IFE
INSTITUTO FEDERAL ELECTORAL
REGISTRO FEDERAL DE ELECTORES

Programa de Actualización y Renovación de la Credencial para Votar

Proyecto del Servicio de Producción de Formatos de Credencial para Votar

Uso y Aplicación de los Códigos PDF 417, QR y de la Zona de Lectura Mecánica de la Credencial para Votar

Versión 1.8

Revisiones

Fecha	Versión	Descripción	Autor
07.03.2013	1.0	Creación del documento	Coordinación de Procesos Tecnológicos. Dirección de Productos y Servicios Electorales. Subdirección de Control de Información.
13.03.2013	1.1	Revisión y actualización del documento	Coordinación de Procesos Tecnológicos. Dirección de Productos y Servicios Electorales. Subdirección de Control de Información.
17.03.2013	1.2	Revisión y actualización del documento	Coordinación de Procesos Tecnológicos. Dirección de Productos y Servicios Electorales. Subdirección de Control de Información.
25.03.2013	1.3	Revisión y actualización del documento	Coordinación de Procesos Tecnológicos. Dirección de Productos y Servicios Electorales. Dirección de Desarrollo y Operación de Sistemas.
25.07.2013	1.4	Revisión y actualización del documento	Coordinación de Procesos Tecnológicos. Dirección de Productos y Servicios Electorales. Dirección de Desarrollo y Operación de Sistemas. Dirección de Infraestructura y Tecnología Aplicada
20.08.2013	1.5	Revisión y actualización del documento	Coordinación de Procesos Tecnológicos. Dirección de Productos y Servicios Electorales. Dirección de Desarrollo y Operación de Sistemas. Dirección de Infraestructura y Tecnología Aplicada. Dirección de Operaciones del CECYRD.
23.09.2013	1.6	Revisión y actualización del documento	Coordinación de Procesos Tecnológicos. Dirección de Productos y Servicios Electorales. Dirección de Desarrollo y Operación de Sistemas. Dirección de Infraestructura y Tecnología Aplicada. Dirección de Operaciones del CECYRD.
28.09.2013	1.7	Revisión y actualización del documento	Coordinación de Procesos Tecnológicos. Dirección de Productos y Servicios Electorales. Dirección de Desarrollo y Operación de Sistemas. Dirección de Infraestructura y Tecnología Aplicada. Dirección de Operaciones del CECYRD. Unidad Técnica de Servicios de Informática (UNICOM)
14.10.2013	1.8	Revisión y actualización del documento	Coordinación de Procesos Tecnológicos. Dirección de Productos y Servicios Electorales.

Contenido

1. Presentación.

Conforme a lo establecido por el artículo 128 del Código Federal de Instituciones y Procedimientos Electorales (COFIPE), la Dirección Ejecutiva del Registro Federal de Electores (DERFE) es la instancia del Instituto Federal Electoral que tiene entre otras atribuciones, el formar el Padrón Electoral, expedir la Credencial para Votar, revisar y actualizar el Padrón Electoral, proporcionar a los órganos competentes del Instituto y a los Partidos Políticos Nacionales (PPN) las Listas Nominales de Electores, mantener actualizada la Cartografía Electoral del país, asegurar que las comisiones de vigilancia nacional, estatales y distritales se integren, sesionen y funcionen en los términos del COFIPE.

Asimismo, y con relación al Acuerdo del Consejo General 732/2012, aprobado el 21 de noviembre de dos mil doce,en el cual se instruye a la DERFE presentar para su aprobación al Consejo General a través de la Comisión del Registro Federal de Electores (CRFE), la función de los códigos de barras bidimensionales, mediante archivo portátil de datos, tipo 417, (PDF-417), de almacenamiento y acceso rápido (QR), así como la zona de lectura mecánica (ZLM), y la función deberá ser previamente conocida y evaluada por la Unidad de Servicios de Informática, para emitir un Dictamen de factibilidad.

Adicionalmente, y con base en el documento denominado "*Servicios de Valor Agregado para los Organismos Públicos y Privados, Uso y Aplicación de los Códigos de Barras en la Credencial para Votar, Plan Estratégico Institucional 2012-2015, Definición del Proyecto, Versión 1*", y a partir de las observaciones que se han realizado al mismo, se definió la construcción del presente documento, el cual considera algunos aspectos adicionales como son las necesidades de los códigos de barras y la ZLM, así como el contenido de la información de dichos elementos de almacenamiento para proporcionar los servicios identificados mediantes dichos códigos de acceso rápido de la información.

En este sentido, este documento se compone de varias secciones de tal manera que facilite su comprensión, asimismo su estructura es de carácter evolutivo y adaptativo, es decir, que a través de las diversas observaciones, sugerencias y/o propuestas se actualiza y se enriquece con el fin de cumplir el objetivo para el que fue creado.

Para tal efecto, este documento se conforma de 7 apartados en donde cada uno de ellos aborda lo siguiente:

En el primer apartado, que refiere a la Presentación, la cual pretende describir de forma general el origen y fundamento del presente documento.

En el apartado 2, se describe el objetivo del documento.

En el apartado 3, se atiende lo relativo al alcance del planteamiento desde los ámbitos normativo, tecnológico, organizacional, temporal y operacional.

En el apartado 4, se hace referencia al marco normativo y jurídico que da soporte al planteamiento que se presenta en el presente documento.

En el apartado 5, se hace referencia al contenido e información que tendrán los códigos de barras y la Zona de Lectura Mecánica que se integrarán a la Credencial para Votar, así como lo relativo a la tecnología identificada para la protección de la información,

En el apartado 6, se describen las áreas de oportunidad identificadas, así como el uso y aplicación de los códigos y de la zona de Lectura Mecánica de la Credencial para Votar.

Y finalmente, en el apartado 7, se especifica el Glosario de Términos y Acrónimos que son utilizados en el presente documento.

2. Objetivo.

Presentar el contenido y las funcionalidades que tendrán los códigos de acceso a información de manera rápida correspondiente al PDF 417 y QR, así como de la Zona de Lectura Mecánica que forman parte del nuevo modelo de la Credencial para Votar con el fin de poder en su caso agilizar la lectura de la información contenida en la Credencial para Votar.

3. Alcance.

El alcance del documento considera los ámbitos tecnológico, organizacional, normativo, temporal y operacional.

Tecnológico. Se considera mediante dispositivos electrónicos, realizar la lectura de los diversos códigos de la credencial, desarrollando los servicios necesarios para la verificación de la Credencial para Votar, así como mediante el uso de la Solución Integral de Identificación Multibiométrica, orientando los servicios en el contexto del Modelo Integral de Procesos garantizando la seguridad de la información en todo momento.

Organizacional. Se considera que la instrumentación de estos servicios tendrá influencia en la estructura organizacional, mediante la integración y formalización de los grupos de trabajo para el desarrollo e instrumentación de las actividades.

Normativo. Se considera atender el marco normativo procedimental para las actividades relacionadas con la definición y validación de las acciones a instrumentar para el desarrollo e instrumentación de los servicios a través del uso de los códigos de barras.

Temporal. Las actividades a realizar están planteadas con un enfoque en el contexto de la Planeación Estratégica de la DERFE para el periodo 2012-2015.

Operacional. La instrumentación de las actividades permitirá obtener información de apoyo para una toma de decisiones proactiva que favorezca la efectividad administrativa y organizacional.

4. Marco Normativo.

El artículo 6 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), señala en su fracción I que toda información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

En su fracción II, se menciona que la información que refiere a la vida privada y los datos personales, será protegida en los términos y con las excepciones que fijen las leyes.

En su fracción III, se establece que toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

En su fracción IV, se establecerán los mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y decisión.

En su fracción V, refiere que los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

En su fracción VI, se establece que las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

Asimismo, el artículo 41, en su fracción III de la CPEUM, señala que el Instituto Federal Electoral tendrá a su cargo en forma integral y directa, además de las que determine la ley, las actividades relativas al Padrón Electoral y Lista Nominal de Electores.

Por otro lado, en el artículo 105 párrafo 2 del COFIPE, refiere los principios rectores de *Certeza, Legalidad, Independencia, Imparcialidad* y *Objetividad* del Instituto Federal Electoral para llevar a cabo sus actividades dentro de las cuales están la actualización y depuración del Padrón Electoral.

En este contexto, la DERFE, es un órgano ejecutivo de la Junta General Ejecutiva del Instituto Federal Electoral, de carácter central, que se encarga en términos generales de la actualización y depuración del Padrón Electoral, de la expedición de la Credencial para Votar con Fotografía y de la emisión de las Listas Nominales de Electores, así como mantener actualizada la Cartografía Electoral del país, clasificada por entidad, distrito electoral federal,

municipio y sección electoral.

De igual manera el ordenamiento legal antes citado establece en su artículo 128, las atribuciones de la DERFE dentro de las cuales, se encuentran las vinculadas a la actualización y depuración del Padrón Electoral:

- Formar el Padrón Electoral.
- Revisar y actualizar anualmente el Padrón Electoral conforme al procedimiento establecido en el Capítulo Tercero del Título Primero del Libro Cuarto del COFIPE.
- 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.
- Proporcionar a los órganos competentes del Instituto y a los Partidos Políticos nacionales, las listas nominales de electores en los términos de este Código.
- Mantener actualizada la Cartografía Electoral del país, clasificada por entidad, distrito electoral federal, municipio y sección electoral.
- Asegurar que las comisiones de vigilancia nacional, estatales y distritales se integren, sesionen y funcionen en los términos previstos por este Código.
- 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.

Adicionalmente, el COFIPE en su artículo 171 párrafo 3 refiere.

> *"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 este Código, serán estrictamente confidenciales y no podrán comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en que el Instituto Federal Electoral fuese parte, para cumplir con las obligaciones previstas por este Código en materia electoral y por la Ley general de Población en lo referente al Registro Nacional Ciudadano o por mandato de juez competente."*

De la misma forma, en el artículo 171 párrafo 4 refiere que:

"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 artículo 181 párrafo 4 refiere lo siguiente.

"La Dirección Ejecutiva del Registro Federal de Electores proveerá lo necesario para que las listas nominales se pongan en conocimiento de la ciudadanía en cada distrito."

Por otro lado, el artículo 192 del COFIPE señala que:

"1. En cada Junta Distrital, de manera permanente, el Instituto pondrá a disposición de los ciudadanos los medios para consulta electrónica de su inscripción en el padrón electoral y en las correspondientes listas nominales, conforme a los procedimientos que determine la Dirección Ejecutiva del Registro Federal de Electores.

2. Los partidos políticos tendrán acceso en forma permanente a la base de datos del padrón electoral y las listas nominales, exclusivamente para su revisión, y no podrán usar dicha información para fines distintos."

En el artículo 196 del COFIPE se señala lo siguiente.

"1. Que los partidos políticos contarán en el Instituto con terminales de cómputo que les permitan tener acceso a la información contenida en el padrón electoral y en las listas nominales de electores. Igualmente y conforme a las posibilidades técnicas, los partidos políticos tendrán garantía de acceso permanente al contenido de la base de datos, base de imágenes, documentos fuente y movimientos del padrón, exclusivamente para su revisión y verificación.

2. De igual manera, la Dirección Ejecutiva del Registro Federal de Electores instalará centros estatales de consulta del padrón electoral para su utilización por los representantes de los partidos políticos ante las comisiones locales de vigilancia, y establecerá además, mecanismos de consulta en las oficinas distritales del propio Registro, a los cuales tendrá acceso cualquier ciudadano para verificar si está registrado en el padrón electoral e incluido debidamente en la lista nominal de electores que corresponda."

Además es conveniente señalar que, en el Acuerdo del Consejo General CG307/2008, el cual refiere el Reglamento del Instituto Federal Electoral en materia de Transparencia y Acceso a la Información Pública (Reglamento), se tiene por objeto establecer los órganos, criterios y procedimientos institucionales para garantizar a toda persona los derechos fundamentales de acceso a la información pública y de protección a los datos personales en posesión del Instituto Federal Electoral y de los partidos políticos.

Por tal motivo, se considera que se deben favorecer los principios de máxima publicidad de la información en posesión del Instituto; de gratuidad y mínima formalidad; de facilidad de acceso y de exhaustividad en la búsqueda y entrega de la información.

Con base en lo anterior, a continuación se hace referencia a algunos de los puntos que se consideran importantes con relación a los planteamientos que se describen en el presente documento.

- Algunas de las obligaciones de transparencia del Instituto referentes a la información a disposición del público que debe difundir, a través de su página de Internet, sin que medie petición de parte son:

  - ✓ Los servicios que ofrece el Instituto deben incluir al menos aquellas actividades que realizan las Unidades Técnicas y Direcciones Ejecutivas y que ofrecen al público en general.

  - ✓ La información socialmente útil o aquella que se considere relevante, que generen los órganos responsables del Instituto y apruebe el Comité de Gestión y Publicación Electrónica, misma que se publicará en un apartado especial del portal de *internet* del Instituto.

- La difusión de la información a disposición del público en general deberá publicarse de manera que se facilite su uso y comprensión y se asegure su calidad, veracidad, oportunidad y confiabilidad. Dicha información estará disponible a través de medios de comunicación electrónica del Instituto.

- Toda la información en poder del Instituto será pública y sólo podrá considerarse reservada o confidencial la prevista en el Artículo 10 de dicho Reglamento.

- Referente a este Reglamento es importante señalar que como información confidencial se considerará:

  - ✓ La entregada con tal carácter por los particulares al Instituto incluyendo la relativa al Registro Federal de Electores.

  - ✓ Los datos personales que requieran el consentimiento de los individuos para su difusión en términos de las disposiciones legales aplicables.

- La información del Instituto que no se encuentre clasificada como reservada o confidencial, deberá ser puesta a disposición del público a través del portal de internet del Instituto, o mediante solicitudes de acceso a la información, o bien, a través de los servicios de orientación que realiza IFETEL por medio de consultas telefónicas.

Por otro lado, y respecto a la Credencial para Votar que en el último recuadro se encuentre con 03, se tiene que:

Conforme a lo dispuesto por el artículo 200, párrafo 4 y Octavo Transitorio del Código Federal de Instituciones y Procedimientos Electorales y lo resuelto por el Consejo General del Instituto, los días 7 de julio y 14 de septiembre de 2010, y por el Tribunal Electoral del Poder Judicial de la Federación, en el Recurso de Apelación SUP-RAP-109/2010, el pasado 25 de agosto de 2010, dice que las Credenciales para Votar "03" no se pueden utilizar legalmente como medio de identificación de los ciudadanos a partir del 1 de enero de 2011, con excepción de los estados de Guerrero, Baja California Sur, Hidalgo, Coahuila, México, Nayarit y Michoacán. En estas entidades federativas las credenciales "03" perderán su cualidad legal como medio de identificación y como documento para ejercer el derecho al voto en forma sucesiva, conforme a las fechas definidas para cada proceso electoral local en el año 2011.

Adicionalmente existe otro universo de credenciales denominadas "09" y "12" para las cuales el 21 de noviembre de 2012 el Consejo General del Instituto mediante el Acuerdo CG712/2012, delimitó la vigencia hasta el 31 de diciembre de 2013 de estas credenciales. El acuerdo indica que los registros de los titulares de las credenciales para votar que tengan como recuadros para el marcaje del año de la elección federal 00 03 06 09, denominadas "09", y 12 03 06 09, llamadas "12", serán excluidos de la Lista Nominal de Electores a partir del 1 de enero de 2014. Esto equivale a 11 millones de credenciales lo cual representa el 13.8% de la Lista Nominal de Electores. Las credenciales "09" y "12" serán vigentes en el 2014 únicamente en las entidades con Procesos Electorales Locales y hasta el día establecido para su Jornada Electoral.

Considerando lo anterior, se observa la necesidad de implementar elementos de control y de acceso rápido a la información de la Credencial para Votar que permitan promover y difundir

los diversos servicios electorales que proporciona el Instituto, a fin de facilitar el acercamiento del ciudadano con la institución y atendiendo lo establecido en el marco jurídico, normativo y procedimental, contribuyendo con ello, en la generación de valor público de la institución.

5. Contenido de los Códigos y de la ZLM de la Credencial para Votar.

5.1 Información en los Códigos y de la ZLM.

A continuación se describe lo relativo a la información que estará contenida en los códigos bidimensionales PDF 417 y QR, así como en la Zona de Lectura Mecánica de la Credencial para Votar,

a) Código de barras unidimensional Tipo 128.

Figura 1. Código de barras unidimensional tipo 128.

El tamaño y la información a incorporar a este código es la siguiente.

Capacidad del código unidimensional 4 X 12.4 mm: 10 bytes

Dato	Visible en la Credencial para Votar	Tamaño en Bytes	Tipo de elemento
Código de Identificador de Credencial (CIC)	No	10	Control

Tabla 1. Contenido del Código tipo 128.

Este código proporciona a la Credencial para Votar la unicidad en su producción, toda vez que es único y asignado desde la creación del archivo para la producción de las credenciales.

b) Código bidimensional tipo PDF-417.

Con la evolución tecnológica de los dispositivos de lectura de códigos de barras, se ha conseguido que para la generación del código bidimensional tipo PDF-417, se pueda incorporar más información que la que se tiene actualmente en la Credencial para Votar (Tipo C), y que ésta sea leída e interpretada de forma rápida y adecuada.

Con la incorporación de las minucias completas de una huella dactilar a la Credencial para Votar, se proporciona mayor certeza para los servicios de autenticación de los ciudadanos

mediante mecanismos biométricos, las minucias de la biometría de la huella a incorporar será del Tipo ANSI-INCITS 378.

Dato	Visible en la Credencial para Votar	Tamaño en Bytes
Las minucias de una huella dactilar	No	600
Edad	No	3
CURP	Sí	18
Clave de Elector	Sí	18
CIC	Sí	9
OCR	Sí	15
Nombre	Sí	32
Apellido Paterno	Sí	32
Apellido Materno	Si	32
Calle, Num. Ext., Num Int.	No u Opcional a solicitud del ciudadano	40
Colonia y Código Postal	Si	40
Nombre de Municipio	Sí	40
Estado	Sí	2
Municipio	Sí	3
Localidad	Si	4
Año de registro	Sí	4
Emisión	Si	4
Vigencia Hasta	Sí	4
Dígitos Verificadores de ZLM	Sí	4
Consecutivo FUAR	Sí	5

Tabla 2. Contenido del Código tipo PDF-417

Por otro lado, y para la corrección de errores para este tipo de códigos, se establecen 9 niveles (0 al 8), este nivel se utiliza para establecer redundancia de la información codificada, para que en caso de que se deteriore por manchas o roturas se pueda recuperar al máximo.

Este nivel es considerado al generar el código PDF 417, sin embargo, para el caso del PDF 417 que será integrado a la Credencial para Votar, el valor del nivel a utilizar estará sujeto al volumen de la información almacenada, ya que existe una limitante para el almacenamiento, tomando en cuenta que la información será cifrada y estará generada en bytes.

No obstante lo anterior, actualmente se han hecho pruebas y se han generado PDF 417 con niveles 0, 1 y 2, los cuales están siendo analizados para determinar el nivel más adecuado que llevará el PDF 417 de redundancia para realizar su lectura. Se está considerando integrar un nivel de corrección que permita la mayor recuperación en caso de daño de dicho código, toda vez que la Credencial para Votar tendrá una vida útil de 10 años, sin embargo esto estará supeditado al tamaño de la información a almacenar en el dispositivo.

c) Código bidimensional tipo QR.

El Código bidimensional tipo QR, tendrá una dimensión de 12 mm por 12 mm, y en el cual se integrarán los datos de acceso rápido que permitan el acceso a páginas *WEB*, con el fin de que el ciudadano pueda verificar el estatus de su situación registral, así como algunos otros servicios que se proporcionarán en materia electoral, como por ejemplo: el domicilio del módulo más cercano o la ubicación de la casilla electoral el día de la Jornada Electoral, entre otros.

Dato	Visible en la Credencial para Votar	Tamaño en Bytes
qr.ife.org.mx *(url)*	No	46
OCR	Si	15
CIC	Si	9

Tabla 3. Contenido del Código tipo QR.

Se ha valorado que con el uso de los datos del OCR como identificador del ciudadano y el CIC como identificador de la credencial, se cuenta con todos los elementos para proporcionar los servicios relacionados con la situación registral del ciudadano, determinando la vigencia de su credencial y algunos otros servicios web. Estos datos no son confidenciales y se encontraran en claro dentro de dicho código.

En este sentido, y considerando que los dispositivos móviles (*Smartphone*, tabletas y laptops) cuentan con aplicaciones diversas para la lectura de códigos QR y acceso a Internet, la demanda de estos servicios se estará incrementando con el tiempo.

Como los servicios estarán basados con el acceso a una página *WEB*, el *url* o dominio no podrán ser cambiados o alterados durante el periodo de la vigencia de la Credencial.

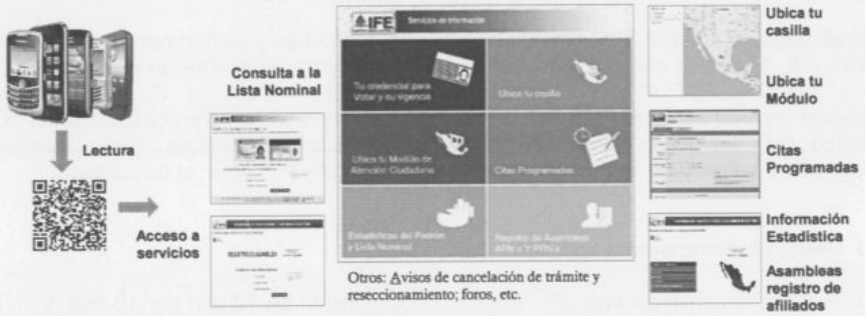


Figura 2. Acceso a Servicios *Web* mediante el código QR de lectura rápida.

Los sistemas y aplicaciones que se generen para brindar estos servicios deberán ser desarrollados por la DERFE y se apegarán a las directrices de seguridad establecidas por la UNICOM determinando que no existen vulnerabilidades de seguridad y garantizando que no existen riesgos en la publicación de los servicios para acceder a la información.

Para la corrección de errores para este tipo de códigos, se establecen 4 niveles (L, M, Q y H), este nivel se utiliza para establecer redundancia de la información codificada, para que en caso de que se deteriore por manchas o roturas se pueda recuperar al máximo. Este nivel es considerado al generar el código QR, considerando como mínimo un nivel M con un 15 % de redundancia hasta el nivel H con un máximo de 30% de redundancia.

d) Zona de Lectura Mecánica

La Zona de Lectura Mecánica se integra a la Credencial para Votar de acuerdo a las especificaciones técnicas de los documentos de viaje oficiales de lectura mecánica normada por el estándar de ICAO (Organización Internacional de Aviación Civil), el cual se puede consultar en la siguiente *url:*

http://www.icao.int/publications/Documents/9303_p3_v1_cons_es.pdf.

La información que se incorporará a la Credencial para Votar atiende lo que establece el estándar de la ICAO y en particular al documento *9303, parte 3 Documentos de viaje oficiales de lectura mecánica (MRTD), volumen 1 MRTD con datos de lectura mecánica*

almacenados en formato de reconocimiento óptico de caracteres, sección IV apartados del 1 al 18, con los apéndices 1 al 14 y sección V apartado 6 conforme a lo siguiente:

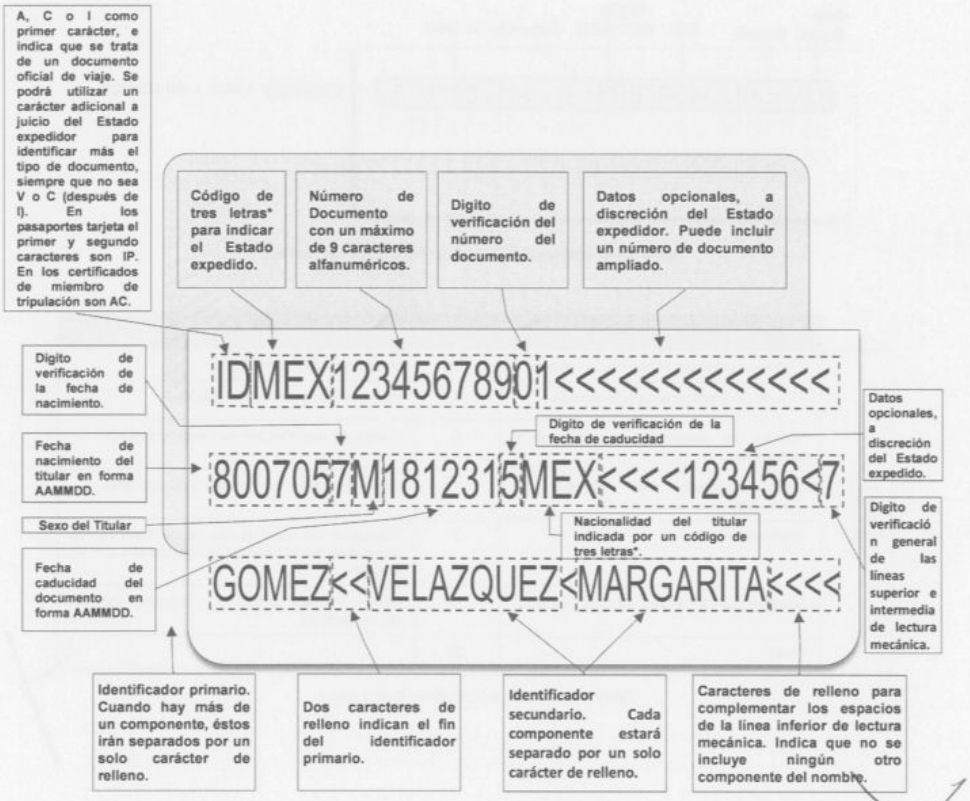


Figura 3. Estándar ICAO, información en la Zona de Lectura Mecánica

Contenido de la primera linea de la Zona de Lectura Mecánica.

Figura 4. Descripción de la Zona de Lectura Mecánica, Línea 1

	Estándar ICAO	Tamaño	Datos
Línea 1 del Código	2 letras para indicar el tipo de documento	2	Documento tipo Identificación
	3 letras para indicar el estado expeditor	3	País que lo expide México (MEX)
	Número de documento en máximo 9 caracteres	9	Código de Identificación de Credencial (CIC)
	Dígito verificador del Número de Documento	1	Dígito verificador del Número de Documento
	Separadores "<"	2	Separador de datos (el uso de los separadores dependerá del tamaño de la información que se integre)
	Datos opcionales a favor del país expedidor	13	OCR (13 dígitos, sección y consecutivo nacional del ciudadano)
	Total	**30**	

Tabla 4. Contenido del Código de ZLM, Línea 1.

Contenido de la segundalinea de la Zona de Lectura Mecánica.

Figura 5. Descripción de la Zona de Lectura Mecánica, Línea 2

	Estándar ICAO	Tamaño	Datos
Línea 2 del Código	Fecha de nacimiento (AAMMDD)	6	Fecha de nacimiento del ciudadano
	Dígito verificador de la fecha de nacimiento	1	Dígito verificador de la fecha de nacimiento del ciudadano
	Sexo	1	Sexo del ciudadano
	Fecha de caducidad (AAMMDD)	6	Fecha de Vigencia (YY1231)
	Dígito verificador de la fecha de caducidad	1	Dígito verificador de la fecha de vigencia
	Nacionalidad (código de 3 letras)	3	Nacionalidad del Ciudadano (MEX)
	Datos opcionales a favor del país expeditor	9	OCR (Dos dígitos para el número de emisión) y 5 dígitos del FUAR
	Dígitoverificador de las dos primeras líneas	1	Dígito verificador de la línea 1 y línea 2
	Separadores "<"	2	Separador de datos (el uso de los separadores dependerá del tamaño de la información que se integre)
	Total	**30**	

Tabla 5. Contenido del Código de ZLM, Línea 2.

Contenido de la tercera línea de la Zona de Lectura Mecánica.

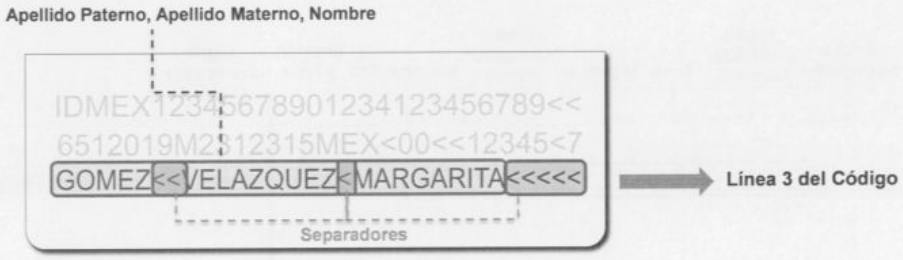


Figura 6. Descripción de la Zona de Lectura Mecánica, Línea 3

	Estándar ICAO	Tamaño	Datos
Línea 3 del Código	Identificador primario (apellido paterno)	7	Apellido paterno del ciudadano
	Identificador secundario (apellido materno y nombre)	19	Apellido Materno y nombre del ciudadano
	Separadores "<"	4	Separador de datos (el uso de los separadores dependerá del tamaño de la información que se integre)
	Total	**30**	

Tabla 6. Contenido del Código de ZLM, Línea 3.

Cabe mencionar que, además de que la Zona de Lectura Mecánica (ZLM), se construye en base a las recomendaciones del ICAO (Organización Internación de Avicación Civil), también la Credencial para Votar considera en su conjunto, atiende las recomendaciones que hace el propio ICAO para prevenir y mitigar las amenazas de seguridad en cada paso del proceso para la emisión de la Credencial para Votar, los cuales se describen en la *Guide for Assessing Security of Handling and Issuance of Travel Documents*.

Para tal efecto, desde las características físicas, técnicas, seguridad, resistencia al ataque, entre otros cumple con dichas recomendaciones, así como al proceso de fabricación y personalización es de alta seguridad, se cuenta con estrictos controles se seguridad de la información, alta seguridad del sitio en donde se personalizará el documento, existe un estricto control de materiales e insumos, destrucción de los merma, almacenes seguros, control de acceso, cumpliendo con las recomendaciones de dicho Organismo Internacional.

Finalmente, los servicios de valor agregado, de los Códigos y de la ZLM mencionados anteriormente, estarán apegados a los lineamientos para el acceso, rectificación, cancelación, oposición y validación de datos personales en posesión de la DERFE, por lo que al tratarse de información confidencial la respuesta de los servicios será de forma binaria, esto es de si se cuenta o no con la información, no proporcionando información de esta índole bajo ninguna circunstancia.

5.2 Tecnologías para la protección de la información

Para garantizar el resguardo de la información en la Credencial para Votar a almacenar en el Código PDF-417, se han identificado algunas formas para cifrar la información, producto de esto se definió la utilización de uno de los esquemas de cifrado para la información que está clasificada como confidencial, este cifrado se conoce como cifrado simétrico, el cual permite ocultar la información y la llave que es utilizada para cifrar la información, es la misma que se utiliza para descifrar la información, por lo que el Instituto sería el único ente para acceder a la información, de manera que solo pueda ser utilizado para los servicios dentro del Instituto, toda vez que que uno de los estándares internacionales más utilizados en este tipo de procesos de seguridad es el conocido como Advanced Encryption Standard (AES), se utilizará dicho algoritmo con un tamaño de llave de 256 bits.

Para este caso, el tamaño de la información que será cifrada por medio del algoritmo simétrico es similar a la información ya cifrada, es decir, no existe un incremento significativo en el volumen de información al utilizar este tipo de cifrado.

Otro de los esquemas considerados para el cifrado de la información, son los algoritmos asimétricos, los cuales consideran el uso de llaves para el manejo de la información, es decir, se utiliza una sola llave para el cifrado, misma que es distinta a la utilizada para realizar el descifrado para poder acceder a los datos, lo que permite garantizar y certificar al generador de la información, toda vez que, se verifica que la información que contiene el medio de almacenamiento fue generada por el dueño de la misma.

En este sentido, solo podrán acceder a la información las entidades autorizadas, sin embargo, el tamaño de este tipo de cifrado se incremente entre el 10% y el 33% con respecto al tamaño de la información a cifrar y depende del tamaño de la robustez de la llave que se considere utilizar (…512, 1024, 2048, 4096…).

Asimismo, y derivado de la conveniencia de poder compartir la llave de acceso a los datos, y que la robustez de los algoritmos asimétricos proporcionan mayor seguridad que los algoritmos simétricos y que los servicios prestados no dependerían de una conexión permanente con el Instituto.

Por todo lo anterior, se determina que el contenido del código PDF-417, se llevará a cabo con un cifrado asimétrico integrado por los datos visibles de la Credencial para Votar, y un cifrado simétrico para la minucia del ciudadano correspondiente y los datos del domicilio correspondientes a la calle, número exterior, número interior, colonia y código postal, tal y como se muestra en la siguiente tabla.

Dato	Tipo de Cifrado
Las minucias de una huella dactilar	Simétrico
Edad	Asimétrico
CURP	Asimétrico
Clave de Elector	Asimétrico
CIC	Asimétrico
OCR	Asimétrico
Nombre	Asimétrico
Apellido Paterno	Asimétrico
Apellido Materno	Asimétrico
Calle, Num. Ext., Num Int.	Simétrico
Colonia y Código Postal	Simétrico

Dato	Tipo de Cifrado
Nombre de Municipio	Asimétrico
Estado	Asimétrico
Municipio	Asimétrico
Localidad	Asimétrico
Año de registro	Asimétrico
Emisión	Asimétrico
Vigencia Hasta	Asimétrico
Dígitos Verificadores de ZLM	Asimétrico
Consecutivo FUAR	Asimétrico

Tabla 7. Cifrado del PDF-417 por dato.

La información a integrar en el código PDF-417 de la Credencial para Votar, estará almacenada por los datos de forma posicional, es decir, que el bloque de datos correspondientes a la Credencial para Votar ocupará el mismo espacio al ser codificadas, y la minucia será el último dato a ser resguardado, por lo que en caso de ser menor a 600 bytes, se rellenará por espacios, y en caso de ser mayor esta se ajustará al tamaño correspondiente.

Adicionalmente, y con el fin de instrumentar las acciones para la incorporación de la información al código PDF 417, se realizaron pruebas de cifrado a través de los algoritmos antes señalados.

Para tal efecto, se realizaron las pruebas para determinar el crecimiento proporcional de las cadenas utilizando el cifrado asimétrico, por lo que se establecieron las siguientes condiciones:

- Las cadenas de datos que se utilizaron fueron de 1155 bytes
- Se utilizó el algoritmo RSA, el cual se encuentra reconocido como uno de los métodos para la generación de firmas electrónicas por el *National Institute of Standards and*

Technology (NIST), del mismo modo es señalado para la autenticación en conexiones *SFTP* en los Estándares Federales de Procesamiento de la Información (FIPS por sus siglas en inglés)

- Se utilizó en todos los casos *encoding* ISO 8859-1 para el manejo de símbolos y caracteres especiales.

Como resultado de las pruebas se obtuvo lo siguiente:

	Tamaño de Llave		
	1024 bits	2048 bits	3072 bits
	Tamaño de la Cadena de Datos (bytes)	*Tamaño de la Cadena de Datos (bytes)*	*Tamaño de la Cadena de Datos (bytes)*
Registro Original	**1155**	**1155**	**1155**
Cifrado Asimétrico Único (CAU)	**1280**	**1280**	**1536**
Porcentaje de incremento	**10.82%**	**10.82%**	**32.99%**
Tiempo promedio descifrado	0.002 seg.	0.003 seg.	0.004 seg.

Tabla 8. Resultados de las pruebas de cifrado asimétrico único.

Como se puede observar, el tamaño de la cadena de datos se incrementa significativamente para el uso de una llave de 3072 bits, lo cual tiene como principal limitante el espacio que ocupará en la capacidad del PDF 417 de la Credencial para Votar.

En este sentido, diversas instituciones de reconocimiento internacional como la "*National Institute of Standards and Technology (NIST)*" y la "*EMC Corporation*" a través de su rama de investigación en seguridad de redes y cómputo la "*RSA Security LLC*", recomiendan que el tamaño mínimo de la llave para algoritmos de cifrado asimétrico sea de 1024 bits en contextos corporativos para garantizar una robustez mínima de seguridad y de 2048 bits en contextos de resguardo con información altamente sensible.
Con base en el comportamiento identificado en las pruebas y los criterios proporcionados por las instituciones mencionadas, se determina que la codificación y cifrado de la información de los datos de la Credencial para Votar a integrar en el código bidimensional tipo PDF 417, se realizará con un algoritmo de cifrado asimétrico con una llave de 2048 bits.

Adicionalmente, y para la generación y resguardo de las llaves para el cifrado y descifrado de la información, se desarrollará un protocolo que permita asegurar y garantizar el buen uso de las mismas, en el cual se establecerán los roles, responsabilidades, así como la forma en que se protegerán las mismas.

Para tal efecto, se está considerando que no exista un solo servidor para la generación de las llaves que conforman la información del Código PDF-417; sino en dos servidores

separados, es decir, sólo se encontraran en cada servidor los parámetros de inicialización para crear la llave, misma que será creada de manera dinámica sin que viaje a través de la red cada que se realicé una consulta a un componente conocido como "Custodio".

El acceso a dicho componente se encontrará restringido y solo podrá acceder otro componente que sea invocado a través del SIIRFE. Del mismo modo, del lado de dicho aplicativo que tiene acceso al "Custodio" se tendrá un archivo con las credenciales de acceso cifradas, las cuales serán el complemento para la generación de la llave, dichas credenciales se encontraran cifradas a través de sistema.

En un servidor se tendrá el Custodio y el archivo con los parámetros para la inicialización de las llaves (*Keystore*), mientras que en otro servidor independiente, se tendrá el componente que realizará las peticiones y las credenciales de acceso cifradas. Para el caso del primer servidor, una entidad tendrá acceso y responsabilidad sobre el mismo pero no podrá acceder al segundo servidor; y de manera inversa habrá una entidad con acceso y responsabilidad para custodiar el segundo servidor, pero no podrá acceder al primero con la excepción del componente destinado para dicho fin.

La generación de la *keystore* y las credenciales cifradas en el ambiente productivo se hará de manera única y posteriormente quedará inhabilitada dicha funcionalidad.

En el siguiente Diagrama se describe de manera general la operación del protocolo para cifrado y descifrado de la información considerando los algoritmos simétrico y asimétrico.

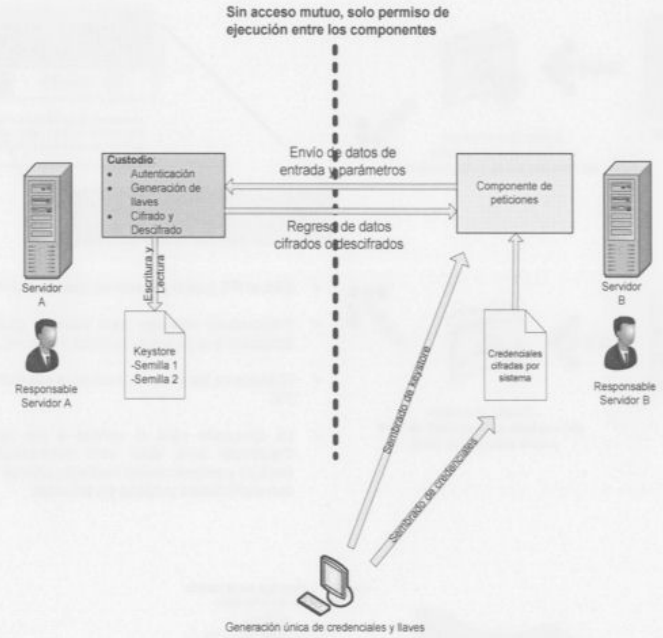
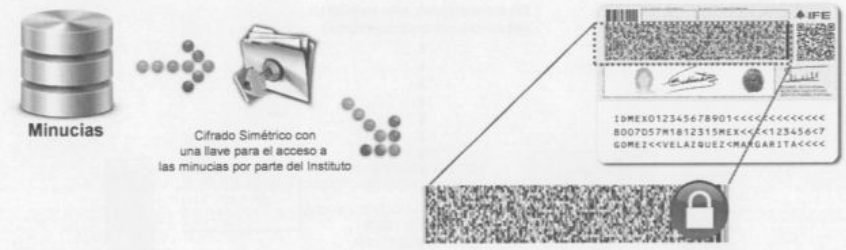
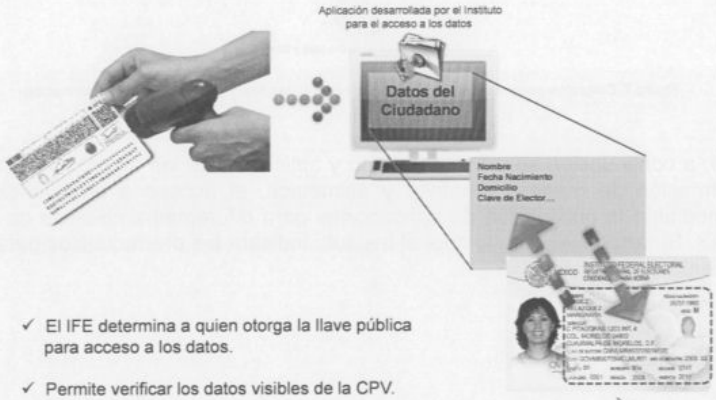


Figura 7. Diagrama general de operación del protocolo para cifrado y descifrado de la información

Finalmente, a continuación se presenta el uso y aplicación de los algoritmos para el cifrado de la información de manera simétrica y asimétrica, el acceso a esta funcionalidad se realizara mediante la publicación de aplicaciones para diferentes ambientes de trabajo PC, MAC, *PDA's*, Smartphone, para lo cual el Instituto indicará los prerrequisitos para el correcto funcionamiento de la misma.



- ✓ Sólo el IFE puede generar los datos en el PDF417.
- ✓ Proporcionar servicios para aquellos ciudadanos o entidades que no tengan acceso a Internet.
- ✓ El acceso a las minucias será para uso exclusivo del IFE.
- ✓ La aplicación para el acceso a los datos de la Credencial para Votar será desarrollada por el Instituto y proporcionada mediante previos convenios con instituciones publicas y/o privadas.



- ✓ El IFE determina a quien otorga la llave pública para acceso a los datos.
- ✓ Permite verificar los datos visibles de la CPV.

Figura 8. Uso y aplicación del PDF 417 mediante el tipo de cifrado.

6. Aplicación de los Códigos y de la ZLM de la Credencial para Votar.

A continuación se describen los planteamientos y requerimientos que se han identificado para el uso de los códigos de acceso rápido a la información, así como la Zona de Lectura Mecánica conforme a las atribuciones del Instituto Federal Electoral, y en particular a la relación que tiene la Institución con la sociedad, considerando los elementos contenidos en la Credencial para Votar mediante las aplicaciones desarrolladas para este fin.

a) Verificación de Afiliados para el registro de Agrupaciones y Partidos Políticos.

La Dirección Ejecutiva de Prerrogativas y Partidos Políticos (DEPPP), la Unidad Técnica de Servicios de Informática (UNICOM) y la DERFE definieron e implementaron un esquema para la verificación de los participantes en las asambleas estatales y distritales relacionadas con las agrupaciones que pretenden constituirse como partido político. Para cumplir con dicho fin se instrumentó la verificación de la Credencial para Votar del ciudadano que la porta, mediante la lectura del Código de Identificación de Credencial que está contenido en el código de barras unidimensional tipo 128, lo que permite realizar la verificación de la información del ciudadano en la base de datos del Padrón Electoral. Adicionalmente, y con la incorporación del código de Acceso Rápido (QR por sus siglas en inglés) será posible hacer más eficientes los procesos de registro en mención.

b) Urna electrónica.

El Instituto ha instrumentado una serie de iniciativas para revisar la factibilidad de llevar a cabo el proceso del voto electrónico. Para tal fin se han realizado algunos ejercicios con urnas electrónicas por parte de la Dirección Ejecutiva de Organización Electoral (DEOE), sin embargo, es necesario complementar los ejercicios realizados con el registro de los ciudadanos a través de una lista nominal electrónica, y para este caso será necesario realizar la verificación de la Credencial para Votar mediante los elementos informáticos que permitan determinar que el ciudadano que presenta la Credencial para Votar, es el mismo que aparece en la misma (autentificación del ciudadano a través de comparaciones y/o validaciones de los datos de la Credencial para Votar, de los datos del ciudadano, y de la información biométrica).

La expectativa del voto electrónico está supeditada directamente a la confianza que se pueda transmitir a los partidos políticos y a la ciudadanía, por lo que se hace esencial promover los mecanismos y procedimientos que permitan proporcionar certeza y legalidad para el ejercicio del voto, así como implementar una plataforma que pueda ser utilizada por los funcionarios de casilla en la jornada electoral para atender las funciones encomendadas.

c) Servicios de información

La DERFE está analizando la factibilidad de acercar los servicios de atención ciudadana a los ciudadanos, por lo que tiene considerado la implementación de servicios electrónicos que permitan el acceso de forma directa a los servicios *WEB* de información del Instituto, con la incorporación del código de acceso rápido QR en la Credencial para Votar, se podrá consultar su situación registral, verificar la vigencia de la Credencial para Votar, ubicar su casilla el día de la jornada electoral, poder realizar un trámite de Reimpresión o Remplazo de la Credencial por Vigencia, entre otros.

d) Servicios al ciudadano.

Derivado de que la Credencial para Votar es uno de los documentos más utilizados como identificación, los ciudadanos para solicitar la apertura de créditos y/o el acceso a servicios diversos (salud, transacciones comerciales, créditos del ISSSTE, IMSS, entre otros) tienen que proporcionar su Credencial para Votar, por lo que las instituciones públicas o privadas han solicitado al Instituto que se pueda llevar a cabo la verificación de los datos de la Credencial para Votar con la información que se encuentra en la base de datos del Padrón Electoral, incluso se ha planteado la necesidad de autenticar mediante el uso de la información biométrica al portador de la Credencial para Votar, esto con el fin de mitigar los fraudes debido a credenciales que no fueron generadas por el Instituto o en su caso por usurpaciones de la identidad.

e) Posibles necesidades

Actualmente, se ha identificado que existen productos en el mercado que realizan la validación de los elementos de la Credencial para Votar, los cuales son desarrollados por empresas que promueven este tipo de servicios con el fin de apoyar a las instituciones públicas y/o privadas en la verificación de los elementos de seguridad y de información de la Credencial para Votar, lo cual contribuye a mitigar los fraudes o suplantaciones de la identidad, sin embargo, se considera que el uso de estos productos no cuentan con la normatividad aplicable y/o procedimientos establecidos por el Instituto, lo que no permite dar certeza a los usuarios de estos productos sobre la autenticidad de la Credencial para Votar.

A partir de todos estos planteamientos o requerimientos, el Instituto tiene el objetivo primordial de promover *Servicios de Valor Agregado* a la Sociedad, que promuevan los servicios que proporciona el Instituto para satisfacer las demandas del uso y aplicación de los productos y servicios electorales, manteniendo en todo momento la confidencialidad de los datos que proporcionan los ciudadanos.

Para tal efecto, se implementaran servicios mediante tecnologías de uso específico (producción de credenciales y uso de biométricos) que permitan identificar y/o autenticar al ciudadano que porta una Credencial para Votar, lo cual contribuirá a mejorar y fortalecer la

percepción ciudadana hacia el Instituto, así como el incremento de la calidad del Padrón Electoral. Dichos servicios están considerados parar operar en línea, sin embargo existe un universo significativo de ciudadanos que carecen de acceso a internet, por lo que el uso y aplicación de los códigos bidimensionales de acceso rápido PDF 417, así como la zona de lectura mecánica permitirán proporcionar servicios con aplicaciones desarrolladas por el Instituto fuera de línea, únicamente con la lectura de dichos elementos que forman parte de la Credencial para Votar.

Finalmente, y como parte de los servicios que se brindarán a los ciudadanos, a través del nuevo Modelo de la Credencial para Votar, se considera el desarrollo y disposición de aplicaciones que permitan mediante la lectura de los códigos de acceso rápido de la Credencial para Votar mediante el uso de dispositivos electrónicos, PC, MAC, *PDA's*, *Smarthphone* y otros dispositivos móviles con el fin de verificar la información que integran de los códigos con los permisos y controles seguros que implementará el Instituto.

En este sentido, se considera que las aplicaciones para el acceso a los códigos (PDF 417 y QR) serán desarrolladas e implementadas por el Instituto con el fin de que puedan ser descargadas o acceder a ellas de manera fácil para que se lleve a cabo la verificación de los datos de la Credencial para Votar. En este sentido, se tiene la visión de que estas aplicaciones vayan evolucionando para que se puedan utilizar sin el uso de la internet o en su caso que promuevan una serie de servicios de información que permitan un acercamiento del Instituto con el Ciudadano para conocer y difundir servicios e información sobre aspectos electorales.

Con base en lo anterior, y con el fin de establecer para el alcance que se tiene actualmente y está descrito en el presente documento, a continuación se describe el uso de los códigos y su aplicación, con un fin enunciativo más no limitativo, toda vez que los usos y aplicaciones estarán evolucionando y adaptando conforme lo permita la tecnología, normatividad, seguridad, etc., con el fin de cumplir con el objetivos.

Para el caso el caso de la minucia, esta será cifrada a través de un algoritmo simétrico con una llave de AES 256 bits, ya a modo similar que en el caso de la llave asimétrica, se tomaron a consideración las directivas establecidas por el Gobierno de los Estados Unidos de América, que dicta que en los casos de uso de cifrado de este tipo la llave debe tener una longitud establecida de 192 o 256 bits para información sensible, siendo la segunda opción es la más robusta.

En general el uso del cifrado por algoritmo simétrico se deriva de la necesidad de que el tamaño en las cadenas resultantes del cifrado, tengan un crecimiento mínimo en comparación con la cadena original. Del mismo modo, el separar la minucia con un cifrado distinto representa mayor fortaleza y seguridad en la totalidad de la cadena.

Uso y aplicación de los Códigos y de la ZLM de la Credencial para Votar	Códigos y Zona de Lectura Mecánica considerados
Verificación de Afiliados para el registro de Agrupaciones y Partidos Políticos.	QR
Urna electrónica.	PDF-417
Servicios de información	QR
Servicios al ciudadano.	PDF-417, QR
Posibles necesidades (Servicios de Valor Agregado)	PDF-417, ZLM

7. Glosario de términos y Acrónimos.

Acrónimos	Definición
AAMMDD	2 dígitos del año, 2 dígitos del mes y 2 dígitos del día
AES	Advanced Encryption Standard
APN	Agrupación Política Nacional
CIC	Código identificador de la Credencial
COFIPE	Código Federal de Instituciones y Procedimientos Electorales
CNV	Comisión Nacional de Vigilancia
CPEUM	Constitución Política de los Estados Unidos Mexicanos
CPV	Credencial para Votar
CURP	Código Único del Registro de Población
DEOE	Dirección Ejecutiva de Organización Electoral
DEPPP	Dirección Ejecutiva de Prerrogativas y Partidos Políticos
DERFE	Dirección Ejecutiva del Registro Federal Electoral
FIPS	Estándares Federales de Procesamiento de la Información
ICAO	International Civil Aviation Organization
IFE	Instituto Federal Electoral
IFETEL	Call Center del IFE
NIST	National Institute of Standards and Technology
OCR	Número identificador de la Credencial se conforma por la sección electoral y un consecutivo.
PPN	Partido Político Nacional
PDF-417	Código de barras de bidimensional tipo PDF-417
QR	Código de barras de bidimensional Quick Response
SFTP	Secure File Transfer Protocol
SIIRFE	Sistema de Integral de Información del Registro Federal Electoral
SIE	Subsistema de Información Ejecutiva
SVA	Servicios de Valor Agregado
SIIM	Solución Integral de Identificación Multibiométrica
OPP	Organismo Público o Privado
UNICOM	Unidad Técnica de Servicios de Informática del IFE
URL	Uniform Resource Locator
WSQ	Wavelet Scalar Quantization
ZLM	Zona de Lectura Mecánica