INE/CG91/2020

ACUERDO DEL CONSEJO GENERAL DEL INSTITUTO NACIONAL ELECTORAL POR EL QUE SE APRUEBAN LAS ADECUACIONES PARA AMPLIAR Y FORTALECER EL SERVICIO DE VERIFICACIÓN DE DATOS DE LA CREDENCIAL PARA VOTAR

G L O S A R I O

CNV	Comisión Nacional de Vigilancia.
CPEUM	Constitución Política de los Estados Unidos Mexicanos.
CPV	Credencial(es) para Votar.
CRFE	Comisión del Registro Federal de Electores.
DERFE	Dirección Ejecutiva del Registro Federal de Electores.
DOF	Diario Oficial de la Federación.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos.
INE	Instituto Nacional Electoral.
Institución(es)	Institución(es) pública(s) y privada(s) u otro tipo, que firma(n) un Convenio de Apoyo y Colaboración en materia del Servicio de Verificación de Datos de la Credencial para Votar.
JGE	Junta General Ejecutiva.
LARCO	Lineamientos para el acceso, rectificación, cancelación y oposición de datos personales que forman parte del Padrón Electoral.
Ley de Datos Personales	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
LFEA	Ley de Firma Electrónica Avanzada.
LGIPE	Ley General de Instituciones y Procedimientos Electorales.
LGP	Ley General de Población.
LGTAIP	Ley General de Transparencia y Acceso a la Información Pública.
Lineamientos de Datos Personales	Lineamientos Generales de Protección de Datos Personales para el Sector Público.
Reglamento de Datos Personales	Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales.

Servicio de Verificación	Servicio de Verificación de Datos de la Credencial para Votar.
SNT	Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
TEPJF	Tribunal Electoral del Poder Judicial de la Federación.
UTTyPDP	Unidad Técnica de Transparencia y Protección de Datos Personales.

A N T E C E D E N T E S

1. **Opinión especializada sobre la viabilidad de la aplicación del Servicio de Verificación.** El 20 de mayo de 2015, el INAI emitió la opinión especializada sobre la viabilidad de la aplicación del Servicio de Verificación, en la que consideró que es una política pública socialmente útil, pues no sólo tendrá beneficios para los titulares de los datos personales, sino para las Instituciones que otorguen créditos, suministren bienes o servicios, o realicen trámites, reconociendo su importancia y valor social. Adicionalmente, el INAI emitió recomendaciones con la finalidad de que en su implementación se cumplan los principios rectores en materia de protección de datos personales.

   El 19 de febrero de 2016, el INAI emitió un resumen ejecutivo de la opinión especializada sobre la viabilidad de la aplicación del Servicio de Verificación, citada en el párrafo que antecede.

2. **Bases de colaboración para inhibir la suplantación de identidad a través del sistema financiero en México.** El 18 de febrero de 2016, el INE participó en la “Firma de Bases de Colaboración para inhibir la suplantación de Identidad a través del Sistema Financiero en México”, junto al INAI, la Procuraduría de la Defensa del Contribuyente, la Asociación Mexicana de Bancos de México y, como testigo, la Secretaría de Hacienda y Crédito Público.

3. **Aprobación del Servicio de Verificación.** El 26 de febrero de 2016, mediante Acuerdo INE/CG92/2016, este Consejo General aprobó la implementación del Servicio de Verificación, que servirá para garantizar el derecho de protección de datos de las y los ciudadanos, contenidos en el Padrón Electoral.

4. **Sentencia de la Sala Superior del TEPJF.** El 17 de agosto de 2016, la Sala Superior del TEPJF emitió la sentencia recaída en el expediente SUP-RAP-127/2016, en la que confirmó el Acuerdo INE/CG92/2016 aprobado por este órgano superior de dirección, al considerar que se apegó a los principios de legalidad y certeza, además de cumplir con la obligación de proteger y custodiar la información privada, así como los datos personales de las y los ciudadanos.

5. **Aprobación de las medidas administrativas para la implementación del Servicio de Verificación.** El 22 de agosto de 2016, la JGE aprobó, mediante Acuerdo INE/JGE200/2016, la instrumentación de las medidas administrativas para la implementación del Servicio de Verificación; entre otras, la relativa a que las cuotas de recuperación que aporten las Instituciones, en el marco de los Convenios de Apoyo y Colaboración para la implementación del Servicio de Verificación, sean destinados al patrimonio de la subcuenta "Fondo para la Atención Ciudadana y Mejoramiento de Módulos del Instituto Nacional Electoral", que forma parte del Fideicomiso de Administración e Inversión denominado "Fondo para el Cumplimiento del Programa de Infraestructura Inmobiliaria y para la Atención Ciudadana y Mejoramiento de Módulos del Instituto Nacional Electoral".

6. **Publicación de la Ley de Datos Personales.** El 26 de enero de 2017, se publicó en el DOF la Ley de Datos Personales.

7. **Aprobación del Reglamento de Datos Personales.** El 22 de noviembre de 2017, mediante Acuerdo INE/CG557/2017, este Consejo General expidió el Reglamento de Datos Personales, con lo cual se armonizó el marco normativo institucional con la Ley de Datos Personales.

8. **Aprobación de los Lineamientos de Datos Personales.** El 19 de diciembre de 2017, mediante Acuerdo ACT-PUB/19/12/2017.10, el Pleno del INAI aprobó los Lineamientos de Datos Personales, los cuales fueron publicados en el DOF el 26 de enero de 2018.

9. **Aprobación de los LARCO.** El 18 de junio de 2018, mediante Acuerdo INE/CG649/2018, este Consejo General aprobó los LARCO, y abrogó los Lineamientos aprobados por el órgano superior de dirección del otrora Instituto Federal Electoral en el Acuerdo CG734/2012.

10. **Actualización del modelo de la CPV.** El 19 de diciembre de 2018, mediante Acuerdo INE/CG1499/2018, este Consejo General actualizó el modelo de la CPV en territorio nacional y desde el extranjero, que había sido aprobado en el diverso CG732/2012 por el órgano superior de dirección del otrora Instituto Federal Electoral, así como los Acuerdos INE/CG36/2014 e INE/CG875/2015.

11. **Opinión 24/19 de la UTTyPDP.** El 28 de agosto de 2019, la UTTyPDP emitió la Opinión 24/19 en materia de protección de datos personales, respecto de si la firma electrónica, firma autógrafa digital y los *Checkbox* cuentan con los elementos suficientes para considerarse como un mecanismo adecuado para recabar el consentimiento expreso y por escrito de las y los ciudadanos. En dicho documento resaltó la necesidad de observar los principios y deberes de la materia; en particular, lo que refiere al principio de consentimiento.

12. **Uso, funcionalidad y verificación de la información contenida en los códigos QR de la CPV.** El 20 de noviembre de 2019, este Consejo General aprobó, mediante Acuerdo INE/CG539/2019, el uso, funcionalidad y verificación de la información contenida en los códigos bidimensionales QR de alta densidad para el almacenamiento y acceso rápido que forman parte de los elementos del modelo de la CPV en territorio nacional y desde el extranjero.

13. **Convenios de Apoyo y Colaboración.** Al 9 de marzo de 2020, el INE ha suscrito 64 convenios con Instituciones, los cuales tienen por objeto establecer los mecanismos de colaboración, por los que este Instituto, a través de la DERFE, bajo la disposición de un servicio web con mecanismos de seguridad, de fácil acceso y eficiente operación, verificará que los datos contenidos en la CPV coincidan con los que obran en poder del INE, sin que por motivo alguno se den datos personales que las y los ciudadanos proporcionen a este Instituto.

14. **Recomendación de la CNV.** El 10 de marzo de 2020, la CNV recomendó a este Consejo General, mediante Acuerdo INE/CNV06/MAR/2020, apruebe las adecuaciones para ampliar y fortalecer el Servicio de Verificación.

15. **Presentación del Proyecto de Acuerdo en la CRFE.** El 13 de mayo de 2020, la CRFE aprobó someter a la consideración de este órgano superior de dirección, mediante Acuerdo INE/CRFE19/02SE/2020, el Proyecto de Acuerdo del Consejo General del INE por el que se aprueban las adecuaciones para ampliar y fortalecer el Servicio de Verificación.

C O N S I D E R A N D O S

PRIMERO. Competencia.

Este Consejo General es competente para aprobar las adecuaciones para ampliar y fortalecer el Servicio de Verificación, conforme a lo previsto en los artículos 41, párrafo tercero, Base V, Apartado A, párrafo segundo de la CPEUM; 29; 30, párrafos 1, incisos a), c) y d) y 2; 31, párrafo 1; 34, párrafo 1, inciso a); 35; 36; 44, párrafo 1, incisos l), gg) y jj) de la LGIPE; 4, párrafo 1, fracción I, apartado A, inciso a); 5, párrafo 1, inciso w) del Reglamento Interior del INE; 24 del Reglamento de Sesiones del Consejo General del INE.

SEGUNDO. Razones jurídicas que sustentan la determinación.

Acorde a lo establecido en el artículo 1º, párrafo primero de la CPEUM, todas las personas gozarán de los derechos humanos reconocidos en la propia Carta Magna y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que la misma establece.

En términos del párrafo segundo de la disposición aludida, las normas relativas a los derechos humanos se interpretarán de conformidad con la CPEUM y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia.

El párrafo tercero del mismo artículo dispone que todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.

El párrafo octavo del artículo 4 de la CPEUM establece que toda persona tiene derecho a la identidad y a ser registrada de manera inmediata desde 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.

El artículo 6, párrafo cuarto, Apartado A, fracción II de la CPEUM establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

El artículo 16, párrafo segundo de la CPEUM señala que 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.

El artículo 41, párrafo segundo, Base V, Apartado A, párrafo segundo de la CPEUM estipula que el INE es un organismo público autónomo dotado de personalidad jurídica y patrimonio propios, en cuya integración participan el Poder Legislativo de la Unión, los Partidos Políticos Nacionales, las 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, el numeral 3, inciso a), Apartado B, Base V, del precepto constitucional antes citado, en relación con el artículo 32, párrafo 1, inciso a), fracción III de la LGIPE, estipulan que corresponde al INE, para los Procesos Electorales Federales y locales, el Padrón Electoral y la Lista Nominal de Electores.

El artículo 30, párrafo 2 de la LGIPE determina que todas las actividades de este Instituto se regirán por los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad, objetividad, paridad y, además, se realizarán con perspectiva de género.

El artículo 54, párrafo 1, incisos b), c) y d) de la LGIPE refiere que la DERFE tiene entre sus atribuciones la de formar el Padrón Electoral, expedir la CPV según lo dispuesto en el Titulo Primero del Libro Cuarto de la misma Ley, además de revisar y actualizar anualmente el Padrón Electoral conforme al procedimiento establecido en el Libro Cuarto de la propia LGIPE.

El artículo 126, párrafos 1 y 2 de la LGIPE establece que el INE prestará por conducto de la DERFE y de sus vocalías en las Juntas Locales y Distritales ejecutivas, los servicios inherentes al Registro Federal de Electores y que el

mismo es de carácter permanente y de interés público, que tiene por objeto cumplir con lo previsto en el artículo 41 de la CPEUM sobre el Padrón Electoral.

Asimismo, el párrafo 3 de la referida disposición legal menciona que los documentos, datos e informes que las y los ciudadanos proporcionen al Registro Federal de Electores, en cumplimiento de las obligaciones que les impone la CPEUM y la propia LGIPE, serán estrictamente confidenciales y no podrán comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en los que el INE fuese parte, para cumplir con las obligaciones previstas por la Ley, en materia electoral y por la LGP en lo referente al Registro Nacional Ciudadano o por mandato de juez competente.

Al respecto, en el Artículo Transitorio Cuarto del Decreto de fecha 14 de julio de 1992, por el que se reformó la LGP, publicado en el DOF el 22 de julio de 1992,[1] se consideró que, en lo relativo al establecimiento del Registro Nacional de Ciudadanos, se utilizaría la información del Padrón Electoral que proporcionaría el Instituto Federal Electoral —ahora INE— en tanto se expidiera la Cédula de Identidad Ciudadana; por lo tanto, la CPV serviría como medio de identificación personal.

El artículo 129 de la LGIPE dispone que el Padrón Electoral del Registro Federal de Electores se formará mediante la aplicación de la técnica censal total o parcial, la inscripción directa y personal de las y los ciudadanos, y la incorporación de los datos que aporten las autoridades competentes relativos a fallecimientos o habilitaciones, inhabilitaciones y rehabilitaciones de derechos políticos de las y los ciudadanos.

El artículo 131 de la LGIPE señala que el INE debe incluir a las y los ciudadanos en las secciones del Registro Federal de Electores y expedirles la CPV, documento indispensable para que las y los ciudadanos puedan ejercer su derecho de voto.

El artículo 133, párrafo 1 de la LGIPE indica que el INE se encargará de formar y administrar el Padrón Electoral y la Lista Nominal de Electores.

El artículo 134 de la LGIPE refiere que, con base en el Padrón Electoral, la DERFE expedirá, en su caso, las CPV.

---

1 http://dof.gob.mx/index.php?year=1992&month=07&day=22.

De conformidad con lo previsto en el artículo 23 de la LGTAIP, el INE es sujeto obligado a transparentar y permitir el acceso a su información y proteger los datos personales que obren en su poder.

En esa lógica, y en términos de lo dispuesto por el artículo 25 de la LGTAIP, los sujetos obligados serán responsables del cumplimiento de las obligaciones, procedimientos y responsabilidades establecidas en dicha Ley, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y las correspondientes de las entidades federativas, en los términos que las mismas determinen.

Asimismo, el artículo 68 de la LGTAIP reitera que los sujetos obligados serán responsables de los datos personales en su posesión y, en relación con éstos, deberán:

a) Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso, rectificación, corrección y oposición al tratamiento de datos, en los casos que sea procedente, así como capacitar a las y los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con la normatividad aplicable;

b) Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido o dicho tratamiento se haga en ejercicio de las atribuciones conferidas por ley;

c) 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 la normatividad aplicable, excepto en casos en que el tratamiento de los datos se haga en ejercicio de las atribuciones conferidas por ley;

d) Procurar que los datos personales sean exactos y actualizados;

e) 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

f) Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

De conformidad con el segundo párrafo de la disposición legal anteriormente aludida, 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 de acuerdo a la normatividad aplicable. Lo anterior, sin perjuicio a lo establecido por el artículo 120 de la LGTAIP.

El artículo 69 de la LGTAIP prevé que las y los particulares, sin perjuicio de que sean considerados sujetos obligados de conformidad con esa Ley, serán responsables de los datos personales de conformidad con la normatividad aplicable para la protección de datos personales en posesión de particulares.

Asimismo, para que los sujetos obligados puedan permitir el acceso a información confidencial, el artículo 120 de la LGTAIP establece que se deberá obtener el consentimiento de las y los particulares titulares de la información.

Por otro lado, el artículo 1° de la Ley de Datos Personales dispone que todas sus disposiciones, según corresponda, y en el ámbito de su competencia, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal. Además, establece que son sujetos obligados en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

El artículo 6 de la Ley de Datos Personales señala que el Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente. El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

El artículo 16 de la Ley de Datos Personales establece que los responsables deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

El artículo 17 de la Ley de Datos Personales señala que el tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

El artículo 18 de la Ley de Datos Personales refiere que todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera. El responsable podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la Ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la referida Ley y demás disposiciones que resulten aplicables en la materia.

El artículo 19 de la Ley de Datos Personales indica que el responsable no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Por su parte, el artículo 21 de la Ley de Datos Personales estipula que el consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

Asimismo, dicha disposición legal señala que el consentimiento será tácito cuando, habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario. Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.

De igual forma, dicho artículo menciona que, tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa o firma electrónica, salvo en los casos previstos en el artículo 22 de la propia Ley de Datos Personales.

Si bien los datos biométricos no están mencionados de manera expresa en el listado de datos personales sensibles que se incluyen en la Ley de Datos

Personales y la Ley Federación de Protección de Datos Personales en Posesión de los Particulares, ello no implica que no se puedan considerar como tales bajo ciertas circunstancias. Para determinar tal característica, se requiere atender las condiciones del caso concreto, a fin de analizar si los datos biométricos en cuestión actualizan alguno de los siguientes tres supuestos que prevén la Ley de Datos Personales y la referida Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para considerar un dato personal como sensible:

a) Que se refieran a la esfera más íntima de su titular;

b) Que su utilización indebida pueda dar origen a discriminación, o

c) Que su uso ilegítimo conlleve un grave riesgo para su titular.

Por ejemplo, el dato biométrico del iris podría considerarse sensible en los casos en que permita obtener información sobre el estado de salud de su titular.

A mayor abundamiento, la Guía para el Tratamiento de Datos Biométricos del INAI,[2] define los datos biométricos como las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles. Dicho documento también señala que la huella dactilar y el rostro (reconocimiento facial), entre otros refieren a características físicas y fisiológicas de las personas.

Asimismo, la guía categoriza los biométricos como datos personales sensibles. Una huella dactilar podría considerarse sensible si a través de un uso indebido de la misma, se puede tener acceso a información privilegiada que pudiera poner en riesgo la seguridad o estabilidad patrimonial o financiera de una persona o incluso su condición jurídica.

El artículo 25 de la Ley de Datos Personales establece que el responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

---

[2] Edición marzo, 2018. Disponible en la página de internet, http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf.

El artículo 26 de la Ley de Datos Personales refiere que el responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable. Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla. Cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el SNT.[3]

Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad, el artículo 30 de la Ley de Datos Personales señala, al menos, los siguientes:

a) Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;

b) Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;

c) Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;

d) Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;

e) Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;

[3] El SNT es una instancia de coordinación y deliberación, que tiene como objetivo la organización de los esfuerzos de cooperación, colaboración, promoción, difusión y articulación permanente en materia de transparencia, acceso a la información y protección de datos personales, de conformidad con lo señalado en la LGTAIP y demás normatividad aplicable. Más información en www.snt.org.mx.

f) Establecer procedimientos para recibir y responder dudas y quejas de las y los titulares;

g) Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la propia Ley de Datos Personales y las demás que resulten aplicables en la materia, y

h) Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en dicha Ley y las demás que resulten aplicables en la materia.

A su vez, el artículo 31 de la Ley de Datos Personales dispone que, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

El artículo 47 de la Ley de Datos Personales prevé que la o el titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:

a) Aun siendo lícito el tratamiento, su persistencia cause un daño o perjuicio al titular, y

b) Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

El artículo 65 de la Ley de Datos Personales estipula que toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la mencionada Ley.

Ahora bien, los Lineamientos de Datos Personales establecen, en su artículo 3, párrafo 1, que dicha normativa será aplicable a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos, del ámbito federal y partidos políticos que en el ejercicio de sus atribuciones y funciones lleven a cabo tratamientos de datos personales de personas físicas, en términos de lo dispuesto en la Ley de Datos Personales, así como al INAI y los organismos garantes en lo que respecta a la sustanciación de los recursos de inconformidad.

Por su parte, el artículo 4 de los Lineamientos de Datos Personales determina que las disposiciones contenidas en ese cuerpo normativo serán aplicables al tratamiento de datos personales de personas físicas que obren en soportes físicos y/o electrónicos a que se refiere el artículo 4 de la Ley de Datos Personales. Dichos datos personales podrán estar expresados en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o en cualquier otro formato, en términos de lo dispuesto en el artículo 3, fracciones IX y X de la Ley de Datos Personales y los propios Lineamientos de Datos Personales.

El artículo 8 de los Lineamientos de Datos Personales establece que el responsable del cuidado de los datos personales deberá tratarlos sujetándose a las atribuciones o facultades que la normatividad aplicable le confiera, con estricto apego y cumplimiento de lo dispuesto en el artículo 17 de la Ley de Datos Personales, los propios Lineamientos, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de las y los titulares.

A su vez, el artículo 9 de los Lineamientos de Datos Personales, para efectos de lo previsto en el artículo 18, primer párrafo de la Ley de Datos Personales, determina que las finalidades del tratamiento de los datos personales son:

a) Concretas, cuando el tratamiento atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular;

b) Explícitas, cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;

c) Lícitas, cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y

d) Legítimas, cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento de la o el titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley de Datos Personales.

El artículo 10 de los Lineamientos de Datos Personales establece que en el tratamiento de datos personales para finalidades distintas a aquéllas que motivaron su tratamiento original a que se refiere el artículo 18, segundo párrafo de la Ley de Datos Personales, el responsable deberá considerar lo siguiente:

a) La expectativa razonable de privacidad de la o el titular basada en la relación que tiene con éste;

b) La naturaleza de los datos personales;

c) Las consecuencias del tratamiento posterior de los datos personales para la o el titular, y

d) Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley de Datos Personales y los Lineamientos de Datos Personales.

Por su parte, el artículo 12 de los Lineamientos de Datos Personales señala que, previo al tratamiento de los datos personales, el responsable deberá obtener el consentimiento de la o el titular, de manera libre, específica e informada, en términos del artículo 20 de la Ley de Datos Personales, salvo que se actualice algunas de las causales de excepción previstas en el artículo 22 del mismo ordenamiento; lo anterior, sin que exima al responsable del cumplimiento de las demás obligaciones establecidas en dicha Ley y dichos Lineamientos.

A su vez, el artículo 13 de los Lineamientos de Datos Personales dispone, en caso de que se requiera el consentimiento de la o el titular para el tratamiento de sus datos personales, que la solicitud del consentimiento deberá ser concisa e inteligible, estar redactada en un lenguaje claro y sencillo acorde con el perfil de la o el titular y, cuando se refiera a diversos asuntos ajenos a la protección de datos personales, deberá presentarse de tal forma que se distinga claramente de dichos asuntos.

El artículo 14 de los Lineamientos de Datos Personales establece que el consentimiento de la o el titular podrá manifestarse de forma expresa o tácita. Por regla general, para todo tratamiento de datos personales que se efectúe será válido el consentimiento tácito, salvo que una ley exija al responsable que la voluntad de la o el titular se manifieste de manera expresa.

De conformidad con el artículo 16 de los Lineamientos de Datos Personales, el consentimiento será expreso cuando la voluntad de la o el titular se manifieste de forma verbal, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología, de acuerdo con lo dispuesto en el artículo 21, primer párrafo de la Ley de Datos Personales. Para la obtención del consentimiento expreso, el responsable deberá facilitar a la o el titular un medio sencillo y gratuito a través del cual pueda manifestar su voluntad, el cual le permita acreditar de manera indubitable y, en su caso, documentar que la o el titular otorgó su consentimiento ya sea a través de una declaración o una acción afirmativa clara. El silencio, las casillas previamente marcadas, la inacción de la o el titular o cualquier otra conducta o mecanismo similar a los mencionados no deberán considerarse como consentimiento expreso de la o el titular. Asimismo, la carga de la prueba para acreditar la obtención del consentimiento expreso correrá a cargo del responsable.

En este sentido, el artículo 17 de los Lineamientos de Datos Personales señala que, para efectos de lo dispuesto en el artículo 21, párrafo 1 de la Ley de Datos, el consentimiento escrito y verbal se entenderá de la siguiente manera:

a) La o el titular otorga su consentimiento de manera verbal cuando lo externe oralmente de manera presencial o mediante el uso de cualquier otra tecnología que permita la interlocución oral, en ambos casos, ante la persona que represente al responsable, y

b) La o el titular otorga su consentimiento por escrito cuando manifieste su voluntad en un documento, físico o electrónico, a través de cierta declaración en sentido afirmativo, firma autógrafa, huella dactilar, firma electrónica o procedimiento equivalente autorizado por la normatividad aplicable.

Por lo que respecta a la obtención del consentimiento de la o el titular, el artículo 18 de los Lineamientos de Datos Personales indica que se deberá realizar de manera previa, cuando los datos personales se recaban directamente de ésta(e) y, en su caso, sea requerido conforme a los artículos 20 de la Ley de Datos Personales y 12 de los mismos Lineamientos. Se entenderá que el responsable obtiene los datos personales directamente de la o el titular cuando ésta(e) los proporciona a la persona que lo representa personalmente o por algún medio que permita su entrega directa como podrían ser medios electrónicos, ópticos, sonoros, visuales, vía telefónica, Internet o cualquier otra tecnología y/o medio.

El artículo 26 de los Lineamientos de Datos Personales prevé que el responsable deberá informar a las y los titulares, a través del aviso de privacidad, la existencia y las características principales del tratamiento al que serán sometidos sus datos personales. Por regla general, todo responsable está obligado a cumplir con el principio de información y poner a disposición de la o el titular el aviso de privacidad, de conformidad con lo dispuesto en los artículos 3, fracción II, 26, 27 y 28 de la Ley de Datos personales y los propios Lineamientos, con independencia de que no se requiera el consentimiento de la o el titular para el tratamiento de sus datos personales.

De conformidad con el artículo 47 de los Lineamientos de Datos Personales, en relación con el diverso 30, fracciones I y II de la Ley de Datos Personales, el responsable deberá elaborar e implementar políticas y programas de protección de datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de protegerlos de manera sistemática y continua. Esas políticas y programas de protección de datos personales deberán ser aprobadas, coordinadas y supervisadas por su Comité de Transparencia. El responsable deberá prever y autorizar recursos, de conformidad con la normatividad que resulte aplicable, para la implementación y cumplimiento de éstos.

Finalmente, el artículo 51 de los Lineamientos de Datos Personales establece que, para el cumplimiento de lo dispuesto en el artículo 30, fracción VII de la Ley de Datos Personales, el responsable deberá aplicar medidas de carácter administrativo, técnico, físico u otras de cualquier naturaleza que, desde el diseño, le permitan aplicar de forma efectiva el cumplimiento de los principios, deberes y demás obligaciones previstas en la Ley de Datos Personales y los propios Lineamientos, en sus políticas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales. Lo anterior, considerando los avances tecnológicos, los costos de implementación, la naturaleza, el ámbito, el contexto y los fines del tratamiento de los datos personales, los riesgos de diversa probabilidad y gravedad que entraña éste para el derecho a la protección de datos personales de las y los titulares, así como otros factores que considere relevantes el responsable.

En relación con la normatividad institucional en materia de protección de datos personales, el artículo 1 del Reglamento de Datos Personales dispone que es de observancia general y tiene por objeto regular el debido tratamiento de los datos personales en posesión del INE, así como establecer los procedimientos que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición a fin de garantizar el derecho que tiene toda persona a la protección de sus datos personales, en concordancia con la Ley de Datos Personales y demás normatividad aplicable.

Asimismo, el artículo 2 del Reglamento de Datos Personales establece que son sujetos obligados de dicho Reglamento, los Órganos y servidores públicos del INE, así como toda persona o institución vinculada con el tratamiento de datos personales que realice el INE.

Además, el artículo 8 del Reglamento de Datos Personales señala que los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de datos personales, 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 de acuerdo a la normatividad aplicable; o bien, que ello atienda a una obligación legal o a un mandato judicial. Los Órganos del Instituto[4] que posean por cualquier título bases que contengan

[4] Órganos de dirección, ejecutivos, técnicos, de vigilancia, de transparencia, de control y otros órganos colegiados del INE (artículo 3, fracción XVII del Reglamento de Datos Personales).

datos personales, deberán hacerlo del conocimiento del Comité,[5] a través de la UTTyPDP, quien coadyuvará a mantener el registro actualizado de los sistemas de datos personales en posesión del INE, conforme a las reglas que emita dicho órgano colegiado.

De conformidad con lo previsto en el artículo 19 del Reglamento de Datos Personales, el principio de consentimiento consiste en que todo tratamiento de datos personales en posesión de los Órganos del INE deberá contar con el consentimiento previo del titular, salvo las causales de excepción previstas en la Ley de Datos Personales.

El artículo 20 del Reglamento de Datos Personales refiere que sólo podrán tratarse datos personales sensibles siempre que se cuente con el consentimiento expreso de su titular o alguna ley así lo disponga. Tratándose de datos personales sensibles, los Órganos del INE deberán obtener el consentimiento expreso y por escrito de la o el titular, para su tratamiento a través de su firma autógrafa o firma electrónica, salvo en los casos previstos en el artículo 22 de la Ley de Datos Personales.

El artículo 26 del Reglamento de Datos Personales señala que el principio de información tiene por objeto hacer del conocimiento del titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto, conforme a la Ley de Datos Personales y demás normatividad que resulte aplicable en la materia.

Aunado a lo anterior, el numeral 6 de los LARCO señala que los datos personales que forman parte del Padrón Electoral serán estrictamente confidenciales; y no podrán comunicarse, darse a conocer, ni utilizarse para fines distintos a los establecidos en la LGIPE.

Asimismo, dicho numeral establece que por ningún motivo se proporcionarán los datos personales que forman parte del Padrón Electoral a terceros, ni a instancias públicas y privadas que lo soliciten, con excepción de lo dispuesto por la LGIPE y la normativa del INE en materia de acceso, verificación y entrega de datos personales y para la atención de requerimientos de autoridades competentes.

---

[5] Comité de Transparencia del INE a que hace referencia el artículo 3, fracción V de la Ley de Datos Personales (artículo 3, fracción II del Reglamento de Datos Personales).

Cabe señalar que, en la sentencia recaída al recurso de apelación con número de expediente SUP-RAP-109/2010, en las fojas 120 y 121, la Sala Superior del TEPJF determinó lo siguiente:

> "[…] es factible concluir que el Consejo General del Instituto Federal Electoral, en lo que atañe al ámbito federal, cuenta con facultades para tomar acuerdos que tiendan a instrumentar, como en el caso sucede, la validez temporal, el uso y sustitución de un determinado formato de credencial para votar con fotografía que se considere haya perdido eficacia; consecuentemente para dar de baja del padrón electoral a los ciudadanos que se encuentren en esa hipótesis e inclusive para generar los acuerdos pertinentes tendientes a inhibir el uso de esas credenciales como medio de identificación oficial."

De la misma forma, en la foja 161 del propio expediente SUP-RAP-109/2010, la Sala Superior del TEPJF refirió lo que sigue:

> "Cabe señalar, que como la credencial para votar con fotografía es un documento en el que confluyen en unidad las dos cualidades de que se habla, esto es, la de documento para votar y de identificación oficial, las mismas deben considerarse indisolubles, de manera tal, que mientras conserve su validez para ejercer el voto la debe conservar para los efectos de identificación oficial, a contrario sensu, cuando pierden su vigencia como instrumento para votar simultáneamente la pierden como medio de identificación por ser características indisolubles del propio y único documento, como sucede, verbigracia en el caso de los pasaportes."

En ese orden de ideas, la Sala Superior del TEPJF ha emitido la Tesis XV/2011 que señala que la CPV, al perder vigencia como instrumento electoral, también la pierde como documento de identificación oficial:[6]

> 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,

[6] https://www.te.gob.mx/jurisprudenciaytesis/compilacion.htm#TEXTO%20XV/2011.

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.

Resulta necesario señalar que, al confirmar el Acuerdo INE/CG92/2016 por el que este Consejo General aprobó la implementación del Servicio de Verificación, la Sala Superior del TEPJF, en la sentencia recaída en el SUP-RAP-127/2016, señaló que "[…] la referida verificación tiene como uno de sus objetivos —precisamente— salvaguardar el mencionado derecho de protección de datos personales, siempre en el contexto de preservar su confidencialidad y evitar su uso indebido por parte de terceros."

Con base en las disposiciones anteriormente expuestas, este Consejo General puede aprobar las adecuaciones para ampliar y fortalecer el Servicio de Verificación.

TERCERO. Motivos para aprobar las adecuaciones para ampliar y fortalecer el Servicio de Verificación.

Es obligación del Estado proporcionar a las y los ciudadanos un documento oficial que les permita identificarse ante las Instituciones, el cual debe contener información personal que los diferencien de otros.

Por lo tanto, en cumplimiento a tal obligación, en el Artículo Transitorio Cuarto del Decreto por el que se reformó la LGP, se invistió a la CPV de legalidad al considerarla un instrumento de identificación oficial, en tanto se instrumente el Registro Nacional de Ciudadanos y se expidiera la Cédula de Identificación Ciudadana, lo cual no se ha hecho a la fecha, lo que ha posicionado a la CPV como la identificación ciudadana por excelencia.

Es por ello que el INE ha implementado mejoras constantes en las medidas de seguridad en el trámite para obtener la CPV, además de incorporar estrictos mecanismos al acceso y tratamiento de la información que integra el Padrón Electoral, con la finalidad de dar un adecuado uso al resguardo de los datos

personales de las y los ciudadanos para proporcionar el instrumento fundamental en materia electoral y para efectos de identificación ciudadana.

Debido a la importancia descrita líneas atrás, el INE, a través de la DERFE, diseñó un mecanismo de verificación de los datos contenidos en la CPV, que presenten las y los ciudadanos en las Instituciones para la realización de algún trámite, que permite cotejar la información con la que obra en el Padrón Electoral, sin que el INE proporcione en algún momento información confidencial. Cobra relevancia que dicho mecanismo consiste en el Servicio de Verificación, aprobado por este Consejo General mediante Acuerdo INE/CG92/2016.

Al respecto, el Servicio de Verificación es un mecanismo de protección y adecuado manejo de la información que resguarda el INE como sujeto obligado, que permite un eficaz y eficiente tratamiento de la información confidencial que es otorgada por las y los ciudadanos para obtener su CPV.

En este sentido, el Servicio de Verificación constituye una política pública que permite aminorar las operaciones con datos falsos, el robo, usurpación de identidad y el mal uso de los datos personales de las y los ciudadanos que acuden ante Instituciones, a solicitar algún servicio y con las que se han suscrito Convenios de Colaboración para su instrumentación.

El Servicio de Verificación ha permitido que las Instituciones verifiquen la vigencia de las CPV, mediante la comparación de los datos de CIC, OCR, número de emisión, clave de elector, nombre(s), apellidos, año de registro, CURP y huellas dactilares, y que la o el portador de la credencial es la misma persona que realizó el trámite con el INE, previniendo así que las y los ciudadanos sean víctimas de una posible usurpación de su identidad o, de un uso ilícito de sus datos personales que pudiera generar múltiples perjuicios a su persona y a su patrimonio.

El 17 de marzo de 2020, la JGE aprobó, mediante Acuerdo INE/JGE34/2020, las medidas preventivas y de actuación, con motivo de la pandemia de Covid-19. El 23 de marzo de 2020, se publicó en la edición vespertina del DOF el acuerdo mediante el cual el Consejo de Salubridad General reconoció la epidemia de enfermedad por el virus SARS-CoV-2 (Covid-19) en México, como una enfermedad grave de atención prioritaria; asimismo, se establecieron las actividades de preparación y respuesta ante dicha epidemia.

El 24 de marzo de 2020, se publicó en el DOF el acuerdo por el que se establecieron las medidas preventivas que se deberán implementar para la mitigación y control de los riesgos para la salud que implica la enfermedad causada por el virus SARS-CoV-2 (Covid-19).

El 30 de marzo de 2020, se publicó en el DOF el acuerdo del Consejo de Salubridad General por el que se declara como emergencia sanitaria por causa de fuerza mayor, a la epidemia de enfermedad generada por el virus SARS-CoV-2 (Covid-19), el cual señala que la Secretaría de Salud determinará todas las acciones que resulten necesarias para atender dicha emergencia sanitaria.

Con la ampliación y fortalecimiento que se propone al Servicio de Verificación, tanto en condiciones normales como de emergencia sanitaria, en las cuales se requiere realizar actividades a distancia, se busca ofrecer mayor flexibilidad para la verificación de los datos y la autenticación mediante tecnologías biométricas (incluyendo la comparación facial) de las y los ciudadanos que portan su CPV, promoviendo así el uso del servicio para proteger los datos personales de la ciudadanía.

En esa tónica de ideas, la Sala Superior del TEPJF, al resolver el recurso de apelación identificado con la clave SUP-RAP-127/2016, en el cual se impugnó la implementación del Servicio de Verificación aprobada en el Acuerdo INE/CG92/2016, señaló, entre otras cosas, lo siguiente:

> "[…] reconoce en primer lugar la obligación constitucional y legal de la autoridad responsable de proteger la información confidencial proporcionada por los ciudadanos, y provee de un mecanismo cierto y determinado tendente a preservar dicha protección de datos personales y, al mismo tiempo, a prestar un servicio que brinde certeza y seguridad jurídica a los propios ciudadanos con motivo del uso de la credencial para votar con fotografía como instrumento de identificación oficial".
>
> […] Es decir, la citada verificación de datos no implica que la autoridad responsable, motu proprio ni a instancia de parte, envié, entregue, transmita o remita en modo alguno a terceros los datos personales que existen bajo su resguardo y protección -con carácter confidencial-, sino tan solo el ejercicio, en respuesta a una solicitud expresa y regulada de determinada institución ante la cual un ciudadano exhibió su credencial para votar como instrumento de

> identificación oficial (previa celebración de convenio específico y consentimiento del propio ciudadano), de comprobar, corroborar, cotejar, compulsar o examinar que los datos contenidos en la misma coincidan con la información que obra bajo custodia de la citada autoridad electoral, la cual, se insiste, es instada para restar dicho servicio de consulta o verificación, con el fin -precisamente- de proteger datos personales, en un contexto de certeza y seguridad jurídica."

Es por ello que la operación actual del Servicio de Verificación se ofrece a las Instituciones, quienes utilizan directamente el servicio para el desarrollo de sus actividades inherentes a sus funciones, con las que se suscriben convenios de colaboración, para verificar los datos de la CPV, sin que en ningún momento se proporcione información confidencial.

En esa tesitura, los datos que se obtienen de la CPV son enviados al INE en tiempo real por las Instituciones con quienes previamente se ha celebrado un Convenio de Apoyo y Colaboración, con la finalidad de que este Instituto verifique la información con la que obra en el Padrón Electoral y se apruebe o niegue la correspondencia de datos, sin que dicha información sea proporcionada por el INE; es decir, la respuesta que otorga el INE sólo se constriñe a una negativa o aprobación de la información que es proporcionada a este Instituto.

Las actividades de verificación actualmente se llevan a cabo de manera presencial. Para que los datos de la CPV puedan ser cotejados y verificados, las y los ciudadanos tienen que acudir de manera presencial a las Instituciones para presentar su credencial y firmar de manera autógrafa el consentimiento; es decir, el consentimiento no se podría obtener actualmente con el uso de medios digitales.

En razón de que las circunstancias mencionadas limitan el alcance del Servicio de Verificación, debido a la evolución del mercado y al avance de la tecnología, se han presentado solicitudes de empresas que ofrecen servicios en plataformas digitales y que no requieren interacción física con las y los ciudadanos, ya que todos los trámites de autentificación se realizan en la modalidad de atención vía remota.

Ante esta problemática, el INE se ve imposibilitado para otorgar el Servicio de Verificación a las Instituciones que contemplan en su flujo de trabajo de

actividades la interacción en la modalidad de atención vía remota con sus clientes, pues actualmente el servicio no prevé la posibilidad de recabar el consentimiento y de presentar la CPV en la modalidad de atención vía remota, aunque el consentimiento sí sea expreso de conformidad con la norma y conste en medios diferentes al papel.

En este sentido, se entiende por modalidad de atención vía remota la que se realiza por parte de las(os) usuarias(os), para acceder a productos y servicios a través de canales o plataformas digitales fuera de las oficinas o sucursales físicas de las Instituciones, ya sea con el apoyo de un operador de la misma Institución o directamente por la o el cliente en modalidad de autoservicio.

El INE no puede ser ajeno a la realidad tecnológica actual; en consecuencia, deberá desempeñar un papel fundamental de apoyo a la difusión de la tecnología ecológica y sustentable, que también será determinante de cara a mejorar el uso de los recursos naturales y ayudar a gestionar de mejor forma los recursos que apremien problemas como el cambio climático, en la que cada vez se sistematizan más procesos y se mudan al entorno digital de datos, documentos e información a través de medios electrónicos. En este sentido, el INE debe contemplar en su normativa la posibilidad legal de otorgar sus servicios a través del uso del internet y de los dispositivos móviles, sin dejar a un lado el cumplimiento irrestricto de sus obligaciones en materia de transparencia y protección de datos personales.

Así las cosas, al desafío actual que significa la migración de requerimientos físicos a documentos electrónicos debe estar acompañado de medidas de seguridad robustas que preserven la confidencialidad de los datos personales, de fácil acceso, que simplifiquen el trámite y que no obstaculicen el resultado. Ello, sin que tal contexto ponga en riesgo el resguardo de la información confidencial de la que el INE es garante, toda vez que la previsión del Servicio de Verificación es única y exclusivamente para la validación de la información proporcionada por las Instituciones públicas o privadas.

En tal razón, en la opinión 24/19, relativa al alcance de la firma electrónica, autógrafa digital y *Checkbox* para recabar el consentimiento de las y los ciudadanos, la UTTyPDP señaló que, conforme a la normativa aplicable, en los sectores público y privado, la firma electrónica cuenta con validez reconocida por las normas jurídicas mexicanas y cumple con los elementos

suficientes para contemplarse como un mecanismo adecuado para recabar el consentimiento de las y los ciudadanos.

No obstante, se reconoce la existencia de otros mecanismos que, en diferentes grados de certeza o trazabilidad, permiten hacer constar el consentimiento de las y los ciudadanos.

Bajo este contexto, se considera que existe la posibilidad legal y material para que las Instituciones que soliciten el Servicio de Verificación puedan realizarlo en línea, en la modalidad de vía remota, previendo:

a) Los mecanismos de seguridad y la protección de los datos personales de las y los ciudadanos;

b) Que el consentimiento puede recabarse, igualmente, en línea, sin que deje de tener el carácter de:

   I. Expreso;

   II. Trazable, y

   III. Comprobable;

c) Que pueda constar en medios digitales, y

d) Que las herramientas informáticas que se utilicen para obtener el consentimiento expreso deben dar cuenta de la voluntad de la o el titular de manera indubitable, de tal forma que se deje evidencia que permita verificar que la o el titular sí otorgó su consentimiento.

En efecto, tomando en cuenta lo que dispone la LFEA en su artículo 8, la firma electrónica avanzada[7] deberá cumplir con los siguientes principios rectores:

[7] De conformidad con el artículo 2, fracción XIII de la LFEA, la firma electrónica avanzada es el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa. En este sentido, y en términos de lo previsto en el artículo 7 de la propia LFEA, la firma electrónica avanzada podrá ser

1. **Equivalencia Funcional.** Consiste en que la firma electrónica avanzada en un documento electrónico o en su caso, en un mensaje de datos, satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos.

2. **Autenticidad.** Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven.

3. **Integridad.** Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que éste ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación.

4. **Neutralidad Tecnológica.** Consiste en que la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular.

5. **No Repudio.** Consiste en que la firma electrónica avanzada contenida en documentos electrónicos garantiza la autoría e integridad del documento y que dicha firma corresponde exclusivamente al firmante.

6. **Confidencialidad.** Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, garantiza que sólo pueda ser cifrado por el firmante y el receptor.

---

utilizada en documentos electrónicos y, en su caso, en mensajes de datos. Los documentos electrónicos y los mensajes de datos que cuenten con firma electrónica avanzada producirán los mismos efectos que los presentados con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos.

De modo que dichos elementos deben ser considerados como indispensables para el uso de medios diversos a la firma electrónica, de forma que garanticen la autenticación del individuo titular de los datos personales.

En ese sentido, resulta recomendable utilizar un factor de reconocimiento múltiple, adaptado a las circunstancias concretas del tratamiento en cuestión, conforme a la Guía para el Tratamiento de Datos Biométricos del INAI.

Cabe subrayar que es invariable la obligación de las Instituciones de recabar el consentimiento que reúna las siguientes características:

a) Libre;

b) Informada;

c) Expresa, e

d) Inequívoca sobre el tratamiento de sus datos personales.

Si no cuentan con el consentimiento, el INE no estará en posibilidades de proporcionar el Servicio de Verificación en cualquier modalidad.

En este orden de ideas, en la comparación de la fotografía de las y los ciudadanos captada por las Instituciones respecto de la fotografía correspondiente a la CPV, se debe considerar que es responsabilidad de las Instituciones asegurarse que expresan la voluntad de las y los ciudadanos de autorizar alguna transacción o servicio. Por lo anterior, las Instituciones deberán asegurarse de que la fotografía fue tomada de manera directa a la o el ciudadano, ya sea de manera presencial con la supervisión de un empleado o funcionario, así como en aplicaciones móviles mediante las que la persona se toma por sí misma la fotografía (*selfie*).

En el caso de que la fotografía sea tomada de manera presencial, se recomienda que ésta sea supervisada por algún(os) empleado(s) o funcionario(s) de la Institución en ambientes controlados —en oficina o sucursal, con luz adecuada y fondo de color mate claro, uniforme y liso— considerando que la cara esté de frente, con base en la guía de la

Organización de Aviación Civil Internacional (OACI o ICAO, por sus siglas en inglés) para la toma de imágenes faciales de documentos de viaje.[8]

Para el caso de que la fotografía sea tomada por la propia persona (*selfie*) mediante el uso de aplicaciones móviles, se deberán implementar mecanismos que realicen prueba de vida, ya sea de manera estática o dinámica, quedando bajo responsabilidad de la Institución que se pueda acreditar que la fotografía fue tomada a la o el ciudadano de manera presencial y no a otra fotografía, figura o similar. Cualquier deficiencia que se pueda dar en la toma de la fotografía es estricta responsabilidad de las Instituciones que las capten, ya que pueden dar como resultado una mala identificación y la deficiencia en los mecanismos para garantizar la prueba de vida podrían derivar en el robo de identidad.

Para realizar la comparación de la imagen que envíen las Instituciones, el INE deberá establecer convenios de colaboración con proveedores de tecnologías de reconocimiento facial que realizan la autenticación biométrica por rasgos faciales entre dos fotografías, que permiten obtener como resultado la similitud de rasgos y, por tanto, determinar si se trata de la misma persona.

Los proveedores de tecnologías de reconocimiento facial con los que se firmen convenios deben haber sido evaluados por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de los Estados Unidos de América en la Evaluación de Fabricantes de Tecnologías de Reconocimiento Facial 1:1.[9] Dicha evaluación consiste en calificar la precisión de los algoritmos de autenticación 1:1 medidos en términos de los errores en la identificación de impostores en varios conjuntos de datos de diferentes características, por lo que resulta acorde con la funcionalidad que requiere el INE para proporcionar el servicio a las Instituciones.

Estos proveedores solo proporcionarán la tecnología necesaria para la comparación facial de la imagen que envíen las Instituciones respecto de la imagen en la base de datos del INE, por lo que de ninguna forma serán intermediarios o proveedores directos del Servicio de Verificación. El costo de la implementación y uso de la comparación facial deberá ser cubierto por la

[8] Portrait Quality, Reference Facial Images for MRTD, https://www.icao.int/Security/FAL/TRIP/Documents/TR%20-%20Portrait%20Quality%20v1.0.pdf.
[9] Face Recognition Vendor Test 1:1, FRVT 1:1, https://pages.nist.gov/frvt/html/frvt11.html.

Institución que utilice el Servicio de Verificación directamente con el proveedor de la tecnología de comparación facial.

Se debe resaltar que, de esta manera, el INE válidamente está en condiciones de atender las solicitudes de la verificación de CPV formuladas por las Instituciones, cuya consulta se realice en la modalidad de atención presencial o vía remota.

Para la implementación del Servicio de Verificación, las Instituciones deberán firmar el Convenio de Apoyo y Colaboración respectivo, contar con la infraestructura necesaria para la verificación de los datos de la CPV y, por lo menos, una de las biometrías —al menos una de las diez huellas dactilares y/o la imagen facial— de las y los ciudadanos, utilizando mecanismos de seguridad y cifrado de punta a punta entre la Institución y el INE que permitan preservar los principios de seguridad y confidencialidad de asociados a la protección de datos personales de las y los ciudadanos.

En consecuencia, el Servicio de Verificación garantizará que el acceso a la información, en aras de integrar y generar solicitudes y recibir respuestas del servicio, sea sólo entre el INE y la Institución correspondiente, sin el acceso de figura intermedia alguna, cualquiera que sea u denominación, en el tratamiento de datos personales.

Lo anterior permitirá garantizar el cumplimiento de la obligación que el INE tiene respecto de la responsabilidad de salvaguardar los datos personales que proporcionan las y los ciudadanos, entre otra, la relacionada con la formación del Padrón Electoral en cuanto a la inscripción y actualización de la ciudadanía, en la elaboración de la Lista Nominal de Electores y la emisión de la CPV, para lo cual deberá tratar datos personales únicamente cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido, así como adoptar las medidas necesarias que preserven su seguridad y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Por otra parte, es de resaltar que este Consejo General, en el Acuerdo INE/CG1499/2018, aprobó la actualización del modelo de la CPV en territorio nacional y desde el extranjero, en el que se consideró la inclusión de los

códigos bidimensionales tipo QR para el almacenamiento y acceso rápido de los datos que forman parte de los elementos de las credenciales.

Como parte de los diversos diseños de la CPV, ésta ha contado con códigos de barras que han aportado elementos de control, seguridad y acceso a información confiable para procesos internos y externos del INE.

Los códigos de barras han evolucionado con el avance tecnológico, lo que ha permitido contener mayor cantidad de información. En el caso de la CPV, se han incorporado códigos de barras unidimensionales tipo Code-128, así como códigos bidimensionales tipo PDF-417 y QR. La evolución de la CPV ha permitido que los códigos de barras y códigos bidimensionales que se integran a la misma, promuevan su uso y aplicación para diversos fines.

Conviene recordar que, mediante Acuerdo CG293/2013, el órgano superior de dirección del otrora Instituto Federal Electoral aprobó la integración de los códigos de barras bidimensionales tipo PDF-417, que contribuyó a que se pudiera incorporar mayor información a la que se tenía anteriormente en las CPV emitidas antes de 2013, con el fin de que dicha información fuera leída e interpretada de forma rápida y adecuada.

En este mismo contexto, mediante Acuerdo INE/CG539/2019, este Consejo General aprobó el uso, funcionalidad y verificación de la información contenida en los códigos bidimensionales QR de alta densidad para el almacenamiento y acceso rápido que forman parte de los elementos del modelo de la CPV en territorio nacional y desde el extranjero. Gracias a la aprobación de ese Acuerdo, los códigos bidimensionales tipo QR contribuyen a que la información que se almacene en ellos con la seguridad necesaria, pueda ser leída de forma ágil y fácil, con el fin de promover el acceso a servicios de información que permitan verificar y validar que la CPV fue elaborada por el INE.

La adopción del código de barras bidimensional tipo QR obedece a una evolución natural en la CPV, permitiendo contar con información de calidad para su control y poder proveer servicios preservando la seguridad en el tratamiento de los datos personales que también se encuentran impresos en la credencial.

Los códigos QR atienden la necesidad de implementar elementos de control y de acceso rápido a la información contenida en la CPV, que permiten promover y difundir de manera clara y precisa el alcance de los diversos servicios electorales y de información que proporciona el INE, a fin de facilitar el acercamiento de la ciudadanía con este Instituto, atendiendo lo establecido en el marco jurídico, normativo y procedimental, contribuyendo con ello en la generación de valor público del INE.

Para la validación de la CPV mediante el uso de los códigos QR, el INE opera una herramienta informática para validar los datos contenidos en la credencial, a través de elementos sencillos al alcance de Instituciones, así como de particular a particular, con los que se pretenden fortalecer los procesos de seguridad, acceso a servicios y confiabilidad de las Instituciones o de los propios particulares.

Para realizar la verificación se desarrollarán mecanismos que permitan la validación de las CPV emitidas por el INE, mediante los códigos de barras, para que las y los ciudadanos, así como las Instituciones, puedan corroborar su autenticidad en modalidades en línea o fuera de línea.

Asimismo, se buscará desarrollar servicios que permitan que la lectura de información de los códigos de barras mejore la calidad de los datos captados por las Instituciones con las que se establezcan los Convenios de Apoyo y Colaboración.

Las Instituciones que estén interesadas en suscribir los Convenios de Apoyo y Colaboración con el INE para tal fin y que establezcan los trámites en la modalidad de atención vía remota, deberán cumplir previamente con los requisitos que determine la DERFE conforme al Anexo Económico y el documento de Especificaciones Técnicas correspondientes. Asimismo, se actualizarán los Convenios de Apoyo y Colaboración vigentes, en la medida en que las Instituciones migren hacia este tipo de tecnologías.

Lo anterior, debido a que en dichos instrumentos se establecerán las bases y condiciones necesarias para el adecuado funcionamiento del Servicio de Verificación, preservando la confidencialidad de la información proporcionada por las y los ciudadanos en términos de la normatividad aplicable, así como los recursos tecnológicos y operativos que aportarán el INE y las Instituciones.

De igual forma, los instrumentos en comento preverán el alcance y las obligaciones de las y los usuarios del Servicio de Verificación y la promoción de la cultura de protección de datos personales entre las y los usuarios y el personal de los Módulos de Atención Ciudadana del INE.

En el mismo sentido, se deberán tomar en cuenta al menos todas las medidas de seguridad técnicas, administrativas y físicas con las que actualmente opera el Servicio de Verificación, con lo cual se reitera la obligación legal de proteger los datos personales de la ciudadanía.

Igualmente, se reitera que en todo momento el Servicio de Verificación será de punto a punto entre la Institución que suscriba el Convenio de Apoyo y Colaboración y el INE, sin que éste último proporcione información confidencial alguna y que la Institución no divulgue la información obtenida del Servicio de Verificación a un tercero; es decir, las Instituciones con quienes se suscribe el Convenio de Apoyo y Colaboración utilizarán dicho servicio única y exclusivamente para el desarrollo de sus actividades inherentes a sus funciones.

Por lo antes expuesto, resulta conveniente que este Consejo General apruebe las siguientes adecuaciones al Servicio de Verificación:

a) Incorporar la modalidad de atención vía remota que podrán brindar las Instituciones a la ciudadanía, mediante los Convenios de Apoyo y Colaboración en materia del Servicio de Verificación que al efecto celebren con el INE;

b) Para realizar el tratamiento de datos personales y/o datos personales sensibles (fotografía o huellas dactilares) que obren en la CPV a través el Servicio de Verificación, las instituciones públicas, privadas y responsables de cualquier otro tipo, recabarán previamente el consentimiento, invariablemente, de manera expresa, conforme a lo previsto por las disposiciones legales en la materia. En cualquier caso, deberá recabarse de forma tal que conste en un documento o registro físico o digital, mismo que deberá ser trazable y verificable y deberá proporcionársele al INE, a petición de éste. La declaración en sentido

afirmativo podrá otorgarse a través de firma autógrafa o firma electrónica avanzada, que otorguen la misma certeza y seguridad dado que cumplen con los principios legales y características que se señalan en el presente Considerando, de modo que sea indubitable e inequívoca;

c) Ampliar los mecanismos de autenticación biométrica y promover el uso de la información contenida en los códigos de barras de los diferentes modelos de CPV vigentes, con el objetivo de brindar a las Instituciones servicios seguros de autenticación a través de medios digitales a las y los ciudadanos, cuando utilicen su CPV como medio de identificación, ya sea en la modalidad presencial o de atención vía remota, y

d) Desarrollar los mecanismos que permitan la verificación de las CPV emitidas por el INE, a través de los códigos de barras, para que las y los ciudadanos, así como las Instituciones, puedan corroborar su autenticidad en modalidades en línea o fuera de línea.

Dichas adecuaciones fortalecerán los mecanismos del Servicio de Verificación para facilitar a las y los ciudadanos la protección de sus datos personales, el acceso a los trámites y servicios, así como la prevención de posibles casos de usurpación o robo de identidad.

De esta manera, se estará contribuyendo para que los servicios que preste el INE sean más rápidos y de mejor calidad, sin dejar de atender en todo momento a los principios rectores del tratamiento y protección de datos personales que la normatividad aplicable establece.

Bajo esa línea, este Consejo General instruye a las áreas competentes del INE, en coordinación con la DERFE, a efecto de que se instrumenten las medidas necesarias para hacer del conocimiento público las adecuaciones para ampliar y fortalecer el Servicio de Verificación, referidas en el presente Acuerdo, con el objetivo de atender el principio de máxima publicidad que rige todas las actividades de este Instituto.

Finalmente, se considera oportuno que la DERFE informe mensualmente a la CRFE y a la CNV, sobre las verificaciones realizadas y los resultados obtenidos de la implementación de las adecuaciones para ampliar y fortalecer el Servicio de Verificación.

En virtud de lo señalado en las consideraciones anteriores, este Consejo General puede aprobar las adecuaciones para ampliar y fortalecer el Servicio de Verificación.

En razón de lo expuesto en las consideraciones de hecho y de derecho, este Consejo General en ejercicio de sus facultades emite los siguientes:

A C U E R D O S

PRIMERO. Se aprueba ampliar y fortalecer el Servicio de Verificación de Datos de la Credencial para Votar, conforme a lo establecido en el Considerando Tercero del presente Acuerdo, consistentes en:

1. Incorporar la modalidad de atención vía remota que podrán brindar las instituciones públicas, privadas o de otro tipo a la ciudadanía, mediante los Convenios de Apoyo y Colaboración en materia del Servicio de Verificación de Datos de la Credencial para Votar que al efecto celebren con el Instituto Nacional Electoral.

2. Para realizar el tratamiento de datos personales y/o datos personales sensibles (fotografía o huellas dactilares) que obren en la Credencial para Votar a través el Servicio de Verificación de Datos de la Credencial para Votar, las instituciones públicas, privadas y responsables de cualquier otro tipo, recabarán previamente el consentimiento, invariablemente, de manera expresa, conforme a lo previsto por las disposiciones legales en la materia. En cualquier caso, deberá recabarse de forma tal que conste en un documento o registro físico o digital, mismo que deberá ser trazable y verificable y deberá proporcionarse al Instituto Nacional Electoral, a petición de éste. La declaración en sentido afirmativo podrá otorgarse a través de firma autógrafa o firma electrónica avanzada, que otorguen la misma certeza y seguridad dado que cumplen con los principios legales y características que se señalan en la

parte considerativa del presente Acuerdo, de modo que sea indubitable e inequívoca.

3. Ampliar los mecanismos de autenticación biométrica y utilizar la información contenida en los códigos de barras de los diferentes modelos de Credenciales para Votar vigentes, con el objetivo de brindar a las instituciones públicas, privadas o de otro tipo servicios seguros de autenticación a través de medios digitales a las y los ciudadanos, cuando utilicen su Credencial para Votar como medio de identificación en la modalidad presencial o de atención vía remota.

4. Desarrollar los mecanismos que permitan la verificación de las Credenciales para Votar a través de los códigos de barras, para que la ciudadanía y las instituciones públicas, privadas o de otro tipo, puedan corroborar su autenticidad en modalidades en línea o fuera de línea.

SEGUNDO. Se instruye a la Dirección Ejecutiva del Registro Federal de Electores realice las acciones necesarias para la implementación de las adecuaciones para ampliar y fortalecer el Servicio de Verificación de Datos de la Credencial para Votar a que se refiere el Punto Primero del presente Acuerdo.

TERCERO. Se instruye a las áreas competentes del Instituto Nacional Electoral, bajo la coordinación de la Dirección Ejecutiva del Registro Federal de Electores, instrumenten las medidas necesarias para hacer del conocimiento público las adecuaciones para ampliar y fortalecer el Servicio de Verificación de Datos de la Credencial para Votar a que se refiere el Punto Primero del presente Acuerdo, así como hacer del conocimiento al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos lo aprobado en el presente Acuerdo por este órgano superior de dirección.

CUARTO. Se instruye a la Dirección Ejecutiva del Registro Federal de Electores informe mensualmente a la Comisión Nacional de Vigilancia y a la Comisión del Registro Federal de Electores, sobre las verificaciones realizadas y los resultados obtenidos de la implementación de las adecuaciones para ampliar y fortalecer el Servicio de Verificación de Datos de la Credencial para Votar a que se refiere el Punto Primero del presente Acuerdo.

QUINTO. Se instruye a la Dirección Ejecutiva del Registro Federal de Electores haga del conocimiento de las y los integrantes de la Comisión Nacional de Vigilancia lo aprobado por este órgano superior de dirección.

SEXTO. El presente Acuerdo entrará en vigor a partir de su aprobación por parte de este Consejo General.

SÉPTIMO. Publíquese el presente Acuerdo en la Gaceta Electoral y un extracto en el Diario Oficial de la Federación.

El presente Acuerdo fue aprobado en sesión extraordinaria del Consejo General celebrada el 15 de mayo de 2020, por votación unánime de los Consejeros Electorales, Doctora Adriana Margarita Favela Herrera, Doctor Ciro Murayama Rendón, Maestra Dania Paola Ravel Cuevas, Maestro Jaime Rivera Velázquez, Doctor José Roberto Ruiz Saldaña, Maestra Beatriz Claudia Zavala Pérez y del Consejero Presidente, Doctor Lorenzo Córdova Vianello.

EL CONSEJERO PRESIDENTE DEL CONSEJO GENERAL	EL SECRETARIO DEL CONSEJO GENERAL
DR. LORENZO CÓRDOVA VIANELLO	**LIC. EDMUNDO JACOBO MOLINA**