye como finalidad del tratamiento, el Servicio de Verificación, sea aprobada de manera oportuna por el órgano competente, y que la misma se utilice en cuanto inicie la implementación del Servicio.

3. Revisar el contenido de la Manifestación y atender las observaciones realizadas por el INAI, a saber:

   - Verificar el listado de datos personales que realmente se recaban, a fin de informar de manera exacta al respecto en la Manifestación.
   - Hacer referencia a los artículos principales de la CPEUM y la LGIPE que habiliten al INE al tratamiento de los datos personales para las finalidades informadas en la Manifestación.
   - Incluir la información de los apartados 3 y 8 en un solo apartado, para que así se haga referencia a los cuatro derechos: acceso, rectificación, cancelación y oposición.

- Valorar la eliminación de los apartados 9 y 10, ya que no aplican al caso particular.
- Incluir el derecho de oposición al que refiere el numeral 33 del Capítulo Segundo de los Lineamientos ARCO.
- Señalar con precisión los vínculos electrónicos en los que, en su caso, se pueden obtener los formatos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, o donde se pueden presentar las solicitudes; o bien proporcionar los números telefónicos donde se puede obtener mayor información al respecto.

4. Implementar las medidas que tienen consideradas para dar a conocer los cambios en la Manifestación y la nueva finalidad del tratamiento a través de medios masivos de comunicación. Al respecto se recomienda:

- Que el texto a utilizar contenga cuando menos la siguiente información: identidad y domicilio del INE, finalidades del tratamiento (señalando de manera expresa el sistema de verificación) y los mecanismos para conocer la Manifestación completa.
- Incluir información adicional que permita a los titulares identificarse como destinatarios de la manifestación.
- Para la elección de los medios de publicación de la Manifestación, tomar en cuenta los siguientes factores:
  - Perfil de los titulares.
  - Medios habilitados para mantener una comunicación general con los titulares.
  - Características del medio en el que se pretende publicar la Manifestación.
  - Atender al criterio de máximo alcance, de tal forma que la elección del medio y periodo resulte más eficiente para la difusión de la Manifestación.

5. Revisar la cédula descriptiva del Servicio de Verificación, a fin de que ésta corresponda con exactitud al tratamiento que se lleva a cabo, principalmente en lo que refiere a los apartados de objetivo del sistema y tipo de datos.

Así como tomar las medidas necesarias para que la cédula descriptiva del sistema de datos personales correspondientes al Sistema de Verificación, previo a la entrada en operación de dicho servicio, sea aprobada de manera oportuna por el órgano competente, hacerlo del conocimiento del Comité de Información y del Órgano Garante de la Transparencia el Acceso a la Información, a efecto de garantizar que se mantenga actualizado dicho listado y que sea publicado en el portal de Internet del INE, de conformidad con lo que establece el artículo 38 del RINEMTAIP.

6. Verificar que, efectivamente, las instituciones privadas a las que se preste el Servicio de Verificación informen en su aviso de privacidad sobre esta finalidad del tratamiento de los datos personales, de conformidad con lo establecido en el numeral 45 de los Lineamientos ARCO.

7. Con relación a los convenios que el INE celebre con instancias públicas, respecto de la cláusula quinta, se sugiere incluir un inciso en el que se establezcan obligaciones en materia de protección de datos personales, como la prevista en la Cláusula quinta del inciso e), del convenio con instancias privadas, a efecto de dichas instituciones establezcan en su leyenda de información, dentro de los propósitos del tratamiento de los datos personales, la posibilidad de verificación de los datos de la Credencial para Votar en el Servicio de Verificación, lo que implica transferencias al INE.

8. Por otra parte, se sugiere valorar la conveniencia de que las instancias públicas y privadas puedan solicitar el consentimiento para el tratamiento de sus datos personales en el Servicio de Verificación por un medio distinto al

aviso de privacidad, ya que de otra forma estarían obligadas a entregar a cada uno de los titulares una copia del aviso de privacidad.

9. Emitir los lineamientos en los que se detallen los diversos principios aplicables en materia de protección de datos personales, como el de información, de conformidad con lo dispuesto en el artículo 36 del RINEMTAIP. Al respecto, se sugiere considerar la inclusión de disposiciones normativas que expresamente señalen cuáles son los elementos informativos que debe contener la manifestación de datos personales, atendiendo los estándares nacionales e internacionales.

6. Principio de calidad

De conformidad con los estándares internacionales, el principio de calidad implica la obligación de los responsables del tratamiento, de procurar que los datos personales contenidos en las bases de datos sean exactos, completos y actualizados, para los fines para los cuales fueron recabados.

En ese sentido, cabe mencionar que los datos personales son **exactos** cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles; están **completos** cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular; y están **actualizados** cuando están al día y corresponden a la situación real del titular.

Asimismo, este principio establece que cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades para las cuales se obtuvieron, así como para las disposiciones legales aplicables, deberán ser eliminados de las bases de datos.

Es importante señalar, que todo responsable está obligado a adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con estas características, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

Con relación a este principio, el artículo 20, fracciones IV y V de la LFTAIPG establece lo siguiente:

> "**Artículo 20.** Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:
> […]
>
> IV. Procurar que los datos personales sean exactos y actualizados;
>
> V. Sustituir, rectificar o completar, de oficio los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y
> […]"

Asimismo, los artículos 54, 127, 138, 144 y 154 de la LGIPE disponen lo siguiente:

> "**Artículo 54.**
>
> 1. La Dirección Ejecutiva del Registro Federal de Electores tiene las siguientes atribuciones:
> d) Revisar y actualizar anualmente el Padrón Electoral conforme al procedimiento establecido en el Libro Cuarto de esta Ley;
> […]
>
> **Artículo 127.**
>
> 1. El Registro Federal de Electores será el encargado de mantener actualizado el Padrón Electoral.
>
> **Artículo 138.**
>
> 1. A fin de actualizar el Padrón Electoral, el Instituto, a través de la Dirección Ejecutiva del Registro Federal de Electores realizará anualmente, a partir del día 1o. de septiembre y hasta el 15 de diciembre siguiente, una campaña intensa para convocar y orientar a la ciudadanía a cumplir con las obligaciones a que se refieren los dos párrafos siguientes.

[…]

Artículo 143.

1. Podrán solicitar la expedición de credencial para votar con fotografía o la rectificación ante la oficina del Instituto responsable de la inscripción, o en el caso de ciudadanos residentes en el extranjero, por el medio determinado por la Dirección Ejecutiva del Registro Federal de Electores, con la aprobación de la Comisión Nacional de Vigilancia del Registro Federal de Electores para que se haga desde el extranjero, aquellos ciudadanos que:
[…]

4. En las oficinas del Registro Federal de Electores, existirán a disposición de los ciudadanos los formatos necesarios para la presentación de la solicitud respectiva.

5. La oficina ante la que se haya solicitado la expedición de credencial o la rectificación resolverá sobre la procedencia o improcedencia de la misma dentro de un plazo de veinte días naturales.
[…]

Artículo 144.

1. La Dirección Ejecutiva del Registro Federal de Electores podrá utilizar la técnica censal parcial en distritos o secciones, o partes de éstos, en aquellos casos en que así lo decida la Junta General Ejecutiva, a fin de mantener actualizado el Padrón Electoral.
[…]

Artículo 154.

1. A fin de mantener permanentemente actualizado el padrón electoral, la Dirección Ejecutiva del Registro Federal de Electores recabará de los órganos de las administraciones públicas federal y estatal la información necesaria para registrar todo cambio que lo afecte.
[…]

Artículo 155.
[…]

7. Asimismo, la Dirección Ejecutiva del Registro Federal de Electores dará de baja del padrón electoral a los ciudadanos que hubiesen avisado su cambio de domicilio mediante solicitud en que conste su firma, huellas dactilares y, en su caso, fotografía. En este supuesto, la baja operará exclusivamente por lo que se refiere al registro del domicilio anterior.

8. En aquellos casos en que los ciudadanos hayan sido suspendidos en el ejercicio de sus derechos políticos por resolución judicial, serán excluidos del Padrón Electoral y de la lista nominal de electores durante el periodo que dure la suspensión. La Dirección Ejecutiva del Registro Federal de Electores reincorporará al padrón electoral a los ciudadanos que sean rehabilitados en sus derechos políticos una vez que sea notificado por las autoridades competentes, o bien cuando el ciudadano acredite con la documentación correspondiente que ha cesado la causa de la suspensión o ha sido rehabilitado en sus derechos políticos.

9. Serán dados de baja del Padrón Electoral los ciudadanos que hayan fallecido, siempre y cuando quede acreditado con la documentación de las autoridades competentes o, en su defecto, mediante los procedimientos que determine la Comisión Nacional de Vigilancia.
[…]"

Por su parte, el artículo 36, párrafo 1 del RINEMTAIP prevé lo siguiente:

> "**ARTÍCULO 36**
>
> Principios de protección de datos personales
> 1. En el tratamiento de datos personales, los servidores públicos del Instituto deberán observar los principios de licitud, calidad de los datos, información al titular, consentimiento, seguridad, confidencialidad y finalidad para la que fueron recabados. Con el propósito de detallar los principios antes aludidos, el Comité emitirá los Lineamientos obligatorios para los órganos que posean datos personales.
> […]"

Asimismo, el numeral 39 de los Lineamientos ARCO dispone lo siguiente:

> "**39.** En los casos en que se hayan incorporado datos falsos en los registros de los ciudadanos, ya sea por un error de procesamiento, por un tercero o en forma dolosa, los ciudadanos o sus representantes legales podrán solicitar el cotejo y posterior supresión de datos personales del padrón electoral. Para tal efecto la Dirección Ejecutiva aplicará los procedimientos técnico-operativos de depuración correspondientes."

De conformidad con lo anterior, se puede advertir que el principio de calidad implica las obligaciones siguientes para el INE:

1. Procurar que los datos personales sean exactos y actualizados, para lo cual, deberá revisar y actualizar anualmente el Padrón Electoral, conforme a las acciones señaladas por la normativa aplicable.
2. Sustituir, rectificar, completar o suprimir, de oficio, los datos personales que fueren inexactos, incompletos o falsos en el momento en que tengan conocimiento de esta situación, aplicando los procedimientos que al efecto se establezcan.

Ahora bien, es importante señalar que el artículo 36 del RINEMTAIP antes citado, establece que el Comité de Información del INE emitirá los lineamientos en los que se desarrollen los principios rectores de la protección de datos personales. Sin embargo, de acuerdo con lo informado por el INE en la reunión celebrada en este Instituto el 27 de febrero de 2015, no se han emitido dichos lineamientos, por lo que no existe documento normativo alguno en el que se detallen los mecanismos para cumplir con el principio de calidad.

En ese sentido, a partir de las obligaciones identificadas en el marco regulatorio que resulta aplicable al tratamiento de datos personales que realiza el INE, a continuación se analizará la forma en que el proyecto de Servicio de Verificación atiende el principio de calidad y se emitirán recomendaciones al respecto.

Obligación 1. Procurar que los datos personales sean exactos y actualizados, para lo cual, se deberá revisar y actualizar anualmente el Padrón Electoral, conforme a las acciones señaladas por la normativa aplicable.

De conformidad con la información proporcionada por el INE en los diversos documentos presentados ante este Instituto con motivo de la presente opinión técnica, los datos personales que se tratarán en el Servicio de Verificación son aquéllos que se obtienen para la integración del Padrón Electoral, la emisión de credenciales para votar y la incorporación de la lista nominal de electores.

En ese sentido, y en virtud de que el INE mediante oficio INE/DERFE/1108/2014, manifestó que la base de datos del Servicio de Verificación está integrada con información del Sistema Integral de Información del Registro Federal de Electores (SIIRFE), la cual integra el Padrón Electoral, la observancia al principio de calidad por parte del INE, será respecto de ambas bases de datos: Padrón Electoral y Servicio de Verificación.

Al respecto, y a través de los Anexos Técnicos versiones 3.1 y 3.2, que el INE adjuntó en sus oficios INE/DERFE/1108/2014 e INE/DERFE/356/2015, en sus páginas 10 y 8, respectivamente, señalan:

> "[…]
>
> 1.La base de datos sobre la cual operarán las consultas de datos, estará conformada con la información necesaria de la base de datos del Sistema Integral de Información del Registro Federal de Electores (SIIRFE), misma que no será accesible por "LA INSTITUCIÓN" bajo ninguna circunstancia.
>
> 2.La base de datos de operación será actualizada por "EL INE" de forma diaria para proporcionar las consultas de verificación que se realicen
> […]"

Lo anterior fue reiterado por el INE en la reunión del 27 de febrero de 2015 en la que señaló:

> "[…]
>
> 8. ¿El INE tiene previsto almacenar los datos personales de la credencial para votar que son cotejados por las instituciones y entidades privadas? En caso de ser afirmativa la respuesta, ¿cuál es tiempo estimado de almacenamiento de los datos personales? ¿cuál es la finalidad que se persigue con dicho almacenamiento? ¿se pretende conformar una base de datos personales a partir de las solicitudes de cotejo y validación de las instituciones públicas y entidades privadas?
>
> RESPUESTA: Como se señaló en preguntas anteriores, es un almacenamiento momentáneo para comparación del dato correspondiente, por lo que no se genera una base de datos adicional a la existente.
>
> 24. Aclarar si la base de datos conformada con la información necesaria del Sistema Integral de Información del Registro Federal de Electores (SIIRFE) se generará con una Query[2], o si se va crear una base de datos adicional e independiente respecto a los datos contenidos en la base de datos del Padrón Electoral.
>
> • En caso de que sea una base paralela e independiente: ¿cada cuánto tiempo se actualizará la misma y cómo se garantiza la calidad de la información en ambas bases de datos?
> • En caso de que sea una Query: ¿cada cuánto tiempo se actualiza la base de datos del Padrón Electoral?
>
> RESPUESTA: A partir de los 10 datos señalados que se extraen de la base del SIIRFE, se genera una base de datos paralela e independiente del mismo, lo cual se realiza a través de una Query, que se crea para el sistema de verificación, y que se utiliza para hacer la confronta. Es una base de datos que se actualiza diariamente. Toda la operación del SIIRFE se refleja en la base del sistema de verificación y se hace una actualización dos veces al día (promedio, cada 12 horas). El INE llevará a cabo el registro del sistema de verificación.
> […]"

A partir de lo anterior, se advierte que con relación al contenido de la base de datos del Sistema de Verificación, ésta se obtendrá a través de una Query (base espejo), para realizar la comparación entre los 10 datos de entrada del servicio web, definidos por el INE y la base de datos del Padrón Electoral. Esto significa que el almacenamiento de dicha consulta sólo será momentáneo.

[2] Query: es una consulta que se ejecuta continuamente en un servidor la cual arroja datos de salida una vez que realiza cálculos continuos a partir de los parámetros de entrada. Consultado en: https://msdn.microsoft.com/es-es/library/ms165911.aspx

Ahora bien, en cuanto al procedimiento para llevar a cabo la actualización de la información que será utilizada para el Servicio de Verificación, el INE señaló que la base de datos de dicho sistema se actualiza diariamente (promedio, cada 12 horas). De igual forma y a pregunta expresa de este Instituto, el INE mediante oficio INE/DERFE/356/2015, informó lo siguiente:

> "[…]
> 25. Especificar el procedimiento para llevar a cabo la actualización de la información que será utilizada para el Servicio de verificación de los datos contenidos en la Credencial para Votar.
>
> RESPUESTA: Procedimiento de actualización de la información del Servicio de Verificación de datos de la Credencial para Votar:

Paso	Descripción
1	Se ingresa al Portal de Administración de la solución para programar trabajos de actualización
2	Se programa un trabajo de actualización para datos y otro para huellas
3	Se ejecutan los trabajos anteriormente indicados, iniciando el proceso de actualización de la base de datos para el Servicio de Verificación.
4	Se verifica que concluya exitosamente el proceso y se ejecutan procedimientos de validación
5	Se envía el reporte diario de trabajos de actualización ejecutados.

> Este procedimiento se realiza cada 12 y 24 horas."

Como se puede observar, el INE tiene considerado para la prestación del Servicio de Verificación llevar a cabo una actualización diaria del Sistema de Verificación, que se realizará cada 12 y 24 horas, lo cual se considera adecuado a fin de garantizar que la comparación de datos que se realiza a través de este servicio, sea con datos actualizados de los titulares y que son extraídos de la base de datos del Padrón Electoral.

Por lo que respecta a la base de datos del Sistema Integral de Información del Registro Federal de Electores, se puede apreciar que, conforme a la normativa aplicable, el INE, a través de la DERFE, está obligado a revisar y actualizar anualmente el Padrón Electoral y para ello, la LGIPE establece una serie de acciones para llevar a cabo dicha revisión y actualización, las cuales se señalan a continuación:

- Llevar a cabo campañas intensas para convocar y orientar a la ciudadanía a cumplir con las obligaciones en materia electoral.
- Utilizar la técnica censal parcial en distritos o secciones o partes de éstos, en aquellos casos en que así lo decida la Junta General Ejecutiva.
- Recabar de los órganos de las administraciones públicas federal y estatal la información necesaria para registrar todo cambio que afecte al Padrón Electoral.

Aunado a lo anterior, de los proyectos de convenios de apoyo y colaboración a suscribirse tanto con instituciones públicas como privadas, que exhibió el INE mediante oficio No. INE/DERFE/356/2015, se aprecia lo siguiente:

- Proyecto de convenio de apoyo y colaboración a suscribirse con instituciones públicas, que en su parte conducente señala:

"[…]

I. DE "EL I.N.E."
[…]

I.7 Que a través de "LA D.E.R.F.E. se realizan campañas de actualización al Padrón Electoral con el objeto de convocar y orientar a la ciudadanía a cumplir con su deber cívico de incorporarse o actualizar sus datos, según lo establecen los artículos 138, párrafos 1 al 4 y 139 de la Ley General de Instituciones y Procedimientos Electorales.

QUINTA.- Las obligaciones de "_____", son las siguientes:
[…]

b) Apoyar a "EL I.N.E." en la difusión y promoción de los programas que dirige a la ciudadanía relacionados con la actualización de la Credencial para Votar, así como para los efectos del presente Convenio.
[…]"

- Proyecto de Convenio de apoyo y colaboración a suscribirse con instituciones privadas, que en su parte conducente señala:

"[…]

I. DE "EL I.N.E."
[…]

I.7 Que a través de "LA D.E.R.F.E. se realizan campañas de actualización al Padrón Electoral con el objeto de convocar y orientar a la ciudadanía a cumplir con su deber cívico de incorporarse o actualizar sus datos, según lo establecen los artículos 138, párrafos 1 al 4 y 139 de la Ley General de Instituciones y Procedimientos Electorales.

QUINTA.- Las obligaciones de "_____", son las siguientes:
[…]

b) Apoyar a "EL I.N.E." en la difusión y promoción de los programas que dirige a la ciudadanía relacionados con la actualización de la Credencial para Votar, así como para los efectos del presente Convenio.

d) "_____" se compromete a cubrir una cuota de recuperación de manera mensual, derivada de las consultas realizadas a "EL I.N.E." en los términos señalados en el Anexo Económico Administrativo en infraestructura dedicada para la verificación de la CPV, con la finalidad de que "EL I.N.E.", a través de la "D.E.R.F.E.", mantenga actualizada de manera permanente la base de datos del Registro Federal de Electores y en consecuencia se cumpla con el objeto del presente Convenio."

En ese sentido, se observa que el cumplimiento de la obligación de actualización por parte del INE, se ve fortalecido con la firma de los convenios que en su caso llegue a celebrar con instituciones tanto públicas como privadas, lo cual permitirá al INE contar con otros medios para allegarse de información sobre la situación de las Credenciales para Votar, además de que también se podrá apoyar para la difusión y promoción de sus programas dirigidos a la ciudadanía para la actualización de los datos de la Credencial para Votar.

Con independencia de lo anterior, se sugiere revisar la redacción del inciso d, de la cláusula Quinta del convenio con instituciones privadas, ya que se da a entender que a partir del pago de la contraprestación, el INE mantendrá actualizado la

base de datos del Registro Federal de Electores, lo cual se considera inexacto, pues eso es una obligación legal del INE, que tiene que cumplir sin la necesidad de recibir esta cuota de recuperación.

Obligación 2. Sustituir, rectificar, completar o suprimir, de oficio, los datos personales que fueren inexactos, incompletos o falsos en el momento en que tengan conocimiento de esta situación, aplicando los procedimientos que al efecto se establezcan.

En virtud de que la base de datos del Servicio de Verificación se integra a partir de la información que conforma el Padrón Electoral, por lo que la primera es sólo un espejo de la segunda, esta obligación se tiene que cumplir necesariamente a través de las acciones que tome el INE con relación al Padrón Electoral.

Ahora bien, de la normatividad referida con anterioridad se tiene que existen las siguientes acciones previstas para el cumplimiento de esta obligación:

- Por lo que se refiere a la acción de rectificar los datos que fueren inexactos o incompletos la LGIPE prevé que:
  - En las oficinas del Registro Federal de Electores existirán a disposición de los ciudadanos los formatos necesarios para la presentación de la solicitud de rectificación.
  - Una vez que se da por concluida la aplicación de la técnica censal total, la DERFE verificará que no existan duplicaciones, a fin de asegurar que cada elector aparezca registrado una sola vez.
  - La DERFE dará de baja del padrón electoral a los ciudadanos que hubiesen avisado su cambio de domicilio mediante solicitud en que conste su firma, huellas dactilares y, en su caso, fotografía.
  - La DERFE reincorporará al padrón electoral a los ciudadanos que sean rehabilitados en sus derechos políticos una vez que sea notificado por las autoridades competentes, o bien cuando el ciudadano acredite con la documentación correspondiente que ha cesado la causa de la suspensión o ha sido rehabilitado en sus derechos políticos.
  - Serán dados de baja del Padrón Electoral los ciudadanos que hayan fallecido, siempre y cuando quede acreditado con la documentación de las autoridades competentes o, en su defecto, mediante los procedimientos que determine la Comisión Nacional de Vigilancia.
- De manera adicional, en los Lineamientos ARCO se prevé que en los casos en que se hayan incorporado datos falsos en los registros de los ciudadanos, ya sea por un error de procesamiento, por un tercero o en forma dolosa, los ciudadanos o sus representantes legales podrán solicitar el cotejo y posterior supresión de datos personales del padrón electoral. Para tal efecto, la DERFE aplicará los procedimientos técnico-operativos de depuración correspondientes.

A partir de lo anterior, y de una consulta que este Instituto realizó al portal del INE, se encontró que éste, a través de la DERFE, cuenta con procedimientos técnico-operativos de depuración para las bases de datos que tiene en su posesión, ya que dentro de la normativa aplicable a la DERFE[3] se contemplan procedimientos relacionados con la obligación de verificar y depurar, dentro de los cuales se encuentran los siguientes procedimientos:

- Procedimiento para la cancelación de solicitudes de trámite y aplicación de las bajas correspondientes.
- Procedimiento para el Tratamiento de Registros y Trámites con Datos Personales Irregulares.
- Procedimiento para la detección y baja de registros duplicados.
- Procedimiento para dar tratamiento a las notificaciones de defunción que emite el Registro Civil.

[3] Disponible para su consulta en: http://norma.ine.mx/es/web/normateca/direccion-ejecutiva-del-registro-federal-de-electores

- Procedimiento alterno para dar de baja del Padrón Electoral los registros de ciudadanos fallecidos.
- Procedimiento para dar tratamiento a las notificaciones de suspensión de derechos políticos que formula la autoridad jurisdiccional.
- Procedimiento de reincorporación al padrón electoral de ciudadanos rehabilitados en sus derechos políticos por notificación judicial.
- Procedimiento para dar tratamiento a las notificaciones de pérdida de la ciudadanía o renuncia a la nacionalidad que formule la Secretaría de Relaciones Exteriores.

Como es posible observar, el INE cuenta con una serie de procedimientos previstos para la implementación de acciones que permitan dar cumplimiento a la obligación de sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos o incompletos en el momento en que tengan conocimiento de esta situación, para los datos contenidos en el Padrón Electoral, lo cual se considera adecuado toda vez que, como ha sido señalado, la base de datos personales que nutre al Sistema de Verificación es la del Padrón Electoral.

En virtud de lo anterior, en relación con el principio de calidad, el INAI emite las siguientes observaciones y recomendaciones:

1. Considerar los diversos escenarios en los cuales, eventualmente, el INE pudiera estar impedido para validar los datos que se aporten en los trámites que realicen los ciudadanos ante las instituciones públicas y privadas con las que suscriba convenios de colaboración, como podrían ser, casos de duplicidad u homonimias, entre otros.

2. Respecto de la base de datos del Sistema de Verificación:

    - Tomar las medidas necesarias a efecto de que la actualización de la información del Sistema de Verificación se lleve a cabo conforme al procedimiento que al efecto indicó el INE, el cual se realiza diariamente, cada 12 y 24 horas, para ello, deberá considerar:
        - Que la programación que se realiza en el portal de administración de la solución funcione de manera correcta, tanto para el caso de datos como en el caso de huellas; y
        - Que no existan factores que afecten el proceso de actualización de la base de datos, permitiendo que se concluya de manera exitosa.
    - Verificar que la información contenida en el Sistema de Verificación se almacene de manera momentánea, de tal forma que sólo cumpla con su objetivo de comparar el dato correspondiente.
    - Contar con evidencia documental de que se actualizan los datos conforme al periodo señalado (diariamente) y que se eliminan aquéllos que recibe el INE.

3. Respecto de la base de datos del Sistema Integral de Información del Registro Federal de Electores, de conformidad con lo previsto en los artículos 54, 127, 138, 144 y 154 de la LGIPE:

    - Tomar las medidas necesarias a efecto de que la actualización de la información del SIIRFE se lleve a cabo de manera expedita.
    - Adoptar las medidas necesarias para garantizar que se sustituyan, rectifiquen o completen, de oficio, los datos personales que fueren inexactos o incompletos en el momento en que tengan conocimiento de esta situación. Lo anterior atendiendo a los procedimientos que el INE tiene establecidos para dichas actividades según lo dispuesto por la LGIPE, y en observancia de lo señalado en el artículo 20, fracciones IV y V de la LFTAIPG.

- Contar con evidencia documental de la actualización que se realiza a la base de datos del SIIRFE, así como de la sustitución, rectificación o complementación de los datos personales que el INE, en su caso, lleva a cabo de oficio.
- Verificar que, efectivamente, las instituciones tanto públicas como privadas, a las que preste el Servicio de Verificación, apoyen en la difusión y promoción de los programas que el INE dirige a la ciudadanía relacionados con la actualización de la Credencial para Votar.

7. Deber de seguridad

Importante: el análisis y recomendaciones del deber de seguridad se realizan a partir de lo informado por el INE en las reuniones celebradas en este Instituto y en los escritos presentados para la elaboración de esta opinión técnica. Este análisis no incluye pruebas de penetración, auditorías, ni peritajes a los sistemas del INE y del Servicio de Verificación, por lo que las manifestaciones del INAI no se pueden entender como vistos buenos a la implementación de medidas de seguridad en dicho servicio, sino que se limitan a realizar recomendaciones y observaciones sobre el sistema de gestión para la seguridad de los datos personales.

De conformidad con los estándares internacionales y mejores prácticas en materia de seguridad de la información y protección de datos, el deber de seguridad obliga a los responsables del tratamiento de datos personales a preservar la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades establecidas por la normatividad aplicable.

El objetivo de implementar controles de seguridad es que cada uno de ellos ayude a reducir el riesgo de que se materialice un incidente como daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado de los datos personales. Así, la práctica internacional recomienda que para establecer medidas de seguridad se lleve a cabo un proceso de mejora continua a través de un *Sistema de Gestión,*[4] de acuerdo con el modelo y objetivos de la organización.

Con relación a este deber, la fracción VI del artículo 20 de la LFTAIPG, establece que los sujetos obligados deberán adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Por su parte, el RINEMTAIP, en su artículo 36, señala que en el tratamiento de datos personales, los servidores públicos del INE deberán observar los principios de licitud, calidad de los datos, información al titular, consentimiento, **seguridad**, confidencialidad y finalidad para la que fueron recabados, y que los datos personales, incluso cuando no conste clasificación alguna al respecto, se entenderán como confidenciales. Además, en el artículo 37 del mismo ordenamiento se menciona que el INE no podrá difundir los datos personales que obren en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado consentimiento expreso.

En particular, los Lineamientos ARCO, con relación a la validación o cotejo de datos personales proporcionados por instancia públicas y privadas, en su artículo 45 señala que el INE, por conducto de la DERFE, a través de la suscripción de convenios de apoyo y colaboración y bajo mecanismos de seguridad, establecerá los procedimientos para verificar los datos personales que soliciten las instancias públicas y privadas, mediante el uso de tecnologías. Además, en su artículo 47 se menciona que la verificación de los datos personales proporcionados por las instancias públicas o privadas, se circunscribirá exclusivamente a su cotejo con los datos personales que obren en el Registro Federal de Electores, sin que esto implique en forma alguna la entrega de los mismos a las referidas instancias.

Asimismo, los Lineamientos ARCO, en su artículo 62, señalan que por ningún motivo se proporcionarán los datos personales de las y los ciudadanos en posesión de la DERFE, a terceros, ni a instancias públicas y privadas que los soliciten, con excepción de lo dispuesto en la normatividad aplicable. En materia de seguridad, el artículo 64 indica que los servidores públicos del INE que utilicen los datos en posesión de la DERFE, deberán garantizar en todo momento su protección y

[4] **Sistema de Gestión:** Se define como un conjunto de elementos y actividades interrelacionadas para establecer metas y los medios de acción para alcanzarlas.

salvaguarda, y que su uso será exclusivamente para el cumplimiento de las obligaciones legales y reglamentarias, con base en las cuales fueron solicitados.

Ahora bien, para coadyuvar al cumplimiento del deber de seguridad, el INAI publicó en el Diario Oficial de la Federación, el 30 de octubre del 2013, las Recomendaciones en materia de Seguridad de Datos Personales.[5] Si bien, éstas fueron concebidas para facilitar el cumplimiento del deber de seguridad por parte de los sujetos obligados de la LFPDPPP, se considera que las mismas son un instrumento que puede servir de base para revisar la conformidad de las medidas de seguridad en el tratamiento de datos personales, debido a que fueron desarrolladas a partir de un ejercicio de análisis y síntesis de las mejores prácticas internacionales en la materia.

En dichas Recomendaciones, el INAI plantea como recomendación general la adopción de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en estándares internacionales y mejores prácticas en materia de seguridad de la información y protección de datos personales, tales como:

- BS 10012:2009, Data protection–Specification for a personal information management system.
- ISO/IEC 27001:2005, Information Technology–Security techniques–Information security management systems – Requirements.
- ISO/IEC 27002:2005, Information Technology–Security techniques–Code of practice for security management.
- ISO/IEC 27005:2008, Information Technology–Security techniques–Information security risk management.
- ISO/IEC 29100:2011, Information technology–Security techniques–Privacy framework.
- ISO 31000:2009, Risk management–Principles and guidelines.
- ISO GUIDE 72, Guidelines for the justification and development of management systems standards.
- ISO GUIDE 73, Risk management–Vocabulary.
- ISO 9000:2005, Quality management systems–Fundamentals and vocabulary.
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.
- OECD Guidelines for the Security of Information Systems and Networks–Towards a Culture of Security.

El SGSDP se define como un sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

El SGSDP tiene como objetivo mantener vigente y mejorar el cumplimiento de las obligaciones establecidas en la normatividad de protección de datos personales, así como fomentar las buenas prácticas, a través de un marco de trabajo para el tratamiento de la información, basado en el modelo denominado “Planificar-Hacer-Verificar-Actuar” (PHVA), a través del cual se dirigen y controlan los procesos o tareas.

Las fases del ciclo PHVA considera diferentes pasos y objetivos específicos para el SGSDP, que pueden observarse en la siguiente tabla:

[5] Las Recomendaciones se encuentran disponibles en: (http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013).

Ciclo	Fases	Pasos	Objetivos Específicos
Planificar	Planear el SGSDP	1. Alcance y objetivos. 2. Política de gestión de datos personales. 3. Funciones y obligaciones de quienes traten datos personales. 4. Inventario de datos personales. 5. Análisis de riesgos de los datos personales. 6. Identificación de las medidas de seguridad y análisis de brecha.	Definir los objetivos, políticas, procesos y procedimientos relevantes del SGSDP para **gestionar los riesgos de los datos personales**, con el fin de **cumplir con la legislación sobre protección de datos** y obtener resultados acordes con las políticas y objetivos generales de la organización.
Hacer	Implementar y operar el SGSDP	7. Implementación de las medidas de seguridad aplicables a los datos personales.	Implementar y operar las políticas, objetivos, procesos, procedimientos y controles o mecanismos del SGSDP, considerando indicadores de medición.
Verificar	Monitorear y revisar el SGSDP	8. Revisiones y auditoría.	Evaluar y medir el cumplimiento del proceso de acuerdo con la **legislación de protección de datos personales**, la política, los objetivos y la experiencia práctica del SGSDP, e informar los resultados a la Alta Dirección para su revisión.
Actuar	Mejorar el SGSDP	9. Mejora continua y Capacitación.	Para lograr la mejora continua se deben adoptar medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión por parte de la Alta Dirección, las auditorías al SGSDP y de la comparación con otras fuentes de información relevantes, como actualizaciones regulatorias, riesgos e impactos organizacionales, entre otros. Adicionalmente, se debe considerar la capacitación del personal.

Tabla 1. Objetivos del SGSDP dentro de las fases del ciclo PHVA

Visto lo anterior, y con el objetivo de brindar una opinión técnica sobre las medidas o mecanismos relacionados al deber de seguridad en el marco del Servicio de Verificación, el INAI utilizará la estructura de las Recomendaciones como base para realizar sus observaciones.

Cabe señalar que respecto a la implementación de un Sistema de Gestión de Seguridad de la Información,[6] el INE, en la minuta de la reunión sostenida el 27 de febrero de 2015, manifestó que "[s]e cuenta con un sistema de gestión de seguridad para la protección de la información del Padrón Electoral" y que "[e]l Sistema de gestión de Seguridad de la Información está basado en el estándar ISO 27001:2005 que inició en diciembre de 2013". Sin embargo, no proporcionó información adicional al respecto.

En ese sentido, a partir de las obligaciones identificadas en el marco regulatorio que resulta aplicable al tratamiento de datos personales que realiza el INE y de los estándares nacionales e internacionales antes descritos, a continuación se analizará la

[6] Sistema de Gestión de Seguridad de la Información (SGSI): Consiste en las políticas, procedimientos, pautas, recursos y actividades asociadas, con el objetivo de la protección de sus activos de información. Un SGSI tiene un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para tratar y gestionar los riesgos con eficacia.

forma en la que el proyecto Servicio de Verificación atiende el deber de seguridad y se emitirán las recomendaciones dentro del esquema del SGSDP.

Fase 1. Planear el SGSDP

Paso 1. Establecer el alcance y objetivos del sistema. Se deberán identificar y definir con precisión los alcances y objetivos del Servicio de Verificación

Al respecto, en el apartado 2, denominado *Objetivo,* del Anexo Técnico 3.2 se señala lo siguiente:

> "Establecer las bases y mecanismos técnicos necesarios que permitan la verificación por parte de **"EL INE"** de los datos de los ciudadanos, contenidos en la credencial para votar que solicite **"LA INSTITUCIÓN"** y que forman parte del alcance del servicio, […]"

Además, en la sección 4.2.3., denominada *Alcances de las consultas de verificación de datos,* del mismo Anexo, se señala que la verificación de datos de la credencial para votar servirá para validar la información (texto y minucias), a partir del número OCR o CIC.

Asimismo, en la reunión celebrada el 20 de abril, el INE manifestó que el Servicio de Verificación permitirá al INE mantener depurado y actualizado el Padrón Electoral.

Como se observa, los alcances y objetivos del Servicio de Verificación están identificados, por una parte, a la institución pública y privada, así como al ciudadano interesado, el servicio les permitirá acreditar la vigencia de la credencial para votar y verificar que los datos contenidos en la misma correspondan a los que obran en el Padrón Electoral, y por otra parte, al INE le permite mantener depurado y actualizado dicho padrón. No obstante, **se recomienda que en los documentos relevantes, como el convenio y sus anexos, quede con mayor claridad y exactitud, definidos estos alcances y objetivos, ya que los mismos se fueron explicando a través de los documentos proporcionados por el INE a este Instituto, sin que los mismos se expliquen de manera conjunta e integral en los documentos.**

Asimismo, en el alcance del Servicio de Verificación es importante que el INE establezca como regla sólo prestar el servicio a aquellas instituciones que estén reguladas en el tratamiento de datos personales que efectúen, y sólo en los casos en las que las finalidades para las cuales se aplicará el Servicio de Verificación sean lícitas y correspondan a sus atribuciones u objetivos establecidos en los documentos que regulen su actuación.

Paso 2. Definir la política de gestión de datos personales. A partir del objetivo y alcances del Servicio de Verificación definidos, se deberán contar con políticas de seguridad que ayuden a preservar la confidencialidad, integridad y disponibilidad de los datos

Con relación a este paso, en el apartado *4.2.2. Seguridad de la Información* del Anexo Técnico 3.2, se identificó que el INE cuenta con las siguientes políticas de seguridad:

- La información que entregue "**LA INSTITUCIÓN**" a "**EL INE**" será utilizada únicamente para la verificación de la misma, comparándola con la existente en el servicio de verificación de datos de la credencial para votar, dicha información no será compartida con institución alguna.
- El acceso al servicio web por parte de "**LA INSTITUCIÓN**" será exclusivamente por los medios que establezca "EL INE" para la solución Hyper Text Transfer Protocol Secure (HTTPS).

- "**LA INSTITUCIÓN**" no tendrá acceso a ningún sistema de la solución vía File Transfer Protocol (FTP), Telecommunication Network (Telnet), Secure SHell (SSH), Secure File Transfer Protocol (SFTP) o cualquiera no autorizado expresamente por "EL INE".
- "**EL INE**" y "**LA INSTITUCIÓN**" establecerán de forma conjunta las especificaciones detalladas de las etapas de implementación de la solución.
- "**EL INE**" mantendrá sincronizados los servidores que soportan los sistemas a través de un servidor de tiempo vía Network Time Protocol (NTP), con el objetivo de identificar las transacciones de acuerdo a la fecha y hora en que éstas se llevaron a cabo.
- El certificado SSL del servidor será tramitado por "**EL INE**".
- La comunicación por parte de "**LA INSTITUCIÓN**" será únicamente al Portal de Verificación y no se permitirá a otra infraestructura provista por "**EL INE**".
- "**EL INE**" y "**LA INSTITUCIÓN**" establecerán los mecanismos de seguridad y los protocolos de comunicación permitidos y puertos de comunicación a utilizar, tanto para el acceso a los sistemas, como de comunicación entre ambas instituciones.
- Los equipos y software requeridos para el aseguramiento de las comunicaciones entre "**EL INE**" y "**LA INSTITUCIÓN**" serán determinadas de forma conjunta y deberán ser provistas por "**LA INSTITUCIÓN**".
- "**EL INE**" se reserva el derecho de detener los sistemas en caso de que se evidencie o manifieste un incidente de seguridad crítico en la infraestructura de "**EL INE**", para lo cual "**EL INE**" notificará a "**LA INSTITUCIÓN**" de forma inmediata a través de los responsables designados.
- En caso de que se identifique una probable vulneración a la protección de datos personales, "**EL INE**" dará vista al Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).
- "**LA INSTITUCIÓN**" deberá establecer al menos las mismas medidas de seguridad y de protección de datos personales con las que cuenta "**EL INE**" para el sistema de verificación.
- El "**Comité Técnico**" deberá establecer los procedimientos para la verificación del cumplimiento de obligaciones en materia de seguridad de la información y protección de datos personales."

Además de lo antes referido, **se recomienda que para establecer las políticas de seguridad del Servicio de Verificación, el INE considere la obligación de cumplir con la normatividad en materia de protección de datos personales por parte de todos los involucrados en el tratamiento.** Algunas reglas a considerar para la elaboración de dichas políticas son:

- Suprimir los datos contenidos en las vistas y consultas realizadas por el Servicio de Verificación cuando éstas hayan dejado de ser necesarias para el cumplimiento de las finalidades previstas.
- Considerar un procedimiento de eliminación seguro de la información.
- Tratar los datos estrictamente el tiempo necesario para los propósitos del Servicio de Verificación.
- Limitar el tratamiento de los datos al cumplimiento de los propósitos del Servicio de Verificación.
- Garantizar la confidencialidad de los datos.
- Identificar el flujo y ciclo de vida de los datos personales: por qué medios se recaban, en qué procesos se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen.
- Documentar la implementación de medidas de seguridad del Servicio de Verificación.

Por otra parte, respecto de las cláusulas contractuales y cartas de confidencialidad, se hace referencia a lo previsto por la cláusula sexta, inciso c), de los convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas, en su versión del 18 de marzo de 2015, que establece lo siguiente:

"SEXTA.- Las obligaciones de ambas partes, son las siguientes: […]

c) Proteger los datos personales de los ciudadanos conforme a lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental [Ley Federal de Protección de Datos Personales en Posesión de

> los Particulares, en el caso del Convenio aplicable a instituciones privadas], la Ley General de Instituciones y Procedimientos Electorales, el Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública y los Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores, en el ámbito de competencia de cada una de estas instituciones. […]"

Visto lo anterior, en el convenio referido se tiene contemplado que las instituciones protejan los datos personales que traten de conformidad con lo previsto por la LFTAIPG, la LFPDPPP, en el caso de instituciones privadas, así como de conformidad con lo previsto por la LGIPE, el RINEMTAIP y los Lineamientos ARCO.

No obstante, no se incluye la referencia a otra normativa que pudiera aplicar, por ejemplo, normativa local de protección de datos personales en caso de que el Servicio de Verificación se proporcione a instituciones públicas locales.

Respecto a este punto, se hace referencia al Anexo 1 del Anexo Técnico 3.2, en donde se prevé una cláusula segunda relacionada con una Declaratoria de confidencialidad y aceptación de las condiciones generales del mecanismo de pruebas en relación al Servicio de Verificación de datos de la Credencial para Votar, los lineamientos para la conexión segura y de la vigencia para la conexión VPN, la cual establece que tanto el INE como el Usuario declaran:

> "[…]
> - Tener conocimiento de que la información a la que tendrá acceso puede ser considerada como CONFIDENCIAL en los términos que marca la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, la Ley General de Instituciones y Procedimientos Electorales, el Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública y los Lineamientos para el Acceso, Rectificación, Cancelación , Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores.
>
> - Tener pleno conocimiento y aceptar que las actividades que desarrollará con el acceso solicitados serán en estricto apego a la Ley, manteniendo absoluta confidencialidad y cuidado para conservar la información, asumiendo la obligación de abstenerse de revelar la información a que tengan acceso a tercero, así como utilizarla en provecho propio y terceros, o reproducirla por cualquier medio obligándose a notificar de inmediato cualquier caso del que tenga conocimiento cuya conducta contravenga la Leo o Políticas Institucionales. […]
>
> Que aceptan que la contravención a la Normatividad vigente y a la presente declaratoria, generará sanciones administrativas y/o de tipo penal a que haya lugar, en materia de transparencia. […]"

Cabe señalar que en la declaratoria de confidencialidad citada, falta claridad respecto de los siguientes puntos: i) con relación al mecanismo de pruebas, que el INE no proporcionará a las instituciones públicas o privadas ningún dato personal en posesión del INE y ii) que las instituciones públicas y privadas están obligadas a guardar la confidencialidad de los datos personales tratados en el contexto del mecanismo de pruebas vinculadas al Servicio de Verificación, con fundamento en la LFTAIPG y las LFPDPPP, respectivamente, así como con fundamento en cualquier otra normativa aplicable.

Adicionalmente, el INE, a través del oficio INE/DERFE/356/2015, presentó el texto de una carta de confidencialidad, transcrita en el apartado correspondiente al Deber de Confidencialidad, la cual, se solicitará ser firmada por personal del INE y prestadores de servicio que traten datos personales del Registro Federal de Electores en el marco del Servicio de Verificación.

De esta manera, se concluye que se tienen previstas cláusulas contractuales, declaratorias de confidencialidad y cartas de confidencialidad que hacen referencia a ciertas obligaciones en materia de protección de datos personales de las partes. No

obstante, se recomienda mayor claridad en dichos textos considerando: la naturaleza de las instituciones con las que el INE celebre un convenio, y ii) los tratamientos de datos personales que se realizaran por parte del INE y de las instituciones públicas y privadas.

Por último, se sugiere incluir como política del INE la suspensión del Servicio de Verificación en los casos en que el INE tenga conocimiento que la institución no está tratando debidamente los datos personales.

Paso 3. Establecer funciones y obligaciones de quienes traten datos personales. Se deben definir los roles, responsabilidades, cadena de rendición de cuentas y estructura organizacional del Servicio de Verificación

La estructura del INE que se encargará de atender las actividades consignadas para el Servicio de Verificación se describen en el apartado 5.1 Definición de Roles y Responsabilidades del Anexo Técnico 3.2.

No se omite señalar que, de conformidad con la reunión del 27 de febrero de 2015, el INE mencionó que únicamente las áreas de la DERFE tendrán acceso al Servicio de Verificación, en tanto que dicha unidad administrativa es la responsable de la conformación del Padrón Electoral.

De lo manifestado por el INE, se advierte que contempla una descripción general de los perfiles del personal con sus funciones y obligaciones. No obstante, **se recomienda que tanto el INE como las instituciones públicas y privadas se aseguren de que todos los servidores públicos y personal tengan clara su contribución para el logro de los objetivos del Servicio de Verificación, así como sus obligaciones y deberes.**

Paso 4. Elaborar un inventario de datos personales. Se deben identificar los tipos de datos involucrados en el tratamiento y su flujo en el Servicio de Verificación.

En diversa información proporcionada por el INE para la elaboración de la presente opinión técnica, dicho Instituto señaló que los datos que se utilizarán para el Servicio de Verificación son los siguientes:

1. Nombre(s).
2. Apellido paterno.
3. Apellido materno.
4. CIC.
5. OCR.
6. Clave de elector.
7. Año de registro.
8. Número de emisión de la credencial de elector.
9. Huellas dactilares de los dedos índices.
10. Clave Única del Registro de Población.

Respecto al flujo de los datos, en el oficio INE/DERFE/356/2015, el INE detalló el uso de la distinta información que se genera en una solicitud, así como el tráfico entre los componentes del Servicio de Verificación.

Por lo anterior, se infiere que el INE cuenta con un inventario de datos personales vinculado al tratamiento al que son sometidos los datos.

Paso 5. Realizar el análisis de riesgo de los datos personales. Se deberán determinar las características de los riesgos que mayor impacto pueden tener sobre los datos personales que se tratan en el Servicio de Verificación

En la reunión del 27 de febrero de 2015, el INE informó que para el segundo semestre de 2015, se tiene contratado realizar un análisis de riesgo a nivel de toda la información que se encuentra contenida en todo el Padrón Electoral, tanto en formato físico, como electrónico, en todos sus procesos. No obstante, **se recomienda al INE realizar un análisis de riesgo dirigido al Servicio de Verificación y de preferencia durante las "pruebas piloto" que se están efectuando, y antes de firmar otros convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas.**

Por otra parte, en la sección III de los compromisos de las "Partes", cláusula Quinta, inciso j, del convenio con instituciones privadas, se establece que se "Deberá implementar las medidas de seguridad, administrativas, técnicas con que cuenta 'EL INE' para el Sistema de verificación de Datos, en los términos del Anexo Técnico del presente Convenio". Al respecto, **se sugiere incluir una cláusula similar en los convenios que firme con las instituciones públicas.**

Paso 6. Identificación de las medidas de seguridad y análisis de brecha. Se deberán evaluar las medidas de seguridad que ya existen en la organización, contra las que podrían faltar para proteger los datos del Servicio de Verificación.

Respecto de las medidas de seguridad, en la reunión del 27 de febrero, el INE informó que cuenta con un enlace dedicado, una *VPN* (Virtual Private Network) sobre este enlace y un canal cifrado de comunicación mediante el protocolo *TLS* (Transport Layer Security).

Por su parte, en el apartado 4.2.2 Seguridad de la Información del Anexo Técnico 3.2, el INE señaló las siguientes medidas de seguridad:

- El servicio web se proporcionará exclusivamente a través del protocolo *HTTPS* (Hyper Text Transfer Protocol Secure).
- Se mantendrán sincronizados los servidores que soportan los sistemas a través de un servidor de tiempo vía *NTP* (Network Time Protocol).
- Se utilizarán certificados *SSL* (Secure Socket Layer) tramitados por el INE.

Asimismo, en el apartado 4.5.1 Infraestructura de comunicaciones (transporte de datos) del Anexo Técnico 3.2, se mencionó que las instituciones públicas y privadas proveerán al INE del equipo de seguridad perimetral y los equipos para el Portal de Verificación con características mínimas definidas en dicho Anexo.

Además en el apartado 4.2.1 Modelo Conceptual del Anexo Técnico 3.2, el INE se comprometió a proveer los servicios básicos necesarios y la infraestructura auxiliar como UPS, aire acondicionado, instalaciones eléctricas, instalaciones de red y espacio físico necesario. Finalmente, en el mismo apartado se observa en la Figura 1. Arquitectura general de la Solución con Portal de Verificación en la red de ***"EL INE"***, que para garantizar los niveles de servicio acordados, el INE podrá disponer de dos centros de cómputo (primario y secundario).

A su vez, en el apartado 4.7.1 Protocolos de Actualización (mantenimientos, hardware, software, baja, actualización de SW) del Anexo Técnico 3.2, el INE indicó lo siguiente:

> **"**[..]**EL INE"** será el responsable y estará a cargo de llevar a cabo la actualización y/o mantenimiento de la Infraestructura Tecnológica que soportará la operación para la verificación de datos, para tal efecto deberá informar con al menos 72 horas las ventanas de mantenimiento programadas."

A partir del análisis realizado, se concluye que además de los mecanismos de seguridad mencionados, **es conveniente que el INE cuente con el resultado del análisis de riesgo aplicado al Servicio de Verificación, y así evaluar las medidas de seguridad que ya existen contra las que sería conveniente tener.** Para establecer los controles de seguridad, se pueden considerar los siguientes dominios:

- Políticas del SGSDP.
- Cumplimiento legal.
- Estructura organizacional de la seguridad.
- Clasificación y acceso de los activos.
- Seguridad del personal.
- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Desarrollo y mantenimiento de sistemas.
- Vulneraciones de seguridad.

Fase 2. Implementar y operar el SGSDP

Paso 7. Implementación de las medidas de seguridad aplicables a los datos personales. Es necesario establecer el plan de trabajo para las medidas de seguridad faltantes en el Servicio de Verificación

En la reunión del 27 de febrero, el INE manifestó que valorarán incluir en los convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas, una cláusula que solicite a las instituciones que tengan implementadas al menos las medidas de seguridad con las que cuenta el INE para el Servicio de Verificación y que esto se especificará, en su caso, en el Anexo Técnico.

Por su parte, en el apartado 4.2.2 Seguridad de la Información del Anexo Técnico 3.2, se señala que:

> "[…]
> - "**EL INE"** y "**LA INSTITUCIÓN"** establecerán los mecanismos de seguridad y los protocolos de comunicación permitidos y puertos de comunicación a utilizar, tanto para el acceso a los sistemas, como de comunicación entre ambas instituciones.
> - Los equipos y software requeridos para el aseguramiento de las comunicaciones entre **"EL INE"** y **"LA INSTITUCIÓN"** serán determinadas de forma conjunta y deberán ser provistas por **"LA INSTITUCIÓN"**."

En ese sentido, **se recomienda que el INE tome en cuenta dentro de los requerimientos del Anexo Técnico de los *convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas*, un plan de trabajo para la implementación de medidas de seguridad alineadas a las políticas, objetivos, procesos y procedimientos del Servicio de Verificación.**

Además, **se considera conveniente que tales controles o mecanismos cuenten con indicadores de medición para identificar de manera oportuna cualquier cambio en el contexto del sistema, y así mantener una visión general de la imagen del riesgo para tomar decisiones más efectivas para proteger los datos personales.**

Fase 3. Monitorear y revisar el SGSDP

Paso 8. Revisiones y Auditoría. Será necesario realizar revisiones del funcionamiento de las medidas de seguridad establecidas respecto de las políticas, alcances y objetivo del Servicio de Verificación.

Respecto a este punto, durante la reunión sostenida el 27 de febrero de 2015, el INE manifestó que en materia de datos personales "[…] no tiene previsto desarrollar mecanismos específicos para el Servicio de Verificación ya que la comprobación del cumplimiento se realizará en el marco del Sistema de Gestión de las Tecnologías de la Información que prevé los procesos de operación de los sistemas, incluido el Servicio de Verificación".

De manera complementaria, el INE indicó que "[s]í hay un procedimiento periódico de revisión a bitácoras y uso adecuado del Servicio de Verificación en el marco del Sistema de Gestión de Tecnologías de la Información".

De manera adicional, de la documentación presentada por el INE, se advierte que una de las funciones del Comité Técnico referido en la cláusula octava de los convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas, en su versión del 18 de marzo de 2015, es la verificación del cumplimiento de obligaciones en materia de protección de datos personales. Dicha cláusula establece lo siguiente:

> **"IV. DEL COMITÉ TÉCNICO**
>
> OCTAVA. Para el adecuado desarrollo de las actividades que se generarán con motivo del cumplimiento del objeto de este convenio, "LAS PARTES" están de acuerdo en integrar un Comité Técnico, mismo que estará formado por un representante de cada institución, quienes podrán ser sustituidos en cualquier tiempo previa notificación por escrito y con 10 días de anticipación a la otra parte. […]
>
> NOVENA. El Comité Técnico referido en la cláusula anterior, tendrá las siguientes atribuciones:
> a) Determinar y apoyar las acciones a ejecutar con el fin de dar cumplimiento al objeto del presente Convenio y su Anexo Técnico.
> b) Coordinar la realización de actividades señaladas en el Anexo Técnico que forma parte del presente instrumento jurídico. […]"

Por su parte, el Anexo Técnico 3.2 establece, en su apartado 5.2, lo siguiente:

> "[…] El "Comité Técnico" será deberá establecer los procedimientos para verificar el cumplimiento de obligaciones en materia de seguridad de la información y protección de datos personales. […]"

Complementariamente, en el apartado 6 del mismo documento se prevé lo siguiente:

> *"[…] Será posible, bajo común acuerdo, llevar a cabo visitas del personal involucrado en este proyecto por parte de "EL INE" y de "LA INSTITUCIÓN" a las instalaciones de ambos, con el objetivo de conocer detalladamente sus procesos. En el futuro y de común acuerdo entre "EL INE" y "LA INSTITUCIÓN", se promoverán mejoras en los sistemas de información, aprovechando los avances tecnológicos disponibles en beneficio de los procesos que relacionan a ambas instituciones, previo establecimiento de fechas y prioridades; así como la revisión previa y en su caso aprobación del "Comité Técnico". […]"*

En ese sentido, se puede observar que la supervisión o verificación relacionada con el cumplimiento de las obligaciones de protección de datos y, en especial, de la confidencialidad de los datos personales tratados durante la etapa del cotejo, se realizará a través de las verificaciones o supervisiones, incluido un procedimiento periódico de revisión a bitácoras y uso

adecuado del Servicio de Verificación, previstas por el Sistema de Gestión de las Tecnologías de la Información, así como por el Comité Técnico referido en la cláusula octava de *los* convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas, en su versión del 18 de marzo de 2015. No obstante, el INE no proporcionó mayor detalle sobre el sistema de gestión referido, ni sobre las verificaciones o supervisiones que realizará el Comité Técnico.

Asimismo, en la reunión realizada el 27 de febrero de 2015, el INE señaló que antes de poner en operación cualquier sistema se pasa por un ciclo de auditorías técnicas, y que como todavía no se tiene en operación el Servicio de Verificación, se tiene contemplada una revisión inicial.

Considerando lo anterior, **se recomienda al INE que antes de firmar nuevos convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas se lleven a cabo las auditorías técnicas que mencionó, así como su revisión inicial.** Cabe señalar que de acuerdo a las mejores prácticas, estas auditorías son necesarias aun cuando el sistema se encuentre operando como "prueba piloto".

En otro orden de ideas, en el apartado 4.2.2 Seguridad de la Información del Anexo Técnico 3.2 se menciona que:

- **"EL INE"** se reserva el derecho de detener los sistemas en caso de que se evidencie o manifieste un incidente de seguridad crítico en la infraestructura de **"EL INE"**, para lo cual **"EL INE"** notificará a **"LA INSTITUCIÓN"** de forma inmediata a través de los responsables designados.
- En caso de que se identifique una probable vulneración a la protección de datos personales, **"EL INE"** dará vista al Instituto Federal de Acceso a la Información y Protección de Datos (IFAI)."

De lo anterior, se advierte que aunque el INE contempla algunas acciones en caso de vulneraciones a la seguridad de los datos, **se recomienda mantener y documentar un plan de contingencia sobre el Servicio de Verificación, así como tener identificada la cadena de rendición de cuentas, para informar y actuar ante un incidente de seguridad. Se sugiere que dicho plan de contingencia considere al menos las siguientes etapas:**

- **Identificación de la vulneración.**
- **Notificación de la vulneración.**
- **Remediación del incidente.**

Es importante destacar que **es una buena práctica documentar las revisiones, auditorías y los tratamientos de una vulneración a la seguridad, incluyendo un resumen de los hallazgos y los planes para aplicar medidas preventivas y correctivas, además de que estos procesos ofrecen información que sirve como entrada para el ciclo de mejora continua.**

Se sugiere que el INE realice el ejercicio de "usuario simulado" para verificar que las instituciones están cumpliendo con sus obligaciones respecto de la operación del Servicio de Verificación.

Fase 4. Mejorar el SGSDP

Paso 9. Mejora continua y capacitación. Se deberán aplicar medidas preventivas y correctivas al Servicio de Verificación, así como los programas de fomento a la cultura y capacitación en protección de datos para el personal que haga uso del Servicio de Verificación.

En el apartado 5.3 Seguimiento y Evaluación del Anexo Técnico 3.2, el INE señaló que:

> "Con el fin de tener un adecuado seguimiento y control en la ejecución de las actividades establecidas en este Anexo Técnico, así como del seguimiento una vez iniciadas las operaciones, el **"Comité Técnico"** definirá las áreas de competencia de ambas Instituciones que estarán dando seguimiento a la operación e informando de la misma, a fin de garantizar el cumplimiento de los objetivos y metas.
> […]
> Será posible, bajo común acuerdo, llevar a cabo visitas del personal involucrado en este proyecto por parte de **"EL INE"** y de **"LA INSTITUCIÓN"** a las instalaciones de ambos, con el objetivo de conocer detalladamente sus procesos. En el futuro y de común acuerdo entre **"EL INE"** y **"LA INSTITUCIÓN"**, se promoverán mejoras en los sistemas de información, aprovechando los avances tecnológicos disponibles en beneficio de los procesos que relacionan a ambas instituciones, previo establecimiento de fechas y prioridades; así como la revisión previa y en su caso aprobación del **"Comité Técnico"**."

De lo anterior se infiere que el INE consideró en su plan de seguimiento y evaluación para el Servicio de Verificación, un proceso de mejora continua, sin embargo no establece alguna periodicidad para su aplicación. Al respecto, siguiendo los estándares en materia de seguridad de la información, **se sugiere que las revisiones para promover mejoras en los sistemas se realicen al menos una vez al año, o bien cuando se identifique un cambio significativo en el contexto del sistema.**

Por otra parte, con relación a la existencia de algún programa de capacitación, actualización y concienciación para el personal, sobre las obligaciones que tiene en materia de protección de datos personales en el contexto del Servicio de Verificación, en la reunión realizada el 27 de febrero de 2015, el INE señaló que está previsto que el personal que manejará el Servicio de Verificación será capacitado en materia de protección de datos personales, en el marco de un programa general de capacitación denominado "Programa de Concientización en Materia de Seguridad dentro de la DERFE", enfocado a la protección de la información del Padrón Electoral. Asimismo, el INE señaló que solicitará al INAI capacitación en la materia, a través del convenio de colaboración celebrado entre el INE y el INAI.

Por otro lado, en el apartado *6.* Otras consideraciones del Anexo Técnico 3.2 se mencionó que:

> "[…]
> Asimismo, **"EL INE"** proporcionará la capacitación que se defina sobre la evolución de la Credencial para Votar y sus elementos de seguridad a una plantilla de máximo 20 personas por curso. **"EL INE"** de común acuerdo con **"LA INSTITUCIÓN",** establecerán las fechas particulares de dichos cursos, así como el lugar de impartición."

Por lo anterior se advierte, que si bien el INE tiene definido un plan de capacitación sobre la evolución de la Credencial para Votar, **se recomienda diseñar e impartir un programa de capacitación continua, y de manera particular un módulo sobre seguridad de los datos personales para todos los involucrados en el Servicio de Verificación**. Cabe destacar que es recomendable generar evidencias de las capacitaciones impartidas, tales como la calendarización correspondiente, listas de asistencia y evaluaciones realizadas a los participantes.

En virtud de lo anterior, en relación con el deber de seguridad, el INAI emite las siguientes observaciones y recomendaciones:

1. Señalar el objetivo general y los objetivos particulares del Servicio de Verificación, así como delimitar el ámbito de aplicación relacionado con el flujo de los datos personales.

2. Que en el alcance del Servicio de Verificación el INE establezca como regla sólo prestar el servicio a aquellas instituciones que estén reguladas en el tratamiento de datos personales que efectúen, y sólo en los casos en las que

las finalidades para las cuales se aplicará el Servicio de Verificación sean lícitas y correspondan a sus atribuciones u objetivos establecidos en los documentos que regulen su actuación.

3. Considerar la obligación de cumplir con la normatividad en protección de datos personales por parte de todos los involucrados en el tratamiento, al momento de establecer las políticas del Servicio de Verificación.

4. Añadir las políticas sugeridas por este Instituto a los convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas que se establezcan en el futuro, para el Servicio de Verificación.

5. Dar claridad a los textos de las cláusulas contractuales, declaratorias de confidencialidad y cartas de confidencialidad que hacen referencia a ciertas obligaciones en materia de protección de datos personales de las partes, considerando la naturaleza que pueden tener las instituciones y los tratamientos de datos personales que se realizarán por parte del INE y de las instituciones públicas y privadas.

6. Incluir como política del INE la suspensión del Servicio de Verificación en los casos en que el INE tenga conocimiento que la institución no está tratando debidamente los datos personales.

7. Asegurar que todo el personal tenga claros sus roles, responsabilidades y contribución para el logro de los objetivos del Servicio de Verificación.

8. Realizar un análisis de riesgo al Servicio de Verificación, para evaluar las medidas de seguridad que ya existen contra las que sería conveniente tener para proteger los datos personales.

9. Incluir una cláusula similar a la de la sección III de los compromisos de las “Partes”, cláusula Quinta, inciso j, del convenio con instituciones privadas, en los convenios que firme con las instituciones públicas.

10. Considerar dentro de los requerimientos del Anexo Técnico de los convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas, un plan de trabajo para la implementación de medidas de seguridad alineadas a las políticas, objetivos, procesos y procedimientos del Servicio de Verificación.

11. Contar con indicadores de medición para los controles o mecanismos, que permitan tener una visión general de la imagen del riesgo para proteger los datos personales.

12. Mantener y documentar un plan de contingencia sobre el Servicio de Verificación, así como identificar la cadena de rendición de cuentas para informar y actuar ante un incidente de seguridad.

13. Documentar las revisiones, auditorías y los tratamientos de una vulneración a la seguridad del Servicio de Verificación.

14. Realizar las revisiones para promover mejoras en los sistemas se realicen al menos una vez al año, o bien cuando se identifique un cambio significativo en el contexto del sistema.

15. Realizar el ejercicio de “usuario simulado” para verificar que las instituciones están cumpliendo con sus obligaciones respecto de la operación del Servicio de Verificación.

16. Diseñar e impartir un programa de capacitación continua, y de manera particular un módulo sobre seguridad de los datos personales para todos los involucrados en el Servicio de Verificación.

17. Generar evidencias de cualquier capacitación impartida al personal.

Con relación a la arquitectura general de la solución del Portal de Verificación en la red del INE, se recomienda lo siguiente:

18. Garantizar que el enlace sea punto a punto, es decir, que se realice exclusivamente entre las instalaciones de las instituciones públicas o privadas y el INE, evitando siempre conexiones inalámbricas. Así como prescindir de conexiones remotas o trabajo desde casa (*home office*).

19. Garantizar que los certificados SSL (*Secure Socket Layer*) tramitados por el INE se mantengan vigentes y actualizados.

20. Realizar pruebas de penetración al Servidor de Punto de Acceso, Servidor de Comparación, Servidor de Administración y al Servidor de Base de Datos que componen el Servicio de Verificación.

21. Aplicar segregación y aislamiento en los privilegios de acceso de los usuarios a los servidores que componen el Sistema de Verificación, en particular, revisar la existencia de conexiones entre el Servidor de Administración y otros sistemas como el SIIRFE.

22. Verificar que la infraestructura de comunicaciones, seguridad y la del Portal de Verificación cuenten siempre con las últimas actualizaciones de software, firmware o hardware.

8. Deber de confidencialidad

El deber de confidencialidad consiste en la obligación de guardar secrecía respecto de los datos personales que se tratan y evitar su difusión, distribución o comercialización no autorizada, así como establecer medidas necesarias para evitar su transmisión o acceso no autorizado.

Al respecto, los artículos 18, fracción II, 20, fracción VI, 21 y 22 de la LFTAIPG señalan lo siguiente:

> "**Artículo 18**. Como información confidencial se considerará: […]
>
> II. Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley. […]
>
> **Artículo 20.** Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán: […]
>
> VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.
>
> **Artículo 21.** Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.
>
> **Artículo 22.** No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:
> I. (Se deroga). Fracción derogada DOF 11-05-2004
> II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
> III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
> IV. Cuando exista una orden judicial;
> V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y
> VI. En los demás casos que establezcan las leyes."

Por su parte, los artículos 39, párrafo 2, y 126, párrafo 3, de la LGIPE, disponen lo siguiente:

> "**Artículo 39.**
> […]
> 2. El Consejero Presidente, los Consejeros Electorales, el Secretario Ejecutivo y los demás servidores públicos del Instituto desempeñarán su función con autonomía y probidad. No podrán utilizar la información reservada o confidencial de que dispongan en razón de su cargo, salvo para el estricto ejercicio de sus funciones, ni divulgarla por cualquier medio.
>
> **Artículo 126.** […]
> 3. Los documentos, datos e informes que los ciudadanos proporcionen al Registro Federal de Electores, en cumplimiento de las obligaciones que les impone la Constitución y esta Ley, serán estrictamente confidenciales y no podrán comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en los que el Instituto fuese parte, para cumplir con las obligaciones previstas por esta Ley, en materia electoral y por la Ley General de Población en lo referente al Registro Nacional Ciudadano o por mandato de juez competente.

4. Los miembros de los Consejos General, locales y distritales, así como de las comisiones de vigilancia, tendrán acceso a la información que conforma el Padrón Electoral, exclusivamente para el cumplimiento de sus funciones y no podrán darla o destinarla a finalidad u objeto distinto al de la revisión del Padrón Electoral y las listas nominales."

A su vez, los artículos 12, 14, párrafo 3, 35, 36, 37 y 55 del RINETAIP y el numeral 9 de los Lineamientos ARCO de la DERFE establecen lo siguiente:

"**Artículo 12.** Como información confidencial se considerará: […]
II. Los datos personales que requieran el consentimiento de los individuos para su difusión en términos de las disposiciones legales aplicables; […]

Artículo 14. Del manejo de la información reservada y confidencial
[…]

3. Las autoridades ministeriales y judiciales a nivel federal o local, o bien aquellas de la Administración Pública Federal, Estatal o Municipal y las autoridades electorales locales tendrán acceso a la información reservada o confidencial en poder del Instituto, siempre y cuando ésta le sea requerida conforme a las disposiciones legales aplicables y en el ámbito de su competencia.

Artículo 35. Protección de datos personales
1.Los datos personales son información confidencial que no puede otorgarse a persona distinta que su titular, a menos que exista una autorización expresa de éste. Los servidores públicos del Instituto que intervengan en el tratamiento de datos personales, deberán garantizar la protección en el manejo de dicha información, por lo que no podrá ser comunicada salvo en los casos previstos por la Ley de Transparencia y la Ley.

Artículo 36.
Principios de protección de datos personales
1. En el tratamiento de datos personales, los servidores públicos del Instituto deberán observar los principios de […] confidencialidad […]. […]
2. Los datos personales, incluso cuando no conste clasificación alguna al respecto, se entenderán como confidenciales.

Artículo 37. De la publicidad de datos personales
1.El Instituto no podrá difundir los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información. […]

Artículo 55.
De las obligaciones
1. Los servidores públicos del Instituto, en el ámbito de sus respectivas competencias, estarán obligados a:
[…]
XIV. Las demás que se deriven de la Ley de Transparencia y el presente Reglamento.

9. Los datos personales que las y los ciudadanos proporcionen a la Dirección Ejecutiva, en cumplimiento con las obligaciones que les impone la Constitución y el Código, serán estrictamente confidenciales, y no podrán comunicarse o darse a conocer, ni utilizarse para otro fin con excepción de lo que dispone el Código."

Por su parte, se destacan los numerales 46, 47, 50, 55, 61 y 62, previstos dentro del Título VI de los Lineamientos ARCO, que específicamente se relacionan con la validación y cotejo de datos personales proporcionados por instancias públicas y privadas y con la verificación de la emisión de la credencial para votar con fotografía, los cuales establecen lo siguiente:

"46. En ningún caso, la Dirección Ejecutiva proporcionará o transmitirá a las instancias públicas o privadas, información confidencial en términos de lo dispuesto en el artículo 171, párrafo 3 del Código [suponiendo la remisión al artículo 126, párrafo 3 de la LGIPE, sustancialmente similar al artículo 171, párrafo 3 del COFIPE derogado].

47. La verificación de los datos personales proporcionados por las instancias públicas o privadas, se circunscribirá exclusivamente a su cotejo con los datos personales que obren en el Registro Federal de Electores, sin que esto implique en forma alguna la entrega de los mismos a las referidas instancias.

50. En virtud de los Convenios de Apoyo y Colaboración suscritos y para efecto de que estén en condiciones de realizar la verificación del instrumento electoral referido, la Dirección Ejecutiva podrá proporcionar a las instancias públicas o privadas información relativa a las características técnicas de las Credenciales para Votar con Fotografía que se han expedido, así como sus modificaciones, sin que de ninguna manera se proporcione o transmita información confidencial en términos de lo dispuesto en el artículo 171, párrafo 3 del Código [suponiendo la remisión al artículo 126, párrafo 3 de la LGIPE, sustancialmente similar al artículo 171, párrafo 3 del COFIPE derogado-].

55. La Dirección Ejecutiva o en su caso, las Vocalías respectivas, informarán por escrito a la instancia solicitante, si la Credencial para Votar con Fotografía fue o no expedida por esta autoridad electoral y en su caso, si se encuentra vigente, sin que de ninguna manera se proporcione o transmita información confidencial en términos de lo dispuesto en el artículo 171, párrafo 3 del Código [suponiendo la remisión al artículo 126, párrafo 3 de la LGIPE, sustancialmente similar al artículo 171, párrafo 3 del COFIPE derogado-].

61. En ningún caso la Dirección Ejecutiva y las Vocalías respectivas, proporcionarán los datos personales en posesión de la Dirección Ejecutiva a las instancias públicas y privadas que lo soliciten, salvo las excepciones que el propio Código determina [suponiendo remisión a la LGIPE, en virtud de que el COFIPE fue abrogado].

62. Por ningún motivo se proporcionarán los datos personales de las y los ciudadanos en posesión de la Dirección Ejecutiva, a terceros, ni a instancias públicas y privadas que lo soliciten, con excepción de lo dispuesto por el Código [suponiendo remisión a la LGIPE, en virtud de que el COFIPE fue abrogado] y el Reglamento."

De los artículos antes citados se puede observar lo siguiente:

- Los datos personales son considerados como información confidencial.
- Los responsables están obligados a guardar secrecía respecto de los datos personales que tratan y evitar su difusión, distribución o comercialización no autorizada.
- La difusión de los datos personales podrá hacerse únicamente cuando haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información, o bien, en los siguientes supuestos:
    - Cuando sean necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran.
    - Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos.
    - Cuando exista una orden judicial.
    - A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido.
    - En los demás casos que establezcan las leyes.
- Los responsables están obligados a establecer medidas necesarias para evitar la transmisión o acceso no autorizado a los datos personales que tratan.

- Los datos personales en posesión del INE serán considerados como información confidencial. De manera específica, la información y los datos [personales] que los ciudadanos proporcionen al Registro Federal de Electores en cumplimiento a la Constitución y a la LGIPE serán estrictamente confidenciales.
- Ni el INE, ni sus servidores públicos, podrán divulgar o comunicar los datos personales que posean en razón de su cargo, salvo para el ejercicio de sus funciones o que exista consentimiento expreso, por escrito o por un medio de autenticación similar, del titular de la información.
- En específico, no podrán comunicar o dar a conocer los datos personales que los ciudadanos proporcionen al Registro Federal de Electores en cumplimiento a la Constitución y a la LGIPE, salvo que:
    - Exista consentimiento expreso, por escrito o por un medio de autenticación similar, del titular de la información.
    - Se trate de juicios, recursos o procedimientos en los que el Instituto fuese parte.
    - La divulgación o comunicación de datos personales se realice para el cumplimiento de las obligaciones previstas por la LGIPE y la Ley General de Población en lo referente al Registro Nacional Ciudadano.
    - Por mandato de juez competente.
- Los miembros de los Consejos General, locales y distritales, así como de las comisiones de vigilancia, tendrán acceso a la información que conforma el Padrón Electoral, exclusivamente para el cumplimiento de sus funciones y no podrán darla o destinarla a finalidad u objeto distinto al de la revisión del Padrón Electoral y las listas nominales.
- Las autoridades ministeriales y judiciales federales o locales, o bien aquellas de la Administración Pública Federal, Estatal o Municipal y las autoridades electorales locales tendrán acceso a la información confidencial, incluidos los datos personales, en poder del Instituto, siempre y cuando ésta le sea requerida conforme a las disposiciones legales aplicables y en el ámbito de su competencia.
- Para la validación o cotejo de datos personales proporcionados por instancias públicas y privadas en el marco del Servicio de Verificación no se podrá involucrar la entrega de datos personales en posesión de la Dirección Ejecutiva a las instancias públicas y privadas que lo soliciten.

En síntesis y considerando que el Servicio de Verificación se circunscribirá únicamente al cotejo de los datos personales proporcionados por instancias públicas y privadas con los datos personales que obren en el Registro Federal de Electores, queda evidenciada la obligación específica de la Dirección Ejecutiva del Registro Federal de Electores y de cualquier otra área del INE involucrada con dicho servicio, de:

- Guardar confidencialidad de los datos personales que obren en el Registro Federal de Electores que posean –ya sea del Padrón Electoral, la Lista Nominal o del Servicio de Verificación-, lo que implica no difundirlos, distribuirlos o divulgarlos, salvo las excepciones previstas por la normativa aplicable, es decir: i) exista consentimiento expreso, por escrito o por un medio de autenticación similar, del titular de la información; ii) se trate de juicios, recursos o procedimientos en los que el Instituto fuese parte; iii) la divulgación o comunicación de datos personales se realice para el cumplimiento de las obligaciones previstas por la LGIPE y la LGP, en lo referente al Registro Nacional Ciudadano o iv) por mandato de juez competente.
- En específico, guardar confidencialidad de los datos personales que obren en el Registro Federal de Electores –ya sea del Padrón Electoral, la Lista Nominal o del Servicio de Verificación- frente a las instancias públicas y privadas con quienes se lleve a cabo dicho servicio.
- Guardar confidencialidad de los datos personales recibidos por instancias públicas y privadas en el marco del Servicio de Verificación.
- Prever medidas para garantizar la confidencialidad señalada en los puntos anteriores y evitar la transmisión y acceso no autorizado a los datos personales referidos.

Con relación a lo anterior, de la información proporcionada por el INE respecto del Servicio de Verificación, se identificó lo siguiente:

1. Que el Servicio de Verificación tiene como principal objetivo que el INE, a través de la DERFE, verifique por medio de un servicio web, la vigencia de las credenciales para votar que presenten los ciudadanos para identificarse ante instituciones públicas o privadas con las que el INE haya celebrado el convenio correspondiente, y se verifique que los datos contenidos en dichas credenciales coincidan con los que obran en el Padrón Electoral.

2. Que dicho servicio implica principalmente las siguientes tres etapas:

a. Primera.- El INE recibe información (datos contenidos en la credencial para votar que los ciudadanos exhiban ante la Institución, el consentimiento del titular para hacer el cotejo correspondiente y, en su caso, información sobre la huella del titular) de parte de las Instituciones públicas y privadas;
b. Segunda.- El INE coteja la información recibida con aquélla contenida en el Sistema de Verificación, que se obtiene del Padrón Electoral, y
c. Tercera.- EL INE comunica a la institución en cuestión, el resultado del cotejo realizado.

3. En relación con la primera etapa del Servicio de Verificación, la institución pública o privada realiza una transferencia de datos personales (en texto o minucia) al INE. Los datos personales que son transferidos de la Institución al INE, de conformidad con el punto 4.2.3.1 del Anexo Técnico del Convenio de apoyo y colaboración entre el Instituto Nacional Electoral "EL INE" y "LA INSTITUCIÓN", en su versión 3.2, son los siguientes:

"Datos de entrada del servicio Web:

- Formato (xml/json)
- Confirmación del consentimiento del titular de la Credencial (obligatorio)
- Número OCR o Número CIC (obligatorio)

Los siguientes datos serán opcionales para ser confrontados y verificados por "El INE" en caso de ser proporcionados por "LA INSTITUCIÓN":

- Apellido Paterno
- Apellido Materno
- Nombre(s)
- Año Registro
- Número de Emisión
- Clave de Elector
- CURP
- Huella del dedo índice de la mano derecha, […]
- Huella del dedo índice de la mano izquierda, […]"

Considerando los datos personales que serán o pueden ser transferidos de la institución al INE, se concluye que la confidencialidad de los mismos debe ser garantizada principalmente a través de medidas tecnológicas que eviten una transmisión o acceso no autorizado a dichos datos personales durante la transferencia en cuestión, como el caso de la interconexión con tipología Punto a Punto prevista en el numeral 4.5.1 del Anexo Técnico del Convenio de apoyo y colaboración entre el Instituto Nacional Electoral "EL INE" y "LA INSTITUCIÓN", en su versión 3.2. Las medidas tecnológicas para asegurar la confidencialidad de los datos personales en la transferencia serán analizadas a mayor detalle en el apartado correspondiente al análisis del Deber de Seguridad.

4. En relación con la segunda etapa del Servicio de Verificación, en la que el INE realiza el cotejo de la información proporcionada por la institución, de conformidad con la documentación proporcionada por el INE, este proceso se realiza en el servidor de comparación ubicado en las instalaciones del INE. En este sentido, la confidencialidad de los datos personales tratados para la realización del cotejo en cuestión debe ser garantizada principalmente a través de medidas de seguridad, las cuales serán analizadas a mayor detalle en el apartado correspondiente al análisis del Deber de Seguridad.

Asimismo, la confidencialidad de los datos personales tratados para la realización del cotejo en cuestión deberá ser garantizada a través de medidas administrativas. Al respecto, se menciona que, derivado del análisis de la información proporcionada por el INE, dicho Instituto tiene previstas las siguientes medidas administrativas para garantizar la confidencialidad de los datos personales tratados en el proceso de cotejo de la información proporcionada por la Institución al INE:

- **Almacenamiento momentáneo/eliminación inmediata de la información proporcionada por la institución para la realización del cotejo de la misma por parte del INE**. Como parte de las respuestas expuestas por el INE durante la reunión de fecha 27 de febrero de 2015, así como las presentadas por el INE a través del oficio INE/DERFE/356/2015, el INE señaló lo siguiente respecto de un posible almacenamiento de los datos personales proporcionados por la Institución para la realización del cotejo correspondiente: "[…] es un almacenamiento momentáneo para comparación del dato correspondiente, por lo que no se genera una base de datos adicional a la existente". Asimismo, manifestó: "[…], el INE informa que sólo guarda la respuesta pero no conserva la huella enviada por la institución pública o privada. La institución manda la imagen que el INE almacena por un momento para generar las minucias, que es lo que comparan y una vez realizada la comparación, el INE elimina la imagen y guarda la respuesta. O bien, la institución pública o privada puede enviar las minucias para que el INE ya sólo haga la comparación. Las respuestas diarias se guardan en las bitácoras del sistema de verificación." y "[l]o que se estará respaldando serán las bitácoras del sistema de verificación. […]."

De las manifestaciones anteriores, se puede concluir que el INE no crea una base de datos personales a partir de la información recibida por la Institución, ya que la misma es eliminada tan pronto se realiza el cotejo correspondiente. La única información que es conservada por el INE son las respuestas derivadas de los cotejos, la cuales son almacenadas en las bitácoras del sistema de verificación y no contienen datos personales.

- **Capacitación del personal involucrado con el Servicio de Verificación**. En relación con la existencia de algún programa de capacitación, actualización y concienciación para personal del INE sobre las obligaciones que tiene en materia de protección de datos personales en el contexto del Servicio de Verificación, y en especial en relación con el deber de confidencialidad, el INE manifestó en el oficio IFAI-OA/SPDP/0039/15, en la reunión del 27 de febrero de 2015, y en el oficio INE/DERFE/356/2015 que: "Está previsto que el personal que manejará el sistema de verificación sea capacitado en materia de protección de datos personales, en el marco de un programa general de capacitación que recibirá el personal de la DERFE, denominado 'Programa de Concientización en Materia de Seguridad dentro de la DERFE', que incluye capacitación sobre la protección de la información del Padrón Electoral, el cual incluye la protección de los datos personales. Asimismo, el INE solicitará al IFAI capacitación en la materia, a través del convenio de colaboración celebrado entre el INE y el IFAI". Aunado a lo anterior, el INE manifestó que "[s]e elaborará oficio para solicitar a la Unidad Técnica de Transparencia y Protección de Datos Personales de este Instituto, la capacitación correspondiente".

No se omite señalar que, de conformidad con lo manifestado por el INE, únicamente áreas de la DERFE tendrán acceso al Servicio de Verificación, en tanto que dicha unidad administrativa es la responsable de la conformación del Padrón Electoral.

- **Cláusulas contractuales y cartas de confidencialidad**. Respecto de este punto, el INE, a través del oficio INE/DERFE/356/2015, señaló que será solicitada a la Dirección Ejecutiva de Administración que incorpore en los contratos

respectivos una cláusula de confidencialidad de datos personales del Registro Federal de Electores que se manejen en el marco del Servicio de Verificación. En relación con lo anterior, se hace referencia a la ya existente cláusula sexta, inciso a), de los Convenios de Apoyo y Colaboración para Instituciones Privadas y para Instituciones Públicas**,** en su versión del 18 de marzo de 2015, en donde se prevé como obligación de ambas partes: "Guardar estricta confidencialidad respecto de la información que se proporcione entre "LAS PARTES".

Asimismo, se hace referencia al Anexo 1 del Anexo Técnico del Convenio de apoyo y colaboración entre el Instituto Nacional Electoral "EL INE" y "LA INSTITUCIÓN", en su versión 3.2, en donde se prevé una cláusula segunda relacionada con una Declaratoria de confidencialidad y aceptación de las condiciones generales del mecanismo de pruebas en relación al Servicio de Verificación de datos de la Credencial para Votar*,* los lineamientos para la conexión segura y de la vigencia para la conexión VPN*,* la cual establece que tanto el INE como el Usuario declaran:

> "[…]
> - Tener conocimiento de que la información a la que tendrá acceso puede ser considerada como CONFIDENCIAL en los términos que marca la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, la Ley General de Instituciones y Procedimientos Electorales, el Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública y los Lineamientos para el Acceso, Rectificación, Cancelación , Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores.
>
> - Tener pleno conocimiento y aceptar que las actividades que desarrollará con el acceso solicitados serán en estricto apego a la Ley, manteniendo absoluta confidencialidad y cuidado para conservar la información, asumiendo la obligación de abstenerse de revelar la información a que tengan acceso a tercero, así como utilizarla en provecho propio y terceros, o reproducirla por cualquier medio obligándose a notificar de inmediato cualquier caso del que tenga conocimiento cuya conducta contravenga la Ley o Políticas Institucionales. […]
>
> Que aceptan que la contravención a la Normatividad vigente y a la presente declaratoria, generará sanciones administrativas y/o de tipo penal a que haya lugar, en materia de transparencia. […]"

Cabe señalar que respecto de la declaratoria de confidencialidad citada, falta claridad respecto de los siguientes puntos: i) que, en relación con el mecanismo de pruebas, el INE no proporcionará a la institución ningún dato personal en posesión de INE y ii) que las instituciones públicas y privadas están obligadas a guardar la confidencialidad de los datos personales, con fundamento en la LFTAIPG y las LFPDPPP, respectivamente, así como con fundamento en cualquier otra normativa aplicable.

Adicionalmente, el INE, a través del oficio INE/DERFE/356/2015, presentó el texto de una carta de confidencialidad la cual, a decir del INE, solicitará que sea firmada por personal del INE y prestadores de servicio que traten datos personales del Registro Federal de Electores en el marco del Servicio de Verificación. A continuación se presenta el texto de la mencionada carta:

CARTA DE CONFIDENCIALIDAD

México, D.F., a de _____ de 2015

Tengo pleno conocimiento que de conformidad con lo dispuesto por el artículo 126 párrafo 3 de la Ley General de Instituciones y Procedimientos Electorales, los documentos, datos e informes que los ciudadanos proporcionen al Registro Federal de Electores, en cumplimiento de las obligaciones que les impone la Constitución y esta Ley, serán estrictamente confidenciales y no podrán comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en que el Instituto fuese parte, para cumplir con las obligaciones previstas por esta Ley en materia electoral y por la Ley General de Población en lo referente al Registro Nacional Ciudadano o por mandato de Juez competente.

En este sentido, a efecto de garantizar la protección de los datos personales, y de conformidad con la normatividad aplicable en materia de Transparencia y Acceso a la Información Pública, reconozco que para el desarrollo de mis funciones dentro de la Secretaría Técnica Normativa, tengo acceso a la siguiente información: expedientes electorales en original y copia, derivados de un trámite o una verificación en campo; imágenes de rostro, huellas y firmas movimientos realizados en el Padrón Electoral, incluyendo las bajas; impresiones del Sistema Integral de Información del Registro Federal de Electores SIIRFE; uso y manejo e impresiones del Subsistema SIIRFE-Consulta de Expediente Electrónico; así como toda documentación en que consten datos personales que los ciudadanos hayan proporcionado al Registro Federal Electorales, información considerada como estrictamente confidencial, acepto que el uso y entrega de esta, durante el desempeño de mis funciones, es única y exclusivamente para el fin que fue solicitado, por lo que asumo la obligación de mantener absoluta confidencialidad y cuidado para conservarla en el estado en que me sea entregada, absteniéndome de revelarla o reproducirla por cualquier medio, así como entregarla a terceros o de utilizarla en provecho propio o de terceros, notificando de inmediato cualquier caso del que tenga conocimiento cuya conducta contravenga la Ley o Normatividad vigente aplicable a esta Institución.

Acepto que la contravención a la Normatividad vigente y a la presente declaratoria, generará sanciones administrativas y/o de tipo penal a que haya lugar, firmando la presente para los efectos conducentes.

_____

C.

Cabe señalar que el INE manifestó que no cuenta con encargados del tratamiento,7 y que únicamente cuentan con "proveedores de infraestructura y licenciamiento", los cuales no tendrán acceso a datos personales.

- **Sistema de Gestión de Seguridad de la Información**. Respecto este punto, el INE, durante la reunión sostenida el 27 de febrero de 2015, señaló que "[s]e cuenta con un sistema de gestión de seguridad para la protección de la información del Padrón Electoral" y que "[e]l Sistema de gestión de Seguridad de la Información está basado en el estándar ISO 27001:2005 que inició en diciembre de 2013". Cabe señalar que el INE no proporcionó información adicional al respecto.

- **Supervisión o verificación del proceso de cotejo**. Respecto de este punto, el INE, durante la reunión sostenida el 27 de febrero de 2015, manifestó que en materia de datos personales "[…] no tiene previsto desarrollar mecanismos específicos para el sistema de verificación ya que la verificación del cumplimiento se realizará en el marco del Sistema de Gestión de las Tecnologías de la Información que prevé los procesos de operación de los sistemas, incluido el sistema de verificación. De manera adicional como una de las funciones del Comité Técnico referido en la cláusula octava del Convenio,

7 Para efectos del presente documento se entendiéndose como "Encargado" a aquella tercera persona física o moral, distinta de la Institución o del INE, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta de los responsables, en este caso, la Institución y el INE.

se verificará el cumplimiento de obligaciones en materia de prevención de datos personales". Dicha cláusula establece lo siguiente:

> "**IV. DEL COMITÉ TÉCNICO**
>
> OCTAVA. Para el adecuado desarrollo de las actividades que se generarán con motivo del cumplimiento del objeto de este convenio, "LAS PARTES" están de acuerdo en integrar un Comité Técnico, mismo que estará formado por un representante de cada institución, quienes podrán ser sustituidos en cualquier tiempo previa notificación por escrito y con 10 días de anticipación a la otra parte. […]
>
> NOVENA. El Comité Técnico referido en la cláusula anterior, tendrá las siguientes atribuciones:
> a) Determinar y apoyar las acciones a ejecutar con el fin de dar cumplimiento al objeto del presente Convenio y su Anexo Técnico.
> b) Coordinar la realización de actividades señaladas en el Anexo Técnico que forma parte del presente instrumento jurídico. […]"

Por su parte, el Anexo Técnico del Convenio de apoyo y colaboración entre el Instituto Nacional Electoral "EL INE" y "LA INSTITUCIÓN", en su versión 3.2., establece, en su apartado 5.2 lo siguiente:

> "[…] El "Comité Técnico" será deberá establecer los procedimientos para verificar el cumplimiento de obligaciones en materia de seguridad de la información y protección de datos personales. […]"

Complementariamente, en el apartado 6 del mismo documento se prevé lo siguiente:

> "[…] Será posible, bajo común acuerdo, llevar a cabo visitas del personal involucrado en este proyecto por parte de "EL INE" y de "LA INSTITUCIÓN" a las instalaciones de ambos, con el objetivo de conocer detalladamente sus procesos. En el futuro y de común acuerdo entre "EL INE" y "LA INSTITUCIÓN", se promoverán mejoras en los sistemas de información, aprovechando los avances tecnológicos disponibles en beneficio de los procesos que relacionan a ambas instituciones, previo establecimiento de fechas y prioridades; así como la revisión previa y en su caso aprobación del "Comité Técnico"."

En este sentido, es viable concluir que la supervisión o verificación relacionada con el cumplimiento de las obligaciones de protección de datos y, en especial, de la confidencialidad de los datos personales tratados durante la etapa del cotejo del Servicio de Verificación, se realizará a través de las verificaciones o supervisiones previstas por el Sistema de Gestión de las Tecnologías de la Información, así como por el Comité Técnico referido en la cláusula octava de los Convenios de Apoyo y Colaboración para Instituciones Privadas para Instituciones Públicas, en su versión del 18 de marzo de 2015. No obstante, el INE no manifestó mayor detalle sobre el sistema de gestión referido ni sobre las verificaciones y supervisiones que serán realizadas por el Comité Técnico.

5. En relación con la tercera etapa del Servicio de Verificación, en la que el INE comunica a la Institución en cuestión, el resultado del cotejo realizado, de conformidad con lo manifestado en distinta documentación proporcionada por el INE, la información que será proporcionada por el INE a la institución, será "[…] el estatus de vigencia de la Credencial, un código respecto de la coincidencia o no de los datos y para el caso de la comparación de minucias de las huellas dactilares, el porcentaje de similitud mediante el uso de la minucia estándar INCITS 378. […]". Igualmente, en la documentación proporcionada por el INE, se reafirma en diversas ocasiones que <u>en ningún caso se proporcionará a la institución datos personales de los ciudadanos.</u>

A mayor abundamiento, el Anexo Técnico del Convenio de apoyo y colaboración entre el Instituto Nacional Electoral "EL INE" y "LA INSTITUCIÓN", en su versión 3.2., describe los posibles resultados de la verificación:

[…]
Resultado de la verificación:

Dato	Respuesta
Identificador de la transacción	Numérico
• Tiempo de respuesta de comparación en el servidor de **"EL INE"** • Tiempo de respuesta desde el Portal de Verificación • En su caso, código de error transacción no exitosa	Cadena – Número de segundos
Estampilla de tiempo de la consulta	Cadena – Fecha de consulta
• Confirmación del consentimiento del titular de la Credencial (obligatorio)	No se da respuesta al servicio en caso de estar nulo o con un valor diferente al acordado
• Número OCR o Número de CIC (obligatorio) • Apellido Paterno • Apellido Materno • Nombre • Año Registro • Número de Emisión • Clave de Elector • CURP	Cadena – Falso/Verdadero
Minucia enviada Tipo Formato Identificador de dedo	Porcentaje de similitud

Asimismo, en el oficio INE/DERFE/356/2015, el INE manifestó, al describir el componente "Servidor de Comparación", que la "repuesta a las peticiones de verificación de datos es construida por un archivo XML o JSON, que contiene los valores de 'true' o 'false' para cada campo disponible a verificar y un porcentaje de similitud para la comparación de las huellas digitales".

Complementariamente, en el oficio INE/DERFE/356/2015, el INE presentó un catálogo con "todos los valores numéricos y el significado de las posibles respuestas". El catálogo proporcionado es el siguiente:

Código	Estado	Descripción
70	Excede el límite de re-intentos de OCR	Se ha intentado un numero N de veces la verificación de un OCR en un periodo de tiempo establecido, tanto el numero N y el periodo son configurables a través del administrador.
80	Tiempo de espera agotado	Ha demorado demasiado el en responder el servidor de comparación.
81	Respuesta incorrecta del Servidor	Se refiere a la mala formación de los mensajes entre el punto de acceso y el Servidor de comparación, esto obliga a reintentar la comparación.
90	OCR No Vigente	El OCR no se encuentra VIGENTE o en su defecto no se encuentra en la base de datos (Para este servicio solo se tiene la base de datos de las credenciales vigentes).
91	OCR Vigente	El OCR enviado es Vigente.
92	OCR Vigente, huella no encontrada.	Este código indica que el OCR es Vigente, pero no se tiene la huella de esta persona y por lo cual no se puede verificar. Este código es visible solo cuando el OCR es Vigente, con lo cual si el OCR no es vigente no importa el estado de la huella.
93	OCR Vigente, Servicio biométrico no disponible.	El OCR es vigente sin embargo el servicio biométrico no se encuentra disponible, por lo cual le verificación de la huella no se llevará acabo.

Asimismo, el INE manifestó que “Con el propósito de proporcionar más información respecto de la situación de la credencial, se está proponiendo complementar las respuestas señaladas en el cuadro anterior con los numerales 90 a 93 y homologar las respuestas que se proporcionan en el servicio de consulta a la Lista Nominal por Internet (http:listanominal.ife.org.mx/) con las siguientes respuestas:

ID	Escenario	Respuesta
1	Happy-path	Si Vigente, Si Vota - Está vigente como medio de identificación y puedes votar. - Tus datos se encuentran en el Padrón Electoral y también en la Lista Nominal de Electores.
2	Re-seccionado	Si Vigente, Si Vota - Está vigente como medio de identificación y puedes votar. - Tu domicilio dejó de pertenecer a la Sección Electoral XXXX y ahora corresponde a la YYYY como resultado de una actualización a la Cartografía Electoral. Por lo que te invitamos a tramitar otra credencial en la cual aparezca tu nueva sección.
3	Re-incorporado	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Tu registro ha sido reincorporado por notificación de una autoridad competente al Padrón Electoral pero no estás en la Lista Nominal de Electores. Tramita una nueva credencial para votar que sea vigente y puedas votar.
4	OCR capturado distinto al registrado en la base de datos.	- El OCR que ingresaste es distinto al registrado en nuestra base de datos, favor de verificarlo. - En caso de que tus datos no se encuentren nuevamente acude al Módulo de Atención Ciudadana para regularizar tu situación.
5	Número de Emisión Diferente	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Esta no es tu última credencial. Realizaste un trámite de actualización de datos, por lo que tu consulta fue con una credencial anterior. - Tu credencial con la que podrás identificarte y votar, debe ser número de emisión XX, que corresponde al último trámite que realizaste. Realiza una nueva consulta con tu última credencial.

ID	Escenario	Respuesta
6	Trámite en proceso	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - No concluiste tu trámite. Iniciaste un trámite en el Módulo del INE el DIA_MES_AÑO; necesitas concluirlo recogiendo tu Credencial y sólo con ella podrás votar e identificarte. - Tus datos si están en el Padrón Electoral pero no en la Lista Nominal de Electores.
7	Credencial 03	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Tu credencial fue dada de baja por pérdida de vigencia. - Tus datos no están en el Padrón Electoral y tu registro fue excluido de la Lista Nominal de Electores.
8	Credencial 09	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Tu credencial tiene recuadro 09. Tus datos si están en el Padrón Electoral pero tu registro fue excluido de la Lista Nominal de Electores. - Sin embargo, si eres mexicano residente en el extranjero, tu credencial es Vigente para utilizarla en territorio extranjero.
9	Credencial 12	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Tu credencial tiene recuadro 12. Tus datos están en el Padrón Electoral pero tu registro fue excluido de la Lista Nominal de Electores. - Sin embargo, si eres mexicano residente en el extranjero, tu credencial es Vigente para utilizarla en territorio extranjero.

ID	Escenario	Respuesta
10	Duplicado	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Existe otro registro a tu nombre que fue identificado por el Programa de Detección de Duplicados, por lo que la credencial que estas consultando corresponde a un registro dado de baja del Padrón Electoral y Excluido de la Lista Nominal de Electores (Liga a Fundamento Legal)
11	Defunción	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Por defunción este registro fue dado de baja del Padrón Electoral y excluido de la Lista Nominal de Electores (Liga a Fundamento Legal)
12	Suspensión de derechos políticos	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Por suspensión de derechos este registro fue dado de baja del Padrón Electoral y excluido de la Lista Nominal de Electores (Liga a Fundamento Legal)
13	Cancelación de Trámite	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - No recogiste tu nueva credencial en el plazo establecido y tu registro fue dado de baja del Padrón Electoral y excluido de la Lista Nominal de Electores (Liga a Fundamento Legal)
14	Pérdida de nacionalidad	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Por pérdida de ciudadanía o por haber renunciado a la nacionalidad, tu registro fue dado de baja del Padrón Electoral y excluido de la Lista Nominal de Electores (Liga a

ID	Escenario	Respuesta
		Fundamento Legal)
15	Datos irregulares	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Tu registro presenta datos irregulares por lo que fue dado de baja del Padrón Electoral y excluido de la Lista Nominal de Electores (Liga a Fundamento Legal)
16	Robada al instituto	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - Esta credencial esta reportada como robada o extraviada por lo que este registro no se encuentra en el Padrón Electoral y ha sido excluido de la Lista Nominal de Electores. - Por favor entrégala en cualquier Módulo de Atención Ciudadana para su destrucción. (Liga a Fundamento Legal)
17	Datos incorrectos	Datos incorrectos o inexistentes por favor verifica e intenta de nuevo. En caso de que tus datos no se encuentren nuevamente, acude al Módulo de Atención Ciudadana para regularizar tu situación.
18	Cambio de Clave de Elector	No Vigente, No Vota - No está vigente como medio de identificación y no puedes votar. - No es tu último trámite. Realizaste un nuevo trámite de corrección de datos en el Módulo del INE el DIA_MES_AÑO; necesitas realizar la consulta con tu última credencial que solicitaste.
19	Lista Nominal Residentes en el Extranjero	Si Vigente, Si Vota - En virtud de que tu solicitud de inscripción a la Lista Nominal de Electores en el Extranjero fue procedente, tu registro fue incorporado a la Lista Nominal de Electores Residentes en el Extranjero.

ID	Escenario	Respuesta
		- Solo podrás emitir tu voto desde el extranjero para presidente de los Estados Unidos Mexicanos, vía postal.

Al respecto, se concluye que:

- En relación con las posibles respuestas que el INE podría proporcionar a las instituciones en el marco del Servicio de Verificación, de conformidad con lo manifestado en el Anexo Técnico del convenio de apoyo y colaboración entre el Instituto Nacional Electoral “EL INE” y “LA INSTITUCIÓN”, en su versión 3.2, no se deriva la transferencia o comunicación de dato personal alguno.

- Igualmente, del catálogo con “todos los valores numéricos y el significado de las posibles respuestas”, de las respuestas enlistadas con números de código 70, 80, 81, 90, 92 y 93, no se deriva la transferencia o comunicación de dato personal alguno.

- En cuanto al catálogo de posibles respuestas a las Instituciones en el marco del Servicio de Verificación, que el INE propone para complementar las respuestas señaladas con los numerales 90 a 93 y homologar las respuestas que se proporcionan en el servicio de consulta a la Lista Nominal por Internet (http:listanominal.ife.org.mx/), se manifiesta que, de las respuestas enlistadas con los números de ID 1 a 18, en caso de implementar dichas respuestas al **Servicio de Verificación**, el INE estaría proporcionando información adicional no necesaria para la prestación de dicho servicio, sobre la causa de falta de vigencia de la credencial para votar e incluso, en algunos supuestos, como, por ejemplo, en las respuestas 2, 5, 6, 12, 14 y 18, el INE estaría transfiriendo datos personales a la institución, entre los que se encuentran:

- La sección electoral vigente del titular.
- El número de emisión de la credencial para votar vigente del titular.
- El día, mes y año en los cuales el titular realizó su último trámite ante el INE.
- La suspensión de derechos del titular de la credencial para votar.
- La pérdida o renuncia de la ciudadanía del titular de la credencial para votar.

Únicamente se considera relevante la respuesta identificada con ID 16, que permite a la institución saber que la credencial para votar presentada no está vigente en razón de que dicha credencial fue reportada como robada o extraviada. En ese sentido, es deseable que esta información sí sea proporcionada por el INE a la Institución, pero no toda la demás.

- Por último, cabe señalar que, de conformidad con la documentación presentada por el INE, éste entregará a la Institución informes estadísticos relacionados con el desempeño del Servicio de Verificación, respecto de los cuales, de conformidad con el análisis realizado, se concluye que no se deriva transferencia o comunicación de dato personal alguno.

En virtud de lo anterior, en relación con el deber de confidencialidad, el INAI emite las siguientes observaciones y recomendaciones:

1. Generar evidencia de la capacitación que sea impartida al personal de la DERFE –y al personal del INE adscrito a cualquier otra área o posibles encargados que pudieran estar involucrados eventualmente en la operación del Servicio de Verificación - en el marco del *Programa de Concientización en Materia de Seguridad dentro de la DERFE* o de cualquier otra capacitación impartida, tales como el programa de dicha capacitación, la calendarización correspondiente, listas de asistencia y evaluaciones realizadas. Lo anterior, previo a la puesta en operación del Servicio de Verificación y de manera continuada a partir de su puesta en operación.

2. Asimismo, se recomienda solicitar al INAI capacitación en materia de protección de datos personales, previo a la puesta en operación del Servicio de Verificación y de manera continuada a partir de su puesta en operación.

3. En relación con la *Declaratoria de confidencialidad y aceptación de las condiciones generales del mecanismo de pruebas en relación al Servicio de Verificación de datos de la Credencial para Votar,* se recomienda al INE redactar claramente dicha cláusula respecto a los siguientes puntos: i) que, en relación con el mecanismo de pruebas, el INE no proporcionará a la Institución ningún dato personal en posesión de INE y ii) que las Instituciones públicas y privadas están obligadas a guardar la confidencialidad de los datos personales tratados en el contexto del mecanismo de pruebas vinculadas al Servicio de Verificación, con fundamento en la LFTAIPG y la LFPDPPP, respectivamente, así como con fundamento en cualquier otra normativa aplicable. Lo anterior, considerando que también podría haber normativa local en materia de protección de datos personales, aplicable a instituciones públicas locales.

4. En relación con el Sistema de Gestión de Seguridad referido por el INE, se recomienda documentar y generar evidencia de las medidas adoptadas en el marco de dicho sistema, para garantizar la confidencialidad de los datos personales tratados para la prestación del Servicio de Verificación.

5. En relación con las verificaciones o supervisiones previstas y realizadas en el marco del Sistema de Gestión de las Tecnologías de la Información señalado por el INE, así como por el Comité Técnico previsto en la cláusula octava del Convenio de apoyo y colaboración entre “EL INE” y “LA INSTITUCIÓN”, sobre el cumplimiento de las

obligaciones en materia de protección de datos personales, se recomienda documentar y generar evidencia de las verificaciones o supervisiones previstas y realizadas.

6. Con objeto de no difundir información confidencial en términos de lo dispuesto por el artículo 18, fracción II, y 21 de la LFTAIPG, así como las disposiciones en materia de confidencialidad de la LGIPE, el INE tendrá que limitarse a dar información genérica sobre la coincidencia o no de los datos proporcionados por la institución para la realización del cotejo correspondiente y el porcentaje de similitud de la huella digital, y evitar proporcionar información adicional sobre las causas de la falta de vigencia de la credencial para votar, así como datos personales. En ese sentido, se recomienda no implementar respuestas complementarias, tales como las identificadas con número de ID 1 a 18, salvo lo relativo al robo o extravío de la Credencial para Votar.

En los casos que la respuesta del INE indicara que una credencial presentada por un titular a la institución no es vigente, la institución podría orientar al particular para que consulte con el INE el detalle personal de la causa de no vigencia de su credencial para votar y, en su caso, realice las aclaraciones y rectificaciones necesarias.

9. Transferencias

Para efectos del presente documento, las transferencias son toda comunicación, difusión o distribución de datos personales que se realice entre el responsable del tratamiento y otro responsable o un tercero distinto del titular de los datos personales o un encargado del tratamiento. Al respecto, cabe señalar que toda transferencia de datos personales realizada en territorio mexicano se encuentra regulada por la normativa en materia de protección de datos personales y debe cumplir con ciertos requisitos.

En ese sentido, cualquier comunicación, difusión o distribución de datos personales entre el INE y la institución, en tanto los dos son responsables del tratamiento de datos personales, es considerada como una transferencia de datos personales.

Ahora bien, de acuerdo con lo descrito en las secciones anteriores, en el Servicio de Verificación existe transferencia de datos personales **de la institución pública o privada hacia el INE**, cuando la primera comunica al INE los datos de las credenciales para votar que presentan los ciudadanos que realizan trámites antes éstas, a fin de que dicho instituto verifique la vigencia y validez de los datos proporcionados, de conformidad con la información que obra en la base de datos del Servicio de Verificación, la cual se integra a partir del Padrón Electoral.

Dado que la transferencia la puede realizar tanto una institución privada, como de una pública, ésta se encuentra regulada por distinta normatividad: i) la LFPDPPP, en caso las instituciones privadas; ii) la LFTAIPG y demás normativa aplicable, en caso de las instituciones públicas federales y iii) por regulación local en materia de protección de datos personales, en el caso de instituciones públicas locales. Siendo así, con fines de claridad, el análisis que a continuación se realiza, se divide por tipo de sujeto obligado.

1. Transferencias realizadas por instituciones privadas

En el caso de que la transferencia sea realizada por **instituciones privadas** –a excepción de las sociedades de información crediticia, reguladas bajo normativa específica, de conformidad con el artículo 2 de la LFPDPPP-, ésta debe cumplir con los requisitos previstos por los artículos 36 y 37 de la LFPDPPP y 68, 69 y 73 del RLFPDPPP, que se citan a continuación:

> "**Artículo 36.-** Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.
>
> El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.
>
> **Artículo 37.-** Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:
>
> I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
> II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
> III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
> IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

Condiciones para la transferencia
Artículo 68. Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en el artículo 37 de la Ley; deberá ser informada a este último mediante el aviso de privacidad y limitarse a la finalidad que la justifique.

Prueba del cumplimiento de las obligaciones en materia de transferencias
Artículo 69. Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realizó conforme a lo que establece la Ley y el presente Reglamento la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.

Formalización de las transferencias nacionales
Artículo 73. La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales."

A partir de lo anterior, se advierte que para llevar a cabo una transferencia nacional de datos personales, la institución privada debe cumplir con las siguientes obligaciones:

1. Informar a los titulares sobre la transferencia en el aviso de privacidad.
2. Solicitar el consentimiento de los titulares para la transferencia, salvo en los supuestos previstos en el artículo 37 de la LFPDPPP, así como incluir la cláusula respectiva en el aviso de privacidad.
3. Comunicar el aviso de privacidad al tercero receptor de los datos personales.
4. Formalizar la transferencia mediante algún mecanismo que permita demostrar que la institución comunicó al tercero receptor las condiciones bajo las cuales el titular consintió el tratamiento de datos personales, y en ese sentido, acreditar, en caso que sea necesario, que la transferencia se realizó conforme a la normatividad.

Si bien estas obligaciones deben ser cumplidas por la institución privada que transfiere los datos personales; en virtud de que el INE es una autoridad federal y está obligada a proteger los datos personales que trate, de conformidad con la normatividad que regule la materia, debe tomar medidas para asegurarse que los datos personales que recibe de la institución privada, son transferidos de manera lícita. En ese sentido, se analizarán los mecanismos considerados en el Servicio de Verificación para que el INE se asegure que los datos que recibe de las instituciones privadas provienen de una transferencia que cumple con la norma.

Obligación 1. La institución privada debe informar al titular la existencia de la transferencia en el aviso de privacidad. Al respecto, la cláusula quinta del Convenio de Apoyo y Colaboración para Instituciones Privadas**,** en su versión del 18 de marzo de 2015, establece lo siguiente:

"QUINTA.- Las obligaciones de "_____", son las siguientes:
[…]
e) Establecer en los avisos de privacidad que se elaboren de conformidad con la Ley de Protección de Datos Personales en Posesión de Particulares, la posibilidad de verificación de los datos personales contenidos en la Credencial para Votar que los ciudadanos proporcionen a "_____".

> […]
>
> g) "_____" se obliga a informar al Titular de los datos Personales la compulsa que se efectuará en el marco del Servicio de Verificación de Datos de la Credencial para Votar.
> […]"

Si bien la cláusula quinta, incisos e) y g) del convenio de apoyo y colaboración para instituciones privadas establece la obligación de las instituciones privadas de incluir en su aviso de privacidad la posibilidad del tratamiento de datos personales para la verificación de los datos contenidos en la credencial para votar y la compulsa que será efectuada; en dicha cláusula no se establece la obligación de la institución de informar en el aviso de privacidad que esta finalidad del tratamiento implica la transferencia de datos personales al INE.

Obligación 2. La institución privada deberá requerir el consentimiento del titular para realizar la transferencia, salvo las excepciones previstas en el artículo 37 de la LFPDPPP, así como incluir la cláusula respectiva en el aviso de privacidad. Al respecto, la cláusula quinta del Convenio de Apoyo y Colaboración para Instituciones Privadas, en su versión del 18 de marzo de 2015, establece lo siguiente:

> "QUINTA.- Las obligaciones de "_____", son las siguientes:
> […]
>
> f) El aviso de privacidad, deberá contener un campo en el que se indique si el titular acepta o no, el tratamiento de sus datos para el Servicio de Verificación de datos de la Credencial para Votar. Dicho aviso de privacidad deberá ser complementado con un campo de conformación del consentimiento de titular de los datos en el que expresamente acepte el cotejo de los datos que presenta con los del Servicio de Verificación de datos de la Credencial para Votar.
> g) […]"

Como es posible observar, la institución privada deberá solicitar el consentimiento de los titulares para el tratamiento de su información personal contenida en la credencial para votar y, en su caso, sus huellas dactilares, para las finalidades previstas en el Servicio de Verificación. Ahora bien, dado que dicho tratamiento requiere de manera forzosa la transferencia de datos personales al INE, al consentir el titular el tratamiento de su información para el Servicio de Verificación, estaría, a su vez, consintiendo la transferencia al INE, siempre y cuando dicha transferencia esté debidamente informada en el aviso de privacidad. En ese sentido, se advierte que no se requiere que el titular otorgue de nueva cuenta su consentimiento para la transferencia de datos personales, si de manera previa consintió el tratamiento de su información personal para los fines del Servicio de Verificación.

Con independencia de lo anterior, como se señaló en el análisis del principio de información, se sugiere valorar la conveniencia de que **las instancias públicas y privadas puedan solicitar el consentimiento para el tratamiento de sus datos personales en el Servicio de Verificación por un medio distinto al aviso de privacidad**, ya que de otra forma estarían obligadas a entregar a cada uno de los titulares una copia del aviso de privacidad.

Obligación 3. La Institución privada que realice la transferencia debe comunicar al INE el aviso de privacidad, para darle a conocer las condiciones a las cuales el titular sujetó el tratamiento de sus datos personales. Al respecto, la cláusula quinta, inciso i), del Convenio de Apoyo y Colaboración para Instituciones Privadas, en su versión del 18 de marzo de 2015, establece lo siguiente:

> "QUINTA.- Las obligaciones de "_____", son las siguientes:
> […]

i) "_____" se obliga a dar a comunicar el aviso de privacidad a "EL I.N.E." y finalidades a las que el titular sujetó su tratamiento, siguiendo los términos del artículo 36 de la Ley Federal de Protección de datos Personales en Posesión de los Particulares.[…]"

Visto lo anterior, el convenio referido prevé que la institución privada comunique al INE el aviso de privacidad que dicha institución puso a disposición de los titulares.

Obligación 4. Formalizar la transferencia mediante algún mecanismo que permita demostrar que la institución comunicó al INE las condiciones bajo las cuales el titular consintió el tratamiento de datos personales y, en ese sentido, que permita acreditar, en caso que sea necesario, que la transferencia se realizó conforme a la normatividad. Al respecto, en reunión celebrada el 27 de febrero de 2015, el INE manifestó que las transferencias quedarán documentadas a través de bitácoras.

En relación con lo anterior, en el oficio INE/DERFE/356/2015, el INE informó la descripción de la bitácora en formato texto, que genera en operación el Servicio de Verificación, de la cual se destaca la siguiente información:

Cons.	Campo	Tamaño en caracteres	Descripción
1	Fecha de envío	6	Fecha de envío del mensaje en formato aaaammdd
2	Hora de envío	6	Hora de envío del mensaje en formato hh:mm:ss
3	Fuente	6	ID del servidor de portal de verificación
4	Consecutivo de mensaje	6	Identificador o consecutivo de mensaje
[…]			
69	XXX	3	Indicador de cantidad de caracteres de la respuesta Tiempo total de consulta
70	XXX	2 o 3	Tiempo total de consulta en milisegundos
71	TS	2	Indicador de Tiempo de servidor
72	XXX	3	Indicador de cantidad de caracteres de la respuesta Tiempo de servidor
73	XXX	2 o 3	Tiempo de servidor en milisegundos
74	TM	2	Indicador de Estampilla de tiempo
75	XXXX	4	Indicador de cantidad de caracteres de la respuesta Tiempo de servidor
76	XXX	21	Estampilla de tiempo en formato aaaammdd hh:mm:ss.mmm

De lo anterior, se puede concluir que la bitácora generada y respaldada prevé una serie de campos relacionados con fechas de envío de mensajes, hora de envío de mensajes, ID del servidor del portal de verificación, indicador consecutivo del mensaje, tiempo de la consulta, indicador de la estampilla de tiempo, entre otros, relacionados con la comunicación entre la institución y el INE, derivado de las solicitudes de verificación de datos de la credencial para votar. No obstante, en dicha bitácora no se aprecian registros relacionados con aspectos de las transferencias de datos personales realizados de la institución al INE, en atención a los previsto por la LFPDPPP, es decir, i) si las transferencias fueron informadas por la Institución a los titulares; ii) si las transferencias de datos personales de la Institución al INE fueron consentidas, en caso de requerirse dicho consentimiento, o la justificación del por qué no es requerido dicho consentimiento y ii) la entrega de los avisos de privacidad de las instituciones privadas al INE.

2. Transferencias realizadas por instituciones públicas federales

En el caso de que la transferencia sea realizada por instituciones públicas federales, dicha transferencia debe cumplir con los requisitos previstos por la LFTAIPG, así como con cualquier otra normativa aplicable por virtud de la naturaleza jurídica de la institución. De los artículos 20, fracción VI, 21 y 22 de la LFTAIPG, citados en el apartado relacionado con el deber de

confidencialidad, se derivan las siguientes obligaciones para las instituciones públicas federales que realicen transferencias de datos personales al INE en el marco del Servicio de Verificación:

1. Establecer las medidas de seguridad necesarias para evitar, entre otras cuestiones, transferencias indebidas de datos personales.
2. Comunicar datos personales a terceros sólo en los casos en los que exista consentimiento expreso del titular, con excepción de los supuestos previstos en el artículo 22 de la LFTAIPG.

Si bien estas obligaciones deben ser cumplidas por la institución pública federal que transfiere los datos personales; en virtud de que el INE es una autoridad federal y está obligada a proteger los datos personales que trate, de conformidad con la normatividad que regule la materia, debe tomar medidas para asegurarse que los datos personales que recibe de la institución pública federal, son transferidos de manera lícita. En ese sentido, se analizarán los mecanismos considerados en el Servicio de Verificación para que el INE se asegure que los datos que recibe de las instituciones públicas federales provienen de una transferencia que cumple con la norma.

Obligación 1. Establecer las medidas de seguridad necesarias para evitar, entre otras cuestiones, transferencias indebidas de datos personales. Con relación a lo anterior, la seguridad de los datos personales durante la transferencia debe ser garantizada principalmente a través de medidas tecnológicas, como el caso de la interconexión con tipología Punto a Punto prevista en el numeral 4.5.1 del Anexo Técnico 3.2 del convenio de apoyo y colaboración entre el Instituto Nacional Electoral "EL INE" y "LA INSTITUCIÓN". Las medidas tecnológicas para garantizar la seguridad de los datos personales en la transferencia son analizadas a mayor detalle en el apartado correspondiente al análisis del deber de seguridad.

Obligación 2. Comunicar datos personales a terceros sólo en los casos en los que exista consentimiento expreso del titular, con excepción de los supuestos previstos en el artículo 22 de la LFTAIPG. Al respecto, es importante aclarar que el convenio de apoyo y colaboración para instituciones públicas no contempla una cláusula, como es el caso del convenio con instituciones privadas, en la que la institución pública se obligue a solicitar el consentimiento de los titulares para el tratamiento de sus datos personales en el marco del Servicio de Verificación, por lo que no aplica el análisis realizado anteriormente, en la obligación 2 de las instituciones privadas.

Ahora bien, el artículo 22 de la LFTAIPG establece lo siguiente:

> "**Artículo 22.** No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:
>
> **I.** (Se deroga).
> **II.** Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
> **III.** Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
> **IV.** Cuando exista una orden judicial;
> **V.** A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y
> **VI.** En los demás casos que establezcan las leyes."

En los supuestos previstos por el artículo antes citado, las instituciones públicas federales no requerirá el consentimiento de los titulares para la transferencia de sus datos personales al INE, para el Servicio de Verificación, en todos los demás casos, el consentimiento será necesario.

3. Transferencias realizadas por instituciones públicas locales

En el caso de que la transferencia sea realizada por **instituciones públicas locales**, dicha transferencia deberá cumplir con los requisitos previstos por la normativa de protección de datos personales aplicable a la institución de que se trate.

4. Transferencias del INE

Por otra parte, con relación a la transferencia de datos personales por parte del INE a las instituciones públicas y privadas, es importante reiterar que el INE señaló de manera consistente que el Servicio de Verificación no contempla transferencia de datos personales de ese Instituto a dichas instituciones. Al respecto, el INE señaló que la información que proporcione será "[…] el estatus de vigencia de la Credencial, un código respecto de la coincidencia o no de los datos y para el caso de la comparación de minucias de las huellas dactilares, el porcentaje de similitud mediante el uso de la minucia estándar INCITS 378. […]".

No obstante, de conformidad con lo expuesto en el apartado correspondiente al deber de confidencialidad y derivado de lo manifestado por el INE, se concluye que del catálogo de posibles respuestas a las instituciones en el marco del Servicio de Verificación, que el INE propone para "[…] complementar las respuestas señaladas […] con los numerales 90 a 93 y homologar las respuestas que se proporcionan en el servicio de consulta a la Lista Nominal por Internet (http:listanominal.ife.org.mx/) […]", con el propósito de "[…] proporcionar más información respecto de la situación de la credencial, […]", se manifiesta que, en caso de implementar las respuestas con número de ID 1 a 18, al Servicio de Verificación, el INE estaría proporcionando información adicional no necesaria para la prestación de dicho servicio, sobre la causa de falta de vigencia de la credencial para votar e incluso, en algunos supuestos, como, por ejemplo, en las respuestas 2, 5, 6, 12, 14 y 18, el INE estaría transfiriendo datos personales a la institución, entre los que se encuentran:

- La sección electoral vigente del titular;
- El número de emisión de la credencial para votar vigente del titular;
- El día, mes y año en los cuales el titular realizó su último trámite ante el INE;
- La suspensión de derechos del titular de la credencial para votar, y
- La pérdida o renuncia de la ciudadanía del titular de la credencial para votar.

Únicamente se considera relevante la respuesta identificada con ID 16, que permite a la institución saber que la credencial para votar presentada no está vigente en razón de que dicha credencial fue reportada como robada o extraviada.

Por otra parte, se sugiere verificar la descripción de la bitácora enviada mediante oficio INE/DERFE/356/2015, ya que en dicha bitácora se encuentran datos que, en principio, no son de los que se verificarán, entre ellos: calle, número, colonia, código postal, municipio y entidad de la dirección del ciudadano, estado, municipio y localidad de la residencial del ciudadano, y edad y sexo del ciudadano.

En virtud de lo anterior, en relación con el cumplimiento de las obligaciones relativas a las transferencias de datos personales realizadas en el marco del Servicio de Verificación, el INAI emite las siguientes observaciones y recomendaciones:

1. Prever explícitamente en los convenios de apoyo y colaboración para instituciones privadas que la institución incluya en su aviso de privacidad la transferencia de datos personales que realiza al INE en el marco del Servicio de Verificación, de conformidad con lo previsto en el artículo 16, fracción V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

2. Establecer en los convenios que se firmen con instituciones públicas y privadas, las consecuencias de no cumplir con sus obligaciones en materia de transferencias de datos personales, como podría ser que los titulares acudan ante el INAI a interponer una queja.

3. Valorar la conveniencia de que las instituciones públicas y privadas puedan solicitar el consentimiento para el tratamiento de sus datos personales en el Servicio de Verificación por un medio distinto al aviso de privacidad, ya que de otra forma estarían obligadas a entregar a cada uno de los titulares una copia del aviso de privacidad.

4. Prever explícitamente en los convenios de apoyo y colaboración para instituciones privadas, la obligación del INE y de la institución, de generar evidencia que permita acreditar transferencias de datos personales de la institución al INE, en cumplimiento a las obligaciones que prevé la LFPDPPP para las transferencias, incluyendo: i) si dichas transferencias son informadas por la institución a los titulares; ii) si el tratamiento de los datos personales para el Servicio de Verificación fue consentido y, en ese sentido, la transferencia de datos personales de la institución al INE, y ii) la entrega de los avisos de privacidad de las instituciones privadas al INE.

5. Prever explícitamente en los convenios de apoyo y colaboración para instituciones públicas federales, la obligación de éstas de requerir el consentimiento de los titulares para la transferencia de datos personales al INE cuando no se actualice alguno de los supuestos previstos en el artículo 22 de la LFTAIPG, y establecer mecanismos para que el INE pueda verificar que en esos casos se solicitó el consentimiento, el cual debe constar de manera expresa y por escrito.

6. Incluir en los convenios con instituciones públicas que éstas sólo podrán hacer uso del Servicio de Verificación y tratar datos personales en el mismo, cuando dicho tratamiento obedezca al ejercicio de sus atribuciones, así como la obligación de informar sobre las transferencias al INE en el sistema de datos que corresponda, si ello se prevé en la normatividad que resulte aplicable.

7. Incluir en la Cláusula sexta, inciso c), de los convenios, la referencia a “demás normativa aplicable”, en virtud de que es distinta la normativa que aplica a una institución privada, a una institución pública federal y a una institución pública local.

8. Revisar la normatividad sobre protección de datos personales que apliquen en lo particular a la institución pública local con la que se vaya a firmar convenio, para considerar en éste las cláusulas que sean necesarias.

9. Limitar la transferencia de datos por parte del INE a información genérica sobre la coincidencia o no de los datos proporcionados por la institución para la realización del cotejo correspondiente y el porcentaje de similitud de la huella digital, y evite proporcionar información adicional sobre las causas de la falta de vigencia de la credencial para votar, así como datos personales, al momento de dar respuesta sobre el cotejo de la información. En ese sentido, se recomienda no implementar respuestas complementarias para el Servicio de Verificación, tales como las identificadas con número de ID 1 a 18 referidas en la respuesta proporcionada por el INE, con excepción de lo

relativo al robo o extravío de las credenciales. Lo anterior con objeto de no difundir información confidencial en términos de lo dispuesto por los artículos 18, fracción II, y 21 de la LFTAIPG.

10. Derechos ARCO

En relación con los derechos de acceso, rectificación, cancelación y oposición, el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos prevé, en su artículo 16, lo siguiente:

> "**Artículo 16.** […]
>
> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."

Por su parte, el artículo 20, fracción I, 24, 25 y 61 de la LFTAIPG señala:

> "**Artículo 20.** Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:
>
> **I.** Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos […].
>
> **Artículo 24.** Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.
>
> La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27.
>
> **Artículo 25.** Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.
>
> **Artículo 61.** El Poder Legislativo Federal, a través de la Cámara de Senadores, la Cámara de Diputados, la Comisión Permanente y la Auditoría Superior de la Federación; el Poder Judicial de la Federación a través de la Suprema Corte de Justicia de la Nación, del Consejo de la Judicatura Federal y de la Comisión de Administración del Tribunal Federal Electoral; los órganos constitucionales autónomos [-como el INE-] y los tribunales administrativos, en el ámbito de sus respectivas competencias, establecerán mediante reglamentos o acuerdos de carácter general, los órganos, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información, de conformidad con los principios y plazos establecidos en esta Ley.
>
> Las disposiciones que se emitan señalarán, según corresponda:
>
> […]
> **VI.** Los procedimientos de acceso y rectificación de datos personales a los que se refieren los artículos 24 y 25, y

VII. Una instancia interna responsable de aplicar la Ley, resolver los recursos, y las demás facultades que le otorga este ordenamiento. […]"

En concordancia con lo anterior, el artículo 2, fracción XIX, y el Título Cuarto del RINEMTAIP establecen lo siguiente:

"**ARTÍCULO 2**
Del Glosario

1. Para los efectos del presente Reglamento, se entenderá por:
[…]

XIX. Derechos ARCO: los derechos de acceso, rectificación, cancelación y oposición de datos personales. Además, se entenderá por:
a) Acceso: poner a disposición del titular sus datos personales;
b) Rectificación: revisión que solicita el titular de los datos, por ser inexactos o incompletos;
c) Cancelación: supresión que solicita el titular de los datos, de uno o varios datos personales en el sistema o base de que se trate;
d) Oposición: negativa del titular de los datos personales al tratamiento de los mismos.

TÍTULO CUARTO
DE LOS DATOS PERSONALES

CAPÍTULO I.
Del acceso y corrección de datos personales

ARTÍCULO 32
Del acceso a datos personales
1. Sólo los interesados, por sí mismos o por medio de sus representantes legales, tendrán derecho a solicitar a la Unidad de Enlace, previa acreditación, que se les proporcione su información del sistema de datos personales.
[…]
3. El acceso, rectificación, cancelación y oposición a los datos personales en posesión del Registro Federal de Electores se regirán conforme a los Lineamientos que presente la Comisión del Registro Federal de Electores a la aprobación del Consejo. Esos Lineamientos deberán ajustarse al procedimiento y plazos que establece el presente Reglamento. […]

10. Para la elaboración de los Lineamientos referidos en los párrafos 2 y 3 de éste artículo se deberán considerar las disposiciones de la Ley, las leyes federales aplicables y del presente Reglamento, garantizando en todo momento la protección de los datos que los ciudadanos proporcionan al Instituto Nacional Electoral. […]"

Visto lo anterior y considerando que el Servicio de Verificación tiene como principal objetivo que el INE, a través de la DERFE, verifique por medio de un servicio web, la vigencia de las credenciales para votar que presenten los ciudadanos para identificarse ante instituciones públicas o privadas con las que el INE haya celebrado el convenio correspondiente y verifique que los datos contenidos en dichas credenciales coincidan con los que obran en el Sistema de Verificación y que se obtiene del Padrón Electoral, es viable concluir que los procedimientos de acceso, rectificación y cancelación de datos personales aplicables a los datos personales contenidos en el Padrón Electoral son los mismos que aplican en el caso de datos personales tratados en el contexto del Servicio de Verificación.

Al respecto, como respuesta a la pregunta 32 del cuestionario enviado al INE por el INAI, mediante oficio IFAI-OA/SPDP/0039/15, de fecha 10 de febrero de 2015, donde se pregunta "[…] si las solicitudes de ejercicio de los derechos de acceso, acceso, rectificación, cancelación y oposición (ARCO) que pudieran presentarse con motivo de la implementación del Servicio de Verificación de la Credencial para Votar, se atenderán de conformidad con el procedimiento que tenga

implementado el INE para atender el ejercicio de estos derechos en el Padrón Electoral, o si se implementarán nuevos procedimientos para ello. […]", el INE manifestó, en la reunión celebrada el 27 de febrero, que "[e]s el mismo procedimiento".

En este sentido, los derechos de acceso, rectificación, cancelación y oposición en el marco del Servicio de Verificación deben ejercitarse por los titulares de conformidad con lo previsto por los Lineamientos ARCO, los cuales se emitieron considerando lo previsto por la LGIPE, el RINETAIP y demás leyes federales aplicables.

Considerando lo expuesto, a continuación se citan los numerales 1, 5, 6, 7 y 11 de los Lineamientos ARCO, que establecen aspectos relevantes del ejercicio de los derechos ARCO respecto de datos personales previstos en el Padrón Electoral y, por ende, tratados en el contexto del Servicio de Verificación:

> "1. Para los efectos de los presentes Lineamientos, se entenderá por:
>
> Acceso a datos personales: Derecho fundamental de las y los ciudadanos para solicitar, conocer o interesarse por sus propios datos personales.
> Cancelación de datos personales: Derecho de las y los ciudadanos para solicitar la supresión de sus datos personales de los archivos y las bases digitales con que se cuente.
> […]
> Oposición de datos personales: Derecho de las y los ciudadanos para solicitar el cese del uso de sus datos personales con el objeto de que no se les dé el tratamiento para fines específicos.
> Órgano Garante: el Órgano Garante de la Transparencia y el Acceso a la Información.
> Rectificación de datos personales: Derecho que tienen las y los ciudadanos para solicitar la corrección o modificación de sus datos personales por ser inexactos, incompletos o inadecuados, derivado de su tratamiento.
>
> 5. El acceso, rectificación, cancelación, oposición y validación de los datos personales en posesión de la Dirección Ejecutiva, se realizará conforme a los procedimientos, plazos y términos que dispone la Constitución, el Código [la remisión se entiende hecha a la LGIPE vigente], el Reglamento, los acuerdos que emita la Comisión Nacional de Vigilancia conforme a sus atribuciones y la normatividad que emita la Dirección Ejecutiva para tal efecto.
>
> 6. La rectificación de datos personales en posesión de la Dirección Ejecutiva, será realizada por la Dirección Ejecutiva y las Vocalías respectivas, en los términos establecidos en el Libro Cuarto del Código [la remisión se entiende hecha a la LGIPE vigente] y demás normatividad que emita esa Dirección Ejecutiva, así como los acuerdos que emita la Comisión Nacional de Vigilancia conforme a sus atribuciones para la atención de las y los ciudadanos en los Módulos de Atención Ciudadana del Instituto.
>
> 7. Para efectos de los presentes Lineamientos son datos personales en posesión de la Dirección Ejecutiva y forman parte del Padrón Electoral, aquéllos que de conformidad con los artículos 184, numeral 1 y 200 del Código [se entiende una referencia a los artículos 140 y 186 de la LGIPE, actualmente vigente] son proporcionados por las y los ciudadanos, para realizar algún trámite de inscripción o actualización al Padrón Electoral, y en consecuencia para la obtención de su Credencial para Votar con Fotografía e incorporación a la Lista Nominal de Electores, siendo los siguientes:
> a) Nombre(s)
> b) Apellido paterno
> c) Apellido materno
> d) Sexo
> e) Edad
> f) Fecha y lugar de nacimiento
> g) Domicilio
> h) Entidad federativa, municipio y localidad que corresponden al domicilio
> i) Tiempo de residencia en el domicilio
> j) Ocupación

k) Firma
l) Fotografía
m) Huellas dactilares
n) Clave única del registro de población
o) Número y fecha del certificado de naturalización, en su caso

11. Los trámites que realice la Dirección Ejecutiva, para acceso, rectificación y en su caso para cancelación y oposición de los datos personales en posesión de ésta, serán gratuitos."

Asimismo, los Lineamientos ARCO desarrollan, de manera específica y considerando lo previsto por la LFTAIPG, la LGIPE y el RINETAIPG, los siguientes procedimientos para el ejercicio de los derechos ARCO respecto de datos personales que forman parte del Padrón Electoral, enlistados en el artículo 7 de los Lineamientos ARCO, incluyendo requisitos, medios de atención, plazos de respuesta y registro de las solicitudes correspondientes, entre otros aspectos:

a) Del acceso de los datos personales en posesión de la DERFE:
   - De las solicitudes de acceso y entrega de datos personales en posesión de la Dirección Ejecutiva presentada ante las oficinas de la DERFE presentadas ante las oficinas de la Dirección Ejecutiva y las Vocalías respectivas.
   - Del acceso a los documentos fuente en posesión de la DERFE.
   - De las solicitudes de acceso y entrega de datos personales en posesión de la DERFE, presentadas ante la Unidad de Enlace.

b) De la rectificación de datos personales en posesión de la DERFE:
   - De las solicitudes de rectificación de datos personales en posesión de la DERFE presentadas ante las oficinas de la DERFE y las Vocalías respectivas.
   - De las solicitudes de rectificación de datos personales en posesión de la DERFE presentadas ante la Unidad de Enlace.

c) De la cancelación y oposición de datos personales en posesión de la DERFE:
   - De la cancelación y oposición de datos personales en posesión de la DERFE y los procedimientos de cotejo, supresión y baja. Al respecto, se destaca que el numeral 28 de los Lineamientos ARCO de la DERFE establece que: "Las solicitudes de cancelación y oposición de datos personales en posesión de la DERFE, son improcedentes, en razón de que estos datos son proporcionados por las y los ciudadanos en cumplimiento de las obligaciones que la Constitución y el Código [se entiende la remisión hecha a la LGIPE vigente] establecen. El tratamiento y uso de los mismos, se encuentra sujeto a lo dispuesto en la propia Constitución y el Código." No obstante, los mismos lineamientos tienen previstos procedimientos de cancelación y oposición de datos personales en posesión de la DERFE y que no forman parte del Padrón Electoral, cuyas solicitudes podrían resultar procedentes.

Asimismo, los numerales 38, 39, y 40 de los Lineamientos ARCO prevén lo siguiente:

"38. En aquellos casos en que la Solicitud de Rectificación de datos personales en posesión de la Dirección Ejecutiva no sea procedente a favor de las o los ciudadanos, éstos podrán interponer, conforme lo dispone el artículo 187, numeral 7 del Código [se entiende como remisión al artículo 143, numeral 7 de la LGIPE vigente], una solicitud de expedición de Credencial para Votar con Fotografía.

> Para el caso que no les sea notificada la resolución recaída a la Solicitud de Expedición de la Credencial para Votar con Fotografía, en un término de 20 días naturales, o no estén conformes con el sentido de la misma, las y los ciudadanos podrán interponer, en un término máximo de 4 días hábiles, siguientes al último del plazo en que la autoridad deba notificar su resolución o al de la notificación de la resolución referida, el Juicio para la Protección de los Derechos Político-Electorales de los Ciudadanos, previsto en la Ley General del Sistema de Medios de Impugnación en Materia Electoral.
>
> 39. En los Módulos de Atención Ciudadana del Instituto estarán a disposición de las y los ciudadanos, los formatos requeridos para la interposición del Juicio para la Protección de los Derechos Político–Electorales del Ciudadano, así como la asesoría necesaria para su llenado.
>
> 40. Las y los ciudadanos o sus representantes legales, podrán interponer el recurso de revisión, previsto en el Capítulo II del Título Quinto del Reglamento, cuando además de los supuestos previstos en el artículo 41 del citado Reglamento, se presente alguno de los siguientes:
> […]
>
> d) La constancia donde se entreguen los datos personales en posesión de la Dirección Ejecutiva, sea entregada en formato incomprensible.
> e) Se estime que la Dirección Ejecutiva o las Vocalías respectivas, no cumplieron adecuadamente con la obligación de otorgarles acceso a dichos datos."

De esta manera, se concluye que se tienen previstos procesos para que los titulares ejerzan sus derechos ARCO ante el INE, en relación con el Padrón Electoral, de donde se obtiene la información necesaria para operar el **Servicio de Verificación**. Asimismo, los Lineamiento ARCO prevén distintos recursos que pueden ser interpuestos por un titular no satisfecho con el resultado del ejercicio de sus derechos ARCO: i) solicitud de expedición de credencial para votar con fotografía, ii) el juicio para la protección de los derechos político-electorales de los ciudadanos y iii) recurso de revisión, según sea el caso.

No se omite señalar que el análisis y recomendaciones antes realizadas se centraron en identificar que en el Servicio de Verificación se contemplaran mecanismos para el ejercicio de derechos ARCO por parte de los titulares.

En virtud de lo anterior, en relación con los procedimientos previstos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, el INAI realiza las siguientes observaciones y recomendaciones:

1. Actualizar los Lineamientos ARCO, en virtud de lo que los mismos fueron emitidos en el 2012 y hacen remisiones a normativa derogada o abrogada, y

2. Prever e informar al titular, mediante la leyenda de información o documento análogo, que los procedimientos para el ejercicio de derechos ARCO aplicables a los datos personales contenidos en el Padrón Electoral, así como los recursos correspondientes, aplican a los datos personales tratados en el marco del Servicio de Verificación.

3. De conformidad con las buenas prácticas, nombrar un oficial para la protección de los datos personales, que tenga entre sus funciones, entre otras:

- Asesorar al interior del INE respecto a los asuntos en materia de protección de datos personales.
- Coordinar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de las obligaciones en la materia.
- Coordinar las acciones de capacitación en materia de protección de datos personales

No se omite señalar que el análisis y recomendaciones antes realizadas se centraron en identificar que en el Servicio de Verificación se contemplaran mecanismos para el ejercicio de derechos ARCO por parte de los titulares.

No se omite manifestar que las consideraciones de la presente opinión tienen como propósito brindar una orientación desde el punto de vista estrictamente técnico, y no prejuzga sobre las determinaciones que en su caso el Pleno del INAI pudiera adoptar al respecto en ejercicio de las facultades que le han sido otorgadas.

Anexo 2.

Resumen Ejecutivo “Opinión técnica sobre el servicio de verificación de Datos de la Credencial para Votar”, emitido por el INAI.

CONACYT
Consejo Nacional de Ciencia y Tecnología

INFOTEC

Coordinación de Protección de Datos Personales
Dirección General de Autorregulación
Dirección General de Normatividad, Consulta y Atención Regional
Mayo 2015

Resumen Ejecutivo

Opinión técnica sobre el Servicio de Verificación de Datos de la Credencial para Votar

Contenido

I. Glosario

Anexo Técnico 3.2	Anexo Técnico del Convenio de apoyo y colaboración entre el Instituto Nacional Electoral "EL INE" y "LA INSTITUCIÓN" Versión 3.2, mediante oficio INE/DERFE/356/2015.
CPEUM	Constitución Política de los Estados Unidos Mexicanos.
Derechos ARCO	Derechos de acceso, rectificación, cancelación y oposición.
DERFE	Dirección Ejecutiva del Registro Federal de Electores.
INAI o Instituto	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos.
INE	Instituto Nacional Electoral.
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
LFTAIPG	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
LGIPE	Ley General de Instituciones y Procedimientos Electorales.
LGP	Ley General de Población.
LOAPF	Ley Orgánica de la Administración Pública Federal.
Lineamientos ARCO	Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores.
Manifestación de datos personales	Manifestación de protección de datos personales recabados por el Registro Federal de Electores.
Recomendaciones	Recomendaciones en materia de Seguridad de Datos Personales.
RINEMTAIP	Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública.
RLFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Servicio de Verificación	Servicio de Verificación de Datos de la Credencial para Votar.
SGSDP	Sistema de Gestión de Seguridad de Datos Personales.

II. Antecedentes

1. El 3 de diciembre de 2014, a través del oficio número INE/DERFE/1108/2014, el INE solicitó al INAI (en ese entonces denominado Instituto Federal de Acceso a la Información y Protección de Datos, IFAI) lo siguiente: *"[…] que se emita un Dictamen sobre la Manifestación de impacto a la privacidad del servicio de Verificación de datos de la Credencial para Votar […]"*. Para tal efecto, los documentos aportados por el Instituto Nacional Electoral comprenden:

   a) Generalidades del servicio de verificación de datos de la credencial para votar.
   b) Convenio de apoyo y colaboración entre el Instituto Nacional Electoral y la institución.
   c) Anexo técnico del convenio de apoyo y colaboración entre el Instituto Nacional Electoral y la institución en su versión 3.1.

2. El 22 de enero de 2015, se celebró una reunión de trabajo en la que participaron servidores públicos del INE y del INAI. La misma tuvo por objeto dimensionar los alcances jurídicos y técnicos de una manifestación de impacto a la privacidad.

3. El 28 de enero de 2015, mediante el oficio número INE/DERFE/0098/2015, el INE solicitó al INAI que emitiera una opinión especializada sobre la viabilidad de la aplicación del proyecto Servicio de Verificación de datos de la credencial para votar, replanteando su solicitud inicial.

4. El 10 de febrero de 2015, mediante oficio IFAI-OA/SPDP/0039/15, y en respuesta al oficio número INE/DERFE/0098/2014, el INAI solicitó al INE que proporcionara elementos informativos adicionales a efecto de estar en condiciones de emitir la opinión técnica correspondiente. Para tal efecto, el INAI remitió al INE un cuestionario de cuarenta reactivos para conocer con mayor detalle el proyecto del Servicio de Verificación.

5. El 23 de febrero de 2015, servidores públicos del INE y del INAI llevaron a cabo una reunión con la finalidad de definir un marco de colaboración que facilitara la atención de dicho requerimiento, acordando la celebración de una reunión de trabajo.

6. El 27 de febrero de 2015, el INAI y el INE se reunieron para abordar y desahogar el requerimiento de información adicional.

7. El 20 de marzo de 2015, a través del oficio INE/DERFE/356/2015, y en respuesta al oficio IFAI-OA/SPDP/0039/15, el INE remitió la siguiente información y documentación adicional en seguimiento a la reunión del 27 de febrero de 2015:

   a) Acuerdo CG734/2012 del Consejo General del Instituto Federal Electoral por el que se aprueban los Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de datos personales en posesión de la Dirección Ejecutiva del Registro Federal de Electores.
   b) Acuerdo INE/CG70/2014 del Consejo General del Instituto Federal Electoral por el que se expide el Reglamento del INE en materia de transparencia y acceso a la información pública.
   c) Acuerdo 1-ORD/14: 18/07/2014 de la Comisión Nacional de Vigilancia, por la que aprueba las Modificaciones a la "Solicitud individual de inscripción o actualización al Padrón Electoral y recibo de la credencial".
   d) Anexo técnico del convenio general de apoyo y colaboración entre el Instituto Nacional Electoral y la Institución en su versión 3.2.
   e) Cédula descriptiva del Registro Federal de Electores.
   f) Convenio de colaboración entre el Instituto Nacional Electoral e Instituciones privadas.

g) Convenio de colaboración entre el Instituto Nacional Electoral e Instituciones públicas.
h) Solicitud individual de inscripción o actualización al Padrón Electoral y recibo de la credencial.
i) Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de datos personales en posesión de la Dirección Ejecutiva del Registro Federal de Electores.
j) Manifestación de protección de datos personales recabados por el Registro Federal de Electores.

8. El 9 de abril de 2015, el INAI celebró una reunión con funcionarios del Tribunal Electoral del Poder Judicial de la Federación con el objeto de conocer su opinión sobre el proyecto de referencia.

9. El 13 de abril de 2015, el INAI celebró una reunión con funcionarios de la Fiscalía Especializada para la Atención de Delitos Electorales, con el objeto de conocer su opinión sobre el proyecto.

10. El 16 de abril de 2015, consejeros del INE, entre los que estuvo presente el Consejero Presidente, realizaron una reunión con los comisionados del INAI, con el objeto de exponer y tratar directamente diversos aspectos relacionados con la operación y funcionamiento del proyecto del Servicio de Verificación de datos de la credencial para votar.

11. El 20 de abril de 2015, el INAI y el INE sostuvieron una reunión que tuvo como objeto analizar los siguientes puntos:

a) Facultades del INE para para verificar los datos personales contenidos en la credencial para votar que soliciten las instituciones públicas y privadas.
b) Datos personales de la credencial para votar que se requieren para asegurar una verificación efectiva de los mismos, y a su vez, cumplir con la finalidad del servicio.
c) Modelos del convenio de colaboración y sus beneficios para las instituciones públicas o privadas que lo suscriban.
d) Alcance de la prueba piloto con Banamex.

12. El 21 de abril de 2015, derivado de los compromisos asumidos en la reunión del 16 de abril del año en curso, el INE, a través de oficio INE/DERFE/STN/6940/2015, remitió al INAI un documento que describe las acciones de depuración permanente del Padrón Electoral.

13. El 30 de abril de 2015, la Fiscalía Especializada para la Atención de Delitos Electorales, mediante oficio 531/DGJMDE/FEPADE/2015, emitió opinión respecto al Servicio de Verificación.

III. Alcance de la solicitud del Instituto Nacional Electoral (INE)

El 2 de diciembre de 2014, el INE solicitó al INAI lo siguiente:

> "[…] En virtud de lo anterior y de conformidad con lo dispuesto en el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, en su Apartado A, fracción VIII, se solicita de manera comedida al Instituto Federal de Acceso a la Información y Protección de Datos su apoyo para que se emita un Dictamen sobre la Manifestación de impacto a la privacidad del servicio de Verificación de datos de la Credencial para Votar […]"

Derivado de la solicitud del INE, el 22 de enero del año en curso se celebró una reunión entre servidores públicos de dicho Instituto y del INAI, en la cual se abordaron los alcances jurídicos y técnicos de una manifestación de impacto a la privacidad respecto al proyecto Servicio de Verificación, asimismo se plantearon una serie implicaciones para la realización de la misma en torno al proyecto aludido.

Derivado de la reunión referida, el INE decidió replantear su solicitud en los siguientes términos:

> "[…]
>
> En virtud de lo antes expuesto, con la finalidad de garantizar la seguridad de la información de los datos personales que proporcionan los ciudadanos al Registro Federal de Electores y tomando en cuenta la naturaleza pública y privada de las instituciones usaurias del servicio de Verfificación, me permito realizar a través de esta vía una Consulta Técnica, a fin de que **tenga a bien emitir una opinión especializada sobre la vaibilidad de la aplicación del "Servicio de Verificación de Datos de la Credencial"**, que se adjunta como anexo al presente escrito.
> […]"

IV. Esquema de colaboración entre el INAI y el INE para la emisión de una opinión técnica

De acuerdo con lo dispuesto en el artículo octavo y décimo transitorios del Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos en materia de trasparencia; los artículos 3, fracción VII, 37, fracción XV y 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; los artículos 3, fracción XIII,[1] primero, segundo, tercero y quinto transitorio de la Ley General de Transparencia y Acceso a la Información Pública; el artículo 24, fracciones III, VI y X del Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos y el acuerdo del Pleno Administrativo del INAI ACT/ORD-PLENO/PA/03/06/14.04, el INAI, a través del Coordinador de Protección de Datos Personales, emite la opinión especializada solicitada por el INE en el

[1] De conformidad con el artículo 6, apartado A, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos, la Federación contará con un organismo garante que se regirá por la ley en materia de transparencia y acceso a la información pública y protección de datos personales en posesión de sujetos obligados, siendo este el Instituto Federal de Acceso a la Información y Protección de Datos, de conformidad con el artículo décimo transitorio del Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, publicado en el Diario Oficial de la Federación el 7 de febrero de 2014, el cual estableció que los recursos financieros y materiales, así como los trabajadores adscritos al entonces IFAI, se transfirieran al organismo público autónomo creado. Ahora bien, el 4 de mayo de 2015, se publicó en el Diario Oficial de la Federación el Decreto por el que se expidió la Ley General de Transparencia y Acceso a la Información Pública, misma que en su artículo 3, fracción XIII, refiere que el órgano garante será denominado como Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. En consecuencia y atendiendo a lo señalado por el artículo segundo transitorio de la Ley General de Transparencia y Acceso a la Información Pública, la denominación de Instituto Federal de Acceso a la Información y Protección de Datos, a que se refiere el artículo 3, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, cambia a Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

contexto de un esquema respetuoso de colaboración cuyo objetivo es brindar las sugerencias a que haya lugar para fortalecer el marco de actuación de los órganos del Estado mexicano en el tratamiento de datos personales. Lo anterior, considerando que actualmente el INE no forma parte de los sujetos obligados bajo la competencia del INAI hasta en tanto se cumplan las condiciones legales previstas en los artículos transitorios antes referidos.

Derivado de lo anterior, el INAI procede a formular una opinión técnica con el objeto de analizar el cumplimiento de los principios, deberes y derechos inherentes a la protección de datos personales con base en lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, Ley General de Población, Ley General de Instituciones y Procedimientos Electorales, Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ley Orgánica de la Administración Pública Federal, Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública, Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores, así como a manera de estricta referencia y buenas prácticas en los Estándares internacionales sobre protección de datos personales y privacidad de 2009 y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

No se omite manifestar que las consideraciones de la presente opinión tienen como propósito brindar una orientación desde el punto de vista estrictamente técnico, y no prejuzga sobre las determinaciones que en su caso el Pleno del INAI pudiera adoptar al respecto en ejercicio de las facultades que le han sido otorgadas.

V. Consideraciones generales en materia de protección de datos personales sobre el Servicio de Verificación de datos de la credencial para votar del INE

Uno de los objetivos del Servicio de Verificación, respecto del cual versa esta opinión técnica, es -según lo manifestado por el propio INE- facilitar a las instituciones públicas y privadas un mecanismo de fácil acceso y eficiente operación, para verificar la autenticidad y vigencia de los datos contenidos en las credenciales para votar que presenten los ciudadanos al momento de realizar un trámite, y con ello evitar robo o suplantación de identidad.

Como es de conocimiento público, uno de los instrumentos más utilizados con fines de identificación es la credencial para votar, a partir de lo dispuesto por el artículo cuarto transitorio de la LGP, que establece que en tanto no se expida la cédula de identidad ciudadana, dicha credencial servirá como medio de identificación personal. En ese sentido, una credencial para votar confiable, no sólo con fines electorales, sino incluso de identificación personal, es fundamental para la seguridad de las personas.

Ahora bien, el robo de identidad es uno de los delitos de más rápido crecimiento en el mundo con el uso de Internet y el comercio electrónico. El robo, usurpación o suplantación de identidad ocurre cuando una persona obtiene, transfiere o utiliza de forma no autorizada datos personales. Es la apropiación de la identidad de una persona para acceder a ciertos recursos o beneficios a nombre de esa persona.

La identidad la constituyen datos personales, como nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia o seguridad social, número de tarjetas de crédito y de cuentas bancarias, nombres de usuario y contraseña, datos de salud o biométricos, información financiera, así como cualquier otro dato que pueda hacer identificable a una persona.

De acuerdo con el Banco de México, en 2010 los fraudes ligados al robo de identidad se estimaron en $108, 000,000.00 de pesos, menor al robo en cajeros automáticos que fue de $87, 000,000 de pesos.[2]

De acuerdo con el estudio sobre los hábitos de los usuarios de Internet en México 2014,[3] nueve de cada diez internautas acceden a una red social en donde dejan datos personales que permiten a los atacantes inferir contraseñas, preguntas de seguridad u otras credenciales de autenticación.

Por otra parte, según cifras proporcionadas por la firma Card Protection Plan México,[4] la cual se dedica a temas de fraudes, protección a tarjetas e identidad, seis de cada diez personas han perdido la cartera al menos una vez en su vida; a cinco de cada diez personas le han robado la cartera, y nueve de cada diez llevan información suficiente en su cartera para ser víctima de robo de identidad, entre ellas, el 86 por ciento lleva en su cartera la credencial para votar.

Los daños y perjuicios causados por este delito no se limitan al ámbito económico, sino que abarcan también aspectos emocionales y psicológicos, ya que la persona es invadida en su privacidad y en algunas ocasiones afectada en su reputación, además de todos los impactos económicos que pudieran existir. Una de las complejidades de este delito es que las personas no se enteran muchas veces que han sido víctimas de robo de identidad hasta que quieren ejercer un derecho o gozar de un beneficio y no lo pueden hacer, o tienen cobros no reconocidos.

Los métodos utilizados para el robo de identidad pueden ser muchos, algunos implican la falta de medidas de seguridad para la protección de las bases de datos que contienen información personal o ataques a servidores con datos personales, otros se llevan a cabo a través de la obtención ilegal de la información personal directamente de su titular. Sin importar el método utilizado para el robo de identidad, este delito involucra un tratamiento ilegal de datos personales.

En ese sentido, al ser el INAI el organismo autónomo garante del derecho a la protección de datos personales, tanto para el sector público federal, como para los entes privados; tiene un legítimo interés en ser partícipe de las políticas públicas que coadyuven a la disminución de la comisión de este delito en nuestro país, ya sea a través de la implementación de mecanismos que eviten que las bases de datos de instituciones públicas y privadas sean vulneradas y con ello se obtengan datos personales de manera ilegal, o bien por medio de acciones de educación cívica y cultura que promuevan la importancia de la protección de los datos personales entre sus titulares.

En el caso que nos ocupa, el Servicio de Verificación, a cargo del INE, es un mecanismo que podrá ayudar a evitar que el robo de identidad se materialice en algún fraude u otro delito en perjuicio de los titulares de los datos personales, a través de la facilitación de una herramienta que permitirá la confronta de los datos de la Credencial para Votar que presente quien realiza el trámite, contra aquéllos contenidos en el Padrón Electoral, a fin de suponer la autenticidad o no de la credencial.

En ese sentido, este Servicio de Verificación se considera una política pública socialmente útil, pues no sólo tendrá beneficios para los titulares de los datos personales, sino para las instituciones públicas y privadas que otorguen créditos, suministren bienes o servicios, o realicen trámites. En ese sentido, este Instituto reconoce su importancia y valor social.

---

[2] Cifras disponibles en Gema Sheyla Ramírez Ricárdez, Robo de identidad, 2014, consultable en el siguiente vínculo electrónico: http://www.infodf.org.mx/dp/doctos/14/presenta/robo_identidad2014.pdf

[3] Estudio realizado por la Asociación Mexicana de Internet (Amipci) y disponible en el siguiente vínculo electrónico: https://www.amipci.org.mx/estudios/habitos_de_internet/Estudio_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf

[4] Cifras disponibles en el estudio denominado "La vulnerabilidad y los riesgos de extraviar una cartera", realizado por Card Protection Plan México y disponible en el siguiente vínculo electrónico: http://mexico.cppdirect.com/prensa-y-medios

Por otra parte, como lo señaló la Fiscalía Especializada para la Atención de Delitos Electorales, en su respuesta a la consulta realizada por este Instituto, debe tomarse en consideración la estricta confidencialidad de los datos contenidos en el Padrón Electoral y los límites que la legislación electoral y la de información pública establecen para su adecuado uso y manejo. En el Servicio de Verificación se debe cuidar no dar a conocer los datos personales de los aportantes, y que esa información siempre sea custodiada por el INE. Además, la implementación de este servicio no debe implicar la vulneración de los derechos de los ciudadanos que aportan sus datos al INE en la formación del Registro Federal de Electores, ni los fines de validación que persigue el Servicio de Verificación deben afectar los derechos políticos.

Con independencia de lo anterior, y aprovechando la oportunidad que brinda la presente opinión técnica solicitada por el INE, se destaca la importancia de resolver el tema pendiente que tiene el Estado mexicano de garantizar a la población su derecho a la identidad a través de la emisión de un documento de identidad, que dé certeza jurídica a las personas con relación a su identidad legal, y que les permita ejercer derechos ciudadanos básicos y evitar problemas para el acceso a prestaciones sociales, al sistema de justicia, al reconocimiento como personas en plenitud, al derecho al bienestar, al desarrollo de capacidades, al acceso a empleos productivos y a la participación política. Si bien en este momento, el INAI no tiene una postura institucional y técnica con relación al documento, base de datos y autoridad que deberán garantizar el derecho a la identidad, sí reconoce la urgencia de retomar los trabajos legislativos y de políticas públicas que sean necesarios para que los mexicanos cuenten con un documento de identidad, como ocurre en los países más avanzados en materia de derechos humanos.

VI. Análisis por principios de protección de datos personales

Ahora bien, en cuanto a la protección de datos personales en el Servicio de Verificación -materia de la presente opinión técnica-, es importante señalar que si bien dicho proyecto está diseñado para garantizar la confidencialidad de los datos personales contenidos en el Padrón Electoral, pues se parte de la premisa de que el INE no comunicará datos personales a las instituciones públicas y privadas a las cuales brinde el servicio; en el análisis realizado por este Instituto se identificaron áreas de mejora y medidas que tendría que tomar el INE para garantizar una adecuada protección de los datos personales en el Servicio de Verificación, para lo cual este Instituto ha realizado una serie de recomendaciones, con base en los principios de protección de datos personales reconocidos nacional e internacionalmente, **y con pleno respeto a la autonomía del INE**, que considera importante su atención para no violentar el derecho de las personas a la protección de su información.

Concretamente los principios, deberes, derechos y demás obligaciones que se analizaron son los siguientes:

- Principio de licitud.
- Principio de finalidad.
- Principio de información.
- Deber de seguridad.
- Transferencias.
- Principio del consentimiento.
- Principio de proporcionalidad.
- Principio de calidad.
- Deber de confidencialidad.
- Derechos ARCO

A continuación se presenta una síntesis del análisis técnico realizado, el cual se desarrolla a detalle en el Anexo Único de la presente opinión, así como las recomendaciones que este Instituto emite con objeto de coadyuvar a la protección de datos personales en el Servicio de Verificación.

1. Principio de licitud

Si bien es cierto, el INAI identificó referencia expresa en el RINEMTAIP y los Lineamientos ARCO para que el INE preste el Servicio de Verificación y la posibilidad de que el Padrón Electoral se use para prestar dicho Servicio, también lo es que sería recomendable que dicha referencia se encontrara de manera expresa en sede constitucional o legal.

2. Principio del consentimiento

El INE está obligado a obtener el consentimiento de las personas que participen en el proceso del Servicio de Verificación, independientemente de la naturaleza pública o privada de la institución con quien suscriba el convenio, siempre que no se actualice alguno de los supuestos del artículo 22 de la LFTAIPG.

Recomendaciones y observaciones del INAI con relación al principio del consentimiento:

1. De acuerdo con lo dispuesto en los artículos 21 y 22 de la LFTAIPG, que la obtención del consentimiento se haga de manera previa al tratamiento de datos personales para el Servicio de Verificación.

2. Que el consentimiento se obtenga de manera:

    a. Libre, sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.
    b. Específica, referido a una o varias finalidades determinadas que justifiquen el tratamiento.

c. Informada, que el titular tenga conocimiento previo de la existencia y características del tratamiento a que serán sometidos sus datos personales.
d. Expresa, lo cual se traduce en que la voluntad del titular se manifieste de forma escrita.
e. Inequívoca, esto es la existencia de elementos que de manera indubitable demuestren su otorgamiento.

3. Que el mecanismo para la obtención del consentimiento procure ser en la mayor medida de lo posible un medio sencillo, gratuito y de fácil acceso para que el titular pueda manifestar su voluntad.

4. Que se prevean las condiciones jurídicas y materiales mínimas para contar con un respaldo suficiente para estar en posibilidades de acreditar, para todos los efectos, que se obtuvo válidamente el consentimiento del ciudadano involucrado por lo que al INE se refiere.

5. Prever en el modelo de convenio de colaboración que el INE que suscriba con instituciones públicas mecanismos para solicitar el consentimiento de las personas que participen en el proceso del Servicio de Verificación previa revisión, caso por caso, de la normativa aplicable, en los casos que resulte procedente.

6. Implementar un mecanismo que permita recabar el consentimiento del titular desde el momento en que acude a obtener la credencial para votar, o bien, actualizar su información personal.

7. Emitir los lineamientos en los que se detallen los diversos principios aplicables en materia de protección de datos personales, como el del consentimiento. Al respecto, se sugiere considerar la inclusión de disposiciones normativas que expresamente señalen los alcances del mismo, así como las obligaciones a observar por parte del INE al respecto.

3. Principio de finalidad

Las finalidades del Servicio de Verificación resultan ser determinadas y explícitas, sin embargo para conocer si las mismas son compatibles con las atribuciones conferidas al INE se requieren de los elementos a que se hace referencia en el análisis del principio de licitud.

Recomendaciones y observaciones del INAI con relación al principio de finalidad:

1. De acuerdo con lo dispuesto en el artículo 20, fracción II de la LFTAIPG, cerciorarse que las atribuciones del INE sean compatibles con las finalidades perseguidas a través del Servicio de Verificación, ello por supuesto, una vez se materialice lo indicado en el numeral 1.

2. Emitir los lineamientos en los que se detallen los diversos principios aplicables en materia de protección de datos personales, como el de finalidad. Al respecto, se sugiere considerar la inclusión de disposiciones normativas que expresamente señalen los alcances del mismo, así como las obligaciones a observar por parte del INE al respecto.

4. Principio de proporcionalidad

Los datos personales a tratar con motivo del Servicio de Verificación son adecuados, pertinentes y no excesivos, a saber: los números OCR y CIC como obligatorios, así como los datos opcionales que podrían ser cotejados como son apellido paterno, apellido materno, nombre, año de registro, número de emisión de la credencial para votar, clave de elector, CURP y huellas dactilares de los dedos índices de la mano derecha e izquierda.

No obstante, se reitera la recomendación al INE de emitir los lineamientos en los que se detallen los diversos principios aplicables en materia de protección de datos personales, específicamente el principio de proporcionalidad. Al respecto, se sugiere considerar la inclusión de disposiciones normativas que expresamente señalen los alcances de éstos, así como las obligaciones a observar por parte del INE al respecto.

Asimismo, en caso de que el INE amplíe el catálogo de respuestas sobre la coincidencia o no de los datos proporcionados por la institución para la realización del cotejo correspondiente y el porcentaje de similitud de la huella digital, se hacen propias las recomendaciones identificadas con los numerales 6 del deber de confidencialidad y 9 del apartado de transferencias.

5. Principio de información

Dado que los datos personales que se tratarán en el Servicio de Verificación son aquéllos que se obtienen para la integración del Padrón Electoral, la emisión de credenciales para votar y la incorporación de la lista nominal de electores, el INE cumplirá con este principio a partir de la puesta a disposición de la *Manifestación de protección de datos personales recabados por el Registro Federal de Electores,* desde el momento en que los titulares acudan a tramitar su credencial para votar.

Recomendaciones y observaciones del INAI con relación al principio de información:

1. De conformidad con lo establecido en el artículo 20, fracción III de la LFTAIPG, el INE deberá dar a conocer la *Manifestación de protección de datos personales recabados por el Registro Federal de Electores* a los titulares de los datos personales al momento en que proporcionan sus datos para la integración del Padrón Electoral, la emisión de credenciales para votar y la incorporación de la lista nominal de electores, y no sólo remitirlos al portal de Internet del INE para conocer el contenido de la Manifestación.

   Es de relevante importancia que se dé a conocer la Manifestación cuando el titular proporciona sus datos personales, y no de manera posterior, pues sólo así se cumplirá con el objetivo del principio de información que, como ya se señaló, se centra en dar a conocer al titular las características principales del tratamiento, a fin de que éste tome decisiones informadas con relación a la entrega de sus datos personales.

   Para ello, será necesario que en los módulos en los que se tramiten las credenciales para votar se cuente con el texto de la Manifestación completo. Es importante señalar que no es necesario que se entregue una copia de la misma a cada titular, sino que es suficiente con que se ponga a su disposición para su lectura, con independencia de que si el titular requiera copia de la misma el INE se la pueda proporcionar o lo invite a obtenerla en versión electrónica a través de su portal de Internet.

   Al respecto se recomienda:

   - La colocación de carteles en los módulos que contengan la Manifestación, o bien la inclusión de esta última en el formato o cédula que se entrega a los titulares cuando tramitan la Credencial para Votar.
   - Capacitar al personal que labora en los mismos para concientizarlos sobre la importancia del cumplimiento de esta obligación.

2. Tomar las medidas necesarias para que la nueva Manifestación, en la que ya se incluye como finalidad del tratamiento, el Servicio de Verificación, sea aprobada de manera oportuna por el órgano competente, y que la misma se utilice en cuanto inicie la implementación del Servicio.

3. Revisar el contenido de la Manifestación y atender las observaciones realizadas por el INAI, a saber:

- Verificar el listado de datos personales que realmente se recaban, a fin de informar de manera exacta al respecto en la Manifestación.
- Hacer referencia a los artículos principales de la CPEUM y la LGIPE que habiliten al INE al tratamiento de los datos personales para las finalidades informadas en la Manifestación.
- Incluir la información de los apartados 3 y 8 en un solo apartado, para que así se haga referencia a los cuatro derechos: acceso, rectificación, cancelación y oposición.
- Valorar la eliminación de los apartados 9 y 10, ya que no aplican al caso particular.
- Incluir el derecho de oposición al que refiere el numeral 33 del Capítulo Segundo de los Lineamientos ARCO.
- Señalar con precisión los vínculos electrónicos en los que, en su caso, se pueden obtener los formatos para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, o donde se pueden presentar las solicitudes; o bien proporcionar los números telefónicos donde se puede obtener mayor información al respecto.

4. Implementar las medidas que tienen consideradas para dar a conocer los cambios en la Manifestación y la nueva finalidad del tratamiento a través de medios masivos de comunicación. Al respecto se recomienda:

- Que el texto a utilizar contenga cuando menos la siguiente información: identidad y domicilio del INE, finalidades del tratamiento (señalando de manera expresa el sistema de verificación) y los mecanismos para conocer la Manifestación completa.
- Incluir información adicional que permita a los titulares identificarse como destinatarios de la manifestación.
- Para la elección de los medios de publicación de la Manifestación, tomar en cuenta los siguientes factores:
  - Perfil de los titulares.
  - Medios habilitados para mantener una comunicación general con los titulares.
  - Características del medio en el que se pretende publicar la Manifestación.
  - Atender al criterio de máximo alcance, de tal forma que la elección del medio y periodo resulte más eficiente para la difusión de la Manifestación.

5. Revisar la cédula descriptiva del Servicio de Verificación, a fin de que ésta corresponda con exactitud al tratamiento que se lleva a cabo, principalmente en lo que refiere a los apartados de objetivo del sistema y tipo de datos.

Así como tomar las medidas necesarias para que la cédula descriptiva del sistema de datos personales correspondientes al Sistema de Verificación, previo a la entrada en operación de dicho servicio, sea aprobada de manera oportuna por el órgano competente, hacerlo del conocimiento del Comité de Información y del Órgano Garante de la Transparencia el Acceso a la Información, a efecto de garantizar que se mantenga actualizado dicho listado y que sea publicado en el portal de Internet del INE, de conformidad con lo que establece el artículo 38 del RINEMTAIP.

6. Verificar que, efectivamente, las instituciones privadas a las que se preste el Servicio de Verificación informen en su aviso de privacidad sobre esta finalidad del tratamiento de los datos personales, de conformidad con lo establecido en el numeral 45 de los Lineamientos ARCO.

7. Con relación a los convenios que el INE celebre con instancias públicas, respecto de la cláusula quinta, se sugiere incluir un inciso en el que se establezcan obligaciones en materia de protección de datos personales, como la prevista en la Cláusula quinta del inciso e), del convenio con instancias privadas, a efecto de dichas instituciones establezcan en su leyenda de información, dentro de los propósitos del tratamiento de los datos personales, la

posibilidad de verificación de los datos de la Credencial para Votar en el Servicio de Verificación, lo que implica transferencias al INE.

8. Por otra parte, se sugiere valorar la conveniencia de que las instancias públicas y privadas puedan solicitar el consentimiento para el tratamiento de sus datos personales en el Servicio de Verificación por un medio distinto al aviso de privacidad, ya que de otra forma estarían obligadas a entregar a cada uno de los titulares una copia del aviso de privacidad.

9. Emitir los lineamientos en los que se detallen los diversos principios aplicables en materia de protección de datos personales, como el de información, de conformidad con lo dispuesto en el artículo 36 del RINEMTAIP. Al respecto, se sugiere considerar la inclusión de disposiciones normativas que expresamente señalen cuáles son los elementos informativos que debe contener la manifestación de datos personales, atendiendo los estándares nacionales e internacionales.

6. Principio de calidad

Este principio se cumple a partir de la actualización y depuración oportuna del Padrón Electoral y la actualización de la base de datos del Servicio de Verificación en los plazos establecidos.

Recomendaciones y observaciones del INAI con relación al principio de calidad:

1. Considerar los diversos escenarios en los cuales, eventualmente, el INE pudiera estar impedido para validar los datos que se aporten en los trámites que realicen los ciudadanos ante las instituciones públicas y privadas con las que suscriba convenios de colaboración, como podrían ser, casos de duplicidad u homonimias, entre otros.

2. Respecto de la base de datos del Sistema de Verificación:

    - Tomar las medidas necesarias a efecto de que la actualización de la información del Sistema de Verificación se lleve a cabo conforme al procedimiento que al efecto indicó el INE, el cual se realiza diariamente, cada 12 y 24 horas, para ello, deberá considerar:
        - Que la programación que se realiza en el portal de administración de la solución funcione de manera correcta, tanto para el caso de datos como en el caso de huellas; y
        - Que no existan factores que afecten el proceso de actualización de la base de datos, permitiendo que se concluya de manera exitosa.
    - Verificar que la información contenida en el Sistema de Verificación se almacene de manera momentánea, de tal forma que sólo cumpla con su objetivo de comparar el dato correspondiente.
    - Contar con evidencia documental de que se actualizan los datos conforme al periodo señalado (diariamente) y que se eliminan aquéllos que recibe el INE.

3. Respecto de la base de datos del Sistema Integral de Información del Registro Federal de Electores, de conformidad con lo previsto en los artículos 54, 127, 138, 144 y 154 de la LGIPE:

    - Tomar las medidas necesarias a efecto de que la actualización de la información del SIIRFE se lleve a cabo de manera expedita.
    - Adoptar las medidas necesarias para garantizar que se sustituyan, rectifiquen o completen, de oficio, los datos personales que fueren inexactos o incompletos en el momento en que tengan conocimiento de esta situación. Lo anterior atendiendo a los procedimientos que el INE tiene establecidos para dichas actividades

según lo dispuesto por la LGIPE, y en observancia de lo señalado en el artículo 20, fracciones IV y V de la LFTAIPG.

- Contar con evidencia documental de la actualización que se realiza a la base de datos del SIIRFE, así como de la sustitución, rectificación o complementación de los datos personales que el INE, en su caso, lleva a cabo de oficio.
- Verificar que, efectivamente, las instituciones tanto públicas como privadas, a las que preste el Servicio de Verificación, apoyen en la difusión y promoción de los programas que el INE dirige a la ciudadanía relacionados con la actualización de la Credencial para Votar.

7. Deber de seguridad

Las recomendaciones y observaciones del INAI se realizaron a partir de lo informado por el INE. El análisis no incluyó pruebas de penetración, auditorías, ni peritajes a los sistemas del INE, por lo que las manifestaciones del INAI se limitan a realizar recomendaciones y observaciones sobre el sistema de gestión para la seguridad de los datos personales.

Recomendaciones y observaciones del INAI con relación al deber de seguridad:

1. Señalar el objetivo general y los objetivos particulares del Servicio de Verificación, así como delimitar el ámbito de aplicación relacionado con el flujo de los datos personales.

2. Que en el alcance del Servicio de Verificación el INE establezca como regla sólo prestar el servicio a aquellas instituciones que estén reguladas en el tratamiento de datos personales que efectúen, y sólo en los casos en las que las finalidades para las cuales se aplicará el Servicio de Verificación sean lícitas y correspondan a sus atribuciones u objetivos establecidos en los documentos que regulen su actuación.

3. Considerar la obligación de cumplir con la normatividad en protección de datos personales por parte de todos los involucrados en el tratamiento, al momento de establecer las políticas del Servicio de Verificación.

4. Añadir las políticas sugeridas por este Instituto a los convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas que se establezcan en el futuro, para el Servicio de Verificación.

5. Dar claridad a los textos de las cláusulas contractuales, declaratorias de confidencialidad y cartas de confidencialidad que hacen referencia a ciertas obligaciones en materia de protección de datos personales de las partes, considerando la naturaleza que pueden tener las instituciones y los tratamientos de datos personales que se realizarán por parte del INE y de las instituciones públicas y privadas.

6. Incluir como política del INE la suspensión del Servicio de Verificación en los casos en que el INE tenga conocimiento que la institución no está tratando debidamente los datos personales.

7. Asegurar que todo el personal tenga claros sus roles, responsabilidades y contribución para el logro de los objetivos del Servicio de Verificación.

8. Realizar un análisis de riesgo al Servicio de Verificación, para evaluar las medidas de seguridad que ya existen contra las que sería conveniente tener para proteger los datos personales.
9. Incluir una cláusula similar a la de la sección III de los compromisos de las “Partes”, cláusula Quinta, inciso j, del convenio con instituciones privadas, en los convenios que firme con las instituciones públicas.

10. Considerar dentro de los requerimientos del Anexo Técnico de los convenios de apoyo y colaboración para instituciones privadas y para instituciones públicas, un plan de trabajo para la implementación de medidas de seguridad alineadas a las políticas, objetivos, procesos y procedimientos del Servicio de Verificación.

11. Contar con indicadores de medición para los controles o mecanismos, que permitan tener una visión general de la imagen del riesgo para proteger los datos personales.

12. Mantener y documentar un plan de contingencia sobre el Servicio de Verificación, así como identificar la cadena de rendición de cuentas para informar y actuar ante un incidente de seguridad.

13. Documentar las revisiones, auditorías y los tratamientos de una vulneración a la seguridad del Servicio de Verificación.

14. Realizar las revisiones para promover mejoras en los sistemas se realicen al menos una vez al año, o bien cuando se identifique un cambio significativo en el contexto del sistema.

15. Realizar el ejercicio de "usuario simulado" para verificar que las instituciones están cumpliendo con sus obligaciones respecto de la operación del Servicio de Verificación.

16. Diseñar e impartir un programa de capacitación continua, y de manera particular un módulo sobre seguridad de los datos personales para todos los involucrados en el Servicio de Verificación.

17. Generar evidencias de cualquier capacitación impartida al personal.

Con relación a la arquitectura general de la solución del Portal de Verificación en la red del INE, se recomienda lo siguiente:

18. Garantizar que el enlace sea punto a punto, es decir, que se realice exclusivamente entre las instalaciones de las instituciones públicas o privadas y el INE, evitando siempre conexiones inalámbricas. Así como prescindir de conexiones remotas o trabajo desde casa (*home office*).

19. Garantizar que los certificados SSL (*Secure Socket Layer*) tramitados por el INE se mantengan vigentes y actualizados.

20. Realizar pruebas de penetración al Servidor de Punto de Acceso, Servidor de Comparación, Servidor de Administración y al Servidor de Base de Datos que componen el Servicio de Verificación.

21. Aplicar segregación y aislamiento en los privilegios de acceso de los usuarios a los servidores que componen el Sistema de Verificación, en particular, revisar la existencia de conexiones entre el Servidor de Administración y otros sistemas como el SIIRFE.

22. Verificar que la infraestructura de comunicaciones, seguridad y la del Portal de Verificación cuenten siempre con las últimas actualizaciones de software, firmware o hardware.

8. Deber de confidencialidad

El INE cuenta con suficiente normatividad que regula la confidencialidad de los datos personales que obran en el Padrón Electoral. No obstante, para que la confidencialidad se garantice es necesaria la implementación de medidas de seguridad para la protección de datos personales, de acuerdo con lo analizado en el deber de seguridad.

Recomendaciones y observaciones del INAI con relación al deber de confidencialidad:

1. Generar evidencia de la capacitación que sea impartida al personal de la DERFE –y al personal del INE adscrito a cualquier otra área o posibles encargados que pudieran estar involucrados eventualmente en la operación del Servicio de Verificación - en el marco del *Programa de Concientización en Materia de Seguridad dentro de la DERFE* o de cualquier otra capacitación impartida, tales como el programa de dicha capacitación, la calendarización correspondiente, listas de asistencia y evaluaciones realizadas. Lo anterior, previo a la puesta en operación del Servicio de Verificación y de manera continuada a partir de su puesta en operación.

2. Asimismo, se recomienda solicitar al INAI capacitación en materia de protección de datos personales, previo a la puesta en operación del Servicio de Verificación y de manera continuada a partir de su puesta en operación.

3. En relación con la *Declaratoria de confidencialidad y aceptación de las condiciones generales del mecanismo de pruebas en relación al Servicio de Verificación de datos de la Credencial para Votar,* se recomienda al INE redactar claramente dicha cláusula respecto a los siguientes puntos: i) que, en relación con el mecanismo de pruebas, el INE no proporcionará a la Institución ningún dato personal en posesión de INE y ii) que las Instituciones públicas y privadas están obligadas a guardar la confidencialidad de los datos personales tratados en el contexto del mecanismo de pruebas vinculadas al Servicio de Verificación, con fundamento en la LFTAIPG y la LFPDPPP, respectivamente, así como con fundamento en cualquier otra normativa aplicable. Lo anterior, considerando que también podría haber normativa local en materia de protección de datos personales, aplicable a instituciones públicas locales.

4. En relación con el Sistema de Gestión de Seguridad referido por el INE, se recomienda documentar y generar evidencia de las medidas adoptadas en el marco de dicho sistema, para garantizar la confidencialidad de los datos personales tratados para la prestación del Servicio de Verificación.

5. En relación con las verificaciones o supervisiones previstas y realizadas en el marco del Sistema de Gestión de las Tecnologías de la Información señalado por el INE, así como por el Comité Técnico previsto en la cláusula octava del Convenio de apoyo y colaboración entre “EL INE” y “LA INSTITUCIÓN”, sobre el cumplimiento de las obligaciones en materia de protección de datos personales, se recomienda documentar y generar evidencia de las verificaciones o supervisiones previstas y realizadas.

6. Con objeto de no difundir información confidencial en términos de lo dispuesto por el artículo 18, fracción II, y 21 de la LFTAIPG, así como las disposiciones en materia de confidencialidad de la LGIPE, el INE tendrá que limitarse a dar información genérica sobre la coincidencia o no de los datos proporcionados por la institución para la realización del cotejo correspondiente y el porcentaje de similitud de la huella digital, y evitar proporcionar información adicional sobre las causas de la falta de vigencia de la credencial para votar, así como datos personales. En ese sentido, se recomienda no implementar respuestas complementarias, tales como las identificadas con número de ID 1 a 18, salvo lo relativo al robo o extravío de la Credencial para Votar.

En los casos que la respuesta del INE indicara que una credencial presentada por un titular a la institución no es vigente, la institución podría orientar al particular para que consulte con el INE el detalle personal de la causa de no vigencia de su credencial para votar y, en su caso, realice las aclaraciones y rectificaciones necesarias.

9. Transferencias

Las instituciones públicas y privadas que transfieren datos personales al INE para su cotejo, requieren cumplir con la normativa que les aplique en materia de protección de datos personales y esta situación debe estar prevista claramente en el convenio del servicio que prestará el INE. Si bien no es intención del INE transferir datos personales, se detectó cierta información no necesaria que el INE está considerando proporcionar en el marco de este servicio.

Recomendaciones y observaciones del INAI con relación a las transferencias de datos personales:

1. Prever explícitamente en los convenios de apoyo y colaboración para instituciones privadas que la institución incluya en su aviso de privacidad la transferencia de datos personales que realiza al INE en el marco del Servicio de Verificación, de conformidad con lo previsto en el artículo 16, fracción V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

2. Establecer en los convenios que se firmen con instituciones públicas y privadas, las consecuencias de no cumplir con sus obligaciones en materia de transferencias de datos personales, como podría ser que los titulares acudan ente el INAI a interponer una queja.

3. Valorar la conveniencia de que las instituciones públicas y privadas puedan solicitar el consentimiento para el tratamiento de sus datos personales en el Servicio de Verificación por un medio distinto al aviso de privacidad, ya que de otra forma estarían obligadas a entregar a cada uno de los titulares una copia del aviso de privacidad.

4. Prever explícitamente en los convenios de apoyo y colaboración para instituciones privadas, la obligación del INE y de la institución, de generar evidencia que permita acreditar transferencias de datos personales de la institución al INE, en cumplimiento a las obligaciones que prevé la LFPDPPP para las transferencias, incluyendo: i) si dichas transferencias son informadas por la institución a los titulares; ii) si el tratamiento de los datos personales para el Servicio de Verificación fue consentido y, en ese sentido, la transferencia de datos personales de la institución al INE, y ii) la entrega de los avisos de privacidad de las instituciones privadas al INE.

5. Prever explícitamente en los convenios de apoyo y colaboración para instituciones públicas federales, la obligación de éstas de requerir el consentimiento de los titulares para la transferencia de datos personales al INE cuando no se actualice alguno de los supuestos previstos en el artículo 22 de la LFTAIPG, y establecer mecanismos para que el INE pueda verificar que en esos casos se solicitó el consentimiento, el cual debe constar de manera expresa y por escrito.

6. Incluir en los convenios con instituciones públicas que éstas sólo podrán hacer uso del Servicio de Verificación y tratar datos personales en el mismo, cuando dicho tratamiento obedezca al ejercicio de sus atribuciones, así como la obligación de informar sobre las transferencias al INE en el sistema de datos que corresponda, si ello se prevé en la normatividad que resulte aplicable.

7. Incluir en la Cláusula sexta, inciso c), de los convenios, la referencia a “demás normativa aplicable”, en virtud de que es distinta la normativa que aplica a una institución privada, a una institución pública federal y a una institución pública local.

8. Revisar la normatividad sobre protección de datos personales que apliquen en lo particular a la institución pública local con la que se vaya a firmar convenio, para considerar en éste las cláusulas que sean necesarias.

9. Limitar la transferencia de datos por parte del INE a información genérica sobre la coincidencia o no de los datos proporcionados por la institución para la realización del cotejo correspondiente y el porcentaje de similitud de la huella digital, y evite proporcionar información adicional sobre las causas de la falta de vigencia de la credencial para

votar, así como datos personales, al momento de dar respuesta sobre el cotejo de la información. En ese sentido, se recomienda no implementar respuestas complementarias para el Servicio de Verificación, tales como las identificadas con número de ID 1 a 18 referidas en la respuesta proporcionada por el INE, con excepción de lo relativo al robo o extravío de las credenciales. Lo anterior con objeto de no difundir información confidencial en términos de lo dispuesto por los artículos 18, fracción II, y 21 de la LFTAIPG.

10. Derechos ARCO

El INE tiene previstos procesos para que los titulares ejerzan sus derechos ARCO, en lo que refiere al Padrón Electoral, de donde se obtiene la información necesaria para operar el Servicio de Verificación. Asimismo, los Lineamiento ARCO prevén distintos recursos que pueden ser interpuestos por un titular no satisfecho con el resultado del ejercicio de sus derechos ARCO.

Recomendaciones y observaciones del INAI con relación a los derechos ARCO:

1. Actualizar los Lineamientos ARCO, en virtud de lo que los mismos fueron emitidos en el 2012 y hacen remisiones a normativa derogada o abrogada, y

2. Prever e informar al titular, mediante la leyenda de información o documento análogo, que los procedimientos para el ejercicio de derechos ARCO aplicables a los datos personales contenidos en el Padrón Electoral, así como los recursos correspondientes, aplican a los datos personales tratados en el marco del Servicio de Verificación.

3. De conformidad con las buenas prácticas, nombrar un oficial para la protección de los datos personales, que tenga entre sus funciones, entre otras:
- Asesorar al interior del INE respecto a los asuntos en materia de protección de datos personales.
- Coordinar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de las obligaciones en la materia.
- Coordinar las acciones de capacitación en materia de protección de datos personales

No se omite señalar que el análisis y recomendaciones antes realizadas se centraron en identificar que en el Servicio de Verificación se contemplaran mecanismos para el ejercicio de derechos ARCO por parte de los titulares.

No se omite manifestar que las consideraciones de la presente opinión tienen como propósito brindar una orientación desde el punto de vista estrictamente técnico, y no prejuzga sobre las determinaciones que en su caso el Pleno del INAI pudiera adoptar al respecto en ejercicio de las facultades que le han sido otorgadas.

Anexo 3.

Convenio de apoyo y colaboración para instituciones privadas del INE.

CONACYT
Consejo Nacional de Ciencia y Tecnología

INFOTEC

CONVENIO DE APOYO Y COLABORACIÓN, QUE CELEBRAN POR UNA PARTE, EL INSTITUTO FEDERAL ELECTORAL, EN LO SUCESIVO "EL I.F.E.", REPRESENTADO EN ESTE ACTO POR EL LICENCIADO EDMUNDO JACOBO MOLINA, SECRETARIO EJECUTIVO, ASISTIDO POR EL ING. RENE MIRANDA JAIMES, ENCARGADO DE DESPACHO DE LA DIRECCIÓN EJECUTIVA DEL REGISTRO FEDERAL DE ELECTORES; POR LA OTRA, "_____", , EN LO SUCESIVO "_____", REPRESENTADO POR _____, EN SU CARÁCTER DE APODERADOS LEGALES, AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

D E C L A R A C I O N E S

I. DE "EL I.F.E.":

I.1. Que de conformidad con los artículos 41, párrafo segundo, base V, párrafos primero y segundo de la Constitución Política de los Estados Unidos Mexicanos y 104, 105, párrafo 2 y 106, párrafo 1 del Código Federal de Instituciones y Procedimientos Electorales, es un organismo público autónomo, de carácter permanente, independiente en sus decisiones y funcionamiento, con personalidad jurídica y patrimonio propios, depositario de la autoridad electoral y responsable del ejercicio de la función estatal de organizar las elecciones federales para renovar a los integrantes de los poderes Ejecutivo y Legislativo de la Unión. Dicha función estatal se rige por los principios de certeza, legalidad, independencia, imparcialidad y objetividad.

I.2. Que en términos del artículo 105, párrafo 1, incisos a), c), d) y f) del Código Federal de Instituciones y Procedimientos Electorales, tiene entre sus fines contribuir al desarrollo de la vida democrática; integrar el Registro Federal de Electores; asegurar a los ciudadanos el ejercicio de sus derechos político-electorales y vigilar el cumplimiento de sus obligaciones, velar por la autenticidad y efectividad del sufragio, llevar a cabo la promoción del voto y coadyuvar a la difusión de la educación cívica y la cultura democrática.

I.3. Que con la finalidad de contar con servicios de información confiable, **"EL I.F.E."** a través de la Dirección Ejecutiva del Registro Federal de Electores, en adelante **"LA D.E.R.F.E."** definió entre otras Estrategias Institucionales, la de Intensificación de Vínculos con la Sociedad, a la que se definieron líneas de acción, como la correspondiente a Servicios Agregados del Padrón Electoral.

I.4. Que como parte de las actividades de la línea de acción de Servicios Agregados del Padrón Electoral, **"EL I.F.E."** a través de **"LA D.E.R.F.E."** plantea la definición del Proyecto de Servicios de Valor Agregado para los Organismos Públicos y/o Privados, que contribuirá con la generación de servicios a partir de los productos y servicios electorales que den un valor agregado a los organismos públicos y/o privados y que de esta forma coadyuven con la estrategia de Intensificación de Vínculos con la Sociedad.

I.5. Que considera que a través del uso de tecnologías de aplicación específica se promueva la interacción con organismos públicos y/o privados que contribuyan a proporcionar servicios de valor agregado para el ciudadano y la sociedad en general.

I.6. Que como parte de esta Estrategia se instrumentan acciones para establecer un vínculo con el ciudadano mediante la suscripción de convenios con organismos públicos y/o privados que contribuyan y promuevan a consolidar a la Credencial para Votar como medio de identificación para realizar trámites, lo que se constituye como un servicio de verificación de los datos de la Credencial para Votar y de esta manera contribuir a fortalecerla como medio de identificación.

I.7. Que a través de **"LA D.E.R.F.E."** realiza campañas de actualización al Padrón Electoral, con el objeto de convocar y orientar a la ciudadanía a cumplir con su deber cívico de incorporarse o actualizar sus datos, según lo establecen los artículos 182, párrafos 1 y 4 y 183, párrafo 1 del Código Federal de Instituciones y Procedimientos Electorales.

I.8. Que además de la facultad señalada en el punto que antecede, **"LA D.E.R.F.E."** tiene como atribuciones la de expedir la Credencial para Votar, mantener actualizada la cartografía electoral del país, clasificada por entidad, distrito electoral federal, municipio y sección electoral, así como elaborar las Listas Nominales de Electores con el nombre de las personas incluidas en el Padrón Electoral, a quienes se ha expedido y entregado su Credencial para Votar, agrupadas por distrito y sección electoral, de acuerdo con lo dispuesto en los artículos 128, párrafo 1, incisos e) y j) y 197, párrafo 1 del Código Federal de Instituciones y Procedimientos Electorales.

I.9. Que al ser **"EL I.F.E.",** la institución que expide la credencial para votar, resulta procedente que informe si el instrumento con el que los ciudadanos pretenden identificarse, coincide con el expedido por **"EL I.F.E."** y sin que ello signifique, transgredir lo dispuesto por el artículo 171, párrafo 3 del código de la materia.

I.10. Que en términos de lo establecido en el numeral 45, párrafo segundo de los Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores, aprobados por el Consejo General de **"EL I.F.E."** el 21 de noviembre de 2012, los Convenios que **"EL I.F.E."** celebre con instancias privadas deberán establecer que los avisos de privacidad que éstas hubiesen elaborado de conformidad con la Ley de Protección de Datos Personales en Posesión de Particulares, incluyan como una posibilidad de tratamiento de datos personales la validación y verificación que soliciten dichas instancias.

I.11. Que de conformidad con lo establecido en numeral 52 de los Lineamientos citados, las instancias públicas y privadas, podrán solicitar por escrito o ante las oficinas de **"LA D.E.R.F.E."** y las Vocalías respectivas o , señalando los datos de la Credencial para Votar a verificar, o en su caso, copia de la misma adjuntando autorización expresa de las y los ciudadanos de la credencial para realizar la verificación.

I.12. Que el Secretario Ejecutivo de **"EL I.F.E."**, Licenciado Edmundo Jacobo Molina, tiene la facultad de representarlo legalmente, en términos de lo dispuesto por el artículo 125, párrafo 1, inciso a) del Código Federal de Instituciones y Procedimientos Electorales.

I.13. Que señala como su domicilio para los efectos del presente instrumento, el ubicado en Viaducto Tlalpan número 100, Colonia Arenal Tepepan, Código Postal 14610, Delegación Tlalpan, México, Distrito Federal.

II. DE "_____":

II.1. Es una sociedad anónima debidamente constituida de conformidad con la legislación mexicana, y cuenta con facultades suficientes y necesarias para la celebración y cumplimiento del presente Convenio.

II.2. Mediante Escritura Pública Número 93,021 de fecha 10 de Julio de 2008, otorgada ante la fe del Licenciado Carlos de Pablo Serna, Notario Público Número 137 del Distrito Federal e inscrita en el Registro Público del Distrito Federal, bajo el Folio Mercantil Número 64010 el 05 de Agosto de 2008, se hizo constar la reforma integral de sus estatutos sociales.

II.3. Señala como su domicilio para todos los efectos del presente Convenio, el ubicado en Avenida Universidad Número 1200, Colonia Xoco, Delegación Benito Juárez, Código Postal 03339, México, Distrito Federal.

II.4. Sus apoderados _____ cuentan con las facultades necesarias y suficientes para obligar a su representada en los términos del presente Convenio, de conformidad con las Escritura Públicas_____, las cuales hasta la fecha no les han sido revocadas o modificadas en forma alguna.

II.5. Es su deseo celebrar el presente convenio con "EL I.F.E." a efecto de verificar los datos de las credenciales para votar que presenten sus clientes contenga los datos registrados por el "EL I.F.E."

III. DE "LAS PARTES":

III.1. Que se reconocen en forma recíproca la personalidad con que se ostentan y comparecen a la suscripción de este Convenio.

III.2. Que están en la mejor disposición de apoyarse para cumplir cabalmente con el objeto del presente instrumento jurídico.

En atención a las declaraciones que anteceden, **"EL I.F.E."** y **"_____"**, en lo sucesivo **"LAS PARTES"** suscriben el presente instrumento, de conformidad con las siguientes:

C L Á U S U L A S

DE SU OBJETO

PRIMERA.- El objeto del presente Convenio consiste en establecer los mecanismos de apoyo y colaboración por los que **"EL I.F.E."** a través de **"LA D.E.R.F.E."**, bajo mecanismos de seguridad, verificará que la credencial para votar que los ciudadanos exhiban ante **"_____"** para la realización de los trámites ante esa institución en territorio nacional, coincida con la que fue generada por el

Instituto, en términos de lo dispuesto en el Anexo Técnico del presente Convenio. En el caso de la huella digital, **"EL I.F.E."** confirmará si corresponde con la plasmada en la credencial para votar. (**Este último caso se realizará si la otra parte cuenta con la infraestructura tecnológica).**

En ningún caso y por ningún motivo, **"EL I.F.E."** proporcionará a **"_____"**, información confidencial de los ciudadanos, acceso a la información, bases de datos o sistemas internos del Instituto en términos de lo dispuesto por el artículo 171, párrafo 3 del Código Federal de Instituciones y Procedimientos Electorales.

En ningún caso, el servicio objeto de este convenio podrá ser compartido por **"_____"** a personas físicas o morales nacionales o extranjeras, en caso contrario, **"EL I.F.E."** dará por terminado de manera inmediata el presente convenio sin necesidad de sujetarse a los plazos estipulados en la CLÁUSULA DÉCIMA SEXTA del presente instrumento jurídico..

LIMITANTES DE LA INFORMACIÓN

SEGUNDA.- "LAS PARTES" convienen que el uso y destino de la información objeto del presente convenio, queda restringido exclusivamente al cumplimiento de éste.

TERCERA.- La autorización para validar la Credencial para Votar a que se refiere el objeto del presente convenio, deberá circunscribirse exclusivamente a la verificación de los datos en la misma. No es responsabilidad de la autoridad electoral federal, ni queda comprendida dentro de la colaboración el determinar respecto de la autenticidad de la Credencial para Votar.

DE LOS COMPROMISOS DE "LAS PARTES"

CUARTA.- Las obligaciones de **"EL I.F.E."**, son las siguientes:

a) **"EL I.F.E."**, a través de **"LA D.E.R.F.E."**, proporcionará al personal que determine **"_____"** la capacitación necesaria que le permita operar satisfactoriamente la información establecida en el Anexo Técnico.

b) Proporcionar a **"_____"**, las características técnicas de la Credencial para Votar que **"EL I.F.E."** ha expedido a los ciudadanos, así como sus modificaciones.

c) **"EL I.F.E."** será responsable de la operación y administración de la Infraestructura Tecnológica para la verificación de los datos de la Credencial para Votar que proporcione **"_____"**.

QUINTA.- Las obligaciones de **"_____"**, son las siguientes:

a) No transmitir ni comercializar, bajo ningún tipo ni modalidad, el uso, posesión o propiedad de la información que **"EL I.F.E."** le proporcionará derivado de la verificación de la credencial para votar

b) Apoyar a **"EL I.F.E."** en la difusión y promoción de los programas que dirige a la ciudadanía, así como para los efectos del presente convenio.

c) Proporcionar a **"EL I.F.E."** los recursos y/o insumos que se requieran para el cumplimiento del objeto y obligaciones pactadas en el presente instrumento legal, su Anexo Técnico y en su caso el Anexo Económico Administrativo.

d) Establecer en los avisos de privacidad que se elaboren de conformidad con la Ley de Protección de Datos Personales en Posesión de Particulares, la posibilidad de validación y verificación de los datos personales que los ciudadanos proporcionen a **"_____"**.

SEXTA.- Las obligaciones de ambas partes son las siguientes:

a) Guardar estricta confidencialidad respecto de la información que se proporcione entre **"LAS PARTES"**.

b) Proporcionarse la información necesaria para el debido cumplimiento del objeto de este acuerdo de voluntades.

d) Proteger los datos personales de los ciudadanos conforme a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, el Código Federal de Instituciones y Procedimientos Electorales, el Reglamento del Instituto Federal Electoral en Materia de Transparencia y Acceso a la Información Pública y los Lineamientos para Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores en el ámbito de competencia de cada una de estas instituciones.

SÉPTIMA.- Los trabajos y aplicaciones que desarrolle **"_____"**, para el objeto de este Convenio serán propiedad intelectual de **"_____"** y tendrá la responsabilidad de administrarlos.

Los trabajos y aplicaciones que desarrolle **"EL I.F.E."**, para el objeto de este Convenio serán propiedad intelectual de **"EL I.F.E."** y tendrá la responsabilidad de administrarlos.

DEL COMITÉ TÉCNICO

OCTAVA.- Para el adecuado desarrollo de las actividades que se generarán con motivo del cumplimiento del objeto de este convenio, **"LAS PARTES"** están de acuerdo en integrar un comité técnico, mismo que estará formado por un representante de cada institución, quienes podrán ser sustituidos en cualquier tiempo previa notificación por escrito y con ___ días de anticipación a la otra parte, el cual estará integrado de la siguiente manera:

Por **"EL I.F.E."**, el titular de la Dirección Ejecutiva del Registro Federal de Electores.

Por **"_____"**, el _____.

NOVENA.- El Comité Técnico referido en la cláusula anterior, tendrá las siguientes atribuciones:

a) Determinar y apoyar las acciones a ejecutar con el fin de dar cumplimiento al objeto del presente Convenio y su Anexo Técnico.

b) Coordinar la realización de actividades señaladas en el Anexo Técnico que forma parte del presente instrumento jurídico.

c) Las demás que acuerden **"LAS PARTES"**.

DE LA CONFIDENCIALIDAD

DÉCIMA.- "LAS PARTES" se comprometen a guardar estricta confidencialidad respecto de los trámites y la información que con motivo del cumplimiento del objeto del presente convenio realice o genere cada institución.

DE LA RELACIÓN LABORAL

DÉCIMA PRIMERA.- El personal designado por cada institución para la realización del objeto materia del presente instrumento jurídico se entenderá relacionado exclusivamente con aquella que lo empleó, por ende, cada una de **"LAS PARTES"** asumirá su responsabilidad por este concepto y en ningún caso será considerada como patrón solidario y/o sustituto.

DE LA RESPONSABILIDAD CIVIL

DÉCIMA SEGUNDA.- Queda expresamente pactado que **"LAS PARTES"** no tendrán responsabilidad civil por los daños y perjuicios que pudieran causarse como consecuencia del caso fortuito o fuerza mayor, en la inteligencia de que una vez superados los eventos se reanudarán las actividades suspendidas en la forma y términos que se determinen los signantes en el Anexo Técnico.

DE LAS MODIFICACIONES

DÉCIMA TERCERA.- El presente instrumento podrá ser modificado o adicionado por escrito por voluntad de **"LAS PARTES"**, quienes se obligarán a cumplir tales

modificaciones a partir de la fecha de su suscripción, en el entendido de que éstas tendrán como única finalidad perfeccionar y coadyuvar en el cumplimiento de su objeto.

DÉCIMA CUARTA.- "LAS PARTES" convienen en gestionar ante sus órganos de dirección, la adopción de los acuerdos necesarios para la adecuada ejecución de las acciones derivadas de la firma del presente Convenio.

DE LA INTERPRETACIÓN

DÉCIMA QUINTA.- "LAS PARTES" manifiestan su conformidad en que el presente Convenio es producto de la buena fe, por lo que todo conflicto que resulte del mismo, en cuanto a su interpretación, aplicación y cumplimiento, así como los casos no previstos en la ley, serán resueltos de común acuerdo.

En caso de subsistir dicho conflicto, **"LAS PARTES"** se someterán a la jurisdicción y competencia de los tribunales federales competentes con sede en el Distrito Federal, renunciando a cualquier otro fuero que pudiera corresponderles por razón de su domicilio presente o futuro o por cualquiera otra causa.

DE LA VIGENCIA

DÉCIMA SEXTA.- El presente Convenio tendrá una vigencia de cinco años. Una vez concluida la vigencia y de no existir una manifestación de **"LAS PARTES"** en sentido contrario, se entenderá renovada por un año más.

Para dar por terminado el presente Convenio será necesario que una de las partes lo notifique por escrito con una anticipación de cuando menos treinta días hábiles y se seguirán los protocolos que se establecen en el Anexo Técnico.

Leído que fue por **"LAS PARTES"** y aceptado en su contenido y alcance legal, se firma el presente acuerdo de voluntades por cuadruplicado en la Ciudad de México, Distrito Federal el día __ de _____ de 2014.

Por “EL I.F.E.”	Por “_____”
El Secretario Ejecutivo	_____
_____	_____
Licenciado Edmundo Jacobo Molina	
Encargado de Despecho de la Dirección Ejecutiva del Registro Federal de Electores	_____
_____	_____
Ing. Rene Miranda Jaimes	_____

TESTIGOS

Por “_____”	Por “_____”
	_____
_____	

Las firmas contenidas en la presente foja, forman parte del Convenio de Apoyo y Colaboración, celebrado entre el Instituto Federal Electoral y el **“_____”**, el __ de ____ de 2014, documento que consta de 10 fojas útiles con texto únicamente en el anverso.

Anexo 4.

Aviso de Privacidad de BBVA Bancomer

ANEXO 4

Aviso de Privacidad de Bancomer vigente al 21 de diciembre de 2015
Fuente: https://www.bancomer.com/personas/aviso-privacidad.jsp

El Banco **BBVA Bancomer, Sociedad Anónima, Institución de Banca Múltiple, Grupo Financiero BBVA Bancomer**, está comprometido con la protección de sus datos personales, al ser responsable de su uso, manejo y confidencialidad, y al respecto le informa lo siguiente:

¿Para qué fines utilizamos sus datos personales?

Los datos personales que recabamos de usted, que podrán ser sensibles, son necesarios para verificar, confirmar y validar su identidad; así como administrar y operar los servicios y productos que solicita o contrata con nosotros, para cumplir con las obligaciones contractuales derivadas de los mismos.

De manera adicional, utilizamos su información personal para comercializar nuestros productos y elaborar perfiles de clientes, para el ofrecimiento de productos y servicios bancarios y financieros. Si bien, estas finalidades no son necesarias para prestarle los servicios y productos que solicita o contrata con nosotros, las mismas nos permiten brindarle un mejor servicio y elevar su calidad. En caso de que no desee que sus datos personales sean tratados para estas finalidades secundarias, usted puede presentar desde este momento su solicitud en cualquier sucursal, manifestando lo anterior. Solicite el formato correspondiente a su ejecutivo en la sucursal.

La negativa para el uso de sus datos personales para estas finalidades secundarias, no será motivo para que le neguemos los servicios y productos que solicita o contrata con nosotros. En caso de que no manifieste su negativa, se entenderá que autoriza el uso de su información personal para dichos fines.

¿Qué datos personales utilizamos para los fines anteriores?

Para prestarle los servicios y productos bancarios o financieros que solicita o contrata con nosotros, requerimos datos de identificación, laborales, académicos, patrimoniales, financieros, en su caso, migratorios y relativos al historial crediticio, los cuales se obtienen a partir de los documentos requisitados por usted.

Asimismo, los datos personales que utilizamos para comercializar nuestros productos y elaborar los perfiles de clientes son los siguientes: identificación del

cliente, demográficos, historial de consumos y tipo de producto o servicio financiero contratado con la Institución.

¿Con quién compartimos sus datos personales?

De forma eventual, sus datos personales se comparten con las empresas pertenecientes al Grupo Financiero BBVA Bancomer, S.A. de C.V., para el ofrecimiento de sus servicios y productos, mismas que podrán contactarlo directamente o con empresas para venta de cartera o consultas con Sociedades de Información Crediticia.

Asimismo, BBVA Bancomer podrá comunicar sus datos personales al Instituto Nacional Electoral para cumplir con las finalidades antes descritas. También podrá comunicar los datos personales para atender requerimientos de autoridades reguladoras competentes, previstas en la Ley de Instituciones de Crédito y demás disposiciones aplicables a las Instituciones Financieras.

En cualquier caso, comunicaremos el presente aviso de privacidad a los receptores de sus datos personales, a fin de que respeten sus términos.

¿Cómo puede ejercer sus derechos ARCO?

Usted podrá acceder, rectificar, cancelar u oponerse al manejo de sus datos personales, presentando su solicitud en el formato correspondiente en cualquier sucursal de BBVA Bancomer. Los procedimientos y requisitos se pueden consultar en los medios siguientes: Línea Bancomer al **5226 2663** en el D.F. o al **01 800 226 2663** (interior de la República sin costo), a través de la página web www.bancomer.com o en cualquier sucursal de BBVA Bancomer.

¿Cómo puede revocar su consentimiento para el uso de sus datos personales?

Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales, presentando su solicitud en el formato correspondiente en cualquier sucursal de BBVA Bancomer.

Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna obligación legal necesitemos seguir tratando sus datos personales. Asimismo, usted deberá considerar que para ciertos fines, la revocación de su consentimiento implicará que no le podamos seguir prestando el servicio que nos solicitó, o la conclusión de su relación jurídica con nosotros.

Para mayor información sobre la protección de sus datos personales, puede contactar a nuestra Dirección de Protección de Datos Personales en el buzónprotecciondedatospersonales.mx@bbva.com.

Otros medios para limitar el uso y divulgación de sus datos personales

Si desea dejar de recibir publicidad o promociones de nuestros productos y servicios bancarios y financieros, puede solicitar su inscripción al Registro Público de Usuarios (REUS) de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF); o bien, solicitar su registro en el sistema de inhibición de publicidad a los ejecutivos de cualquiera de nuestras sucursales.

¿Cómo manejamos las Cookies y/o Web Beacons?

Le informamos que BBVA Bancomer en los productos y servicios que ofrece a través de Internet se utilizan mecanismos como son Cookies, Web Beacons y otras tecnologías a través de las cuales se recaban datos de manera automática y simultánea, como la dirección IP de origen, navegador utilizado, sistema operativo, momento en que se accedió a la página, siendo posible monitorear su comportamiento como usuario de los servicios de Internet.

Para lo anterior, BBVA Bancomer les informa a los titulares que en todo momento pueden deshabilitar el uso de estos mecanismos, de acuerdo a las instrucciones que cada empresa propietaria de los browsers (navegador o visor de Internet) tiene implementado para activar y desactivar las citadas Cookies y Web Beacons.

¿Cómo Tratamos los Datos Personales de Menores y de Personas con Capacidades Diferentes?

Se tratan a través del padre o tutor, previa acreditación legal, para la contratación de productos y/o servicios bancarios.

¿Cómo le informaremos sobre cambios al presente aviso de privacidad?

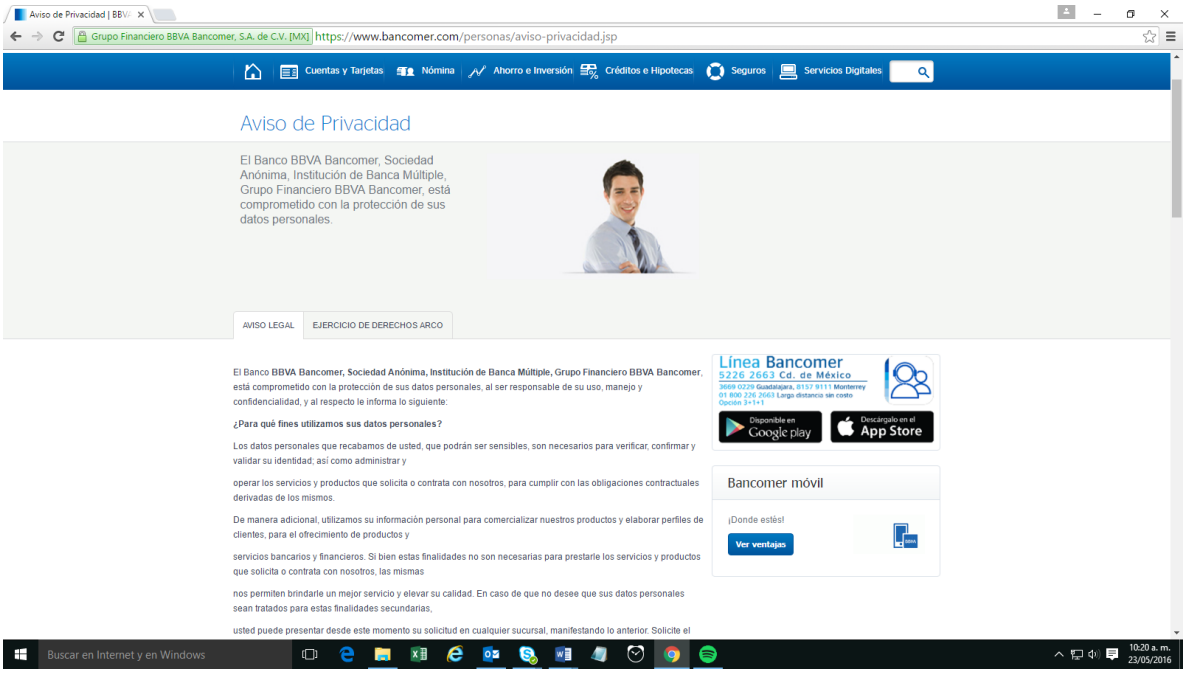
Los cambios y actualizaciones del presente aviso de privacidad se harán de su conocimiento en cualquiera de nuestras sucursales; en la red de cajeros automáticos disponibles de BBVA Bancomer; en nuestro portal financiero www.bancomer.com

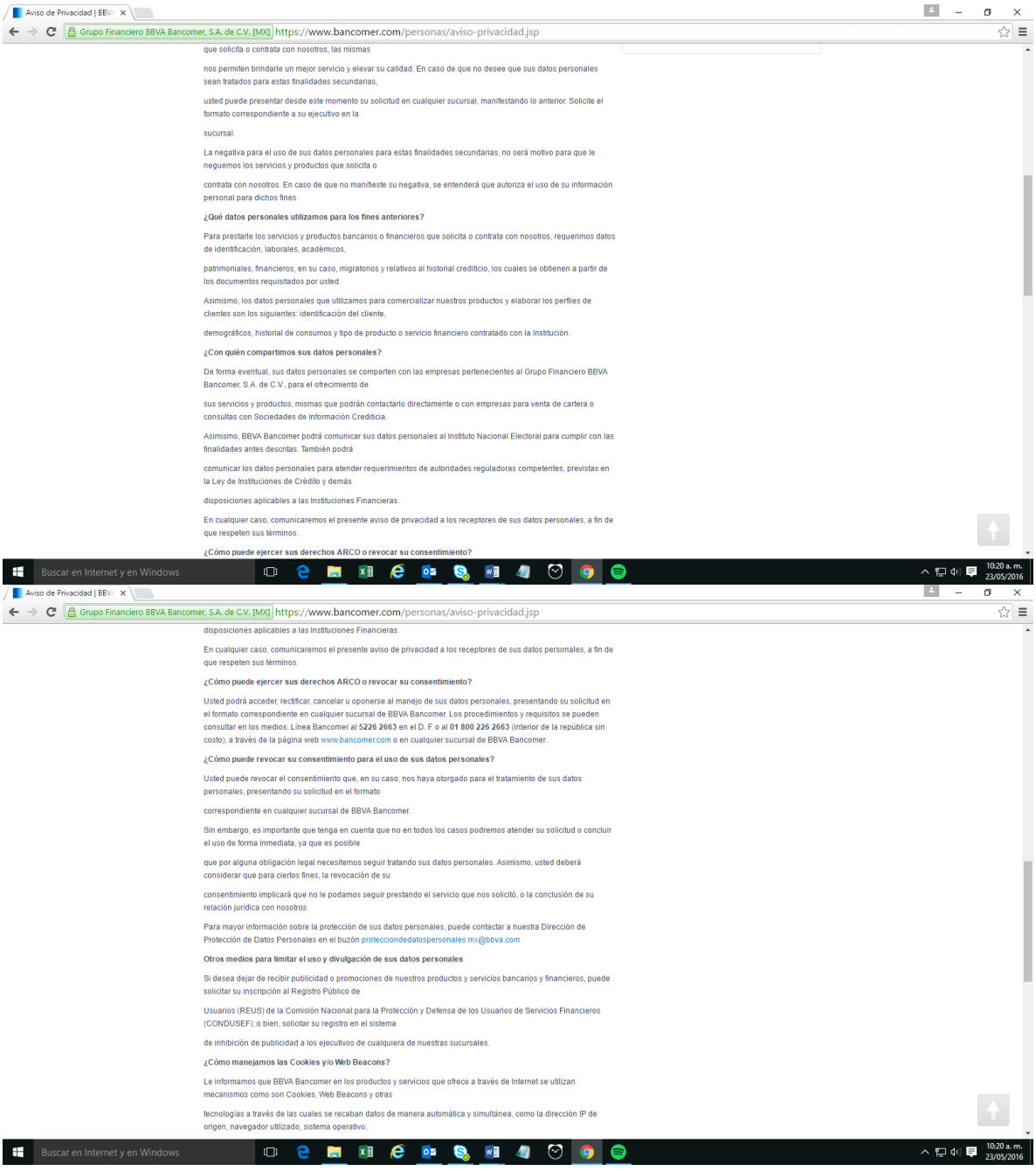
Si usted considera que su derecho de protección de datos personales ha sido vulnerado por alguna conducta de nuestros empleados o de nuestras actuaciones o respuestas, puede contactar a nuestra Dirección de Protección de Datos

Personales, en el buzón:protecciondedatospersonales.mx@bbva.com sin perjuicio de su derecho de acudir ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Para mayor información visite www.inai.org.mx

BBVA Bancomer, S.A.
Av. Paseo de la Reforma No. 510, Col Juárez
Del. Cuauhtémoc
C.P. 06600, México, D.F.
www.bancomer.com
Última actualización: julio, 2015.

Pantallas del aviso:




Aviso de Privacidad | BBV
Grupo Financiero BBVA Bancomer, S.A. de C.V. [MX]
https://www.bancomer.com/personas/aviso-privacidad.jsp
que solicita o contrata con nosotros, las mismas
nos permiten brindarle un mejor servicio y elevar su calidad. En caso de que no desee que sus datos personales sean tratados para estas finalidades secundarias,
usted puede presentar desde este momento su solicitud en cualquier sucursal, manifestando lo anterior. Solicite el formato correspondiente a su ejecutivo en la
sucursal.
La negativa para el uso de sus datos personales para estas finalidades secundarias, no será motivo para que le neguemos los servicios y productos que solicita o
contrata con nosotros. En caso de que no manifieste su negativa, se entenderá que autoriza el uso de su información personal para dichos fines
¿Qué datos personales utilizamos para los fines anteriores?
Para prestarle los servicios y productos bancarios o financieros que solicita o contrata con nosotros, requerimos datos de identificación, laborales, académicos,
patrimoniales, financieros, en su caso, migratorios y relativos al historial crediticio, los cuales se obtienen a partir de los documentos requisitados por usted.
Asimismo, los datos personales que utilizamos para comercializar nuestros productos y elaborar los perfiles de clientes son los siguientes: identificación del cliente,
demográficos, historial de consumos y tipo de producto o servicio financiero contratado con la Institución.
¿Con quién compartimos sus datos personales?
De forma eventual, sus datos personales se comparten con las empresas pertenecientes al Grupo Financiero BBVA Bancomer, S.A. de C.V., para el ofrecimiento de
sus servicios y productos, mismas que podrán contactarlo directamente o con empresas para venta de cartera o consultas con Sociedades de Información Crediticia.
Asimismo, BBVA Bancomer podrá comunicar sus datos personales al Instituto Nacional Electoral para cumplir con las finalidades antes descritas. También podrá
comunicar los datos personales para atender requerimientos de autoridades reguladoras competentes, previstas en la Ley de Instituciones de Crédito y demás
disposiciones aplicables a las Instituciones Financieras.
En cualquier caso, comunicaremos el presente aviso de privacidad a los receptores de sus datos personales, a fin de que respeten sus términos.
¿Cómo puede ejercer sus derechos ARCO o revocar su consentimiento?
Buscar en Internet y en Windows
10:20 a. m.
23/05/2016

Aviso de Privacidad | BBV
Grupo Financiero BBVA Bancomer, S.A. de C.V. [MX]
https://www.bancomer.com/personas/aviso-privacidad.jsp
disposiciones aplicables a las Instituciones Financieras.
En cualquier caso, comunicaremos el presente aviso de privacidad a los receptores de sus datos personales, a fin de que respeten sus términos.
¿Cómo puede ejercer sus derechos ARCO o revocar su consentimiento?
Usted podrá acceder, rectificar, cancelar u oponerse al manejo de sus datos personales, presentando su solicitud en el formato correspondiente en cualquier sucursal de BBVA Bancomer. Los procedimientos y requisitos se pueden consultar en los medios: Línea Bancomer al 5226 2663 en el D. F. o al 01 800 226 2663 (interior de la república sin costo), a través de la página web www.bancomer.com o en cualquier sucursal de BBVA Bancomer.
¿Cómo puede revocar su consentimiento para el uso de sus datos personales?
Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales, presentando su solicitud en el formato
correspondiente en cualquier sucursal de BBVA Bancomer.
Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible
que por alguna obligación legal necesitemos seguir tratando sus datos personales. Asimismo, usted deberá considerar que para ciertos fines, la revocación de su
consentimiento implicará que no le podamos seguir prestando el servicio que nos solicitó, o la conclusión de su relación jurídica con nosotros.
Para mayor información sobre la protección de sus datos personales, puede contactar a nuestra Dirección de Protección de Datos Personales en el buzón proteccióndedatospersonales.mx@bbva.com
Otros medios para limitar el uso y divulgación de sus datos personales
Si desea dejar de recibir publicidad o promociones de nuestros productos y servicios bancarios y financieros, puede solicitar su inscripción al Registro Público de
Usuarios (REUS) de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF); o bien, solicitar su registro en el sistema
de inhibición de publicidad a los ejecutivos de cualquiera de nuestras sucursales.
¿Cómo manejamos las Cookies y/o Web Beacons?
Le informamos que BBVA Bancomer en los productos y servicios que ofrece a través de Internet se utilizan mecanismos como son Cookies, Web Beacons y otras
tecnologías a través de las cuales se recaban datos de manera automática y simultánea, como la dirección IP de origen, navegador utilizado, sistema operativo,
Buscar en Internet y en Windows
10:20 a. m.
23/05/2016


Aviso de Privacidad | BBV
Grupo Financiero BBVA Bancomer, S.A. de C.V. [MX]
https://www.bancomer.com/personas/aviso-privacidad.jsp
Le informamos que BBVA Bancomer en los productos y servicios que ofrece a través de Internet se utilizan mecanismos como son Cookies, Web Beacons y otras
tecnologías a través de las cuales se recaban datos de manera automática y simultánea, como la dirección IP de origen, navegador utilizado, sistema operativo,
momento en que se accedió a la página, siendo posible monitorear su comportamiento como usuario de los servicios de Internet.
Para lo anterior, BBVA Bancomer les informa a los titulares que en todo momento pueden deshabilitar el uso de estos mecanismos, de acuerdo a las instrucciones
que cada empresa propietaria de los browsers (navegador o visor de Internet) tiene implementado para activar y desactivar las citadas Cookies y Web Beacons.
¿Cómo Tratamos los Datos Personales de Menores y de Personas con Capacidades Diferentes?
Se tratan a través del padre o tutor, previa acreditación legal, para la contratación de productos y/o servicios bancarios.
¿Cómo le informaremos sobre cambios al presente aviso de privacidad?
Los cambios y actualizaciones del presente aviso de privacidad se harán de su conocimiento en cualquiera de nuestras sucursales; en la red de cajeros automáticos disponibles de BBVA Bancomer; en nuestro portal financiero www.bancomer.com
Si usted considera que su derecho de protección de datos personales ha sido vulnerado por alguna conducta de nuestros empleados o de nuestras actuaciones o respuestas, puede contactar a nuestra Dirección de Protección de Datos Personales, en el buzón proteccióndedatospersonales.mx@bbva.com, sin perjuicio de su derecho de acudir ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Para mayor información visite www.inai.org.mx
BBVA Bancomer S.A.
Av. Paseo de la Reforma 510, Col. Juárez
Del. Cuauhtémoc
C.P. 06600. México, D.F.
www.bancomer.com
Última actualización: Julio, 2015.
CENTRO DE AYUDA
INFORMACIÓN CORPORATIVA
OTROS SITIOS BBVA
BBVA EN REDES SOCIALES
Buscar en Internet y en Windows
10:20 a. m.
23/05/2016

Anexo 5.

Propuesta de texto para el Aviso de Privacidad actual de Bancomer.

CONACYT
Consejo Nacional de Ciencia y Tecnología

INFOTEC

ANEXO 5
Aviso de Privacidad de Bancomer modificado para el "Proyecto".

El Banco **BBVA Bancomer, Sociedad Anónima, Institución de Banca Múltiple, Grupo Financiero BBVA Bancomer**, está comprometido con la protección de sus datos personales, al ser responsable de su uso, manejo y confidencialidad, y al respecto le informa lo siguiente:

¿Para qué fines utilizamos sus datos personales?

Los datos personales que recabamos de usted, que podrán ser sensibles, son necesarios para verificar, confirmar y validar su identidad; así como administrar y operar los servicios y productos que solicita o contrata con nosotros, para cumplir con las obligaciones contractuales derivadas de los mismos.

De manera adicional, utilizamos su información personal para comercializar nuestros productos y elaborar perfiles de clientes, para el ofrecimiento de productos y servicios bancarios y financieros. Si bien, estas finalidades no son necesarias para prestarle los servicios y productos que solicita o contrata con nosotros, las mismas nos permiten brindarle un mejor servicio y elevar su calidad. En caso de que no desee que sus datos personales sean tratados para estas finalidades secundarias, usted puede presentar desde este momento su solicitud en cualquier sucursal, manifestando lo anterior. Solicite el formato correspondiente a su ejecutivo en la sucursal.

La negativa para el uso de sus datos personales para estas finalidades secundarias, no será motivo para que le neguemos los servicios y productos que solicita o contrata con nosotros. En caso de que no manifieste su negativa, se entenderá que autoriza el uso de su información personal para dichos fines.

¿Qué datos personales utilizamos para los fines anteriores?

Para prestarle los servicios y productos bancarios o financieros que solicita o contrata con nosotros, requerimos datos de identificación, laborales, académicos, patrimoniales, financieros, en su caso, migratorios y relativos al historial crediticio, los cuales se obtienen a partir de los documentos requisitados por usted.

También podrán ser recabados los datos contenidos en la credencial para votar que usted proporcione a la institución como identificación, así como sus huellas dactilares para ser cotejados con la información con que cuenta el Instituto Nacional Electoral.

Comentado [a1]: Se propone este texto para cumplir cabalmente los principio de información y consentimiento como se señala en el trabajo, además de cumplir con las obligaciones contractuales en este sentido previstas en el modelo del Convenio de Apoyo y Colaboración entre el INE y las instituciones privadas (Anexo 3).

Asimismo, los datos personales que utilizamos para comercializar nuestros productos y elaborar los perfiles de clientes son los siguientes: identificación del cliente, demográficos, historial de consumos y tipo de producto o servicio financiero contratado con la Institución.

¿Con quién compartimos sus datos personales?

De forma eventual, sus datos personales se comparten con las empresas pertenecientes al Grupo Financiero BBVA Bancomer, S.A. de C.V., para el ofrecimiento de sus servicios y productos, mismas que podrán contactarlo directamente o con empresas para venta de cartera o consultas con Sociedades de Información Crediticia.

Asimismo, BBVA Bancomer podrá comunicar sus datos personales al Instituto Nacional Electoral para cumplir con las finalidades antes descritas. También podrá comunicar los datos personales para atender requerimientos de autoridades reguladoras competentes, previstas en la Ley de Instituciones de Crédito y demás disposiciones aplicables a las Instituciones Financieras.

Comentado [a2]: Este párrafo ya se encontraba en el aviso de privacidad de Bancomer al 21 de diciembre de 2015. Con este párrafo se da por cumplida la obligación de informar a los titulares de la transferencia de sus datos al Instituto Nacional Electoral (INE) para cotejo.

Asimismo, en virtud de que la transferencia de los datos al INE no requiere el consentimiento del titular como se señaló en el trabajo, no es necesario incluir un campo para recabar el consentimiento del titular respecto a dicha transferencia.

En cualquier caso, comunicaremos el presente aviso de privacidad a los receptores de sus datos personales, a fin de que respeten sus términos.

¿Cómo puede ejercer sus derechos ARCO?

Usted podrá acceder, rectificar, cancelar u oponerse al manejo de sus datos personales, presentando su solicitud en el formato correspondiente en cualquier sucursal de BBVA Bancomer. Los procedimientos y requisitos se pueden consultar en los medios siguientes: Línea Bancomer al **5226 2663** en el D.F. o al **01 800 226 2663** (interior de la República sin costo), a través de la página web www.bancomer.com o en cualquier sucursal de BBVA Bancomer.

¿Cómo puede revocar su consentimiento para el uso de sus datos personales?

Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales, presentando su solicitud en el formato correspondiente en cualquier sucursal de BBVA Bancomer.

Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna obligación legal necesitemos seguir tratando sus datos personales. Asimismo, usted deberá considerar que para ciertos fines, la revocación de su consentimiento implicará que no le podamos seguir prestando el servicio que nos solicitó, o la conclusión de su relación jurídica con nosotros.

Para mayor información sobre la protección de sus datos personales, puede contactar a nuestra Dirección de Protección de Datos Personales en el buzónprotecciondedatospersonales.mx@bbva.com.

Otros medios para limitar el uso y divulgación de sus datos personales
Si desea dejar de recibir publicidad o promociones de nuestros productos y servicios bancarios y financieros, puede solicitar su inscripción al Registro Público de Usuarios (REUS) de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF); o bien, solicitar su registro en el sistema de inhibición de publicidad a los ejecutivos de cualquiera de nuestras sucursales.

¿Cómo manejamos las Cookies y/o Web Beacons?
Le informamos que BBVA Bancomer en los productos y servicios que ofrece a través de Internet se utilizan mecanismos como son Cookies, Web Beacons y otras tecnologías a través de las cuales se recaban datos de manera automática y simultánea, como la dirección IP de origen, navegador utilizado, sistema operativo, momento en que se accedió a la página, siendo posible monitorear su comportamiento como usuario de los servicios de Internet.

Para lo anterior, BBVA Bancomer les informa a los titulares que en todo momento pueden deshabilitar el uso de estos mecanismos, de acuerdo a las instrucciones que cada empresa propietaria de los browsers (navegador o visor de Internet) tiene implementado para activar y desactivar las citadas Cookies y Web Beacons.

¿Cómo Tratamos los Datos Personales de Menores y de Personas con Capacidades Diferentes?

Se tratan a través del padre o tutor, previa acreditación legal, para la contratación de productos y/o servicios bancarios.

¿Cómo le informaremos sobre cambios al presente aviso de privacidad? Los cambios y actualizaciones del presente aviso de privacidad se harán de su conocimiento en cualquiera de nuestras sucursales; en la red de cajeros automáticos disponibles de BBVA Bancomer; en nuestro portal financiero www.bancomer.com

Si usted considera que su derecho de protección de datos personales ha sido vulnerado por alguna conducta de nuestros empleados o de nuestras actuaciones o respuestas, puede contactar a nuestra Dirección de Protección de Datos Personales, en el buzón:protecciondedatospersonales.mx@bbva.com sin perjuicio de su derecho de acudir ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Para mayor información visite www.inai.org.mx

BBVA Bancomer, S.A.
Av. Paseo de la Reforma No. 510, Col Juárez
Del. Cuauhtémoc
C.P. 06600, México, D.F.
www.bancomer.com
Última actualización: julio, 2015.

Acepto el tratamiento de mis datos

Nombre y firma del titular de los datos

Comentado [a3]: Como se mencionó en el trabajo de investigación, los datos biométricos de identificación eventualmente pudieran ser considerados como "sensibles", por lo tanto, se propone la inserción de un campo de firma para recabar el consentimiento del titular. Esta acción también favorece a la institución para comprobar a las autoridades competentes que el consentimiento para el tratamiento de datos en general fue recabado.

Anexo 6.

Anexo Técnico del INE,
integrante del Convenio de
Apoyo y Colaboración del INE
con las instituciones particulares.

CONACYT
Consejo Nacional de Ciencia y Tecnología

INFOTEC

Convenio de apoyo y colaboración entre el Instituto Nacional Electoral "EL INE" y "LA INSTITUCIÓN"

Anexo Técnico

Versión 3.2

Revisiones

Fecha	Versión	Descripción	Autor
26/04/2013	*2.7*	*Se integran cambios solicitados por la Dirección General Jurídica*	*Dirección Ejecutiva del Registro Federal de Electores* *Dirección de Infraestructura y Tecnología Aplicada*
2/05/2013	*2.8*	*Se eliminan los datos particulares para hacerlo universal*	*Dirección Ejecutiva del Registro Federal de Electores* *Dirección de Infraestructura y Tecnología Aplicada*
03/07/2013	*2.9*	*Se modifican los requerimientos del Portal de Verificación*	*Dirección Ejecutiva del Registro Federal de Electores* *Dirección de Infraestructura y Tecnología Aplicada*
13/05/2014	*3.0*	*Se actualiza a Instituto Nacional Electoral*	*Dirección Ejecutiva del Registro Federal de Electores* *Dirección de Infraestructura y Tecnología Aplicada*
11/06/2014	*3.1*	*Se incluye anexo 1.*	*Dirección Ejecutiva del Registro Federal de Electores* *Dirección de Infraestructura y Tecnología Aplicada*
04/03/2015	*3.2*	*Se realizan adecuaciones derivado de una revisión con el IFAI.*	*Dirección Ejecutiva del Registro Federal de Electores* *Coordinación de Procesos Tecnológicos* *Dirección de Infraestructura y Tecnología Aplicada* *Dirección de Productos y Servicios Electorales* *Dirección de Desarrollo y Operación de Sistemas*

Contenido

1 Glosario de Términos y Acrónimos.

Término/ Acrónimo	Definición
"INSTITUCIÓN"	*Nombre de INSTITUCIÓN.*
CAU	*Centro de Atención a Usuarios del Instituto Nacional Electoral*
CECYRD	*Centro de Cómputo y Resguardo Documental.*
CIC	*Código de Identificación de la Credencial*
DAC	*Dirección de Atención Ciudadana*
DDOS	*Dirección de Desarrollo y Operación de Sistemas*
DERFE	*Dirección Ejecutiva del Registro Federal de Electores.*
DITA	*Dirección de Infraestructura y Tecnología Aplicada*
DO-CECYRD	*Dirección de Operaciones del Centro de Cómputo y Resguardo Documental*
DPSE	*Dirección de Productos y Servicios Electorales*
"EL INE"	*Instituto Nacional Electoral*
FTP	*File Transfer Protocol (Protocolo de Transferencia de Archivos).*
IFAI	*Instituto Federal de Acceso a la Información y Protección de Datos*
NTP	*Network Time Protocol, es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del ruteo de paquetes en redes con latencia variable*
Padrón Electoral	*En él se encuentran todos los ciudadanos mexicanos que solicitaron su inscripción al mismo, con la finalidad de obtener su Credencial para Votar y así ejercer su derecho al voto*
Portal de Verificación	*Se refiere al sistema de envío de solicitudes hacia el servidor de Verificación de Datos residente en **"EL INE"**.*
SIIRFE	*Sistema Integral de Información del Registro Federal de Electores.*
SFTP	*Secure File Transfer Protocol (Protocolo Seguro de Transferencia de Archivos).*
SSH	*Secure SHell, en español: intérprete de órdenes seguro, es un protocolo y el programa que lo implementa, para acceder a máquinas remotas a través de una red.*
SSL	*Secure Sockets Layer; en español capa de conexión segura, es un protocolo criptográfico que proporciona comunicaciones seguras por una red, comúnmente Internet.*
Telnet	*Telecommunication Network (telecomunicación de red)* es *un protocolo de red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.*
Web Service	*Se refiere al servicio basado en protocolos y estándares para el intercambio de datos entre aplicaciones independientemente del lenguaje y plataforma en el que se encuentren.*
WSQ	*Wavelet Scalar Quantization, estándar creado por el FBI que define el formato para la compresión de imágenes de huellas dactilares.*

2 Objetivo.

*"Establecer las bases y mecanismos técnicos necesarios que permitan la verificación por parte de **"EL INE"** de los datos de los ciudadanos, contenidos en la credencial para votar que solicite **"LA INSTITUCIÓN"** y que forman parte del alcance del servicio, garantizando la confidencialidad de la información proporcionada por los ciudadanos, así como los recursos tecnológicos y operativos de ambas instituciones".*

3 Alcances.

El presente Anexo Técnico considera los siguientes alcances:

- *Describir el esquema de operación, su alcance y definir los esquemas de calidad (tiempo de respuesta, cantidad de consultas y disponibilidad de las aplicaciones de consulta para la verificación).*
- *Definir las características generales de la infraestructura tecnológica y de comunicaciones que soportará las aplicaciones de consulta de verificación.*
- *Establecer los mecanismos de seguridad que permitan garantizar la confidencialidad de la información.*
- *Establecer los roles y responsabilidades de cada Institución para la aplicación de los procedimientos a seguir para la implementación de las aplicaciones de consulta para la verificación de los datos de la Credencial para Votar, así como la creación de un Comité Técnico que estará integrado por personal de ambas instituciones para el seguimiento y control a la implementación del servicio, análisis de propuestas de mejora y verificación del cumplimiento de obligaciones en materia de protección de datos personales y seguridad de la información.*

4 Requerimientos técnicos para la verificación de datos de la Credencial para Votar.

4.1 Información.

*El extracto de la información de la base de datos del Sistema Integral de Información del Registro Federal de Electores (SIIRFE) para la verificación de los datos de la Credencial para Votar estará bajo resguardo y protección de **"EL INE"** y la misma, no será proporcionada a **"LA INSTITUCIÓN"** bajo ninguna circunstancia.*

*La infraestructura tecnológica en donde resida la información para la verificación de los datos de la credencial para votar, será accesible únicamente por personal de la Dirección Ejecutiva del Registro Federal de Electores del **"EL INE".***

La información estadística y cualquier otra que se genere producto de este convenio, estará bajo resguardo y protección de ambas instituciones y será accesible de acuerdo a los protocolos que establezca el Comité Técnico.

*La información relativa a la seguridad informática de la solución que estará implementada en las Instalaciones del Instituto estará bajo resguardo y protección de **"EL INE"** Indicado en el apartado de seguridad.*

*Los respaldos de la información generada a partir de la operación de la solución serán propiedad de **"EL INE"**.*

***"EL INE"** entregará a **"LA INSTITUCIÓN"** los resultados de las consultas realizadas en formato electrónico, mismos que no contendrán información y datos personales de los ciudadanos consultados, adicionalmente se entregarán estadísticas de uso de la aplicación.*

Para garantizar los niveles de servicio acordados, "EL INE" podrá disponer de dos centros de cómputo (primario y secundario). "LA INSTITUCIÓN"** será responsable de establecer un Plan de Continuidad de Operaciones de **"LA INSTITUCIÓN"**, en caso de intermitencias o paro de los sistemas por parte de **"EL INE"**. Dicho plan no será responsabilidad de **"EL INE".

4.2 Arquitectura de Solución.

*La arquitectura de solución contempla el uso de un Portal de Verificación encargado de recibir las solicitudes de las terminales de consulta de **"LA INSTITUCIÓN"** y enviarlas al Servidor de Verificación de **"EL INE"**, mismo que devolverá como respuesta la coincidencia de la verificación de los datos recibidos respecto de los datos contenidos en el Padrón Electoral.*

4.2.1 Modelo Conceptual.

A continuación se presenta el modelo conceptual que se considera para el uso de las aplicaciones de consulta para la verificación de datos de la Credencial para Votar.

1. La base de datos sobre la cual operarán las consultas de datos, estará conformada con la información necesaria de la base de datos del Sistema Integral de Información del Registro Federal de Electores (SIIRFE), misma que no será accesible por ***"LA INSTITUCIÓN"*** bajo ninguna circunstancia
2. La base de datos de operación será actualizada por **"EL INE"** de forma diaria para proporcionar las consultas de verificación que se realicen.
3. **"EL INE"** proporcionará el servicio Web para las consultas de verificación de datos (texto y minucia) conforme a los alcances establecidos en el presente Anexo Técnico.
4. **"EL INE"** contará con el personal para la operación y administración de las aplicaciones para la consultas de verificación de datos. Los equipos de seguridad perimetral y la infraestructura de cómputo necesaria para la operación y administración de las aplicaciones para las consultas de verificación de datos serán provistos por **"LA INSTITUCIÓN"**.
5. La ubicación del Portal de Verificación estará dentro de la Red de **"EL INE"**.- Este esquema requiere que el Portal de Verificación se encuentre dentro de las instalaciones de **"EL INE"** lo que significa que los datos deberán viajar en modo seguro sin procesar de la red de **"LA INSTITUCIÓN"** hasta la red de **"EL INE"**. **"LA INSTITUCIÓN"** es responsable de establecer el crecimiento de infraestructura tecnológica requerida para el adecuado funcionamiento del sistema previo acuerdo con **"EL INE"**. **"EL INE"** es responsable de los tiempos de respuesta hasta que la solicitud se reciba en el Portal de verificación.
6. **"EL INE"** se compromete a proveer los servicios básicos necesarios y la infraestructura auxiliar como UPS, Aire acondicionado, instalaciones eléctricas, instalaciones de red y espacio físico necesario.

Este modelo podrá ser actualizado con autorización del Comité Técnico de acuerdo a los requerimientos en materia de seguridad y protección de datos personales de ambas instituciones.

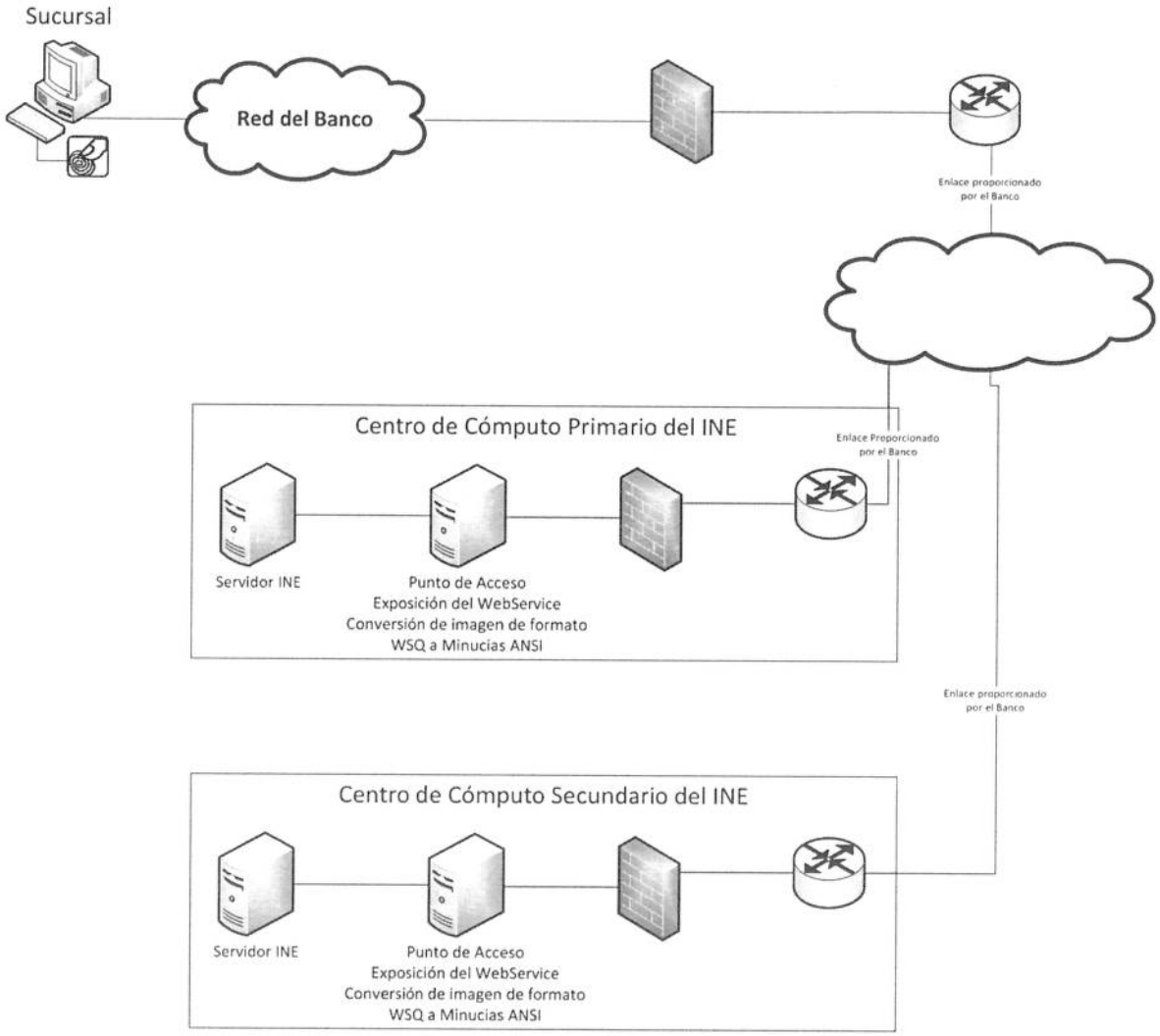


*Figura 1. Arquitectura general de la Solución con Portal de Verificación en la red de **"EL INE"***

4.2.2 Seguridad de la Información.

- *La información que entregue **"LA INSTITUCIÓN"** a **"EL INE"** será utilizada únicamente para la verificación de la misma, comparándola con la existente en el servicio de verificación de datos de la credencial para votar, dicha información no será compartida con institución alguna.*
- *El acceso al servicio web por parte de **"LA INSTITUCIÓN"** será exclusivamente por los medios que establezca **"EL INE"** para la solución Hyper Text Transfer Protocol Secure (HTTPS).*
- ***"LA INSTITUCIÓN"** no tendrá acceso a ningún sistema de la solución vía File Transfer Protocol (FTP), Telecommunication Network (Telnet), Secure SHell (SSH), Secure File Transfer Protocol (SFTP) o cualquiera no autorizado expresamente por **"EL INE".***
- ***"EL INE"** y **"LA INSTITUCIÓN"** establecerán de forma conjunta las especificaciones detalladas de las etapas de implementación de la solución.*
- ***"EL INE"** mantendrá sincronizados los servidores que soportan los sistemas a través de un servidor de tiempo vía Network Time Protocol (NTP), con el objetivo de identificar las transacciones de acuerdo a la fecha y hora en que éstas se llevaron a cabo.*
- *El certificado SSL del servidor será tramitado por **"EL INE".***
- *La comunicación por parte de **"LA INSTITUCIÓN"** será únicamente al Portal de Verificación y no se permitirá a otra infraestructura provista por **"EL INE"**.*
- ***"EL INE"** y **"LA INSTITUCIÓN"** establecerán los mecanismos de seguridad y los protocolos de comunicación permitidos y puertos de comunicación a utilizar, tanto para el acceso a los sistemas, como de comunicación entre ambas instituciones.*
- *Los equipos y software requeridos para el aseguramiento de las comunicaciones entre **"EL INE"** y **"LA INSTITUCIÓN"** serán determinadas de forma conjunta y deberán ser provistas por **"LA INSTITUCIÓN"**.*
- ***"EL INE"** se reserva el derecho de detener los sistemas en caso de que se evidencie o manifieste un incidente de seguridad crítico en la infraestructura de **"EL INE"**, para lo cual **"EL INE"** notificará a **"LA INSTITUCIÓN"** de forma inmediata a través de los responsables designados.*
- *En caso de que se identifique una probable vulneración a la protección de datos personales, **"EL INE"** dará vista al Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).*
- ***"LA INSTITUCIÓN"** deberá establecer al menos las mismas medidas de seguridad y de protección de datos personales con las que cuenta **"EL INE"** para el sistema de verificación.*
- *El **"Comité Técnico"** deberá establecer los procedimientos para la verificación del cumplimiento de obligaciones en materia de seguridad de la información y protección de datos personales.*

4.2.3 Alcances de las consulta de verificación de datos.

4.2.3.1 Verificación de datos de la Credencial para Votar

*La verificación de datos de la Credencial para Votar provista por **"EL INE"** tiene por objetivo validar la información (texto y minucias) del ciudadano a partir del número OCR o el CIC (Código de Identificación de la Credencial) ubicados en el reverso de la Credencial para Votar a través de un Web Service que puede ser utilizado por aplicaciones desarrolladas por **"LA INSTITUCIÓN"**.*

Datos de entrada del servicio Web:

- Formato (xml/json)
- *Confirmación del consentimiento del titular de la Credencial (obligatorio)*
- *Número OCR o Número CIC (obligatorio)*

*Los siguientes datos serán opcionales para ser confrontados y verificados por **"El INE"** en caso de ser proporcionados por **"LA INSTITUCIÓN"**:*

- *Apellido Paterno*
- *Apellido Materno*
- *Nombre(s)*
- *Año Registro*
- *Número de Emisión*
- *Clave de Elector*
- *CURP*
- *Huella del dedo índice de la mano derecha, los formatos válidos son los siguientes:*
  - *Registro de minucias (ANSI INCITS 378 2004).*
  - *Imagen en escala de grises usando el algoritmo de compresión WSQ (Wavelet Scalar Quantization).*
  - *Imagen en formato raw, en caso de proporcionar esta imagen, se tendrán que adicionar los siguientes valores:*
    - *Ancho en pixeles.*
    - *Alto en pixeles.*
    - *Resolución Horizontal en pixeles por pulgada.*
    - *Resolución Vertical en pixeles por pulgada.*
- *Huella del dedo índice de la mano izquierda, los formatos válidos son los siguientes:*
  - *Registro de minucias (ANSI INCITS 378 2004).*
  - *Imagen en escala de grises usando el algoritmo de compresión WSQ (Wavelet Scalar Quantization).*
  - *Imagen en formato raw, en caso de proporcionar esta imagen, se tendrán que adicionar los siguientes valores:*

- *Ancho en pixeles.*
- *Alto en pixeles.*
- *Resolución Horizontal en pixeles por pulgada.*
- *Resolución Vertical en pixeles por pulgada.*

Resultado de la verificación:

Dato	Respuesta
Identificador de la transacción	Numérico
• Tiempo de respuesta de comparación en el servidor de **"EL INE"** • Tiempo de respuesta desde el Portal de Verificación • En su caso, código de error transacción no exitosa	Cadena – Número de segundos
Estampilla de tiempo de la consulta	Cadena – Fecha de consulta
• Confirmación del consentimiento del titular de la Credencial (obligatorio)	No se da respuesta al servicio en caso de estar nulo o con un valor diferente al acordado
• Número OCR o Número de CIC (obligatorio) • Apellido Paterno • Apellido Materno • Nombre • Año Registro • Número de Emisión • Clave de Elector • CURP	Cadena – Falso/Verdadero
Minucia enviada • Tipo Formato • Identificador de dedo	Porcentaje de similitud

4.2.4 Niveles de Servicio

El nivel de servicio de soporte a la infraestructura del Servicio de Verificación por parte de **"EL INE",** dependerá del soporte del hardware y software contratado por parte de ***"LA INSTITUCIÓN"***.

Con relación al tiempo de respuesta y capacidad de atención por parte del Servicio de Verificación, dependerá de la infraestructura de comunicaciones y de procesamiento proporcionada por ***"LA INSTITUCIÓN"*** a **"EL INE"**. El tiempo de respuesta será considerado a partir de que la solicitud de la verificación de datos de la Credencial para Votar llegue al Portal de Verificación.

"EL INE" entregará a ***"LA INSTITUCIÓN"*** un reporte de los tiempos de respuesta de forma periódica mediante los formatos establecidos en el punto 4.3.1 Informes estadísticos.

"LA INSTITUCIÓN" podrá solicitar en caso de retraso en la atención de peticiones un reporte del tiempo de respuesta de la solución, previa entrega de un reporte de su proveedor del enlace de comunicación que indique el uso que tienen dicho enlace y que no existen fallas en el mismo.

4.3 Reportes

4.3.1 Informes estadísticos

"EL INE" *dispondrá a* ***"LA INSTITUCIÓN"*** *los siguientes informes estadísticos para cada Portal de Verificación de forma electrónica:*

- *Reporte diario del número de transacciones y tiempo promedio de respuesta dividido por hora, de acuerdo al Formato 1.*
- *Reporte semanal del número de transacciones y tiempo promedio de respuesta dividido por día, de acuerdo al Formato 2.*
- *Reporte mensual de número de transacciones y tiempo promedio de respuesta dividido por semana, de acuerdo al Formato 3.*
- *Reporte mensual de transacciones y tiempo promedio de respuesta integrando todos los puntos de acceso, de acuerdo al Formato 4.*

La adecuación o cambios a los formatos, así como la generación de nuevos reportes dependerá de los acuerdos que se establezcan en el Comité Técnico.

4.3.2 Información detallada de transacciones

Por petición expresa de ***"LA INSTITUCIÓN"****,* ***"EL INE"*** *podrá entregar la traza detallada de alguna transacción en específico. Para identificar la transacción específica,* ***"LA INSTITUCIÓN"*** *deberá entregar la fecha y hora exacta de la transacción (dd-mm-yyyy hh:mm:ss.ms) zona horaria de la ciudad de México (UTC-06:00) y el OCR enviado.*

4.4 Desarrollo de Sistemas de Información.

"EL INE" *es el encargado del desarrollo del Web Service de verificación de datos de la Credencial para Votar, y es el propietario del mismo, así como de los programas y demás software utilizado para este fin.*

"LA INSTITUCIÓN" *es responsable y dueña del desarrollo de las aplicaciones que utilicen el sistema de verificación de datos proporcionado por* ***"EL INE".***

Para la integración de nuevos Web Services o sistemas específicos, se requiere que los mismos sean aprobados por el Comité Técnico y de cada uno de éstos se entregará un plan de trabajo para su incorporación de acuerdo con la estructura de costos determinada por el mismo Comité.

"EL INE" *colaborará con* ***"LA INSTITUCIÓN"*** *para la integración de nuevos dispositivos de lectura a la aplicación Web desarrollada.*

4.5 Infraestructura Tecnológica.

4.5.1 Infraestructura de comunicaciones *(transporte de datos).*

"EL INE" *proporcionará a* ***"LA INSTITUCIÓN"*** *el espacio físico y acceso para establecer los enlaces digitales de comunicaciones entre las redes de datos de ambas instituciones conforme al diagrama anexo, los cuales serán utilizados única y exclusivamente para los fines y alcances del presente convenio.*

Para ello, ***"LA INSTITUCIÓN"*** *contratará el servicio de enlaces de comunicación entre los centros de datos del Instituto con los centros operativos que designe* ***"LA INSTITUCIÓN",*** *los cuales deberán contar con capacidad suficiente de acuerdo al cálculo que realicen* ***"EL INE"*** *y* ***"LA INSTITUCIÓN"****. Asimismo,* ***"LA INSTITUCIÓN"*** *cubrirá los costos por concepto de instalación y renta mensual de la prestación de dichos servicios, así como la adquisición de equipos y licencias que fueran necesarias para este fin y será el responsable de su administración y operación ante el proveedor de los mismos, hasta el equipo de comunicación WAN con la red de* ***"EL INE".***

"EL INE" *proporcionará en sus instalaciones a* ***"LA INSTITUCIÓN"****, la interfaz de conexión a la red local para acceder a los sistemas de verificación de datos, la cual será a través de 1000 BASE-TX.*

"EL INE" *proporcionará las condiciones ambientales y de energía eléctrica regulada e ininterrumpible, para la adecuada operación de los equipos de comunicación necesarios para la recepción de los enlaces de comunicación, los cuales deberán ser provistos por* ***"LA INSTITUCIÓN".***

En caso de requerirse adecuaciones, equipamiento o accesorios adicionales para la instalación de los enlaces y recepción de los mismos, estos deberán ser provistos por ***"LA INSTITUCIÓN"****, previa autorización y supervisión de* ***"EL INE".***

Para la interconexión entre los sitios de ***"LA INSTITUCIÓN"*** *y* ***"EL INE",*** *se realizara bajo la siguiente topología:*

Topología Punto a Punto.- Es un enlace de comunicación simétrico dedicado, en el cual solo participan ambas partes; interconectar "directamente" el Centro de Datos de ***"LA INSTITUCIÓN"*** *con los Centros de Datos de* ***"EL INE"*** *pasando únicamente por la red del proveedor del servicio de transporte de datos.*

En la Figura 2, se indica la imposibilidad de tener intercomunicación o tráfico entre los Centros de Datos de ***"EL INE"*** *por ser una tecnología Punto a Punto. En caso de presentarse una falla en algún Centro de Datos de* ***"EL INE"****,* ***"LA INSTITUCIÓN"*** *deberá cambiar la ruta de tráfico al Centro de Datos funcional.*

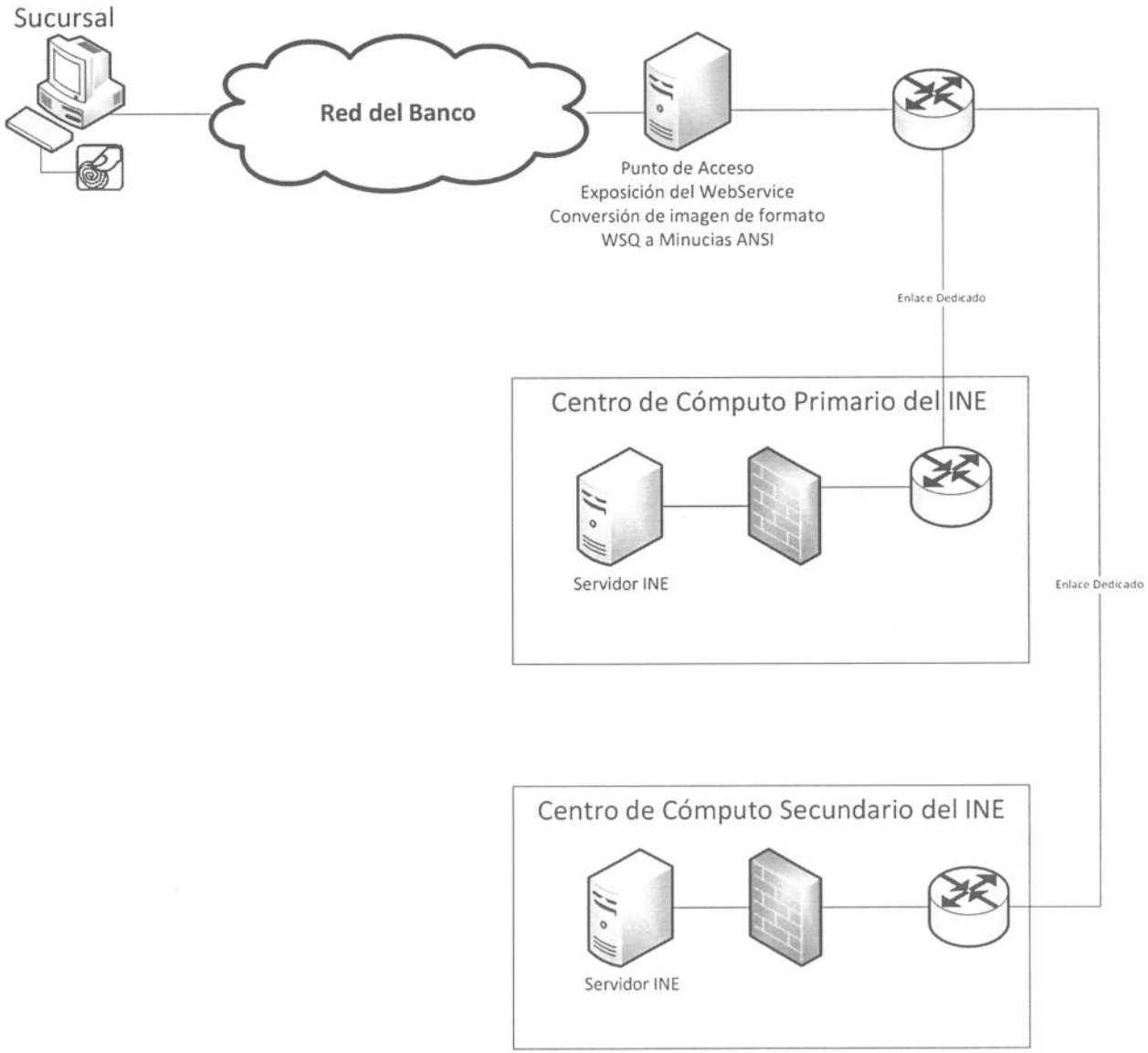


*Figura 2. Diagrama de interconexión Punto a Punto entre Centro(s) de Datos **"LA INSTITUCIÓN"** y Centros de Datos **"EL INE"***

Para la operación de esta topología se deberán tener en cuenta las siguientes consideraciones:

<table>
<tr>
<td>Consideraciones aplicables a la Topología Punto a Punto.</td>
<td>

"LA INSTITUCIÓN" debe proporcionar el(los) enlace(s) de comunicaciones junto con los equipos que lo reciban con todos los accesorios correspondientes, considerando todos los elementos para su instalación y operación.
Los equipos que proporcione "LA INSTITUCIÓN" para montaje en "EL INE" deberán ser para montaje en rack y/o con los accesorios para montaje en rack de 19 pulgadas.
Los equipos y enlace(s) serán administrados por parte de "LA INSTITUCIÓN" con excepción del equipo de seguridad perimetral del lado del Instituto.
"LA INSTITUCIÓN" establecerá los niveles de servicio tanto del(los) enlace(s) como de los equipos de comunicaciones que permitan garantizar los niveles de servicio que requiere.
Adicionalmente "LA INSTITUCIÓN" proveerá a "EL INE" el equipo de seguridad perimetral y los equipos para el Portal de Verificación con al menos las siguientes características, el cual será administrado por "EL INE":
<table>
<tr><th>Dispositivo *</th><th>Características</th></tr>
<tr><td>Firewall *</td><td>Cisco ASA 5510 Adaptive Security Appliance with AIP-SSM-10 (chassis, software, 250 VPN peers, 4 Fast Ethernet interfaces, Triple Data Encryption Standard/Advanced Encryption Standard [3DES/AES])</td></tr>
<tr><td>Portal de Verificación *</td><td>2 Servidores de procesamiento
• 2 procesadores Hexa core a 2.8 GHz.
• 128 GB en RAM.
• 500GB de Disco Duro a 15000 RPM en Raid 1.
• 6 interfaces de 1000
• 2 interfaces independientes de fibra canal (HBA)
• Fuentes redundantes
• Chasis tipo rack (incluir rieles de montaje para gabinete de 19 pulgadas).
• Sistema operativo Linux, con virtualización activa y soporte técnico durante la vigencia del convenio.</td></tr>
<tr><td></td><td>Actualización de firmas del módulo IPS durante la duración del convenio.</td></tr>
<tr><td>Almacenamiento compartido *</td><td>Requerido para la verificación de huellas dactilares.
3 TB de almacenamiento compartido.</td></tr>
</table>
* Los dispositivos descritos se consideran necesarios para la operación o funcionamiento de un centro de datos de "EL INE".

</td>
</tr>
</table>

	• **"EL INE"** ha realizado pruebas de capacidad con los equipos descritos anteriormente, obteniendo una capacidad de atención de 180 solicitudes de verificación de datos y huellas por minuto. • En caso de utilizar los dos Centros de Datos de **"EL INE"**, los equipos anteriormente listados deberán ser entregados por duplicado a **"EL INE".** • Todo equipo entregado deberá incluir sistema operativo y garantía de soporte técnico durante la vigencia del Convenio. **"EL INE"** será responsable de la instalación y configuración para la operación de los mismos.

Se podrán utilizar otros mecanismos de comunicación que convengan a ambas partes de común acuerdo y bajo la autorización del Comité Técnico.

Para la transmisión de datos, se utilizarán protocolos de seguridad y direcciones IP versión 4, privadas y/o homologadas (IP homologada es aquella IP pública FIJA que tiene una correspondencia con una única IP privada) en caso de ser necesario.

Se implementarán las políticas de seguridad necesarias para garantizar que los accesos se realicen únicamente a los equipos designados por **"EL INE"**. En caso de ser necesario, **"EL INE"** y **"LA INSTITUCIÓN"** implementarán políticas, procedimientos y mecanismos de seguridad adicionales, que aseguren los principios de confidencialidad, integridad y disponibilidad de la información.

4.6 Verificación de las minucias.

En lo que se refiere a la verificación de la minucia se consideran los siguientes puntos:

- ***"EL INE"** verificará con las minucias existentes en el servicio de verificación de datos de la Credencial para Votar almacenadas con el estándar ANSI INCITS 378 2004.*
- *Los sistemas de verificación de minucias utilizados al interior de las aplicaciones desarrolladas por **"EL INE"**, hacen uso de las librerías de comparación neurotechnology.*
- *La aplicación Web, capta la huella dactilar y envía la imagen en formato raw a los programas de conversión a WSQ y extracción de minucias.*
- *Los dispositivos lectores de huella dactilar deberán ir acompañados con el desarrollo de la API que le permite integrarse al sistema de verificación a través del cliente WEB.*
- ***"EL INE"** es propietario de la licencia de uso de las librerías neurotechnology.*
- *Aun y cuando el **"EL INE"** utilizó para la construcción de los sistemas las librerías de neurotechnology, esto no obliga a **"LA INSTITUCIÓN"** a la adquisición de algún tipo de licenciamiento o de dispositivos específicos.*
- ***"LA INSTITUCIÓN"** podrá utilizar cualquier dispositivo para la captación de huellas dactilares, bajo las siguientes premisas:*
    - *Deberá cumplir con los estándares* ANSI/NIST ITL 1-2000 / IAFIS-ic-0010 (v3) IAFIS WSQ
    - *Para utilizar los servicios Web de verificación de huella dactilar, podrá enviar de acuerdo a la siguiente especificación:*
        - *imagen de las huellas en formato raw*
        - *imagen WSQ de las huellas*
        - *minucias ANSI INCITS 378 2004 extraídas de las imágenes*
    - *Una vez establecido el o los dispositivos que utilizará **"LA INSTITUCIÓN"**, se realizarán de forma conjunta pruebas de precisión para conocer los porcentajes de similitud que entregará la herramienta de comparación de minucias ANSI INCITS 378 2004.*
- *La herramienta de comparación entrega únicamente el porcentaje de similitud, por lo que queda bajo responsabilidad de **"LA INSTITUCIÓN"** el establecimiento de umbrales para determinar la correspondencia o no de las minucias.*

4.7 Procedimientos de Soporte.

Procedimientos de soporte.

Las áreas técnicas de **"EL INE"** y **"LA INSTITUCIÓN",** darán aviso mutuo y con al menos 72 horas de anticipación, en caso de ser necesaria la aplicación de cualquier tipo de servicio programado a la infraestructura y que pudiera afectar la operación normal de ésta y por ende los sistemas, tal como se señala en el presente Anexo Técnico.

*De igual forma se define de común acuerdo, que los niveles de servicio sobre la disponibilidad de la infraestructura de cómputo y comunicaciones empleada por parte de ambas instituciones para establecer las verificaciones objeto del presente Anexo Técnico, será del 99.6 % de disponibilidad mensual considerando 7 días a la semana con 24 de servicio de los sistemas que proporcionará **"EL INE".***

***"LA INSTITUCIÓN"** proporcionará todo el soporte técnico de primer nivel derivado de la implantación de este convenio. Para la atención de requerimientos específicos de soporte de 2do nivel, **"LA INSTITUCIÓN"** designará un contacto para reportar a **"EL INE"** las incidencias de 2do nivel que requieran atención de **"EL INE"**. Los reportes de atención de 2do nivel podrán ser ingresados mediante correo electrónico. Para este propósito, se definirá entre ambas instituciones los mecanismos de soporte específicos que se implantarán.*

*Adicionalmente, **"EL INE"** y **"LA INSTITUCIÓN"** definirán el plan de comunicación para atender requerimientos relacionados con la operación, continuidad de la misma y situaciones que pudieran presentarse en la verificación de datos.*

4.7.1 Protocolos de Actualización (mantenimientos, hardware, software, baja, actualización de SW).

***"EL INE"** será el responsable y estará a cargo de llevar a cabo la actualización y/o mantenimiento de la Infraestructura Tecnológica que soportará la operación para la verificación de datos, para tal efecto deberá informar con al menos 72 horas las ventanas de mantenimiento programadas.*

***"LA INSTITUCIÓN"** será el responsable y estará a cargo de llevar a cabo la actualización y/o mantenimiento de la Infraestructura de comunicaciones entre las dos instituciones para la verificación de datos, para tal efecto deberá informar con al menos 1 mes las ventanas de mantenimiento programadas*

***"EL INE"** será el responsable y estará a cargo del desarrollo, mantenimiento y despliegue de las aplicaciones para la verificación de datos de la Credencial para Votar.*

4.8 Ambiente de pruebas.

"LA INSTITUCIÓN" *podrá validar y ajustar la integración del Servicio de Verificación mediante un acceso al ambiente de pruebas, debiendo firmarse por ambas partes el formato del* ***ANEXO 1 "Condiciones generales del mecanismo de pruebas, en relación a la conexión al Servicio de Verificación de la CPV",*** *en el que se especifican las características y condiciones de operación de la conexión a dicho ambiente.*

5 Estructura Organizacional.

5.1 Definición de Roles y Responsabilidades.

Con la finalidad de garantizar el cumplimiento a lo establecido en el presente Anexo Técnico, ***"EL INE"*** *y* ***"LA INSTITUCIÓN"*** *deberán de determinar el personal que se encargará de atender las actividades consignadas en el presente instrumento, conforme a lo siguiente:*

Cons	Perfil de Roles	Descripción general	Roles	"EL INE"	"LA INSTITUCIÓN"
1	Alta Dirección.	• Realiza el seguimiento del Proyecto a alto nivel en el Instituto. • Toma decisiones de carácter ejecutivo a nivel Institucional. • Apoya en la gestión administrativa del proyecto.	Seguimiento y toma de decisiones.	• Secretaría Ejecutiva de **"EL INE"**. • Comité Técnico	•
			Dirección del Proyecto.	• Dirección Ejecutiva del Registro Federal de Electores (DERFE).	•
2	Coordinación de Actividades.	• Planea y organiza el desarrollo del Proyecto. • Controla y da	Coordinación del Proyecto.	• Coordinación de Procesos Tecnológicos (CPT).	•

Cons	Perfil de Roles	Descripción general	Roles	"EL INE"	"LA INSTITUCIÓN"
		seguimiento a la ejecución del Proyecto. • Informa y comunica las actividades y avances al Grupo de Seguimiento y Toma de Decisiones y a la Dirección del Proyecto.	Ejecución del Proyecto.	• Dirección de Infraestructura y Tecnología Aplicada	•
3	Técnico.	• Define e integra los requerimientos técnicos del Proyecto. • Analiza las alternativas técnicas del proyecto. • Realiza las actividades que permitan integrar lo correspondiente a la viabilidad técnica del Estudio de Factibilidad del Proyecto.	Análisis y definición de la Arquitectura Técnica.	• Coordinación de Procesos Tecnológicos (CPT). • Dirección de Productos y Servicios Electorales (DPSE). • Dirección de Infraestructura y Tecnología Aplicada (DITA). • Dirección de Desarrollo y Operación de Sistemas (DDOS). • Dirección de Operaciones del CECYRD (DO-CECYRD).	•
			Apoyo técnico y normativo en materia de informática.	• Coordinación de Procesos Tecnológicos (CPT). • Dirección de Productos y Servicios Electorales (DPSE). • Dirección de Infraestructura y Tecnología Aplicada (DITA). • Dirección de Desarrollo y Operación de Sistemas (DDOS). • Dirección de Operaciones del CECYRD (DO-CECYRD). • Secretaría Técnica Normativa (STN)	•
4	Operativo.	• Proporciona información de los Procesos Operativos Sustantivos relacionados con	Análisis de procesos operativos.	• Dirección de Infraestructura y Tecnología Aplicada (DITA) • Dirección de Operaciones del CECYRD (DO-CECYRD). • Dirección de Operación y Seguimiento (DOS).	•

Cons	Perfil de Roles	Descripción general	Roles	"EL INE"	"LA INSTITUCIÓN"
		el Proyecto. • Analiza y propone mejoras a los procesos, subprocesos y actividades relacionadas con el Proyecto. • Realiza las actividades que permitan integrar lo correspondiente a la viabilidad operativa del Estudio de Factibilidad del Proyecto.	Revisión y análisis de procesos, subprocesos y procedimientos en campo.	• Dirección de Infraestructura y Tecnología Aplicada (DITA) • Dirección de Operaciones del CECYRD (DO-CECYRD). • Dirección de Operación y Seguimiento (DOS). • Dirección de Atención Ciudadana (DAC)	•
5	Administrativo.	• Realiza las actividades relativas a la Gestión Administrativa del Proyecto. • Establece los convenios de tipo administrativo que sean necesarios llevar a cabo durante el desarrollo del proyecto. • Realiza las actividades que permitan integrar lo correspondiente a la viabilidad Económico-Financiera del Estudio de Factibilidad del Proyecto.	Apoyo para la Gestión Administrativa Institucional.	• Dirección Ejecutiva de Administración • Coordinación de Administración y Gestión (CAG). • Dirección de Infraestructura y Tecnología Aplicada (DITA)	•
			Integrador de convenios con entidades externas.	• Dirección Jurídica de **"EL INE"**. • Secretaría Técnica Normativa (STN). • Coordinación de Administración y Gestión (CAG). • Secretaría Técnica (ST).	•
			Apoyo logístico-administrativo para actividades del proyecto con órganos colegiados.	• Dirección Ejecutiva del Registro Federal de Electores • Coordinación de Administración y Gestión (CAG). • Dirección de Infraestructura y Tecnología Aplicada (DITA)	•

Cons	Perfil de Roles	Descripción general	Roles	"EL INE"	"LA INSTITUCIÓN"
6	Jurídico.	• Proporciona apoyo jurídico y normativo sobre las actividades del proyecto. • Valida los aspectos legales y jurídicos de los documentos administrativos relativos al proyecto. • Realiza y valida los diversos proyectos de Acuerdo relativos al Proyecto para someter a consideración de los Órganos Colegiados competentes del Instituto. • Realiza las actividades que permitan integrar lo correspondiente a la viabilidad jurídica del Estudio de Factibilidad del • Proyecto.	Análisis y definición de aspectos jurídico-normativos.	• Dirección Jurídica de **"EL INE"**. • Secretaría Técnica Normativa (STN).	•

5.2 Integración del Comité Técnico.

"EL INE" *y* ***"LA INSTITUCIÓN"*** *definirán un* ***"Comité Técnico"*** *el cual tendrá entre sus funciones la de llevar a cabo el seguimiento y control de los alcances establecidos en el presente Anexo Técnico, así como proponer las actualizaciones del mismo, como resultado de los cambios tecnológicos y operativos que puedan generarse durante la vigencia del mismo. Dicho comité estará integrado por dos personas de* ***"LA INSTITUCIÓN"*** *y dos personas de* ***"EL INE".*** *Dichas personas deberán ser de al menos nivel dirección o equivalente y con responsabilidades técnicas o de negocio, debiendo ser designadas por los titulares firmantes del convenio de colaboración.*

El ***"Comité Técnico"*** *deberá establecer los procedimientos para verificar el cumplimiento de obligaciones en materia de seguridad de la información y protección de datos personales.*

El ***"Comité Técnico"*** *será el responsable de proponer cambios de infraestructura tecnológica y de comunicaciones para el mantenimiento y mejora de los sistemas, sin que por ello se tenga que actualizar el Anexo Técnico.*

El ***"Comité Técnico"*** *revisará los niveles de servicio y podrá actualizarlos de acuerdo a la factibilidad técnica de implementación de los mismos.*

Para la incorporación, modificación y/o suspensión de los alcances de las consultas para la verificación de la Credencial para Votar será necesaria la integración de adendas a este Anexo Técnico.

5.3 Seguimiento y Evaluación.

*Con el fin de tener un adecuado seguimiento y control en la ejecución de las actividades establecidas en este Anexo Técnico, así como del seguimiento una vez iniciadas las operaciones, el **"Comité Técnico"** definirá las áreas de competencia de ambas Instituciones que estarán dando seguimiento a la operación e informando de la misma, a fin de garantizar el cumplimiento de los objetivos y metas.*

La aplicación de controles de seguimiento y evaluación permitirá identificar oportunamente las desviaciones y deficiencias, así como proponer alternativas de solución.

6 Otras consideraciones.

***"EL INE"** brindará al personal de **"LA INSTITUCIÓN"** la asesoría técnica necesaria para el uso de las consultas de verificación.*

*Asimismo, **"EL INE"** proporcionará la capacitación que se defina sobre la evolución de la Credencial para Votar y sus elementos de seguridad a una plantilla de máximo 20 personas por curso. **"EL INE"** de común acuerdo con **"LA INSTITUCIÓN",** establecerán las fechas particulares de dichos cursos, así como el lugar de impartición.*

*Será posible, bajo común acuerdo, llevar a cabo visitas del personal involucrado en este proyecto por parte de **"EL INE"** y de **"LA INSTITUCIÓN"** a las instalaciones de ambos, con el objetivo de conocer detalladamente sus procesos. En el futuro y de común acuerdo entre **"EL INE"** y **"LA INSTITUCIÓN"**, se promoverán mejoras en los sistemas de información, aprovechando los avances tecnológicos disponibles en beneficio de los procesos que relacionan a ambas instituciones, previo establecimiento de fechas y prioridades; así como la revisión previa y en su caso aprobación del **"Comité Técnico"**.*

7 Formatos.

Formato 1:
Reporte diario del número de transacciones y tiempo promedio de respuesta dividido por hora

INE Instituto Nacional Electoral	**VERIFICACIÓN DE LOS DATOS DE LA CREDENCIAL PARA VOTAR** **INFORME DIARIO DE CONSULTAS** **Usuario:** 00000 (Número de usuario/Portal de Verificación) Nombre de la institución **Fecha:** ## / ## / #### **Fecha y hora de generación:** ## / ## / #### ## : ## : ##	
Hora	**# Consultas**	**Tiempo Promedio (milisegundos)**
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
TOTAL	####	####

Formato 2: Reporte semanal del número de transacciones y tiempo promedio de respuesta dividido por día

INE Instituto Nacional Electoral	**VERIFICACIÓN DE LOS DATOS DE LA CREDENCIAL PARA VOTAR** **INFORME SEMANAL DE CONSULTAS** **Usuario:** 00000 (Número de usuario/Portal de Verificación) Nombre de la institución **Fecha de Inicio: ## / ## / #### Fecha de Fin: ## / ## / ####** **Fecha y hora de generación: ## / ## / #### ## : ## : ##**	
Fecha	**# Consultas**	**Tiempo Promedio (milisegundos)**
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
##:##:##	####	####
TOTAL	####	####

Formato 3: Reporte mensual de número de transacciones y tiempo promedio de respuesta dividido por semana

INE Instituto Nacional Electoral	**VERIFICACIÓN DE LOS DATOS DE LA CREDENCIAL PARA VOTAR** **INFORME MENSUAL DE CONSULTAS** **Usuario:** 00000 (Número de usuario/Portal de Verificación) Nombre de la institución **Mes / Año:** ## / #### **Fecha y hora de generación:** ## / ## / #### ## : ## : ##	
Semana	**# Consultas**	**Tiempo Promedio (milisegundos)**
####	####	####
####	####	####
####	####	####
####	####	####
####	####	####
####	####	####
####	####	####
####	####	####
####	####	####
TOTAL	####	####

Formato 4: Reporte mensual de transacciones y tiempo promedio de respuesta integrando todos los puntos de acceso

INE Instituto Nacional Electoral	**VERIFICACIÓN DE LOS DATOS DE LA CREDENCIAL PARA VOTAR** **INFORME MENSUAL DE CONSULTAS POR PORTAL DE VERIFICACIÓN** **Usuario:** 00000 (Número de usuario/Portal de Verificación) Nombre de la institución **Mes / Año: ## / ####** **Fecha y hora de generación: ## / ## / #### ## : ## : ##**					
Fecha	**# Consultas**	**Promedio**	**# Consultas**	**Promedio**	**# Consultas**	**Promedio**
##:##:##	####	####	####	####	####	####
##:##:##	####	####	####	####	####	####
##:##:##	####	####	####	####	####	####
##:##:##	####	####	####	####	####	####
##:##:##	####	####	####	####	####	####
##:##:##	####	####	####	####	####	####
##:##:##	####	####	####	####	####	####
##:##:##	####	####	####	####	####	####
##:##:##	####	####	####	####	####	####
TOTAL	####	####	####	####	####	####

8 Anexos.

ANEXO 1

____ / ____ / ____
Día Mes Año

Folio:

ANTECEDETENTES

Acceso al Servicio de Verificación de datos de la Credencial para Votar.

El Instituto Nacional Electoral, a quien en lo sucesivo se le denominará el **"INSTITUTO"**, a través de su Modelo Integral de Planeación Institucional aprobado el 25 de mayo de 2011 mediante el Acuerdo del Consejo General CG173/2011, plantea como Objetivo Estratégico Institucional el Consolidar a la Credencial para Votar como el medio preferente de identidad ciudadana, por lo que en el ámbito de competencia de la Dirección Ejecutiva del Registro Federal de Electores (DERFE), corresponde establecer los mecanismos para que terceras instituciones, públicas o privadas, cuenten con la posibilidad de verificar la validez y legitimidad de los datos en la Credencial para Votar.

En este sentido la DERFE pone a disposición el Servicio de Verificación de datos de la Credencial para Votar que permite comparar los datos que se obtienen de la identificación contra los que obran en el Padrón Electoral sin que ello signifique transgredir lo dispuesto por el Artículo 126, párrafo 3, de la Ley General de Instituciones y Procedimientos Electorales (LGIPE).

Precisando que el Servicio de Verificación se hace a través del uso de una conexión segura (VPN) con vigencia máxima de 90 días naturales ofreciendo un mecanismo de pruebas con NOMBRE COMPLETO DEL USUARIO, a quien en lo sucesivo se le denominará el **"USUARIO"**, permitiendo valorar la implementación del Servicio de Verificación de la Credencial para Votar entre el **"INSTITUTO"** y el **"USUARIO"**.

En razón de lo anterior, es voluntad de los firmantes, establecer las condiciones generales del mecanismo de pruebas en relación al Servicio de Verificación de datos de la Credencial para Votar, por lo que ambas partes están de acuerdo en llevar a cabo la realización de las pruebas de acuerdo a las siguientes:

CLÁUSULAS

PRIMERA.- Lineamientos para realización de pruebas del Servicio de Verificación de datos de la Credencial para Votar

- Los parámetros para el establecimiento de la conexión VPN serán proporcionados por el **"INSTITUTO"**.

Responsabilidades para la conectividad.

- El **"USUARIO"** deberá proporcionar un plan de trabajo que describa las actividades a realizar durante la vigencia de la pruebas.
- El **"USUARIO"** designará un responsable y una segunda persona adicional en caso de ausencia del primero, proporcionando una relación con nombre completo, puesto, correo electrónico y número telefónico para tratar cualquier asunto relacionado a la conexión.

Vigencia de la conectividad.

- La vigencia de la conexión VPN solo se limitará al tiempo que dure la fase de pruebas o validación de funcionalidad del servicio, la cual no será mayor a 90 días naturales. Una vez concluido el plazo establecido, el **"INSTITUTO"** procederá a desactivar la conexión VPN.

Recursos disponibles en la conexión.

- Una vez establecida la conexión VPN, el único recurso disponible será el Portal de Verificación, ejemplo: https://<direcciónIP>/verifyData.
- Por parte del **"INSTITUTO"**, no se habilitará otro acceso o recurso dentro de la conexión VPN.
- El **"INSTITUTO"** no dispondrá de ningún equipo adicional para la realización de las pruebas.

Operación de la conectividad.

- El horario de uso para las pruebas será de lunes a viernes de 09:00 a 18:00 horas.

- Las pruebas estarán limitadas a máximo 5 solicitudes por minuto para el envío de verificaciones de datos y huellas.

Causas de suspensión de la conectividad.

- Si el **"INSTITUTO"** identifica que se está rebasando el límite máximo establecido de solicitudes enviadas por el **"USUARIO"**, causará la suspensión de la conexión.
- Si el **"USUARIO"** ejecuta procesos por lote (número de solicitudes concurrente en un periodo corto de tiempo), se procederá a suspender la conectividad.
- En caso de que el **"USUARIO"** envié tráfico de red que no corresponda a la demanda del servicio, se procederá con la suspensión.
- Por alguna actividad anormal identificada que ponga en riesgo la seguridad de la red del **"INSTITUTO"**.
- A solicitud expresa del **"USUARIO"** de suspender las pruebas.

SEGUNDA.- Declaratoria de confidencialidad y aceptación de las condiciones generales del mecanismo de pruebas en relación al Servicio de Verificación de datos de la Credencial para Votar, de los lineamientos para la conexión segura y de la vigencia para la operación de la conexión VPN.

Los abajo firmantes declaran:

- Tener conocimiento de que la información a la que tendrá acceso puede ser considerada como **CONFIDENCIAL** en los términos que marca Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, la Ley General de Instituciones y Procedimientos Electorales, el Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública y los Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores.
- Tener pleno conocimiento y aceptar que las actividades que desarrollará con el acceso solicitado, serán en estricto apego a la Ley, manteniendo absoluta confidencialidad y cuidado para conservar la información, asumiendo la obligación de abstenerse de revelar la información a la que tengan acceso a terceros, así como de utilizarla en provecho propio o de terceros, o reproducirla por cualquier medio, obligándose a notificar de inmediato cualquier caso del que tenga conocimiento cuya conducta contravenga la Ley o Políticas Institucionales.
- Que el acceso solicitado está reservado únicamente a la institución solicitante **"USUARIO"** y sólo para la realización de las tareas descritas en la presente solicitud, por ningún motivo podrá ser compartido a personas físicas o morales nacionales o extranjeras, distintas al **"USUARIO"**.

Que aceptan que la contravención a la Normatividad vigente y a la presente declaratoria, generará sanciones administrativas y/o de tipo penal a que haya lugar, en materia de transparencia .Que aceptan las condiciones **generales del mecanismo de pruebas en relación** al servicio de verificación de datos de la Credencial para Votar, los Lineamientos **para realización de pruebas del Servicio de Verificación de datos de la Credencial para Votar y** la vigencia para la operación de la conexión VPN.

Se firma el presente por duplicado, a los ___ días de _____ de 2014, haciendo constar que el uso del presente es única y exclusivamente para los firmantes.

Por el "INSTITUTO"	Por el "USUARIO"
Nombre y firma	Nombre y firma