UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Servicio de Cifrado de la Información contenida en el código PDF-417 de la Credencial para Votar

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Alan Peña Islas

ASESOR DE INFORME

Mtro. César Sanabria Pineda

Ciudad Universitaria, Cd. Mx., 2016

A mis padres porque sin ellos no estaría aquí. Gracias por su amor y comprensión.

A mis hermanos, gracias por enseñarme el camino.

A Yenetzi, porque en mi silencio está tu palabra.

Gracias a la Universidad Nacional Autónoma de México y a la Facultad de Ingeniería por forjar mi formación académica y profesional.

Gracias al Instituto Nacional Electoral, especialmente a la Dirección de Infraestructura y Tecnología Aplicada por permitirme colaborar en sus proyectos y, particularmente, al Mtro. César Sanabria por su asesoría profesional y académica.

Contenido

Tablas

Figuras

INTRODUCCIÓN

El INSTITUTO FEDERAL ELECTORAL (IFE) ha sido el órgano garante de la democracia en México desde su creación a principios de la década de los 90 hasta el momento de su renovación como el INSTITUTO NACIONAL ELECTORAL (INE). Durante este periodo, dentro de sus principales atribuciones se encontraba el diseño y producción de uno de los documentos de identidad más difundidos y utilizados en el país: la Credencial para Votar.

Abordado más adelante en el presente informe, dicho documento de identidad ha evolucionado conforme a las necesidades imperantes del contexto, mediante el aprovechamiento de las Tecnologías de la Información disponibles. Con relación a lo estipulado por el Plan Estratégico Institucional 2012-2015, el IFE creó el *Proyecto del Servicio de Producción de Formatos de Credencial para Votar* como parte del *Programa de Actualización y Renovación de la Credencial para Votar.* Principalmente, el Proyecto consistió en incluir diversos elementos de seguridad y proveer a la ciudadanía servicios de valor agregado para su beneficio a través de códigos de datos.

Los códigos de datos son el PDF-417, el código QR y la Zona de Lectura Mecánica, cuyas funciones son especificadas en este trabajo. Al respecto es importante señalar que el código PDF-417 ya era utilizado en el modelo vigente de

ese entonces —modelo Tipo C—, sin embargo, la Subdirección de Seguridad Informática[1] propuso una modificación del uso del código, a fin de albergar un control más de seguridad para proteger la información de los ciudadanos y a la Credencial misma.

La propuesta radicó en emplear el código PDF-417 para almacenar el criptograma de cierta información del ciudadano y con ello dar certeza de la autenticidad de la Credencial, es decir, con dicho elemento de seguridad se buscó reducir el riesgo de producción de credenciales apócrifas. Además, al mismo tiempo se conseguía dar cumplimiento a lo indicado en el numeral 3 del Artículo 171 del Código Federal de Instituciones y Procedimientos Electorales:

> Los documentos, datos e informes que los ciudadanos proporcionen al Registro Federal de Electores, en cumplimiento de las obligaciones que les impone la Constitución y 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. (Congreso de la Unión, 2008, pág. 59)

Una vez establecido el proyecto y la consiguiente planeación del Servicio de Cifrado de la Información Contenida en el código PDF-417 de la Credencial para Votar, la Dirección Ejecutiva del Registro Federal de Electores[2] (DERFE) recibió su aprobación durante una sesión extraordinaria del Consejo General del INSTITUTO FEDERAL ELECTORAL, celebrada el 23 de octubre de 2012, mediante el Acuerdo CG293/2013 en "el que se aprueba la función de los códigos de barras bidimensionales en el modelo aprobado por este Órgano de Dirección mediante

[1] Área establecida dentro de la Dirección Ejecutiva del Registro Federal de Electores del IFE.

[2] Instancia del INSTITUTO FEDERAL ELECTORAL cuyas atribuciones, entre otras, radican en formar, revisar y actualizar el Padrón Electoral, expedir la Credencial para Votar, proporcionar a los órganos competentes las Listas Nominales de Electores, mantener actualizada la Cartografía Electoral y asegurar que las comisiones de vigilancia —tanto nacionales como estatales y distritales— se integren, sesionen y funcionen en los términos del Código Federal de Instituciones y Procedimientos Electorales. (Congreso de la Unión, 2008, pág. 46)

Acuerdo CG732/2012[3]" (Instituto Federal Electoral, 2013), el cual formaba parte del ya mencionado *Proyecto del Servicio de Producción de Formatos de Credencial para* Votar.

Debido a lo anterior, el presente informe tiene como objetivo principal describir las fases relacionadas al establecimiento del servicio mencionado, así como mi participación profesional en dicho proceso. Para ello, este documento fue dividido en tres capítulos. El primero da un panorama de la historia y funciones del INSTITUTO FEDERAL ELECTORAL, del INSTITUTO NACIONAL ELECTORAL y del Registro Federal de Electores; así como del puesto que he desempeñado en estas instituciones.

El segundo abarca las características de la Credencial para Votar y los instrumentos técnicos de seguridad con los que cuenta; se hace especial mención del código QR, de la Zona de Lectura mecánica y, sobre todo, del código PDF-417. De igual forma, este capítulo cubre los elementos de Tecnologías de la Información que fueron necesarios para concretar el servicio de cifrado.

Finalmente, el tercero expone las fases técnicas relacionadas a la implementación del servicio de cifrado y la descripción de cada una de las capas que lo componen. Resulta importante señalar que la información reservada relacionada con el servicio de cifrado no fue incluida en este informe por políticas de seguridad del INSTITUTO NACIONAL ELECTORAL.

[3] Acuerdo por el que se aprueba modificar el modelo existente de la Credencial para Votar.

CAPÍTULO I
Acercamientos al Instituto Nacional Electoral

1.1 Historia del Instituto Nacional Electoral

El INSTITUTO NACIONAL ELECTORAL (INE) tiene sus orígenes desde la promulgación de la Constitución Política de los Estados Unidos Mexicanos, particularmente en la Junta Empadronadora, las Juntas Computadoras Locales y los Colegios Electorales. Dichos organismos se encargaban de organizar y calificar los procesos electorales correspondientes al Presidente de la República y a los miembros del Congreso de la Unión (Instituto Nacional Electoral, 2015); mientras a nivel local, los jefes políticos se ocupaban de la realización de las elecciones para renovar los poderes.

Durante la presidencia de Manuel Ávila Camacho (1946), se promulgó la Ley Federal Electoral y, consecuentemente, se creó la Comisión Federal de Vigilancia Electoral, las Comisiones Electorales Locales y el Consejo del Padrón Electoral. Cuando en 1951 se ampliaron sus funciones, la Comisión fue capaz de arbitrar el registro de nuevos partidos políticos y emitir constancias de mayoría. En 1973 es sustituida por la Comisión Federal Electoral, con lo que todos los partidos con registro legal pueden participar activamente con derecho a voz y voto. Durante este mismo año, el Registro Nacional de Electores fue dotado de autonomía.

Cuatro años después, el Gobierno promulgó la Ley de Organizaciones Políticas y Procesos Electorales (LOPPE) en la que se permitía el ingreso a la vida institucional de fuerzas públicas “no incluidas”; adicionalmente, la estructura de la Comisión Federal Electoral sufrió cambios importantes, ahora se conformaba por el Secretario de Gobernación, un representante de cada una de las cámaras legislativas, un representante de cada partido político y un notario público.

A raíz de los conflictos postelectorales derivados del proceso de 1988, se realizaron reformas constitucionales, de las cuales surgió una nueva legislación en materia electoral. En consecuencia, el 15 de agosto de 1990 se expide el Código Federal de Instituciones y Procedimientos Electorales, dando lugar a la creación del INSTITUTO FEDERAL ELECTORAL (IFE) como un órgano garante de certeza, transparencia y legalidad en las elecciones federales. Asimismo, se establece su carácter permanente en oposición a la temporalidad de sus predecesores.

Dentro de las atribuciones conferidas al INSTITUTO FEDERAL ELECTORAL, se encuentran la responsabilidad de contribuir al desarrollo de la democracia en el país, fortalecer el régimen de partidos políticos, velar por los derechos político-electorales de los ciudadanos y proporcionar autenticidad y efectividad al sufragio. Del mismo modo, le fueron otorgadas funciones que anteriormente se encontraban aisladas o dispersas, tales como la actualización permanente del Padrón Electoral, el registro de partidos, la capacitación electoral, la educación cívica y la profesionalización del servicio electoral.

Para el año de 1996, se impulsó una nueva reforma electoral a causa de las modificaciones hechas al artículo 41 constitucional, cuyo resultado fue la creación de un nuevo Código Federal de Instituciones y Procedimientos Electorales. Con lo anterior, el IFE adquiere mayor autonomía e independencia al deslindar por completo su integración del Poder Ejecutivo, y fue reservado el derecho de voto dentro de los órganos de dirección para los Consejeros Ciudadanos. Por otro lado, fueron eliminadas las figuras de Director y Secretario General, siendo reemplazadas por la Presidencia del Consejo General y la Secretaría Ejecutiva.

La tarea del Instituto Federal Electoral continuó sin cambios hasta que en 2007 el Congreso de la Unión aprobó un Código Federal de Instituciones y Procedimientos Electorales con el cual se le asignan un total de 53 atribuciones que tienen por objetivo: el fortalecimiento de la confianza y la credibilidad depositada por la ciudadanía en los procesos electorales llevados a cabo por el Instituto; la regularización del acceso de los partidos políticos y autoridades electorales a los medios de comunicación; la promoción de la participación ciudadana en cada elección federal; el aseguramiento de condiciones de equidad y civilidad en las campañas electorales; favorecer la transparencia del proceso de organización y difusión de resultados de cada elección.

Después de más de dos décadas, el Instituto Federal Electoral dio fin a sus funciones el 4 de abril de 2014, a partir de la aprobación de la reforma político-electoral que pretendía rediseñar el régimen electoral mexicano. Así, se creó el Instituto Nacional Electoral (INE), una autoridad de carácter nacional encargada de la organización de todos los comicios tanto federales como locales, garantizando los más altos niveles de calidad en la democracia del país. Dentro de las nuevas funciones destacan:

1. Organización de los procesos electorales federales y locales. Estos últimos mediante la coordinación con los organismos electorales locales de cada entidad federativa.
2. Designación de consejeros de los organismos locales.
3. Organización de elecciones de los dirigentes de partidos políticos, únicamente si se realiza la petición.
4. Velar por la igualdad de condiciones para los candidatos independientes, de tal forma que puedan acceder a tiempos del Estado en radio y televisión para difundir sus campañas.
5. Verificación del cumplimiento de requisitos mínimos para la realización de consultas populares, así como su organización, cómputo y publicación de resultados.

6. Fiscalización de recursos de los partidos políticos a nivel federal y local durante el transcurso de sus campañas.

1.2 Misión, visión y objetivos del INE

La misión del INSTITUTO NACIONAL ELECTORAL consiste en "contribuir al desarrollo de la vida democrática, garantizando el ejercicio de los derechos político-electorales de la sociedad a través de la promoción de la cultura democrática y la organización de comicios federales en un marco de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad".

De esta manera, en su visión, el INE se: "consolida como un organismo público autónomo, transparente y eficiente, en el que la sociedad cree y deposita plenamente su confianza, que se distingue por proporcionar servicios cada vez más confiables y de mayor calidad a la ciudadanía y ser el principal promotor de la cultura democrática en el país."

Así mismo, para dar cumplimiento a las actividades encomendadas al Instituto, éste define 15 objetivos estratégicos divididos en 4 perspectivas (Tabla 1.1 Objetivos estratégicos):

Tabla 1.1 Objetivos estratégicos

Perspectivas	Objetivos estratégicos
Valor público	Preservar y fortalecer la confianza de la sociedad
	Ser el referente principal en el desarrollo de la cultura democrática
Sociedad	Ampliar y mejorar la interacción con la sociedad
	Consolidar a la Credencial para Votar como medio preferente de identidad ciudadana
	Incrementar la eficiencia en la organización de los procesos electorales federales
Materia electoral	Incrementar la calidad del Padrón Electoral
	Incrementar la cobertura, servicios y calidad de la atención ciudadana
	Incrementar la eficiencia de los procesos sustantivos

Perspectivas	Objetivos estratégicos
Innovación y transformación institucional	Aumentar la eficiencia y transparencia de la administración de los recursos financieros
	Implantar una nueva cultura de planeación e innovación
	Implantar una nueva cultura laboral
	Mejorar la comunicación y coordinación interna
	Optimizar el uso, aplicación e inversión en TIC
	Optimizar la gestión administrativa

Fuente: (Instituto Federal Electoral, 2000)

1.3 Registro Federal de Electores

El Registro Federal de Electores (RFE) es el registro exacto y oportuno que contiene el nombre y los datos de identificación de todos los ciudadanos con derecho al voto, por lo que se trata de un elemento para garantizar la integridad y confiabilidad de los procesos electorales en el país (Instituto Federal Electoral, 2000). Por ser de carácter activo, indica que cada ciudadano con el total de requisitos estipulados debe acudir, realizar y completar su inscripción.

Tiene su origen en 1990 dentro del marco de la reforma político-electoral llevada a cabo en ese año, razón por la cual requirió de un gran esfuerzo para su construcción, pues en un periodo de 8 meses (noviembre de 1990 a julio de 1991) se recabaron 42.5 millones de registros en el Catálogo General. Posteriormente, el Padrón Electoral quedó conformado por 39.2 millones de ciudadanos que fueron tomados del Catálogo, de los cuales 36.6 millones tuvieron asignada una Credencial para Votar (Instituto Federal Electoral, 2000).

En los siguientes años, se llevó a cabo un trabajo constante de depuración del Padrón Electoral y la producción de Credenciales para Votar con mayor número de opciones de seguridad contra falsificaciones. Es importante señalar que la depuración se realizó de manera continua para asegurar que el Padrón Electoral estuviera compuesto únicamente por registros de ciudadanos con derecho al voto y así asegurar el principio democrático “un hombre, un voto”.

Para lo anterior, el Registro Federal de Electores se conforma por cuatro instrumentos fundamentales: el Catálogo General de Electores, el Padrón Electoral, la Credencial para Votar y las Listas Nominales (Tabla 1.2 Instrumentos fundamentales del Registro Federal de Electores).

Tabla 1.2 Instrumentos fundamentales del Registro Federal de Electores

Instrumento	Descripción
Catálogo General de Electores	Se trata de un catálogo que contiene la información básica de un ciudadano: nombre completo, lugar de nacimiento, fecha de nacimiento, edad, sexo, domicilio actual, tiempo de residencia y ocupación. Esta información es obtenida a partir de la técnica censal (aplicación de entrevistas casa por casa en todo el país).
Padrón Electoral	Es la base de datos cuyo contenido consiste en el nombre e información básica de los ciudadanos mexicanos incluidos en el Catálogo General de Electores y que han solicitado formalmente su registro o empadronamiento para fines electorales. Además, en el Padrón Electoral también se incluye la firma del ciudadano, sus huellas dactilares y su fotografía.
Credencial para Votar	Es un documento indispensable para que los ciudadanos inscritos en el Padrón Electoral puedan ejercer su derecho al voto. Las características de este documento se verán en el siguiente capítulo.
Listas Nominales	Se trata de documentos que contienen el nombre de las personas incluidas en el Padrón Electoral, agrupadas por distrito y sección electoral y que cuentan con Credencial para Votar. Su objetivo es servir como instrumento para la verificación de las elecciones, ya que solamente aquellas personas que aparezcan listadas podrán ejercer el voto.

Fuente: (Instituto Federal Electoral, 2000)

1.4 Puesto desempeñado

Durante mi estancia en el actual denominado INSTITUTO NACIONAL ELECTORAL, laboré dentro de la Subdirección de Seguridad Informática, instancia perteneciente a la Dirección Ejecutiva del Registro Federal de Electores. Los siguientes diagramas (Fig.1 Organigrama Secretaría Ejecutiva INE y Fig.2 Organigrama Dirección Ejecutiva del Registro Federal de Electores) muestran la posición jerárquica de la Dirección y Subdirección antes nombradas en la estructura orgánica del INE.

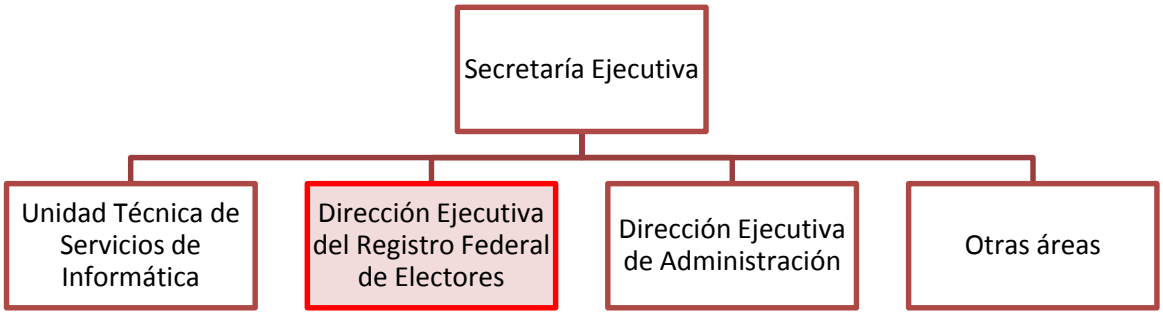


Fig. 1 Organigrama Secretaría Ejecutiva INE

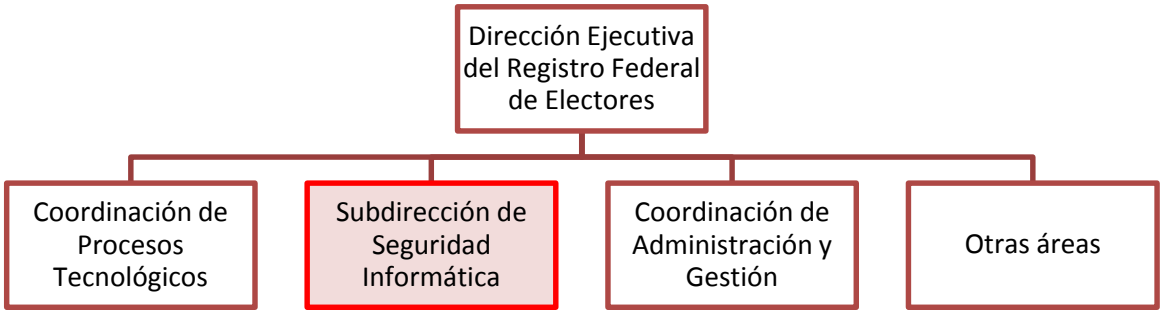


Fig. 2 Organigrama Dirección Ejecutiva del Registro Federal de Electores

Fuente: Elaboración propia a partir de (Instituto Nacional Electoral, 2015)

De manera general, las funciones de la Subdirección de Seguridad Informática (Tabla 1.3 Funciones de la Subdirección de Seguridad Informática) están orientadas a proteger en términos informáticos el Padrón Electoral, razón por la cual, sus actividades se distribuyen en seis rubros principales: cumplimiento del Plan Integral de Seguridad; diseño metodológico en la Dirección Ejecutiva; capacitación y fomento de la cultura en seguridad informática; documentación de incidentes de seguridad; análisis de riesgos internos; divulgación e innovación estratégica.

Tabla 1.3 Funciones de la Subdirección de Seguridad Informática

Coordinar tareas de investigación, análisis, evaluación, propuesta, y en su caso instrumentación de tecnologías y herramientas que faciliten las actividades del Plan Integral de Seguridad con objeto de identificar, prevenir y atender los riesgos o vulnerabilidades en la seguridad, disponibilidad, integridad, confidencialidad y autenticidad de la información del Padrón Electoral.
Coordinar el diseño, evaluación y propuesta a las áreas de la Dirección Ejecutiva, a fin de implantar procedimientos y/o metodologías conforme a las mejores prácticas internacionales, para identificar riesgos o vulnerabilidades respecto de las características de seguridad informática del Padrón Electoral.
Verificar el diseño, evaluación y propuesta a las áreas de la dirección ejecutiva, de programas de capacitación al personal sobre el uso y manejo de la información vulnerable del Padrón Electoral y del Registro Electoral, a fin de crear una cultura de seguridad en este rubro.
Informar a la Dirección Ejecutiva sobre las incidencias detectadas que pongan en riesgo la seguridad, disponibilidad, integridad, confidencialidad y autenticidad de la información del Padrón Electoral, así como las soluciones que se hayan instrumentado.
Coordinar la realización de auditorías internas y/o externas en materia de seguridad al interior de la Dirección Ejecutiva, para proteger la información confidencial del Padrón Electoral.
Mejorar continuamente el Plan Integral de Seguridad con la puesta en marcha de medidas preventivas y correctivas en la materia, así como la difusión de las acciones de mejora a las áreas de la Dirección Ejecutiva.

Fuente: (Instituto Nacional Electoral, 2014)

Capítulo II
La Credencial para Votar: elementos de seguridad y tecnologías asociadas.

2.1 La Credencial para Votar

De acuerdo a lo estipulado por la Ley General de Instituciones y Procedimientos Electorales (LGIPE), la Credencial para Votar es el documento único emitido por el INSTITUTO NACIONAL ELECTORAL, a través del Registro Federal de Electores, para que los ciudadanos puedan ejercer su derecho al voto; de igual manera, es considerado un documento de carácter oficial para la validación de la identidad personal[4].

En términos históricos, la Credencial para Votar surgió en 1992 a partir de las reformas político-electorales que le dieron origen al IFE; sin embargo, resulta

[4] Artículo cuarto del régimen transitorio del decreto que reforma y adiciona diversas disposiciones de la Ley General de Población, publicado en el Diario Oficial de la Federación el 22 de julio de 1992, dispone que en el establecimiento del Registro Nacional de Ciudadanos se utilizará la información que proporcionará el Instituto Federal Electoral proveniente del Padrón Electoral y de la base de datos e imágenes obtenidas con motivo de la expedición y entrega de la Credencial para Votar con fotografía previsto en el artículo 164, del Código Federal de Instituciones y Procedimientos electorales, en tanto no se expida la Cédula de Identidad Ciudadana esta credencial podrá servir como medio de identidad personal en trámites administrativos de acuerdo a los convenios que para tal efecto suscriba la autoridad electoral. (Secretaría de Gobernación, 2015)

importante señalar, no es el primer documento de este tipo emitido por el Gobierno, ya que la Comisión Federal Electoral ya había utilizado otros formatos. Después de distintas modificaciones, el último modelo de la credencial empezó su producción el 25 de noviembre de 2013, pero su diseño fue cambiado en julio de 2014 a raíz de la creación del INSTITUTO NACIONAL ELECTORAL. A grandes rasgos, el cambio radicó en la modificación del nombre del Instituto y los logos correspondientes al del órgano recién instituido, así como la ubicación de algunos elementos.

Un aspecto importante en la evolución de la Credencial para Votar, presentada en la Tabla 2.1 Historia de la Credencial para Votar, es la innovación de cada modelo a favor de la seguridad del documento, aumentando la confiabilidad y seguridad de los datos proporcionados a la ciudadanía, y la inclusión de elementos que permitan ofrecer servicios adicionales de valor para los ciudadanos (Instituto Nacional Electoral, 2015).

Tabla 2.1 Historia de la Credencial para Votar[5]

Órgano electoral	Año	Imagen	Características
Comisión Federal Electoral	1976		Documento impreso en papel que permitía identificar al ciudadano para la emisión de su voto.

[5] Las imágenes usadas en la tabla son únicamente para fines ilustrativos y no corresponden a los de una persona real.

Órgano electoral	Año	Imagen	Características
	1981		Se emplea en un esquema descentralizado y con un nivel de seguridad muy bajo.
	1991		Formato de transición de la Comisión Federal Electoral al Instituto Federal Electoral.

Órgano electoral	Año	Imagen	Características
Instituto Federal Electoral	1992 – Sep. 2001		CPV Tipo A -Se integra una fotografía instantánea del ciudadano al momento de recogerla. -Empleo de código de barras unidimensional tipo 128 cubierto por un filtro infrarrojo.
	Oct. 2001 – Sep. 2008		CPV Tipo B -La fotografía pasa a ser digital. -Las dimensiones corresponden a estándares internacionales. -Integración de código PDF-417. -El código de barras tipo 128 ahora contiene el Código de Identificación de Credencial (CIC). -El filtro infrarrojo se hereda del modelo anterior.

Órgano electoral	Año	Imagen	Características
	Sep. 2008 – Nov. 2013		CPV Tipo C -Se incorpora el CURP -Se agregan diversas medidas de seguridad en contra del fraude y la alteración como marcas de agua y tinta ultravioleta.
	Nov. 2013 – Jul. 2014		CPV Tipo D -Es capaz de autenticarse a sí misma al ofrecer datos firmados y cifrados por el Instituto. -Protección y resistencia mayor al

Órgano electoral	Año	Imagen	Características
			FADDS[6]. -La fotografía pasa al lado izquierdo de la credencial y se agrega una Zona de Lectura Mecánica para cumplir con normas internacionales. -Se agrega una zona de código QR para vinculación a servicios proporcionados a la ciudadanía. -El código PDF-417 puede ser usado para la emisión de votos electrónicos.

[6] Término cuyas siglas significan Falsificación, Duplicación, Diversificación y Simulación.

Órgano electoral	Año	Imagen	Características
Instituto Nacional Electoral	7 julio 2014 – A la fecha		CPV Tipo E -Es el mismo modelo que el anterior, salvo por el cambio en el nombre y logos del Instituto y el reacomodo de algunos elementos.

Fuente: (Instituto Nacional Electoral, 2015)

2.2 Elementos de seguridad en el modelo actual de la Credencial para Votar

El diseño vigente de la Credencial para Votar comenzó su emisión a partir de julio de 2014 y se le denominó “Tipo E”. Esta nueva credencial contiene varios mecanismos de seguridad que no se encontraban en los modelos anteriores. El Instituto Nacional Electoral (2014) describe dichos elementos de la siguiente manera (Tabla 2.2 Anverso de la Credencial para Votar: "Tipo E" y Tabla 2.3 Reverso de la Credencial para Votar: "Tipo E"):

› Anverso

› Reverso

Tabla 2.2 Anverso de la Credencial para Votar: "Tipo E"

Elemento	Descripción
1. Tinta UV	En el anverso, este modelo integra un diseño de seguridad basado en colores de tintas ultravioleta que son perceptibles con luz negra. Contiene impresos datos fijos (INE, MÉXICO), imágenes y datos variables del ciudadano.
2. Patrón debilitado	El diseño del fondo de seguridad se integra con el borde de la fotografía. Esto da la apariencia de fusionar el marco de la fotografía con el resto del diseño de la credencial.
3. Diseños "Guilloche"	Todas las credenciales tienen un patrón de figuras formadas con líneas finas que generalmente son difíciles de imitar con impresoras o fotocopiadoras, ya que al intentarlo se obtienen imágenes a base de puntos y no de líneas.
4. Microtexto	En el anverso, las credenciales contienen un microtexto con la leyenda INSTITUTO NACIONAL ELECTORAL, que no es legible a simple vista.
5. Impresión arcoíris	Las credenciales tienen impresos patrones de líneas con dos o más colores de tinta simultáneos. La impresión se realiza utilizando un equipo especializado para crear una fusión controlada de colores semejantes que simulen el efecto de colores de un arcoíris.
6. Elemento táctil	El diseño de la credencial cuenta con un elemento de seguridad perceptible al tocarlo con las yemas de los dedos. Este elemento contiene las siglas del INE y la boleta electoral entrando a la urna.

Elemento	Descripción
7. Fotografía fantasma con datos variables	La fotografía fantasma se fortalece como elemento de seguridad al aplicar un software que crea la imagen a partir de datos del ciudadano con un patrón variable, lo que la hace única y difícil de reproducir.
8. Tinta OVI	Tinta de impresión especializada que cambia de color en función del ángulo de la luz con que se observe. En la Credencial para Votar se puede observar el cambio de color del mapa de la República Mexicana que se encuentra en la parte inferior derecha, así como de la franja izquierda que se ubica junto a la fotografía del ciudadano.
9. Diseño en relieve	Todas las credenciales tienen líneas con diseños especiales que simulan un efecto de relieve. Este efecto es muy difícil de reproducir con escáner o fotografías digitales. En el reverso de las credenciales se puede apreciar una imagen formada con los nombres de todas las entidades del país.
10. Elemento Ópticamente Variable (OVD)	El dispositivo cambia de color, dependiendo del ángulo de la luz con que se observe. Este elemento de seguridad tiene la leyenda “Instituto Nacional Electoral”, la palabra “INE” y la urna con la boleta electoral entrando a la misma. Adicionalmente cuenta con radiofrecuencia para revisar su autenticidad.

Fuente: (Instituto Nacional Electoral, 2015)

Tabla 2.3 Reverso de la Credencial para Votar: "Tipo E"

Elemento	Descripción
11. Tinta UV	El dispositivo cambia de color, dependiendo del ángulo de la luz con que se observe. Este elemento de seguridad tiene la leyenda “Instituto Nacional Electoral”, la palabra “INE” y la urna con la boleta electoral entrando a la misma. Adicionalmente cuenta con radiofrecuencia para revisar su autenticidad.
12. Microtexto	En el contorno donde se ubican la firma y la huella del ciudadano, se encuentra un microtexto que no es legible a simple vista, conformado por el nombre del ciudadano.
13. Diseño en relieve	Todas las credenciales tienen líneas con diseños especiales que simulan un efecto de relieve. Este efecto es muy difícil de reproducir con escáner o fotografías digitales. En el reverso de las credenciales se puede apreciar una imagen formada con los nombres de todas las entidades del país.
14. Impresión arcoíris	Las credenciales tienen impresos patrones de líneas con dos o más colores simultáneos de tinta. La impresión se realiza utilizando un equipo especializado para crear una fusión controlada de colores semejantes que simulen el efecto de colores de un arcoíris.
15. Código QR	Este elemento puede ser escaneado por un teléfono “inteligente” y dirige a una botonera de servicios que ofrece el INE para el ciudadano, donde puede acceder a programar una cita, ubicar el módulo que le corresponde, verificar la vigencia de su Credencial.

Elemento	Descripción
16. Tinta OVI	Las credenciales se imprimen con una tinta especial que es ópticamente variable, la cual presenta grandes cambios de color en función del ángulo de observación o de la iluminación que se tenga. En el anverso de cada credencial puede observarse que el mapa de la República Mexicana ubicado en la parte inferior derecha cambia de color, así como la franja ubicada junto a la fotografía del ciudadano.

Fuente: (Instituto Nacional Electoral, 2015)

Aunque todos estos elementos reducen significativamente las posibilidades de falsificar la Credencial para Votar, el modelo más reciente posee tres características que la ponen por encima de sus predecesores:

1. Domicilio opcional: el ciudadano puede elegir si su domicilio será impreso en el anverso, es decir, puede optar por no mostrar el nombre de su calle, el número exterior e interior. En los modelos anteriores tales datos eran visibles en la parte frontal de la credencial.
2. Zona de Lectura Mecánica (ZLM): de acuerdo a lo establecido por la Organización Internacional de Aviación Civil (ICAO) en el rubro de "Documentos de viaje oficiales de lectura mecánica (MRTD)", la ZLM permite a la Credencial para Votar ser reconocida internacionalmente como un documento oficial de identificación.
3. Código bidimensional: es la zona correspondiente a la parte superior del reverso de la credencial, su función principal es la de automatizar las lecturas de datos para evitar errores humanos al momento de la captura de datos. Dentro de este código son almacenados distintos datos, cifrados y firmados, del ciudadano con la finalidad de certificar su autenticidad.

Este último elemento, cabe señalar, es de suma importancia para el presente documento, debido a que mi participación en los proyectos del INSTITUTO NACIONAL ELECTORAL se relacionó directamente con la información contenida en el código bidimensional. Por ello, para cumplir con los objetivos de este escrito, profundizaré en los puntos que lo caracterizan, así como en la infraestructura que hace posible su realización.

2.3 El código PDF-417 del modelo vigente de la Credencial para Votar

El código PDF-417 es de tipo bidimensional, permite una mayor codificación de información en menor espacio comparado a sus contrapartes de tipo lineal o unidimensional. Esta ventaja ha propiciado la rápida aceptación de este tipo de códigos en los ámbitos empresariales y de gobierno, pues se usan en gran cantidad de operaciones, e incluso, en documentos oficiales de distintos países. El nombre bidimensional fue asignado por el tipo de lector óptico necesario para leerlo, el cual debe ser capaz de leer toda la superficie del código (Espinosa García, Hernández Encinas, & Martín del Rey).

Los códigos bidimensionales se dividen dependiendo de su representación gráfica en dos categorías: apilados y matriciales. Los primeros se relacionan directamente con los códigos de barras tradicionales, ya que se componen de barras y espacios apilados, unos encima de otros; los segundos son más parecidos a matrices de puntos. El código PDF-417 es del tipo apilado (Espinosa García, Hernández Encinas, & Martín del Rey).

Su creación se remonta a 1990 en la empresa Symbol Technologies, cuyas siglas significan *Portable Data File* y se compone de diferentes partes (Fig.3 Partes del código PDF-417): separador de inicio —indica en dónde comienza el código—, indicador izquierdo e indicador derecho —entre ellos se localiza la información

codificada distribuida en filas (entre 3 y 30) y en columnas (de 1 a 30) — y el separador de fin, que señala el término del código. Debido a esta distribución, el PDF-417 es capaz de almacenar hasta 1850 caracteres de texto, 2710 dígitos o 1108 bytes (Espinosa García, Hernández Encinas, & Martín del Rey).

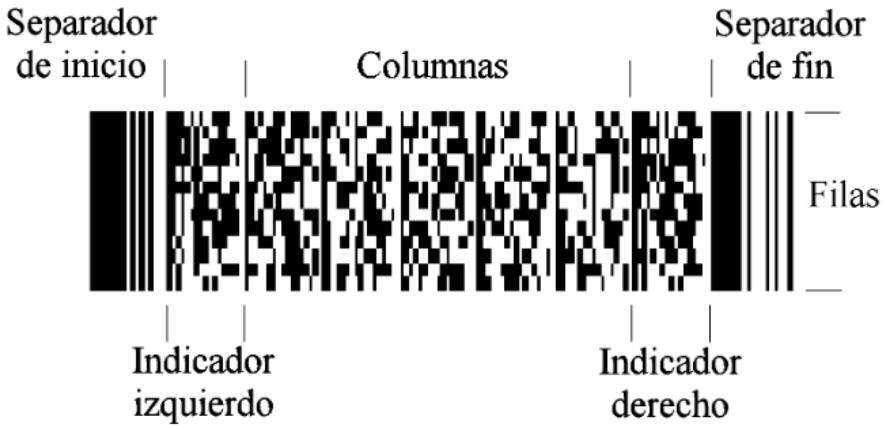


Fig. 3 Partes del código PDF-417

Fuente: (Espinosa García, Hernández Encinas, & Martín del Rey)

Como ya se mencionó, el código bidimensional usado en el modelo actual de la Credencial para Votar es del tipo PDF-417 y contiene mayor información que su predecesor en el modelo Tipo C. La principal razón de este cambio fue para admitir el almacenamiento de datos adicionales del ciudadano (Tabla 2.4 Contenido del PDF-417), permitiendo una mayor certeza a la autenticación del individuo, para así utilizar la credencial como un medio fiable, especialmente, en la emisión de votos electrónicos.

Tabla 2.4 Contenido del PDF-417[7]

Dato	Visible en la Credencial para Votar
Edad	No
CURP	Sí
Clave de Elector	Sí
CIC	Sí
OCR	Sí
Nombre	Sí
Domicilio	No u Opcional a solicitud del ciudadano
Estado	Sí
Municipio	Sí
Año de registro	Sí
Emisión	Sí
Vigencia	Sí

Fuente: (Instituto Federal Electoral, 2013)

Para proveer la protección y la verificación de los datos almacenados en el código PDF-417 se optó por usar un esquema híbrido de cifrado y firmado de información. Por un lado, se cifran los datos por medio de un algoritmo simétrico, mientras que por otro se firman mediante un algoritmo asimétrico. Los algoritmos usados son reservados por el INSTITUTO NACIONAL ELECTORAL.

Resulta destacable mencionar que el INE es el único organismo que resguarda y accede a las llaves criptográficas empleadas para los procesos de firmado y cifrado del PDF-417, motivo por el cual se han tomado diversas medidas encaminadas a proteger esta información. Como se verá más adelante, una de estas medidas fue la del resguardo de la información mediante módulos de hardware especialmente diseñados para esta tarea.

[7] Los datos almacenados en el código PDF-417 son tratados como Reservados, por lo que la información de la tabla únicamente se presenta para fines ilustrativos y de ninguna manera representa la conformación real del código.

2.4 Tecnologías de cifrado y firmado asociadas al código PDF-417

Como se expuso en el apartado anterior, la información contenida en el código PDF-417 se encuentra cifrada y firmada mediante dos tipos de algoritmos criptográficos, motivación del Instituto para adoptar un manejo de llaves criptográficas adecuado y seguro. Con el propósito de conocer mejor estos dos puntos, se ofrece una descripción general de la criptografía simétrica y asimétrica, se presenta la solución para el manejo de las llaves empleadas y la forma en cómo se realiza el proceso de cifrado y firma de información.

Primeramente, es necesario entender a la criptografía como “la ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar (cifrar) la información y hacerla irreconocible a todos aquellos usuarios no autorizados de un sistema informático, de modo que sólo los legítimos propietarios puedan recuperar (descifrar) la información original.” (Gómez Vieites, 2011)

Debido a lo antes definido, para realizar el proceso de cifrado/descifrado, se emplea un *sistema criptográfico* (Fig.4 Sistema criptográfico) basado en un algoritmo de cifrado, el texto a cifrar o *texto en claro* y el texto cifrado o criptograma. Adicionalmente, algunos sistemas requieren el uso de llaves para poder efectuar las transformaciones necesarias al texto en claro o al criptograma.

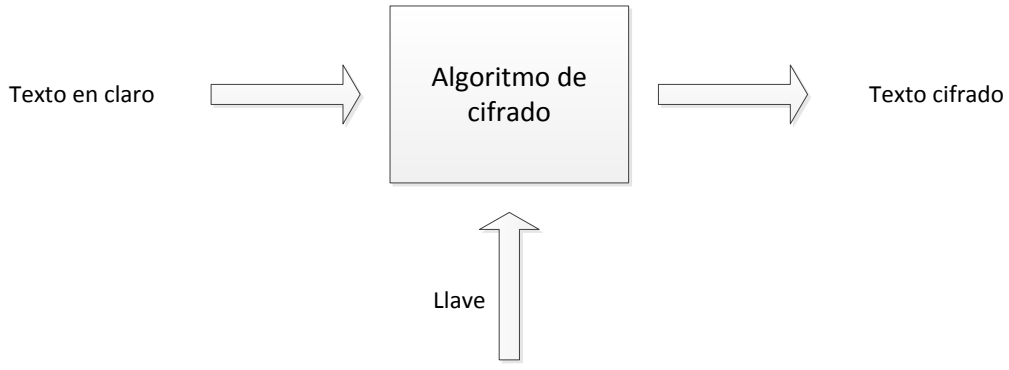


Fig. 4 Sistema criptográfico

Fuente: Elaboración propia a partir de (Stallings, 2004)

De acuerdo a Álvaro Gómez Vieites (2011), dado que el algoritmo de cifrado utilizado debe ser público, la robustez de un sistema criptográfico depende en gran medida de la llave; ésta actúa como modificador del algoritmo, de tal forma que permite que un mismo algoritmo criptográfico pueda ser usado por diferentes sujetos. Si la llave es cambiada, se modificará por completo el proceso de cifrado, en consecuencia, no es necesario cambiar o utilizar un nuevo algoritmo para cada proceso en el que se requiera cifrar información.

La llave es una secuencia aleatoria de bits de una determinada longitud, la cual está definida por un *espacio de llaves*. El espacio de llaves es el conjunto de todos los posibles valores que pueden ser usados como llave, en este sentido, entre mayor sea el espacio de llaves, la longitud de la llave será mayor. Actualmente las longitudes más comunes van de 128 a 2048 bits, por lo que la cantidad de llaves disponibles sería de 2^{128} y 2^{2048} respectivamente. (Gómez Vieites, 2011)

Asimismo, el autor señala que la robustez de un método de cifrado radica en el algoritmo, la secrecía de la llave, la longitud de la llave y cómo estos trabajan dentro de un sistema criptográfico. Los intentos de *romper* un sistema criptográfico están basados en descifrar un mensaje mediante el empleo de todos los posibles valores que puede tomar la llave, es decir, se trata de recorrer todo el espacio de llaves: éste es llamado “ataque de fuerza bruta”. Desde este ángulo, la robustez de un método de cifrado es el poder de cómputo, recursos y tiempo requerido para poder romperlo.

Entonces, los algoritmos de cifrado actuales han sido diseñados para hacer que los ataques de fuerza bruta contra ellos sean demasiado caros o que requieran una gran cantidad de tiempo comparados con el beneficio o el valor que la información descifrada representa, dejando a la llave en la posición de ser el único valor que puede cifrar o descifrar mensaje. Si ésta no es protegida adecuadamente, toda la información relacionada podrá ser accedida por sujetos no autorizados. (Gómez Vieites, 2011)

Con relación a lo expuesto, es posible identificar dos tipos de criptografía dependiendo del tipo de llave utilizada: simétrica y asimétrica. La diferencia entre estos tipos de criptografía es el número de llaves involucradas en el proceso: para el primer caso se utiliza una sola llave; para el segundo, son empleadas dos llaves. La criptografía de carácter simétrico está basada en sistemas criptográficos que emplean la misma llave para cifrar y descifrar la información (Fig. 5 Sistema criptográfico simétrico).

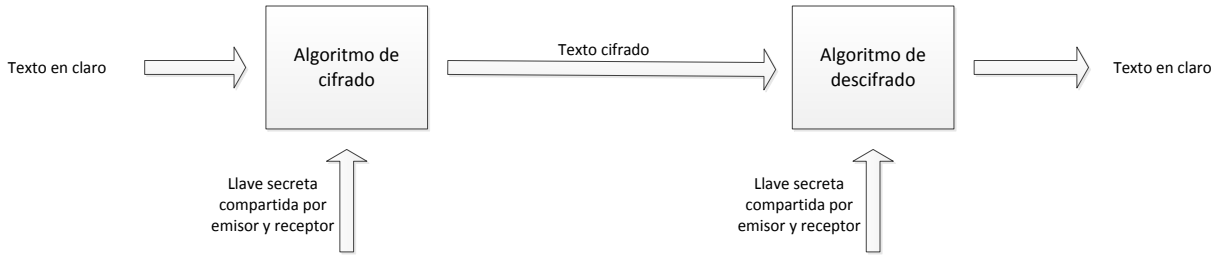


Fig. 5 Sistema criptográfico simétrico

Fuente: Elaboración propia a partir de (Stallings, 2004)

Estos algoritmos empleados se caracterizan por su velocidad y eficiencia, ya que usan operaciones simples que no requieren mucho poder de cómputo, en otras palabras, el tiempo usado para cifrar o descifrar la información es reducido. Por otro lado, el principal problema de la criptografía simétrica es el intercambio de las llaves: el emisor del mensaje cifrado necesita compartirle al receptor la misma llave que él usó, por lo que el canal usado debe ser seguro.

La contraparte de la criptografía de llave privada —otra forma en que se le conoce a la criptografía simétrica— es la de llave pública o asimétrica; su principal característica es el empleo de dos llaves distintas, pero relacionadas entre sí, para realizar las operaciones de cifrado o descifrado, aunque dada su naturaleza, también permite ejecutar procesos de autenticación de mensajes (firma) y distribución de llaves. Tiene su origen en la propuesta de Diffie y Hellman en 1976

para intercambiar de forma segura las llaves necesarias para un proceso de cifrado o descifrado posterior (Stallings, 2004).

Un sistema criptográfico de índole asimétrica está formado por seis componentes básicos: el texto en claro, el algoritmo de cifrado, la llave (dividida en llave pública y llave privada para evitar confusiones con la criptografía simétrica), el texto cifrado y el algoritmo de descifrado (Fig. 6 Sistema criptográfico asimétrico).

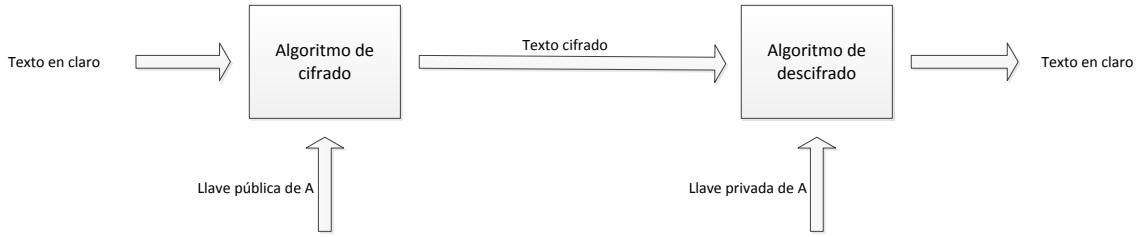


Fig. 6 Sistema criptográfico asimétrico

Fuente: Elaboración propia a partir de (Stallings, 2004)

Los algoritmos asimétricos solventan los problemas relacionados al proceso de creación, mantenimiento e intercambio de llaves simétricas, ya que un usuario necesitaría recordar solamente su llave privada para hacer uso del sistema criptográfico, dado que las llaves públicas son accesibles a todos. De esta naturaleza surge el concepto de autenticación de mensajes o firma digital.

Si una persona, por medio de la llave pública, es capaz de descifrar un mensaje cifrado con la llave privada de otro sujeto, significa inequívocamente que sólo el dueño del par de llaves pudo emitir el mensaje cifrado, ya que nadie más tiene la llave privada y nadie más podría alterar el mensaje. Para el caso del Instituto, es posible verificar la autenticidad de los datos cifrados en la Credencial por medio de la llave pública del algoritmo asimétrico (algoritmo de firma digital) empleado y así asegurar que el documento de identidad es válido y fue emitido por el mismo INE.

2.4.1 HSM

De acuerdo a lo mencionado en la descripción de la criptografía simétrica y asimétrica, el punto principal sobe el que radica la mayor parte de la seguridad de la información cifrada o firmada es la llave criptográfica. Debido a esta importancia, se han desarrollado diferentes procedimientos para emplearla, entre ellos los dispositivos de hardware especializados. Estos dispositivos son construidos para salvaguardar las llaves criptográficas en todo momento, por lo que también se especializan en la ejecución de los algoritmos, es decir, en el proceso de convertir el texto en claro en un criptograma, y viceversa.

Así, los HSM (Hardware Security Module) son piezas de hardware, así como todo el firmware y software asociados para su funcionamiento, los cuales pueden ser incluidos dentro de una computadora o estar construidos como *appliance*. Estos permiten ejecutar tareas de cifrado, descifrado, generación y administración de llaves, obtención de hash, entre otras. Adicionalmente, los HSM ofrecen funcionalidades contra la manipulación física de sus componentes.

El SysAdmin Audit, Networking and Security Institute (NIST) considera que algunas de las configuraciones más usuales para los HSM son (Attridge, 2002, pág. 3):

- Generación y almacenamiento seguro de llaves criptográficas para autoridades de certificación.
- Herramienta para la autenticación mediante la verificación de firmas digitales.
- Acelerador para transmisiones mediante SSL o TLS.
- Herramienta para cifrar información sensible en ambientes con poca seguridad.
- Herramienta para la verificación de la integridad de la información almacenada en una base de datos.
- Generación segura de llaves para la producción de “smartcards”.

En general, los fabricantes de módulos criptográficos desarrollan sus productos para el cumplimiento de diversas normas y características que les permitan competir en el mercado, entre los que destacan (Attridge, 2002, pág. 4):

- Validación de FIPS 140-2: Este estándar define cuatro niveles para la validación de los HSM, lo que no significa que el producto sea perfecto, sino que éste ha pasado por un proceso de verificación de requerimientos mínimos de seguridad mediante pruebas realizadas en instalaciones especializadas.
- Implementación de algoritmos de código abierto y ampliamente aceptados. Es preferible que el módulo criptográfico no use algoritmos propietarios.
- Generación robusta de números aleatorios.
- Fuente segura de tiempo: La auditoría y el no repudio requieren el registro de mensajes que incluyan la fecha y la hora que provengan de una fuente protegida. En caso de que no sea así, todas las transacciones registradas perderían su validez.
- Interfaz estandarizada para desarrolladores.
- Interfaz de usuario sencilla y segura: esta interfaz debe implementar un método de autenticación para operador.
- Instalación física bien documentada.
- Mecanismo seguro de respaldo de llaves.
- Protección de llaves: El módulo criptográfico no debe permitir que las llaves a su resguardo sean almacenadas o enviadas fuera de sus límites. Toda llave que sea exportada, debe ser cifrada.
- Resistencia a manipulaciones: El HSM debe implementar mecanismos para detectar intentos de manipulación física y, en caso de ser así, deberá tener la capacidad de borrar toda la información que contenga.
- Escalabilidad: El módulo debe ser capaz de adaptarse a los cambios producidos en la red donde opera. Debe tener la capacidad de instalarse dentro de un clúster y ofrecer alta disponibilidad.

- HMAC: El módulo debe poder verificar la integridad de los datos almacenados en alguna base mediante MAC.[8]

Por otro lado, los HSM tienen ciertas desventajas con respecto a otras soluciones criptográficas implementadas a través de software. En este punto es necesario evaluar el costo-beneficio de utilizar una u otra solución (Attridge, 2002, pág. 6):

- El mayor problema de los HSM es el precio. Dependiendo del nivel de funcionalidad y seguridad, los módulos criptográficos pueden costar una cantidad considerable de dinero comparados con las soluciones de software.
- La mayoría de los fabricantes retienen información acerca de cómo está construido el HSM y cómo es su funcionamiento. Se limitan a indicar que su producto funciona y cumple con ciertos requisitos y estándares.
- Por último, otra gran desventaja de los HSM es la dificultad para actualizarlos, es decir, si es necesario actualizar el software o firmware del módulo, esto resulta muy complicado e impacta directamente al negocio.

2.4.2 FIPS

FIPS es el acrónimo de *Federal Information Processing Standards*, considerado una serie de publicaciones de los requerimientos de seguridad del gobierno estadounidense. Es desarrollado y mantenido por el NIST (*National Institute of Standards and Technology*) para proporcionar las líneas base que deben cumplir todos los productos de seguridad con la finalidad de ser adquiridos por el gobierno de Estados Unidos. Dentro de los FIPS existentes, el 140-2 es de especial relevancia por relacionarse con los HSM.

[8] Message Authentication Code: Algoritmo que combina una llave con un hash para proveer un código que pueda ser ligado a un conjunto de datos para asegurar su integridad.

Concretamente, el FIPS 140-2 es el estándar que especifica los requerimientos de seguridad que deben satisfacer los HSM utilizados para proteger información sensible. Según el *National Institute of Standards and Technology* (2001) está compuesto por cuatro niveles de seguridad y cubre 11 aplicaciones y ambientes donde los módulos son desplegados:

- **Nivel 1**: Cubre el nivel más bajo de seguridad y requiere al menos un algoritmo o función de seguridad aprobada[9]. No es necesario el cumplimiento de mecanismos físicos de protección más allá de los requisitos para componentes de un ambiente de producción. Un ejemplo claro son las tarjetas criptográficas para equipos de cómputo personales. Los componentes de firmware y software de este tipo de módulos pueden ser ejecutados en cualquier sistema operativo de propósito general y por cualquier usuario.

- **Nivel 2**: Este nivel demanda mecanismos de seguridad física contra ataques de manipulación, esto incluye sellos de evidencia o candados en cada tapa removible del dispositivo. Dichos mecanismos son puestos de tal manera que necesiten ser rotos si se quiere tener acceso a las llaves criptográficas en claro o a los parámetros críticos de seguridad del módulo (CSP, del inglés *Critical Security Parmeters*). Adicionalmente, este nivel necesita autenticación por roles, de tal forma que un operador realice únicamente las funciones que le fueron conferidas. Estos módulos pueden ser usados en un sistema operativo de propósito general que cumpla con lo dispuesto en los *Perfiles de Protección* (PP) del Anexo B del *Common Criteria* (CC) y que sea evaluado mediante el nivel EAL2[10] o uno superior.

[9] Se considera una función aprobada a aquellos algoritmos criptográficos, mecanismos de administración de llaves criptográficas o técnicas de autenticación que han sido admitidos en algún estándar o fueron listados en las funciones de seguridad aprobadas por FIPS o recomendadas por el NIST (NIST, 2001, pág. iv).
[10] *Evaluation Assurance Level del Common Criteria*

- **Nivel 3**: Aquí se implementan los mismos mecanismos que en el nivel anterior y a ello se suma la posibilidad de prevenir que un intruso obtenga acceso a los CSP mediante el uso de cerraduras más fuertes o la posibilidad de borrar completamente la información del módulo en caso de ser abierto. Para la autenticación, el nivel 3 especifica que debe realizarse mediante la verificación de la identidad del operador (incrementando con ello la seguridad de la autenticación por roles del segundo nivel). El HSM autentica la identidad de un operador y verifica que cuente con los suficientes permisos para asumir el rol y ejecutar las tareas que le corresponden.

  Por otro lado, en este nivel es necesario que la entrada y salida de los CSP en claro sea realizado por medio de puertos que se encuentren físicamente separados del resto de los puertos, o por medio de interfaces que estén lógicamente separadas de otras interfaces a través de una "ruta de confianza". Con respecto al sistema operativo, se debe cumplir con lo especificado en los PP, la funcionalidad de "ruta de confianza" y ser evaluado con el nivel EAL3 (o superior).

- **Nivel 4**: Nivel de seguridad más alto especificado por el FIPS 140-2, ya que el módulo tiene mecanismos de seguridad capaces de detectar y responder a todos los intentos no autorizados de acceso físico. Todo intento de entrar al módulo desde cualquier dirección tiene una muy alta probabilidad de ser detectado y, por ende, toda la información contenida sería borrada de inmediato. Este tipo de módulos son generalmente usados en ambientes en donde no exista o sea muy reducida la seguridad física donde se sitúa el dispositivo.

  Igualmente, los HSM cuentan con protección contra condiciones ambientales o fluctuaciones fuera de los rangos normales de voltaje o

temperatura provocados o no provocados por un atacante. Para el caso del sistema operativo se deben cumplir los mismos requisitos del nivel 3 con la diferencia de que el nivel de evaluación es el EAL4 o superior.

En otros aspectos, el FIPS 140-2 define una sección de “requerimientos de seguridad” (Tabla 2.5) que deben ser cubiertos por los módulos criptográficos que pretendan ser validados a través de este estándar. Dichos requerimientos cubren áreas relacionadas al diseño e implementación del módulo. Esto se refleja, a modo de resumen, en la siguiente tabla tomada del FIPS PUB 140-2 (NIST, 2001, pág. 12).

Tabla 2.5 Requerimientos de seguridad del FIPS 140-2

	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Especificación de Módulo Criptográfico	Especificación del módulo criptográfico, alcances del módulo, algoritmos aprobados y modos de operación aprobados. Descripción del módulo criptográfico, incluyendo todo el hardware, software y componentes de firmware. Declaración de póliza del módulo de seguridad.			
Puertos e interfaces del módulo criptográfico	Interfaces requeridas y opcionales. Especificación de todas las interfaces y de todas las rutas de datos de salida y entrada.		Puertos de datos para parámetros críticos de seguridad no protegidos lógica o físicamente separados de los otros puertos de datos.	
Roles, Servicios, y Autenticación	Separación lógica de roles y servicios requeridos y opcionales.	Autenticación basada en roles o identidad.	Autenticación basada en identidad.	
Modelo de estados finitos	Especificación del modelo de estados finitos. Estados requeridos y opcionales. Diagrama de transición de estados y especificación de transiciones de estado.			
Seguridad física	Equipamiento	Cerraduras y	Detección y	Detección y

	de nivel de producción.	evidencia de manipulación.	respuesta a manipulaciones en puertas y cubiertas.	respuesta a manipulaciones en toda la construcción del módulo.
Ambiente de operación	Un solo operador. Código ejecutable. Técnica aprobada de integridad.	Perfiles de protección del *Common Criteria* y evaluación de EAL2 con la especificación de controles de acceso discrecionales y mecanismos de auditoría.	Perfiles de protección del *Common Criteria* más evaluación EAL3 con ruta de confianza y modelo de políticas de seguridad.	Perfiles de protección del *Common Criteria* más ruta de confianza evaluada en EAL4.
Administración de llaves criptográficas	Mecanismos de manejos de llaves: generación de números aleatorios y llaves, establecimiento de llave, distribución de llaves, entrada y salida de llaves, almacenamiento de llaves y el borrado de la llave.			
	Llaves secretas y privadas son establecidas a través de métodos manuales y puede que sean ingresadas u obtenidas (sacadas) como texto en claro.		Las llaves secretas y privadas son establecidas usando métodos manuales y deben ser ingresadas u obtenidas en su forma cifrada o mediante procedimientos de secreto compartido.	
EMI/EMC[11]	Requerimientos aplicables del FCC para la radio. Uso para negocio.		Para uso doméstico de acuerdo a la FCC	
Pruebas	Pruebas de encendido: pruebas de algoritmos criptográficos, pruebas de integridad de software/firmware, pruebas de funciones críticas. Pruebas condicionales.			

[11] Interferencia electromagnética y compatibilidad electromagnética.

Garantía de diseño	Gestión de la configuración, Generación e instalación segura. Correspondencia entre diseño y política. Guías documentadas	Sistema de administración. Distribución segura. Especificaciones funcionales.	Implementación de lenguajes de alto nivel.	Modelo formal. Explicaciones detalladas. Precondiciones y pos-condiciones.
Mitigación de otros ataques	Especificación de mitigaciones contra ataques para los cuales no hay requerimientos que puedan ser sometidos a pruebas.			

Fuente: Traducción libre de (NIST, 2001, pág. 12)

Todos los módulos criptográficos son probados en cada uno de los requerimientos mencionados en la tabla anterior. Con ello, se puede verificar el nivel de cumplimiento en cada sección además de ofrecer un resultado general de todos los requerimientos.

Capítulo III
Participación en el Servicio de Cifrado de la Credencial para Votar

El proyecto que es descrito en el presente documento forma parte del proceso de generación de la Credencial para Votar, por lo que sólo se aborda una parte de todo el trabajo realizado por el Instituto para generar y entregar la Credencial a un ciudadano. A grandes rasgos, se puede representar según la Fig. 7 Proceso de generación de una Credencial para Votar:

1. El ciudadano reúne todos los documentos solicitados por el Instituto[12].
2. Posteriormente, el ciudadano acude a un Módulo de Atención Ciudadana, entrega sus documentos y proporciona los datos adicionales solicitados por el Instituto[13].
3. El Instituto verifica los datos y documentación del ciudadano, si todo es correcto, se genera o actualiza el registro del ciudadano en el RFE.
4. En el proceso interno de fabricación de la Credencial, se envían los datos del ciudadano hacia el servicio de cifrado. Aquí, se cifra la información mediante el algoritmo simétrico y se firma mediante el algoritmo asimétrico.

[12] A fecha de abril de 2016, el INE solicita: Documento de acreditación de nacionalidad, comprobante de domicilio y una identificación con fotografía. (Instituto Nacional Electoral, 2014)
[13] A fecha de abril de 2016, el INE solicita: Nombre y domicilio actual, huellas dactilares, fotografía (tomada en sitio), firma autógrafa en Pad de firma, copia digitalizada de los documentos del paso 1 (realizado en sitio). (Instituto Nacional Electoral, 2014)

5. Una vez que se cuenta con la información cifrada, ésta es usada para generar el PDF-417, mismo que es impreso en la Credencial.
6. Finalmente, la Credencial es entregada al ciudadano en el módulo donde realizó su trámite.

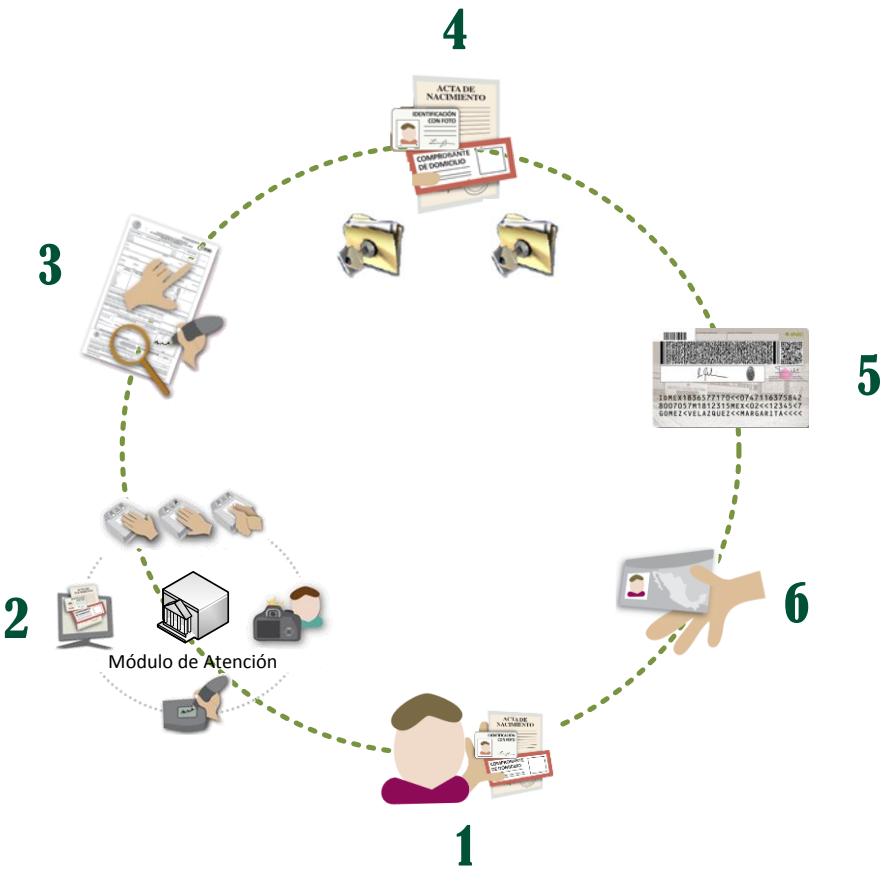


Fig. 7 Proceso de generación de una Credencial para Votar

Fuente: Elaboración propia a partir de (Instituto Federal Electoral, 2013)

Entendido el proceso y con la finalidad de llevar a cabo la construcción del servicio, se definió la división del proyecto en dos fases. La primera de ellas consistió en la instalación de equipos criptográficos en las instalaciones Centrales del INSTITUTO NACIONAL ELECTORAL, con el objetivo de crear una infraestructura capaz de proveer el servicio de cifrado y descifrado de la información contenida en la Credencial para Votar. La segunda fase, en la que participé directamente,

consistió en la migración de la infraestructura creada en la fase anterior hacia las instalaciones del Centro de Datos principal del Instituto.

La FASE 1 se describirá únicamente para dar el contexto en el que se desarrolló mi actividad profesional; mientras, la FASE 2 será descrita con mayor detalle, aquí cabe advertir que la información descrita es ficticia y no representa la implementación real del servicio, ya que se encuentra catalogada como reservada en los términos que determina el INSTITUTO NACIONAL ELECTORAL. Adicionalmente, resulta importante señalar que el proyecto se inició en el entonces INSTITUTO FEDERAL ELECTORAL, por lo cual hago referencia a normatividades que fueron sustituidas a causa de la Reforma Electoral llevada a cabo entre 2013 y 2014. La FASE 2 inició sus actividades con el recién creado INSTITUTO NACIONAL ELECTORAL.

3.1 Descripción del proyecto

El sub-proyecto de "Consolidación de la solución de cifrado para la protección de la información del Padrón Electoral", que formó parte del *Proyecto del Servicio de Producción de Formatos de Credencial para Votar*, tuvo, entre otros, el objetivo de:

> Robustecer las medidas de seguridad a corto plazo para la protección del Padrón Electoral mediante el cifrado de la información contenida en el código bidimensional de la Credencial para Votar. (Instituto Federal Electoral, 2013)

Los requerimientos generales asociados al objetivo mencionado fueron (Instituto Federal Electoral, 2013):

1. Creación de llaves criptográficas: Contar con un mecanismo robusto para la generación de llaves criptográficas con niveles elevados de aleatoriedad (entropía) y que impida su generación por sujetos no autorizados.
2. Uso seguro de llaves criptográficas: Contar con un mecanismo que haga un uso seguro de las llaves criptográficas generadas por el Instituto, evitando así comprometerlas en el proceso.
3. Volumen de operaciones criptográficas: Contar con una solución criptográfica que pueda atender un gran volumen de peticiones para cifrar o

descifrar información, en el entendido de que una operación de cifrado corresponde a una credencial generada.

Por otro lado, se enlistan algunas consideraciones en la materia (Instituto Federal Electoral, 2013):

a. El tiempo de vida de las llaves criptográficas se estimó a un número de años determinado.
b. El servicio de seguridad principal proporcionado por la solución criptográfica debe ser la confidencialidad. Esto se debe a que, a través de la información cifrada, se podrá identificar si una credencial es auténtica o se trata de un documento apócrifo.
c. El Instituto contaba con módulos criptográficos previamente adquiridos.
d. El límite de tiempo para poner en marcha la solución correspondía a noviembre de 2013, mes en el que debía comenzar la producción del nuevo modelo de la Credencial para Votar.

Como posibles soluciones, se consideraron las siguientes opciones:

I. Escenario 1: Desarrollo de un módulo de generación y uso de llaves criptográficas, así como de operaciones de cifrado y descifrado de información. Este módulo sería desarrollado por el área de sistemas del Instituto.
II. Escenario 2: Hacer uso de los módulos criptográficos del Instituto para la generación de las llaves criptográficas.
III. Escenario 3: Hacer uso de los módulos criptográficos con los que ya contaba el Instituto para todas las operaciones que impliquen la generación o uso de las llaves criptográficas.

Con respecto a los escenarios uno y dos, se identificaron una serie de riesgos que se presentan en la Tabla 3.1 Riesgos del Escenario 1 y 2.

Tabla 3.1 Riesgos del Escenario 1 y 2

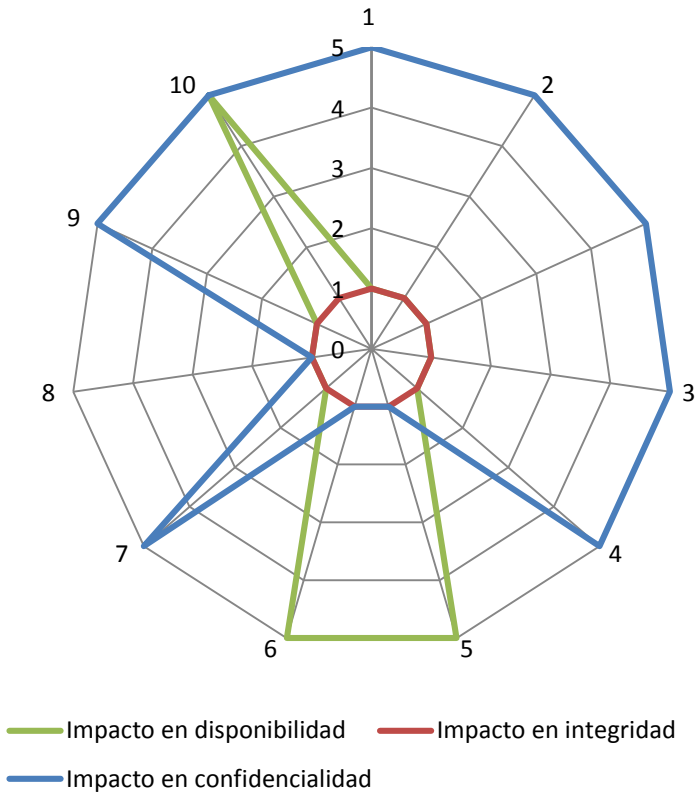
	Activo	Descripción	Vulnerabilidades	Amenazas	Impacto
1	Generador de semillas para las llaves	Un usuario malintencionado podría predecir la generación de las semillas si se utilizan APIs no seguras.	Existen paquetes de software que no usan tamaños robustos de semillas. Por ejemplo, la clase javax.crypto.cipher usa una semilla de 64 bits, lo que implica 2^{64} operaciones para obtenerla. Computacionalmente es posible obtenerla en tiempos cortos.	Criptoanálisis e ingeniería inversa	Obtención de semillas y reproducción de las llaves criptográficas por un tercero.
2	Llaves simétrica y asimétrica	Procesamiento de llave simétrica y asimétrica en memoria. El manejo inadecuado de llaves en memoria puede provocar la obtención de las llaves.	Una vez construidas en memoria las llaves, se puede provocar un error en la aplicación evitando el proceso de borrado de estas y pudiendo acceder a ellas.	Robo de información mediante técnicas que provoquen un mal funcionamiento de la aplicación.	Obtención de las llaves con las que se cifra y se firman los datos personales en la CPV.
		Un usuario interno con acceso al servidor donde reside el módulo de cifrado y descifrado podría obtener las llaves almacenadas en RAM.	Las llaves de cifrado están en claro en la memoria RAM.	Robo de información mediante técnicas que provoquen un mal funcionamiento de la aplicación.	Obtención de las llaves con las que se cifra y se firman los datos personales en la CPV.

	Activo	Descripción	Vulnerabilidades	Amenazas	Impacto
3	Módulo de cifrado y descifrado de información	1.-Dentro del código se encuentran almacenadas las llaves que permiten descifrar la información de la base de datos. 2.-Dentro del código se encuentran las funciones para reconstruir las llaves.	La aplicación no cuenta con un mecanismo que permita el ocultamiento de código. (Ofuscamiento de código).	Mediante herramientas de fácil acceso se puede realizar la recuperación del código fuente de la clase obteniendo las funciones para reconstruir las llaves.	Obtención de las llaves con las que se cifra y se firman los datos personales en la CPV.
4	Canal de comunica-ción hacia los servidores que almacenan las semillas	Un usuario malintencionado interno no autorizado podría interceptar el canal y obtener la información que viaja a través de él.	La comunicación no se realiza a través de un canal seguro de comunicación.	Intercepción del canal de comunicación.	Obtención de las semillas que generan las llaves de cifrado y de la llave que descifra la información de la base de datos.
5	Servidor de almacena-miento de semillas.	Sería poco probable recuperar las llaves si alguna de las semillas es eliminada del servidor debido a un error por parte del administrador y/o debido a un ataque por parte de un tercero.	No se cuenta con un esquema de alta disponibilidad para el almacenamiento de la llave.	Acceso no autorizado a los servidores. Errores no intencionales por parte de los administradores.	Imposibilidad de reconstruir las llaves.

	Activo	Descripción	Vulnerabilidades	Amenazas	Impacto
6	Dispositivos de comunica-ción, servidores (web y de aplicación)	La cantidad de operaciones de cifrado podría provocar la interrupción del servicio.	Falta de una arquitectura redundante para el cifrado y descifrado de la información.	Dimensiona-miento no acorde al número de transacciones de cifrado y descifrado no esperadas.	Detener por completo el proceso de producción de la CPV. Operación del servicio con niveles poco aceptables.
7	Servidores de generación de semillas	En caso de sustitución o mantenimiento de los servidores que almacenan las semillas utilizadas en el cifrado de la CPV, se puede revelar información si no se realiza un borrado seguro.	Falta de borrado seguro de servidores.	Análisis forense *a posteriori*.	Recuperación de las semillas generadoras de las llaves de cifrado.
8	Bitácoras	Falta de bitácoras que indiquen las actividades realizadas en el servidor o en el módulo.	Falla en la implementación de bitácoras en el módulo o los servidores.	Los administradores no activen y configuren adecuadamente las bitácoras	No se podrá detectar la causa o el origen de una falla o error en los sistemas por lo que existiría retrasos en la solución de los mismos No se tendrá trazabilidad en caso de un incidente.

	Activo	Descripción	Vulnerabilidades	Amenazas	Impacto
9	Servidores de aplicación	Acceso no autorizado a los servidores de aplicación.	Existencia de usuarios con acceso a los servidores.	Usuarios con acceso a los servidores, de manera no intencional o dolosa, obtengan permisos no autorizados.	Obtener las llaves por un usuario no autorizado.
10	Servidores de generación de semillas	La configuración inadecuada de los parámetros de seguridad en los servidores de semillas conforme a las buenas prácticas para la generación de las llaves criptográficas (NIST 800-133 *recomendation for cryptographic key generation)*.	Carencia de procedimientos para el fortalecimiento de los servidores de acuerdo a lo establecido en las buenas prácticas para la generación de llaves criptográficas.	Los posibles atacantes que aprovechen alguna vulnerabilidad para obtener acceso no autorizado.	Obtener las llaves por un usuario no autorizado.

Fuente: (Instituto Federal Electoral, 2013)



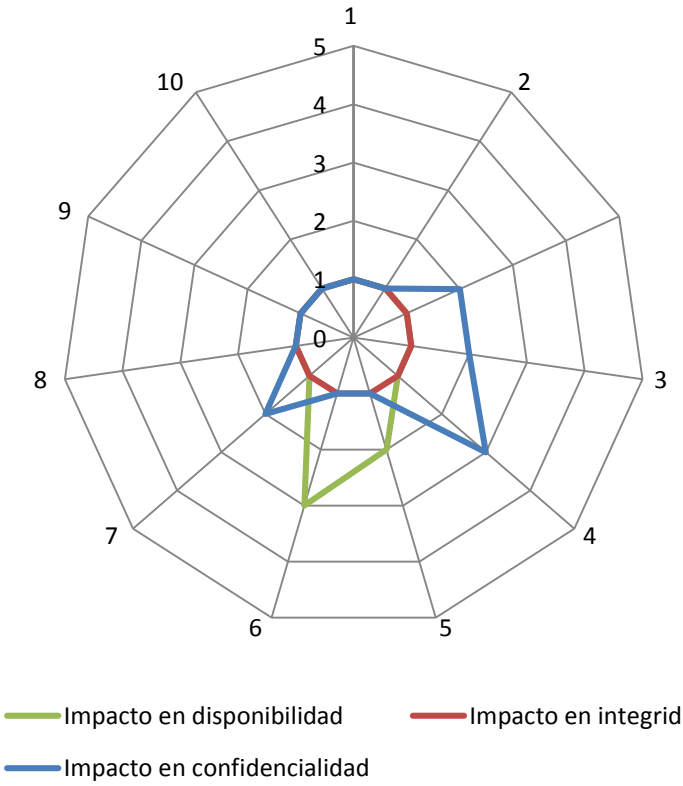
Valor del impacto	Confidencialidad / Integridad / Disponibilidad
5	Muy alto impacto
4	Alto impacto
3	Impacto moderado
2	Bajo impacto
1	Sin impacto

Fig. 8 Impacto del riesgo de escenarios 1 y 2

Fuente: (Instituto Federal Electoral, 2013)

Por otro lado, el NIST generó el documento *800-133 Recommendation for Cryptographic Key Generation,* el cual establece que el uso de la criptografía recae en dos componentes básicos: el algoritmo empleado y la llave criptográfica; por lo tanto, se recomienda que las llaves a emplear en operaciones criptográficas sean generadas mediante un *Generador de Bits aleatorios* (RGB – *Random Bit Generator*) aprobado, esto significa que las llaves criptográficas deben ser generadas dentro de módulos criptográficos (HSM) que cumplan con el estándar FIPS 140-2. El mismo documento también recomienda que las llaves no sean extraídas de los módulos y su uso sea únicamente dentro de los límites del equipo.

De acuerdo a lo mencionado por el NIST, el impacto del riesgo asociado al escenario 3 (Fig.9 Impacto del riesgo de escenario 3) sería muy poco con relación al resto de los escenarios, ya que estos implican demasiadas brechas de seguridad que deben ser aceptadas.



Valor del impacto	Confidencialidad / Integridad / Disponibilidad
5	Muy alto impacto
4	Alto impacto
3	Impacto moderado
2	Bajo impacto
1	Sin impacto

Fig. 9 Impacto del riesgo de escenario 3

Fuente: **(Instituto Federal Electoral, 2013)**

En conclusión, a raíz de los riesgos que implicaban los escenarios uno y dos, aunado a la capacidad de proteger las llaves criptográficas, la posibilidad de identificar la autenticidad de una Credencial y el beneficio de seguir las buenas prácticas internacionales establecidas por el NIST, el Instituto optó por escoger el escenario tres. En efecto, se lograrían mitigar todos los riesgos encontrados en el análisis correspondiente. Además, siguiendo las consideraciones iniciales del proyecto, el entonces IFE ya contaba con módulos criptográficos adecuados para ofrecer el servicio, por lo que se procedió a la creación de dos fases.

3.2 Fase 1

Los principales puntos a tener en cuenta durante esta fase fueron el tiempo de conclusión y la puesta en marcha de los equipos criptográficos con los que ya contaba el Instituto. Como se mencionó, la fecha límite establecida para disponer del servicio fue noviembre de 2013, pues se trataba de la fecha acordada para comenzar con la producción de credenciales; cualquier retraso en la FASE 1 significaba impactar en los compromisos del IFE.

Dada la sensibilidad del punto mencionado, se usaron los módulos criptográficos ya adquiridos en lugar de comenzar un proceso para adquirir nuevos. Iniciar una licitación para equipos nuevos implicaba recursos y tiempo de los que no disponía el IFE; por el contrario, usar los módulos en existencia aseguraba llevar a buen término la FASE 1. Sin embargo, dichos equipos eran usados para proveer otros servicios dentro de la Institución, a causa de esta situación, fue necesario planear una segunda fase.

Una vez establecidos todos los requerimientos y condiciones, el personal del INSTITUTO FEDERAL ELECTORAL adscrito al área de Infraestructura de la DERFE, en conjunto con personal de una empresa del sector privado, instaló y configuró el servicio de cifrado de la Credencial para Votar. Con esto se logró concluir la FASE 1 a tiempo, iniciando la producción del nuevo modelo de credencial en la fecha previamente estipulada.

3.3 Fase 2

Para la segunda etapa del proyecto se identificaron algunos puntos a mejorar que no pudieron ser implementados en la fase anterior y que el INSTITUTO NACIONAL ELECTORAL[14] debía atender para proveer un servicio más robusto y confiable. De los puntos principales destacan cuatro:

[14] Como ya se dijo, la FASE 2 dio inicio en el recién creado INSTITUTO NACIONAL ELECTORAL.

a) Debido a la ubicación física del servicio de cifrado y los sistemas que lo consumían, existía una latencia amplia que podía ser mejorada para que el proceso de cifrado de la información de la credencial fuera más rápido.
b) Nuevamente, a causa de la distribución física de los equipos, se vio la oportunidad de reducir la carga de tráfico en la red institucional. Si el servicio de cifrado era instalado en la misma ubicación que los clientes que lo utilizaban, todo el tráfico relativo circularía en la red local.
c) Los módulos criptográficos usados en la FASE 1 eran empleados para proveer otros tipos de servicios internos, por lo que la separación de ellos implicaría una mejora sustancial en su capacidad y rapidez.
d) Aunque la infraestructura de la FASE 1 fue configurada en alta disponibilidad, existían varios puntos de mejora del servicio que debían ser solventados en la segunda etapa.

Mi participación profesional, de la que deriva el presente escrito, fue llevada a cabo en el transcurso de esta fase del proyecto, principalmente en todo lo referente a la configuración de la nueva infraestructura. A raíz de esto, se enlistan algunas consideraciones sobre las circunstancias bajo las cuales desarrollé las actividades que me fueron asignadas.

1. Previo al arranque de la FASE 2, el INSTITUTO NACIONAL ELECTORAL realizó un proceso de licitación para la adquisición de los HSM que serían usados en la nueva infraestructura. Este punto concluyó con la compra y posterior instalación física de los equipos en el mismo Centro de Datos donde se encontraban los clientes.
2. Se hizo una transferencia de las llaves criptográficas de los HSM originales hacia los nuevos, mediante un protocolo. Para dar fe al proceso, en el evento participaron un notario público y todos los sujetos involucrados en el *secreto compartido*[15].

[15] Se denomina “secreto compartido” al proceso mediante el cual una llave criptográfica (específicamente, aquella que permite modificar la configuración del HSM o las llaves que almacena) es dividida en múltiples componentes —para no compartir individualmente el

3. La configuración de red donde fue instalado el servicio contemplaba el uso de distintas redes virtuales (VLAN) para cada componente.
4. La infraestructura que pretendía actualizarse hacía uso de un *servicio web* como interfaz entre el cliente y el HSM. Para la actualización del servicio, se usó el mismo software, así que no fue necesario desarrollar uno nuevo.

3.4 Implementación del Servicio de Cifrado de la Credencial para Votar

Arquitectura

Para el diseño de la infraestructura se tomaron en cuenta los requerimientos antes descritos, estableciendo tres capas separadas lógicamente por medio de VLANs, cada una correspondiente a un elemento diferente. Además, el diseño contempló un esquema de alta disponibilidad más robusto, por lo cual, en caso de falla o error de algún dispositivo, el servicio continuaría operando. A continuación, en la Fig. 10, se muestra la arquitectura simplificada en donde se incluye una VLAN dedicada a la administración de cada elemento.

conocimiento de la llave original— que pueden ser introducidos o extraídos por entidades separadas y, posteriormente, combinados para reconstruir la llave original (NIST, 2001, pág. 8). Una de sus características principales es la capacidad de obtener la llave original sin la necesidad de contar con todos los componentes en los que fue fraccionada, en otras palabras, la llave criptográfica original puede ser dividida en *N* partes, de las cuales, únicamente son requeridas un número *K* de ellas, en dónde *K* es menor o igual a *N.* Con el fin de evitar problemas, *N* y *K* no deben ser iguales, ya que si un elemento de *K* se corrompe sería imposible recuperar la llave original.

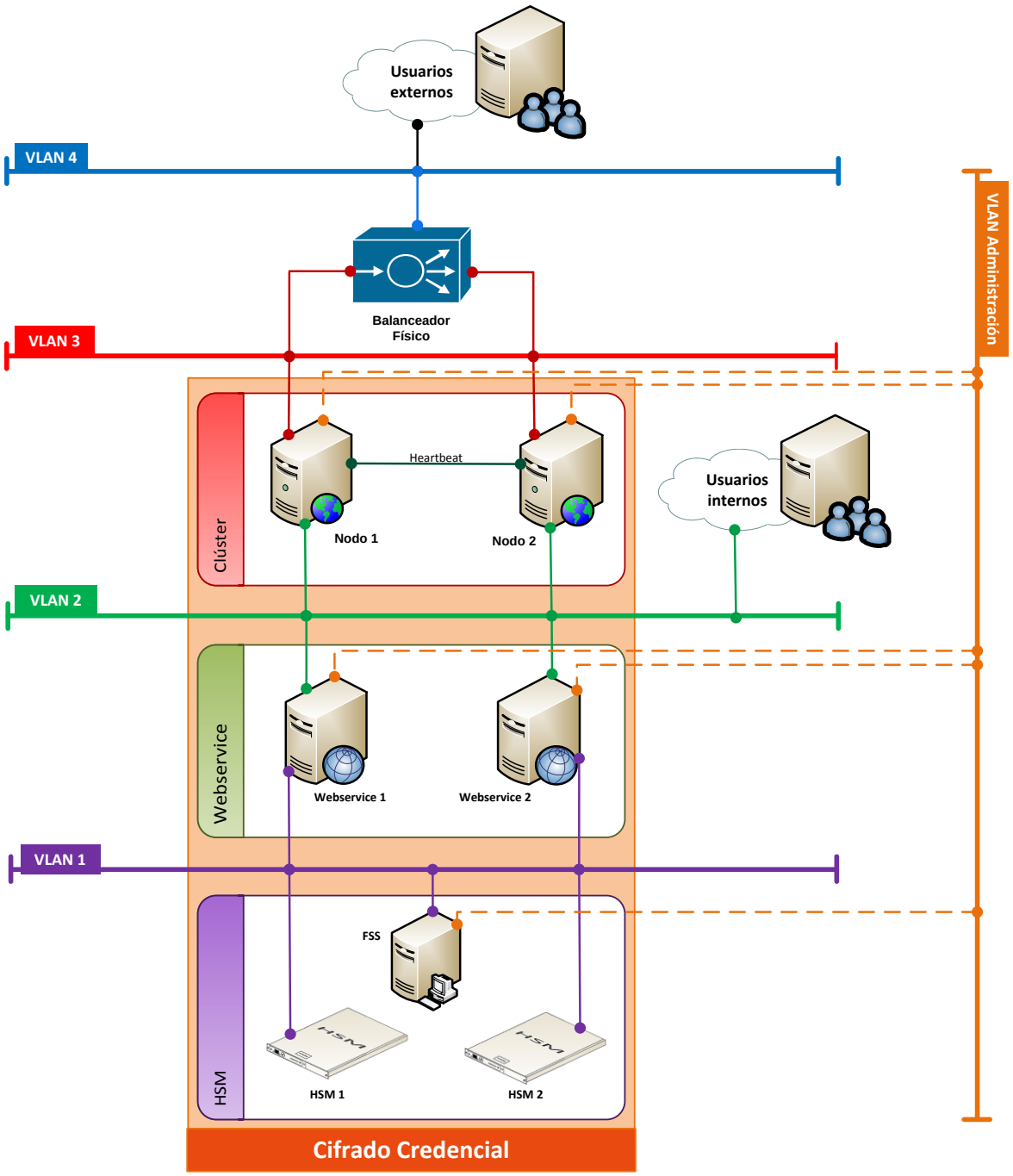


Fig. 10 Diagrama de arquitectura

Fuente: Elaboración propia, 2015

Capa HSM

Esta capa alberga todo lo relacionado con los módulos criptográficos. En ella se emplearon varios dispositivos con el propósito de brindar un servicio más confiable; si alguno tuviera fallas físicas o de comunicación, cualquiera de los otros no se vería afectados. Esto gracias a que cada dispositivo fue colocado en un *rack* diferente, de tal manera que no compartan alimentación eléctrica ni se conecten a los mismos dispositivos de comunicaciones; no obstante, a nivel lógico, los HSM se encuentran en la misma VLAN.

Por otro lado, en dicha capa se presenta un tercer dispositivo denominado *File Sharing Server* (FSS). Tal servidor hace las veces de almacenamiento compartido entre cada HSM, pues se almacena —de forma cifrada— toda la información que necesitan los módulos para operar (con excepción de las llaves criptográficas, las cuales no deben ser extraídas de los equipos).

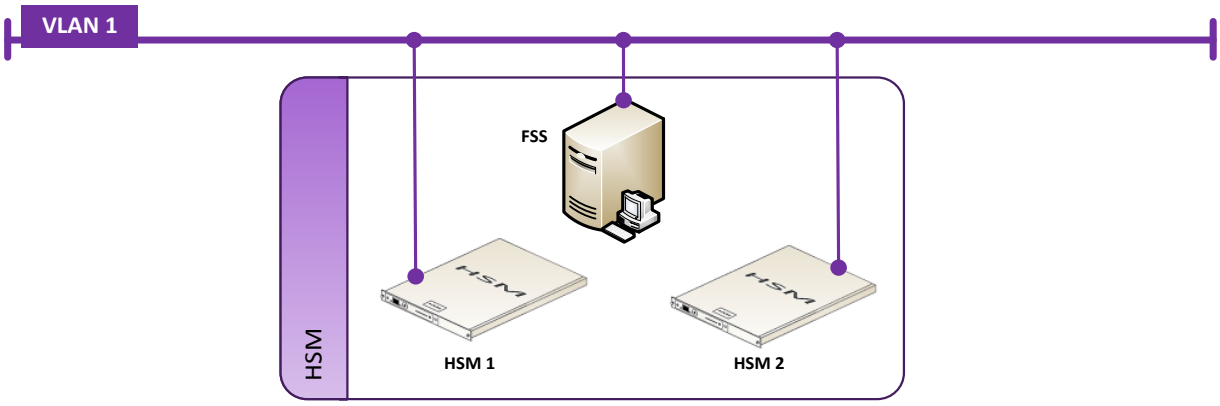


Fig. 11 Estructura de la Capa HSM

Fuente: Elaboración propia, 2015

Capa de Servicio Web

La segunda capa está compuesta por el mismo *servicio web* (del inglés *Web Service* o *WS*) usado en la FASE 1. El WS es una interfaz entre usuarios y HSM que facilita la realización de operaciones de cifrado o descifrado de la información sin que los primeros tengan conocimientos profundos acerca del funcionamiento de los módulos. El número de WS corresponde al mismo número de dispositivos criptográficos, esto es, por cada HSM instalado existe una instancia del WS.

Las instancias de WS son independientes de las demás, cada una puede atender sus propias peticiones sin afectar el funcionamiento del resto. Para continuar con un esquema robusto de alta disponibilidad, los WS deben ser ejecutados en un servidor diferente. Cabe destacar que los servicios web no tienen acceso directo a las llaves criptográficas, únicamente mandan instrucciones al HSM con la configuración correcta para enviar la respuesta al usuario.

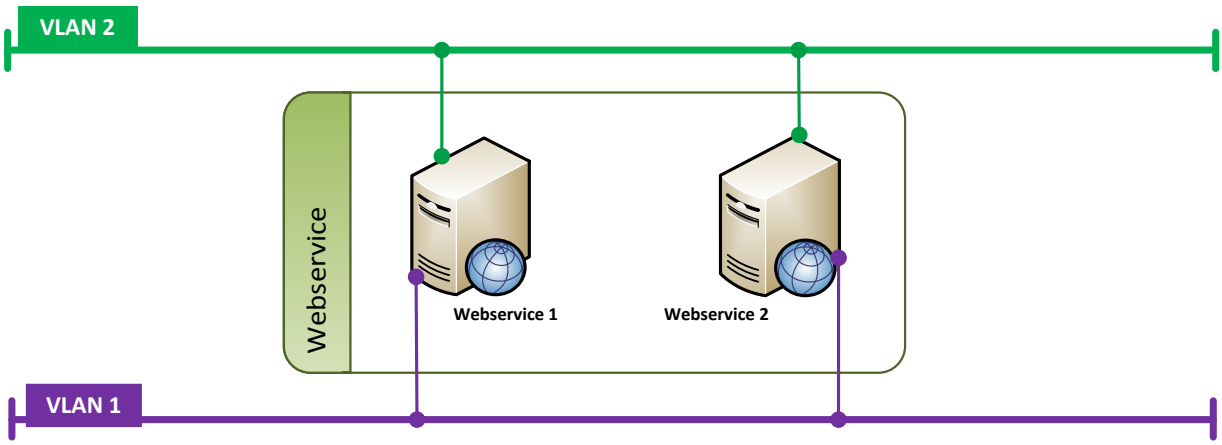


Fig. 12 Estructura de la Capa Servicio Web

Fuente: Elaboración propia, 2015

Capa de Clúster

Los usuarios[16] del servicio de cifrado de la información contenida en la Credencial para Votar son clasificados en internos y externos. Los usuarios internos son aquellos que consumen el servicio desde la misma VLAN, representan el conjunto de entidades que más peticiones realizan al servicio, por lo que la mayor parte de la carga proviene de ellos, en otras palabras, están involucrados en la producción de credenciales. Por otra parte, los usuarios externos son los que realizan peticiones fuera de la VLAN mencionada, pero siguen perteneciendo a la red del Instituto; su propósito, entre otros, es el de verificar la autenticidad de los datos de la Credencial para Votar.

Para proveer el servicio a los dos tipos de usuarios y mantener el esquema de alta disponibilidad, se estableció una tercera capa que alberga un conjunto de máquinas configuradas en forma de clúster. Esta configuración permite agregar servicios en modo de alta disponibilidad, además de ofrecer una solución para el balanceo de carga.

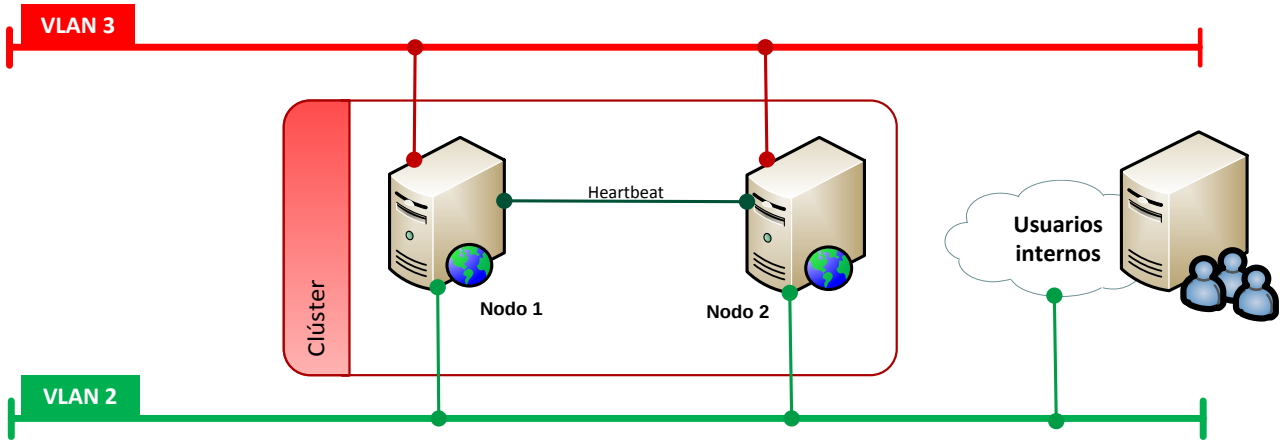


Fig. 13 Estructura de la Capa de Clúster

Fuente: Elaboración propia, 2015

[16] En este contexto, un usuario puede ser entendido como una máquina, un servidor, un proceso o un conjunto de ellos que requieren usar el servicio de cifrado o descifrado de información.

Capa de Balanceo de carga

Esta capa no es considerada parte de la nueva infraestructura que se configuró, sin embargo, es mencionada por ser el punto de unión entre la infraestructura nueva y los usuarios externos. Esto se debe a que las redes virtuales usadas no están configuradas para ser accesibles más allá de sus propios componentes, por lo que sin esta capa un usuario externo no podría hacer uso del servicio.

Los balanceadores de carga de esta sección son dispositivos físicos empleados para brindar distintos tipos de servicios internos en el Instituto; no obstante, se decidió usarlos porque su configuración era la requerida para comunicar a los usuarios externos. Su uso conllevó un mayor beneficio para el servicio de cifrado sin que ello significara un aumento en el costo.

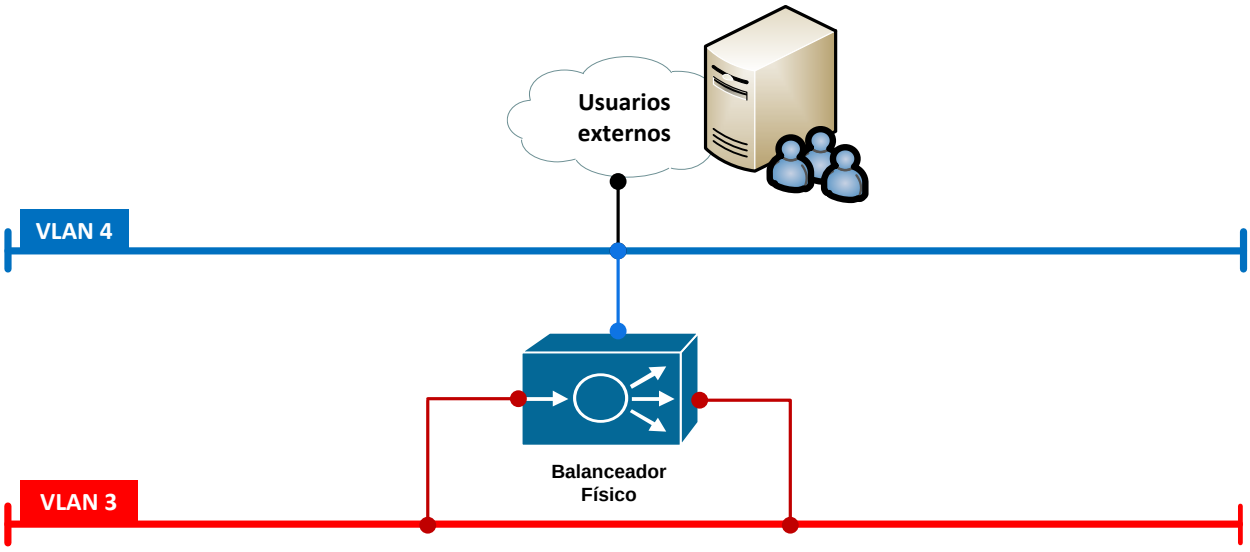


Fig. 14 Estructura de la Capa de Balanceo de carga

Fuente: Elaboración propia, 2015

3.5.1 Configuración de HSM

Cada dispositivo criptográfico fue instalado en el mismo Centro de Datos, el cual, cumple con las condiciones ambientales recomendadas por su fabricante de acuerdo a la Tabla 3.2 Condiciones ambientales de operación.

Tabla 3.2 Condiciones ambientales de operación

Condición ambiental	Rango de operación	
	Mín.	**Máx.**
Temperatura	0 °C	35 °C
Temperatura de almacenamiento	-20 °C	60 °C
Humedad	5%	95%
Presión	0	2000 milibar

Fuente: Elaboración propia a partir de (SafeNet Inc., 2015)

Dentro del Centro de Datos, los dispositivos fueron colocados en *racks* diferentes, cada uno con alimentación propia y redundante, así como conexiones a dispositivos de comunicaciones distintos. Con ello se proporciona alta disponibilidad a nivel físico para cada módulo. El *rack* es un modelo estándar de 19'' o 48.26 cm y con herrajes de tamaño regular para fijar los rieles de los HSM (Fig.15 Montaje en rack de un HSM). El aseguramiento de cada riel es sumamente importante, pues los modelos de HSM usados tienen sensores que enviarían alertas si detectan algún cambio en su posición.

Fig. 15 Montaje en rack de un HSM

Fuente: Elaboración propia, 2015

Después de la instalación física de los equipos, se realizó la migración de las llaves criptográficas establecidas en la FASE 1. En un HSM que cumpla con FIPS 140-2 nivel 3, las llaves únicamente pueden ser creadas o transferidas con la autorización de varias personas; es decir, la manipulación se realiza mediante el secreto compartido. En el caso de los HSM, el secreto compartido es manejado a través de tarjetas que le pertenecen a cada sujeto involucrado[17]; el uso de cada tarjeta es protegido por una contraseña que sólo es conocida por su dueño.

Ya que se trató de información confidencial del INE, la migración fue realizada en un acto formal ante notario público. Se dio fe a la ejecución correcta de la transferencia y al consentimiento de las personas involucradas a través del empleo de sus tarjetas. Además, también quedó asentado que los nuevos equipos HSM estaban completamente limpios y no habían sido manipulados para permitir el robo de la información.

De este punto en adelante, la configuración de cada componente de la infraestructura corrió por mi cuenta. En el caso de los módulos HSM, su administración la realicé con apoyo de una empresa privada que brindó sus servicios para la compra e instalación de los módulos. Durante esta actividad fue necesario acudir personalmente al Centro de Datos en donde se encontraban los HSM, ya que cualquier configuración que se efectúe sobre ellos debe ser a través de su interfaz física: no es posible realizar configuraciones, por seguridad, desde un lugar remoto.

La interfaz del dispositivo consta de una pantalla LCD que muestra la información sobre la que se está trabajando, junto con botones para introducir los datos requeridos. Opcionalmente, algunos módulos soportan teclados externos (completos o únicamente numéricos), lo que facilita sustancialmente el uso de los dispositivos. En la Fig.16 se muestra un diagrama sencillo de cómo luce un

[17] Cada tarjeta contiene un componente de la llave original, es decir, un elemento de K^{15}

HSM[18]. En la parte frontal se pueden apreciar la pantalla y los botones mencionados, así como el puerto de conexión para el teclado.

Fig. 16 Representación de un HSM

Fuente: Elaboración propia, 2015

Para realizar la configuración de los HSM se realizaron los siguientes pasos, donde cabe señalar, cada una de las actividades descritas se realizó —de ser aplicable— en cada módulo criptográfico instalado para la nueva infraestructura.

1. Instalación del software cliente en cada servidor que alberga el Servicio Web desarrollado. Adicionalmente, se instaló el software en el servidor FSS.

2. Para el servidor FSS se realizó un *hardening* a nivel sistema operativo, lo que implicó realizar configuraciones acordes a los estándares de seguridad en infraestructura establecidos por el INE; esto incluye configuraciones de usuarios, parámetros de kernel, sistema de archivos, demonios activos, actualizaciones de seguridad, software de monitoreo, firewall de host, NTP

[18] El diagrama presentado no corresponde a ningún modelo existente en el mercado. Las características mencionadas son cubiertas por varios productos, por lo que las imágenes tratan de representar a los módulos criptográficos en general.

(el tiempo marcado por el servidor debe estar sincronizado con el del HSM), entre otros. El servidor FSS fue instalado de tal manera que sólo pudiera comunicarse por la interfaz de administración y con cada uno de los HSM que lo utilizarían.

3. Ya en el módulo HSM, se estableció su dirección y máscara de red correspondientes a la VLAN 1, el *gateway* y la velocidad del enlace.

4. A continuación, se verificó, por medio de un ping, que la comunicación se estableciera entre cada HSM y cada cliente, además de que el FSS pudiera conectarse sin problemas.

5. Se configuró el FSS. Dentro de una línea de comandos en el servidor se ejecutó:

```
bash$ get-esn <dirección IP HSM
```

El comando regresa el ESN (*Electronic Serial Number*) del dispositivo. Para este caso, se usará el valor `42535-36356-65678ab98d`

```
bash$ FSS-setup <dirección IP HSM> 42535-36356-65678ab98d
```

Este comando crea todos los archivos que necesita el HSM para poder operar y ocupar el servidor como su sistema de archivos remoto.

6. Regresando al HSM, se le indica, por medio de su interfaz, cuál es el FSS que usará. También se establece que el servidor FSS será usado como almacenamiento de Logs.

7. Se reinicia el software cliente (demonio) en el servidor FSS.

8. Continuando con la configuración, se le debe ordenar al HSM cuáles serán los únicos clientes que se podrán conectar a ellos. De esta forma se asegura que sólo las máquinas configuradas podrán realizar procedimientos de cifrado o descifrado de la información. Para ello, se ejecuta lo siguiente en cada cliente (en este caso se trata de los servidores que albergan el web service):

```
$ enroll <dirección IP HSM>
```

   Este comando le indica al cliente que se va a conectar al HSM, por lo que únicamente debe esperar que le sea permitido.

9. En el HSM se agregan todos los clientes en la interfaz física. De acuerdo al diagrama de arquitectura, un web service (cliente) se conecta únicamente con un HSM, sin embargo, se configuró para que todos los clientes se conecten a cualquier módulo. La razón radica en la disponibilidad del servicio: puede suceder que un módulo tenga fallas físicas o su enlace no permita la comunicación con el cliente; pero con la configuración mencionada no sería necesario acudir a la ubicación de los módulos funcionales y asignarle el cliente que ha quedado “libre”.

   En el cliente, se termina de configurar el enrolamiento al instalar el servicio (demonio) al ejecutar:

```
$ config-startup
```

Se comprueba que el cliente pueda realizar operaciones con el HSM:

```
$ enquiry

Module #1:
 enquiry reply flags   none
 enquiry reply level   Six
 serial number
 mode                  operational
 version
 speed index           552
 rec. queue            19..152
 level one flags       Hardware HasTokens
 version string
 checked in            00000000          Mon Jun 16 10:19:23
 level two flags       none
 max. write size
 level three flags     KeyStorage
 level four flags



 module type code      7
 product name
 device name
 Enquiry    version
 impath kx groups
 feature ctrl flags    LongTerm
 features enabled              KM
 version serial
 connection status     OK
```

La respuesta debe indicar que el HSM se encuentra en operación (“operational”) y que la conexión se está llevando a cabo (“OK”).

Con estas acciones, los módulos criptográficos han sido ajustados y no es necesario volver a tocar su configuración.

3.5.2 Configuración de Web service

El web service o servicio web es un software hecho a la medida para fungir como interfaz entre usuario y HSM. Establece todos los parámetros necesarios para que las operaciones de cifrado y descifrado se realicen sin que el usuario conozca a profundidad el funcionamiento de los módulos criptográficos. Basa su

funcionamiento en el protocolo estándar SOAP[19], por lo que basta realizar una petición HTTP para que el software lo reconozca.

Para su operación, el software necesita (Instituto Nacional Electoral, 2014):

- Java instalado
- Software de cliente HSM (el mismo instalado en el FSS)
- Dar de alta el servidor como un cliente del HSM
- Llaves criptográficas almacenadas dentro del HSM
- Llaves en formato PKCS#11
- JCE – Debido a que los algoritmos usados se consideran robustos es necesario configurar Java para utilizar la "Unlimited Strength Jurisdiction Policy".

Los pasos de configuración de los servicios web consistieron, principalmente, en la instalación y entrada de parámetros del software, así como en la verificación de las operaciones de cifrado/descifrado de los HSM.

1. Cubrir los requisitos mencionados en el servidor destinado a albergar los servicios web. Para el caso de la configuración del JCE se realizó:

   Sustituir los archivos de la nueva política (`local_policy.jar` y `US_export_policy.jar`) en la carpeta `%JAVA_HOME%/lib/security`

[19] *Simple Object Access Protocol* (SOAP) es una forma de comunicar aplicaciones que sean ejecutadas en diferentes sistemas operativos y desarrollados con tecnologías y lenguajes de programación diferentes. Para su funcionamiento, SOAP usa mensajes construidos con XML (define sus propios elementos y sintaxis), por lo que cualquier aplicación que sea capaz de entender este lenguaje podrá enviar o recibir información de su contraparte. Por otro lado, SOAP únicamente define la composición de los mensajes, mas no la forma en cómo son intercambiados; para solventarlo se crearon los "SOAP bindings": mecanismos que permiten que los mensajes sean intercambiados usando un protocolo de la capa de transporte del modelo OSI. El protocolo más comúnmente usado y al que se hace referencia en este documento es el HTTP. (Refsnes Data, 2015)

2. Se agregó un nuevo proveedor criptográfico a la configuración de Java:

```
# vi %JAVA_HOME%/lib/security

security.provider.1=ruta.del.nuevo.proveedor
```

   Es necesario reescribir la lista predefinida del archivo, para que la numeración sea consistente.

3. Luego del paso anterior, se procedió a verificar la conectividad con el HSM mediante un comando del proveedor recién agregado. La salida corresponde a todos los algoritmos de cifrado que soporta el HSM

```
Cipher.AESWrap
Cipher.ArcFour
Cipher.Blowfish
Cipher.CAST
Cipher.CAST256
Cipher.DES
Cipher.DES2
Cipher.DESede
Cipher.DESedeWrap
Cipher.RSA
Cipher.Rijndael
Cipher.Serpent
Cipher.Twofish
…
…
…
```

4. Se instaló el software desarrollado a medida.

5. El paso anterior crea un ejecutable capaz de configurar servicios (demonios) en el servidor, los cuales son los servicios web ya mencionados. Es posible crear un número indefinido de servicios, sin

embargo, esto no se consideró, ya que se instaló el mismo número de servidores que de servicios web.

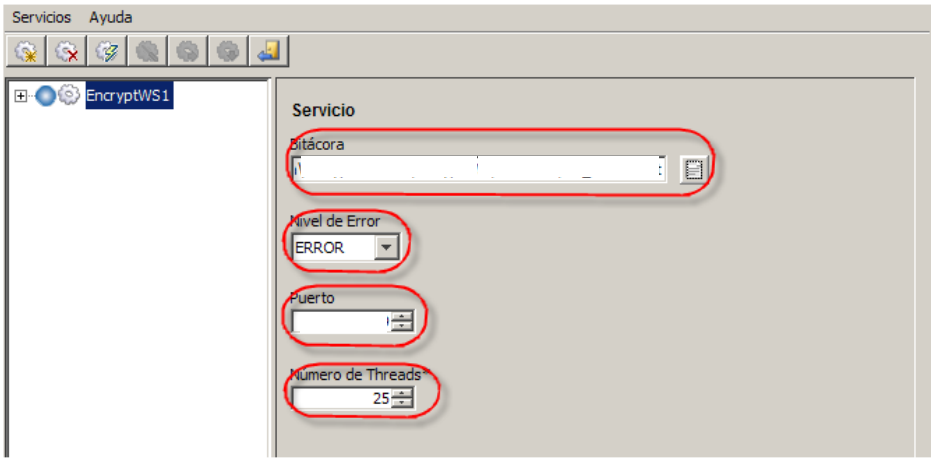


Fig. 3 Configuración de servicios web I

Fuente: (Instituto Nacional Electoral, 2014)

Para crear el servicio fue necesario indicar la ruta del archivo de Logs y el nivel de error que será registrado en al archivo; el programa soporta desde el modo *debug* hasta el registro únicamente de los errores graves ocurridos. Adicionalmente, se indica el puerto de escucha del servicio web —como ejemplo se usará el puerto `54321` para futuras referencias— y el número de hilos que se utilizarán.

6. Dentro del mismo programa, se debe indicar la librería que contiene el código para comunicarse con el HSM, así como la contraseña del operador que se encuentra en el dispositivo. Durante la migración de las llaves de la infraestructura de la FASE 1 a la nueva fue necesario ocupar las tarjetas pertenecientes a los dueños del secreto compartido (como se mencionó en secciones anteriores). Del mismo modo, para poder realizar configuraciones en el HSM o hacer uso de sus llaves almacenadas es requisito utilizar una tarjeta de operador.

La tarjeta de operador es una pieza especialmente diseñada para permitir diversas tareas dentro del HSM. Dos de las tareas asignadas a esta tarjeta son las de configurar parámetros sensibles del HSM (como los mencionados en la configuración de la capa anterior) y hacer uso de las llaves para operaciones de cifrado, descifrado y firma digital. Sin embargo, esta tarjeta no puede manipular ningún dato relacionado a las llaves, ya sea su almacenamiento, distribución, cambio o borrado.

En este contexto, se le indica al programa la librería mencionada, la contraseña de la tarjeta de operador y los alias de las llaves que serán usadas. El alias es el nombre por el cual el HSM reconoce a las llaves bajo su resguardo, si este dato no coincide completamente, el proceso que involucre el uso de la llave referenciada no podrá ser efectuado.

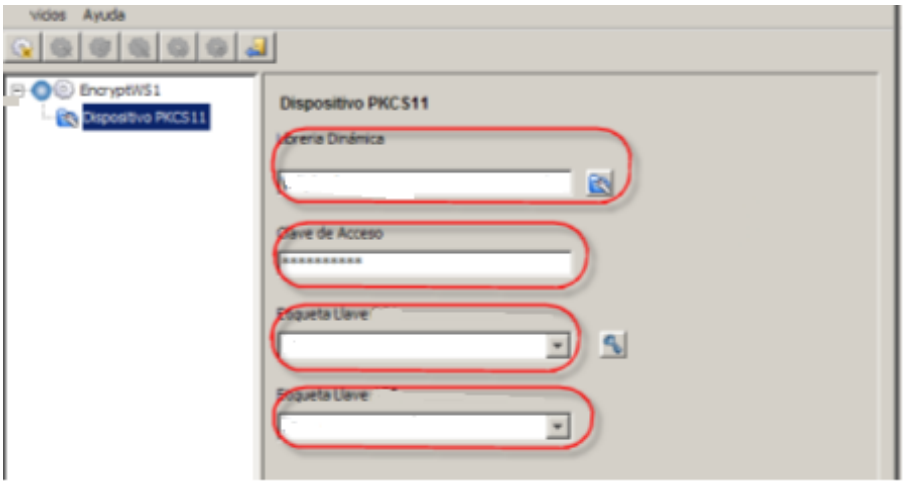


Fig. 4 Configuración de servicio web II

Fuente: (Instituto Nacional Electoral, 2014)

7. Llegado a este punto, se guarda la configuración y se inicia el servicio. El sistema operativo reconocerá el servicio web con el mismo nombre asignado, en este caso sería “EncryptWS1”.

8. Por último, se deben realizar pruebas puntuales para determinar que el servicio web se encuentre funcionando adecuadamente. Para ello, se diseñó otra herramienta que haga las veces de un usuario del servicio. Basta con seleccionar el algoritmo a emplear y proporcionar la información adecuada (ya sea el texto en claro o el texto cifrado). Se debe tomar en cuenta la dirección IP del servidor en donde se instaló el servicio web, sin embargo, también es posible utilizar el nombre DNS asignado.

   Para este ejemplo, se cifra con el algoritmo simétrico la letra 'a'. La siguiente imagen muestra una petición al servicio web mediante el protocolo HTTP y con la sintaxis de SOAP. Al respecto, cabe destacar que la información próxima a cifrar es convertida a base 64 con el fin de evitar problemas en su codificación.

```
POST / HTTP/1.1
Accept: text/xml, multipart/related
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
User-Agent:
Host: IP servidor:54321
Connection: keep-alive Content-Length: 313

<?xml version="1.0" ?>
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
<S:Body>
    <ns2:ProcessMessage xmlns:ns2="urn:sgdata">
        <request xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            <PlainText>YQ==</PlainText>
        </request>
    </ns2:ProcessMessage>
</S:Body>
</S:Envelope>
```

Fig. 19 Petición al servicio web

Fuente: Elaboración propia, 2015

Una vez enviada la petición, el WS contesta con el criptograma correspondiente, el cual fue originado en el módulo criptográfico.

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: 498
X-Frame-Options: deny
X-Content-type-options: nosniff
X-XSS-Protection: 1; mode=block
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
 xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    <SOAP-ENV:Body>
        <Response>
            <out xsi:type="   ">
                <CipherText>KqcZAsfmOm6QDwAIznJIVw==</CipherText>
            </out>
        </Response>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

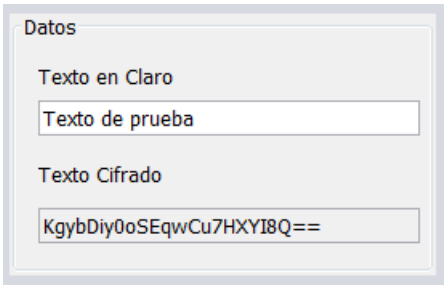
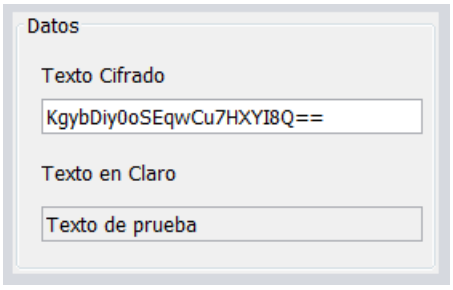
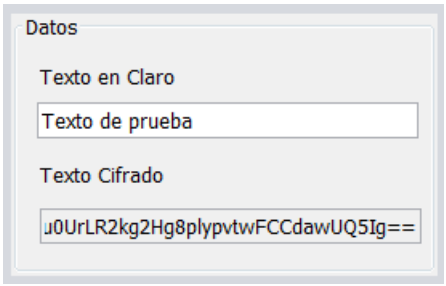
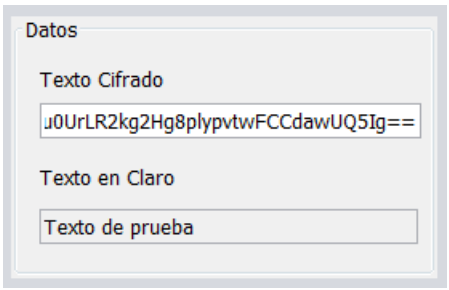
Fig. 20 Respuesta del servicio web

Fuente: Elaboración propia, 2015

Continuando con las pruebas, se empleó una herramienta desarrollada a medida, evitando así la manipulación directa del XML de las peticiones o respuestas del WS. En la Tabla 3.3 Verificación del servicio web se ejemplifica lo anterior.

Tabla 3.3 Verificación del servicio web

Operación	Respuesta
Servicio web a consumir	Web Service Ruta del Servicio: https://IP servidor:54321

Operación	Respuesta
Cifrado con algoritmo simétrico	
Descifrado con algoritmo simétrico	
Cifrado con algoritmo asimétrico	
Descifrado con algoritmo asimétrico	

Fuente: Elaboración propia, 2015

9. Como se observa, el servicio fue instalado correctamente ya que todas las operaciones fueron exitosas.

3.5.3 Configuración de Clúster

La capa de clúster fue diseñada para dotar de alta disponibilidad a los Servicios Web con los que se conecta, ya que estos últimos no cuentan con opciones para definir un esquema capaz de soportar la falla de sus componentes. Para ello, se definió un clúster en modo Activo-Activo, con el cual, todos los nodos del clúster pudieran recibir las peticiones de los usuarios del servicio, evitando así que sólo un nodo soportara toda la carga. Con el objetivo de facilitar las configuraciones descritas se usará como ejemplo un clúster de dos nodos.

El software elegido para configurar esta capa fue Pacemaker, un programa de código abierto derivado del proyecto de alta disponibilidad para Linux. Tuvo sus inicios en el 2003 como un manejador de recursos para Heartbeat y, en el 2007, se separa del proyecto original con el fin de soportar otro tipo de pilas (*stacks*) como OpenAIS. La primera versión de Pacemaker en esta etapa fue la 0.6.0, liberada en 2008. Posteriormente, el software se actualizó hasta la serie de versiones más recientes, la 1.0. (ClusterLabs, 2015)

De acuerdo al sitio de ClusterLabs previamente citado, las principales características de Pacemaker son:

- Detección y recuperación de fallos a nivel de equipo y aplicación.
- Soporte de cualquier configuración redundante.
- Soporte de *quorum* y clúster dirigido por recursos.
- Estrategias de pérdida de *quorum.*
- Soporte para inicio/apagado de aplicaciones en un orden definido.
- Soporte de aplicaciones que deben/no deben correr en el mismo nodo.
- Soporte de aplicaciones distribuidas.

- Soporte de aplicaciones con múltiples modos (por ejemplo, maestro/esclavo).
- Respuestas para todo tipo de fallas que se puedan dar en el clúster, así como la oportunidad de probar cualquier escenario antes de que ocurran.

Para que Pacemaker pueda proporcionar todas las características mencionadas se conforma de 5 componentes principales (ClusterLabs, 2015):

1. Pacemaker: Se trata de una máquina distribuida de estados finitos capaz de coordinar el inicio y recuperación de servicios configurados en un conjunto de máquinas. Soporta diferentes tipos de recursos, entre ellos `SYSV`, `systemd` y `Docker`.
2. Corosync: Es una API involucrada en el envío de mensajes entre los miembros de un clúster. Entre sus tareas se encuentra la de proporcionar la funcionalidad necesaria para establecer la pertenencia del *quorum* (mayoría).
3. libQB: Es una librería encargada de proveer distintos servicios con un gran rendimiento, entre ellos se destaca el establecimiento de registros o la comunicación entre procesos que corren en diferentes máquinas.
4. *Agentes de recursos*: Es una abstracción realizada por Pacemaker para poder realizar actividades de administración en los servicios que son dados de alta en el clúster, pero que no son conocidos por él. En otros términos, es un conjunto de especificaciones que contienen la lógica de lo que debe hacer Pacemaker cuando se requiera iniciar, consultar o parar un servicio.
5. *Agentes de cercado*[20]: Esta abstracción permite a Pacemaker aislar los nodos que presentan comportamientos extraños o inesperados a partir de mecanismos que permiten apagar físicamente el nodo (retirar alimentación) o son capaces de quitar el acceso del nodo a la red o al almacenamiento compartido.

[20] Traducción libre del término en inglés *Fence Agents.*

Para la configuración de un clúster de dos nodos no se aplicará la configuración del *quorum* (se dejará por defecto), pues esta característica de Pacemaker está pensada para operar en un clúster de tres nodos o más. En lo referente a los *Agentes de Cercado* tampoco se mostrará su configuración a través de *STONITH*[21], dado que implica la configuración de otros componentes que están fuera del alcance de este documento.

Adicionalmente, el clúster fue establecido para poder otorgar alta disponibilidad a los servicios web instalados, sin embargo, por la naturaleza de estos últimos, no fue posible agregarlos directamente al clúster como servicios, por esta razón fue necesario implementar un proxy. Éste se encargó de dirigir todas las peticiones recibidas hacia el servicio web correspondiente. El proxy elegido se configuró a través del módulo *proxy_balancer* de Apache. Teniendo en cuenta lo anterior, la Capa de Clúster tuvo la siguiente arquitectura (Fig. 21):

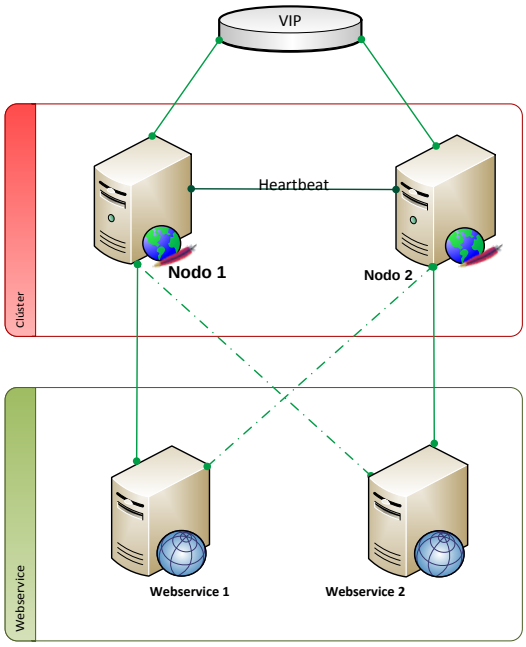


Fig. 21 Diagrama detallado de la Capa de Clúster

Fuente: Elaboración propia, 2015

[21] *Shoot The Other Node In The Head*, literalmente, disparar al otro nodo en la cabeza. Es un mecanismo de los *Fence Agents* para poder parar/apagar un nodo del clúster en estado de error.

La principal diferencia con respecto al diagrama de la arquitectura completa del servicio de cifrado es la aparición de las líneas punteadas que van de cada nodo del clúster a cada web service. Con el fin de garantizar la disponibilidad del servicio, se eligió configurar el proxy de Apache para conectarse con el mayor número de servicios web posibles (para el ejemplo serían dos); así, si el web service asignado tuviera alguna falla, inmediatamente serían enviadas todas las peticiones al servicio web configurado como pasivo. Para lograr esto, se instaló en cada nodo del clúster un servidor Apache con la siguiente configuración:

```
<VirtualHost IP VLAN3:54321 VIP-HSM:54321>
    DocumentRoot "/var/www/html"
    <Proxy balancer://cluster-hsm>
        BalancerMember http://webservice1:54321 connectiontimeout=1 retry=0
        BalancerMember http://webservice2:54321 connectiontimeout=1 retry=0 status=+H
    </Proxy>
    ProxyPreserveHost On
    ProxyPass / balancer://cluster-hsm/
    ProxyPassReverse / http://webservice1:54321/
    ProxyPassReverse / http://webservice2:54321/
</VirtualHost>
```

Fig. 22 Configuración de Apache como proxy en nodo 1

Fuente: Elaboración propia, 2015

Para este Apache, se eligió el web service 2 como la conexión pasiva (`status=+H`): en caso de que el web service 1 no respondiera las peticiones serían atendidas por el segundo. Todo esto se creó dentro de un grupo (`cluster-hsm`) de tal modo que el servidor Apache pudiera reconocer la configuración. Además, se agregaron líneas para indicar el comportamiento del proxy, donde cualquier petición dirigida a la raíz del servidor (`/`) era rápidamente enviada al servicio web que le correspondía.

La anterior configuración corresponde al nodo uno del clúster de Pacemaker. La configuración del segundo nodo cambia en el establecimiento del miembro pasivo:

```
<VirtualHost IP VLAN3:54321 VIP-HSM:54321>
    DocumentRoot "/var/www/html"
    <Proxy balancer://cluster-hsm>
        BalancerMember http://webservice1:54321 connectiontimeout=1 retry=0 status=+H
        BalancerMember http://webservice2:54321 connectiontimeout=1 retry=0
    </Proxy>
    ProxyPreserveHost On
    ProxyPass / balancer://cluster-hsm/
    ProxyPassReverse / http://webservice1:54321/
    ProxyPassReverse / http://webservice2:54321/
</VirtualHost>
```

Fig. 23 Configuración de Apache como proxy en nodo 2

Fuente: Elaboración propia, 2015

Posteriormente, se procedió a configurar el clúster (para mayor detalle, ver el Anexo I) de Pacemaker de acuerdo a la novena edición de la guía *Clusters from Scratch*, en ésta se dan indicaciones para establecer el clúster de dos nodos ya mencionado.

3.5.4 Balanceador de carga

Para la arquitectura final del Servicio de Cifrado de la Credencial para Votar, se considera como última capa la que contiene los nodos del clúster de Pacemaker; sin embargo, aquí se describe la configuración de un balanceador de carga físico, pues funge como la entrada al servicio de los usuarios externos. Sin esta capa estos no podrían acceder al servicio, debido a que las VLAN usadas para la solución no son accesibles por otras redes del Instituto.

Para la configuración de los balanceadores de carga, físicos en alta disponibilidad, se usó la Tabla 3.4 Parámetros de configuración del balanceador de carga físico:

Tabla 3.4 Parámetros de configuración del balanceador de carga físico

Configuración de balanceador de carga					
Configuración	**VLAN**	**IP**	**Param0**	**Param1**	**Param2**
Client_Side	VLAN 4				
Server_Side	VLAN 3				
VIP	VLAN4	VIP Balanceador			
Servidor Real 1	VLAN 3	Nodo1	Port=54321	Weigth=10	State=Inservice
Servidor Real 2	VLAN 3	Nodo2	Port=54321	Weigth=10	State=Inservice

Fuente: Elaboración propia, 2015

De acuerdo a la tabla, el balanceador físico envía la misma cantidad de peticiones a cualquier nodo del clúster de Pacemaker, los cuales tienen abierto el puerto 54321 por la VLAN 3. En caso de que un nodo no pueda responder correctamente a las peticiones de los usuarios, el balanceador físico redirigiría el tráfico hacia el nodo que se encuentre en operación.

3.6 Pruebas de volumen y estadísticas

Luego de realizar las configuraciones descritas en los apartados anteriores, fue necesario evaluar la mejora del Servicio con respecto a la infraestructura de la FASE 1. Por consiguiente, se llevaron a cabo una serie de pruebas de volumen y pruebas de *failover*, que consistieron en enviar un número significativo de peticiones al servicio, mientras se desactivaban sistemáticamente los

componentes involucrados. Por ejemplo, se lanzaron mil peticiones al servicio desde la entrada para usuarios externos y, durante el proceso, se apagaron algunos nodos del clúster, servicios web y módulos criptográficos.

Las pruebas de este tipo resultaron exitosas, aún con un número mayor de peticiones (desde mil hasta cien mil). Asimismo, se realizaron las mismas pruebas desde la perspectiva de un usuario interno, las cuales se llevaron a cabo sin problemas. De esta manera, el servicio fue validado y se encontró listo para ser mudado a producción: la infraestructura de la FASE 1 quedó obsoleta y todos los usuarios, tanto externos como internos, fueron configurados para consumir el servicio desde la nueva infraestructura.

Una vez en funcionamiento la nueva infraestructura y los clientes consumiendo el Servicio, se obtuvieron estadísticas referentes a la cantidad de peticiones diarias y los tiempos de respuesta. Esto con el objetivo de tener evidencia certera que indique la mejora del servicio, además de su estado de salud. Las estadísticas son tomadas automáticamente y se presenta un extracto de las mismas, así como una comparación con los tiempos de la infraestructura de la Fase 1 (Tabla 3.5 Tiempos de respuesta del Servicio de Cifrado).

Para ejemplificar, en enero de 2014, el entonces INSTITUTO FEDERAL ELECTORAL informó a la ciudadanía que se generaban 60 mil Credenciales diarias, atendiendo con ello el alza en la demanda originada por la renovación de las que perdían su vigencia. Con la nueva infraestructura le tomaría al Instituto cerca de 33 minutos generar la información que va cifrada en la Credencial para Votar; validando así la eficiencia del servicio.

Tabla 3.5 Tiempos de respuesta del Servicio de Cifrado

Número de peticiones	Tiempo promedio de respuesta x petición FASE 1	Tiempo de respuesta total FASE 1	Tiempo promedio de respuesta x petición FASE 2	Tiempo de respuesta total FASE 2
150,000	45.2	113 min	33.2 ms	83 min
160,000	44.6	119 min	33.8 ms	90 min
170,000	44.9	127 min	33.1 ms	94 min
180,000	44.7	134 min	32.9 ms	99 min
190,000	44.9	142 min	32.1 ms	102 min
200,000	45.1	150 min	32.6 ms	109 min

Fuente: Elaboración propia, 2015

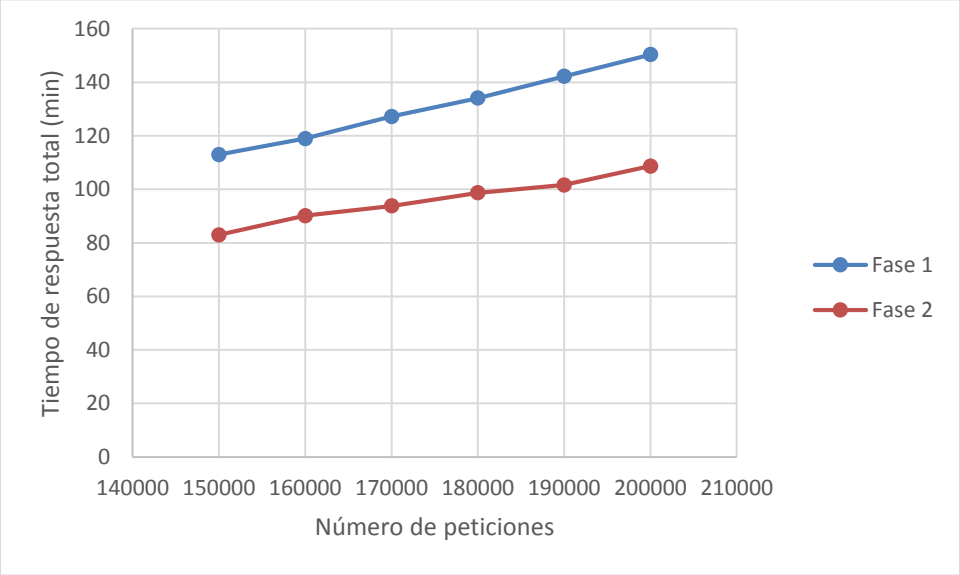


Fig. 24 Tiempos de respuesta del servicio de cifrado por Fase

Fuente: Elaboración propia, 2015

Conclusiones

La generación de la Credencial para Votar surgió como un servicio proporcionado a toda la ciudadanía con la finalidad de brindarle un documento oficial que validara su derecho al voto y, por ende, su continua participación en la vida democrática de la nación. Debido a la inclusión de nuevas tecnologías en los procesos electorales, la constante especialización en el campo de la seguridad informática, así como la creación y continua depuración de la base de datos más grande de registros de la población adulta mexicana, la Credencial para Votar rebasó su papel e importancia en los comicios, convirtiéndose en un documento facultado para acreditar en términos oficiales la identidad de los ciudadanos mayores de 18 años.

Consecuentemente, las grandes responsabilidades que implica el manejo de información personal de carácter confidencial concentraron las tareas y esfuerzos del INE en la adecuada administración y resguardo del Padrón Electoral. De esta forma, se diseñaron y aplicaron estrategias computacionales e informáticas capaces de garantizar la integridad del sufragio y los datos; esto es, una serie de mecanismos y elementos para regular el uso del padrón electoral y evitar su manipulación o robo.

Como se mencionó en el Capítulo I del presente documento, el INSTITUTO NACIONAL ELECTORAL tiene establecidos 15 objetivos estratégicos agrupados en cuatro grandes perspectivas, todos ellos enfocados al cumplimiento de su misión y visión. De entre ellos destacan los indirectamente impactados por el Servicio de Cifrado de la Credencial para Votar: 1) el fortalecimiento de la confianza de la sociedad en el Instituto; 2) la ampliación y mejora de la interacción con la sociedad; 3) el aumento de la cobertura, servicios y calidad de la atención ofrecida a la ciudadanía; 4) la consolidación de la Credencial para Votar como el medio preferente de identificación oficial utilizado por los ciudadanos mexicanos. (Instituto Nacional Electoral, 2015)

Particularmente, los dos primeros se ven beneficiados por el establecimiento del Servicio de Cifrado, ya que éste logra aumentar la seguridad del documento de identidad y, por consiguiente, permite que el Instituto logre salvaguardar la información personal de los ciudadanos. Al mismo tiempo, la confianza depositada por los ciudadanos en la Credencial para Votar es reafirmada y esto a su vez la consolida como el principal medio de identificación de la ciudadanía.

Siguiendo con los objetivos, el aumento de la cobertura, servicios y calidad de atención fueron logrados mediante el establecimiento de sistemas asociados a tres de los elementos del reverso de la Credencial: el código QR, el PDF-417 y la Zona de Lectura Mecánica. De acuerdo al Instituto Nacional Electoral, algunos de estos servicios podrían ser los de la Tabla 4.1 Servicios asociados:

Tabla 4.1 Servicios asociados

Servicios	Elemento de la CPV
Verificación de afiliados para el registro de Agrupaciones y Partidos Políticos	QR
Voto electrónico	PDF-417
Servicios de información	QR
Servicios al ciudadano	PDF-417 y QR
Servicios de valor agregado como la identificación y autenticación de ciudadanos	PDF-417 y ZLM

Fuente: (Instituto Federal Electoral, 2013)

Por último, cabe destacar que estas mejoras son posibles gracias al empleo de las Tecnologías de la Información descritas en el capítulo tercero, razón por la cual se puede aseverar que el Servicio de Cifrado impacta el objetivo estratégico adicional referente a la optimización del uso, aplicación e inversión en TIC. En este sentido y como se expuso en el trabajo, la Fase 2 del proyecto puede resumirse en la mejora total del Servicio a través de inversiones en infraestructura nueva, el empleo de software potente, así como la afinación de las configuraciones de cada uno de sus componentes.

Por esta razón, el trabajo realizado por la Dirección Ejecutiva del Registro Federal de Electores (DERFE) se puede considerar una tarea vital en el abanico de responsabilidades del INSTITUTO NACIONAL ELECTORAL, ya que de éste depende la seguridad de la información personal de las mexicanas y mexicanos que han cumplido la mayoría de edad, así como el ejercicio de prácticas democráticas organizadas y transparentes. Si bien el nivel de complejidad de la operación del Servicio de Cifrado es mínimo, su existencia tiene efectos favorecedores tanto a nivel institucional como nacional, ya que, sin elementos ni mecanismos que ratifiquen la autenticidad de los datos contenidos en la CPV, ésta perdería su credibilidad y, en consecuencia, se pondría en duda la función e importancia del INE en la organización, regulación y fomento de la vida democrática en México.

Esto último permite imaginar el reto profesional que significó para los involucrados llevar a cabo dicho proyecto. De manera personal, llevar a buen término el Servicio de Cifrado y cumplir cabalmente sus objetivos, significó el empleo de muchos de los conocimientos adquiridos a lo largo de mis estudios en la Facultad de Ingeniería, especialmente lo aprendido en criptografía, redes y seguridad informática. Sin embargo, debido a la complejidad y especialización del proyecto fue necesario realizar una investigación más profunda, así como una lectura pormenorizada de todos los elementos tecnológicos involucrados.

Sobre lo anterior, por ejemplo, en el plan de estudios de la Facultad el acercamiento a los sistemas operativos tipo Unix puede ser mejorado, de tal manera que las grandes cualidades de esos sistemas operativos sean correctamente aprovechadas a través de la mención de tecnologías empresariales que operan bajo ese sistema; tal es el caso de los balanceadores de carga, software para proveer alta disponibilidad o servidores proxy y web. Otro ejemplo claro como área de oportunidad, en el ámbito de la programación, es la ampliación de la cobertura que se le otorga a tecnologías y arquitecturas usadas por las empresas tecnológicas actuales, como es el caso de los *frameworks* de desarrollo o la arquitectura básica de un servicio web.

Por otra parte, también es preciso señalar que los conocimientos generales de criptografía adquiridos durante mi estancia en la Facultad resultaron de suma importancia para mi colaboración en este proyecto, ya que en esencia, el Servicio de Cifrado es la aplicación pura de las operaciones criptográficas básicas: cifrado, descifrado, firma y verificación. Lo mismo sucede con los conceptos fundamentales vistos en las materias relacionadas a redes de datos, que sin duda me fueron de gran ayuda para el desarrollo acertado del trabajo.

Por último, un factor primordial a lo largo del proyecto, desde su concepción hasta su operación y terminación, fue lo referente a la Seguridad Informática. Esto debido a que, por un lado, el Servicio de Cifrado es el encargado de dotar a la Credencial para Votar de algunos de sus mecanismos de seguridad para evitar su falsificación y determinar la autenticidad del documento de identidad; y por el otro, el Servicio en sí requirió la aplicación de conceptos clave en materia de seguridad, al mismo nivel de lo implementado en la protección del Padrón Electoral y de la misma Credencial.

En suma, el texto aquí presentado recupera uno de los proyectos más importantes y enriquecedores en mi desarrollo como profesional de la Ingeniería en Computación. Particularmente, las tareas desempeñadas en el Servicio de Cifrado han puesto en práctica y, mejor aún, potencializado mis conocimientos y habilidades en el área de la Seguridad Informática. Asimismo, dicha experiencia laboral me permitió comprender la importancia y necesidad del quehacer de los especialistas en Computación en aspectos sociopolíticos del país; ya que, a causa de las características del contexto actual, la consolidación de un gobierno democrático, abierto y transparente requiere indudablemente de una aplicación certera y segura de las Tecnologías de la Información y Comunicación.

De alguna manera, el trabajo realizado por el INE a través de la DERFE marca un precedente en manejo adecuado y oportuno de la información personal por medio de las TIC. Espero el presente documento incentive el interés de más compañeros, profesores e investigadores en el tema.

Referencias

Attridge, J. (2002). *An Overview of Hardware Security Modules.* Obtenido de SANS Institute: https://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757

Beekhof, A. (2015). *Clusters from Scratch.* Recuperado el 5 de Noviembre de 2015, de ClusterLabs: http://clusterlabs.org/doc/en-US/Pacemaker/1.1-pcs/html-single/Clusters_from_Scratch/index.html

ClusterLabs. (2015). *ClusterLabs*. Recuperado el 5 de Noviembre de 2015, de Pacemaker: clusterlabs.org

ClusterLabs. (2015). *Core Components*. Recuperado el 5 de Noviembre de 2015, de Pacemaker: http://clusterlabs.org/components.html

Congreso de la Unión. (14 de Enero de 2008). *Código Federal de Instituciones y Procedimientos Electorales.* Obtenido de http://www.diputados.gob.mx/LeyesBiblio/abro/cofipe/COFIPE_abro_14ene08.pdf

Espinosa García, F. J., Hernández Encinas, L., & Martín del Rey, A. (s.f.). *Codificación de información mediante códigos bidimensionales.* Recuperado el 27 de Marzo de 2016, de http://digital.csic.es/bitstream/10261/21259/1/Codbidimens.pdf

Gómez Vieites, Á. (2011). *Enciclopedia de la Seguridad Informática* (Segunda ed.). México: Alfaomega.

Instituto Federal Electoral. (2000). *El régimen Electoral Mexicano y las Elecciones Federales.* Recuperado el 20 de Octubre de 2015, de Biblioteca Jurídica Virtual: http://biblio.juridicas.unam.mx/libros/3/1131/5.pdf

Instituto Federal Electoral. (2013). *Acuerdo del Consejo General del Instituto Federal Electoral por el que se aprueba la función de los códigos de barras bidimensionales en el modelo aprobado por este órgano de dirección mediante acuerdo CG732/2012.* Recuperado el 8 de Octubre de 2015, de Diario Oficial de la Federación: http://dof.gob.mx/nota_detalle.php?codigo=5322758&fecha=20/11/2013

Instituto Federal Electoral. (2013). Documento Reservado. México, México.

Instituto Federal Electoral. (2013). Documento Reservado 2. México, México.

Instituto Federal Electoral. (2013). Matriz de análisis de riesgos del Servicio de Cifrado. México, México.

Instituto Nacional Electoral. (2014). *Conoce el trámite en el Módulo para obtener tu Credencial para Votar.* Recuperado el 14 de Abril de 2016, de Instituto Nacional Electoral: http://www.ine.mx/archivos2/portal/credencial/pdf-credencial/pasos-en-el-modulo-INE2014.pdf

Instituto Nacional Electoral. (2014). Memoria técnica. México.

Instituto Nacional Electoral. (2014). *Modelo Actual de la Credencial para Votar.* Obtenido de http://www.ine.mx/archivos2/portal/credencial/pdf-credencial/ModeloActual2014-INE.pdf

Instituto Nacional Electoral. (2014). *NormaINE.* Obtenido de Catálogo de Cargos y Puestos de la Rama Administrativa del Instituto Nacional Electoral: http://norma.ine.mx/documents/27912/1363696/2014_cargos_puestos_rama_administrativa.pdf

Instituto Nacional Electoral. (2015). *Acerca del INE*. Recuperado el 22 de Junio de 2016, de Instituto Nacional Electoral: http://www.ine.mx/archivos3/portal/historico/contenido/Que_es/

Instituto Nacional Electoral. (2015). *Acerca del INE*. Recuperado el 22 de Junio de 2016, de Instituto Nacional Electoral: http://www.ine.mx/archivos3/portal/historico/contenido/Que_es/

Instituto Nacional Electoral. (2015). *Estructura Orgánica.* Obtenido de https://directorio.ine.mx/chartByAreaOrganigrama.ife?idArea=996

Instituto Nacional Electoral. (8 de Octubre de 2015). *Historia del Instituto Federal Electoral*. Obtenido de http://www.ine.mx/archivos3/portal/historico/contenido/menuitem.cdd858023b32d5b7787e6910d08600a0/

Instituto Nacional Electoral. (2015). Presentación Interna: Credencial para Votar. Distrito Federal, México.

Neria, I. (8 de Octubre de 2015). *Artes e Historia México*. Obtenido de http://www.arts-history.mx/sitios/index.php?id_sitio=735655&id_seccion=3028135&id_subseccion=19032&id_documento=2777

NIST. (2001). *FIPS PUB 140-2.* Obtenido de National Institute of Standards and Technology: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

NIST. (Diciembre de 2012). *Special Publication 800-133: Recomendation for Cryptographic Key Generation.* Obtenido de National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133.pdf

Ramió Aguirre, J. (Marzo de 2015). Proyecto Thoth, píldoras formativas. *Píldora nº 30: ¿Cómo se cifra con el algoritmo AES?* Madrid, España.

Refsnes Data. (2015). *XML Soap*. Recuperado el 22 de Octubre de 2015, de W3Scools: http://www.w3schools.com/xml/xml_soap.asp

SafeNet Inc. (2015). *Gemalto SafeNet Luna SA.* Recuperado el 21 de octubre de 2015, de http://www.safenet-inc.com/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=8589949133

Secretaría de Gobernación. (10 de Octubre de 2015). *Diario Oficial de la Federación*. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/ref/lgp/LGP_ref07_22jul92_ima.pdf

Stallings, W. (2004). *Fundamentos de seguridad en redes. Aplicaciones y estándares* (Segunda ed.). (L. Cruz García, & M. González Rodríguez, Trads.) Madrid, España: Pearson Educación , S.A.

Anexo I

Para propósitos de este documento, los nombres de referencia de los dos nodos del clúster serán “cluster1” y “cluster2”:

1. Instalación de los paquetes `pacemaker`, `pcs` y `resource-agents` en cada nodo del clúster.

2. Se abrieron los puertos necesarios en la configuración del *firewall* de *host* de cada nodo.

Tabla 5.1 Puertos usados por Pacemaker

Puerto	Protocolo
2224	TCP
3121	TCP
21064	TCP
5405	UDP

Fuente: Elaboración propia a partir de (Beekhof, 2015)

3. A continuación, se inició el servicio `pcsd`, demonio principal de Pacemaker; mediante él, el resto de los servicios necesarios fueron levantados. Es importante señalar que este servicio fue habilitado para correr desde el inicio del sistema operativo.

4. Con la instalación de los paquetes mencionados, se creó un usuario local llamado `hacluster`. Este usuario es el que permite replicar las configuraciones de un nodo a otro, evitando la modificación de la configuración la misma cantidad de veces que de nodos agregados al clúster, por lo tanto, es necesario que el usuario tenga la misma contraseña en cada nodo:

```
# passwd hacluster

Changing password for user hacluster.

New password:

Retype new password:

passwd: all authentication tokens updated successfully.
```

5. Una vez realizado el paso anterior en todos los nodos que formarán el clúster, se ejecuta:

```
[root@cluster1 ~]# pcs cluster auth cluster1 cluster2

Username: hacluster

Password:

cluster1: Authorized

cluster2: Authorized
```

Con esto, se le indica a `pcs` que se autentique en cada nodo a través del usuario `hacluster`. De este punto en adelante, las configuraciones se realizan únicamente en el cluster1.

6. Con el siguiente comando se crea el clúster del servicio de cifrado:

```
[root@cluster1 ~]# pcs cluster setup --name hsm-cluster
cluster1 cluster2
Shutting down pacemaker/corosync services...
stop pacemaker
stop corosync
Killing any remaining services...
Removing all cluster configuration files...
cluster1: Succeeded
cluster2: Succeeded
```

El contenido de `corosync.conf` (archivo de texto en donde se refleja la configuración del clúster) sería el siguiente:

```
totem {
version: 2
secauth: off
cluster_name: hsm-cluster
transport: udpu
}
nodelist {
  node {
        ring0_addr: cluster1
        nodeid: 1
       }
  node {
        ring0_addr: cluster2
        nodeid: 2
       }
}
quorum {
provider: corosync_votequorum
two_node: 1
}

logging {
to_syslog: yes
}
```

7. El clúster se inicia con:

```
[root@cluster1 ~]# pcs cluster start --all

cluster1: Starting Cluster...

cluster2: Starting Cluster...
```

8. Se verifica que el servicio esté operando correctamente:

```
[root@cluster1 ~]# pcs status

Cluster name: hsm-cluster

WARNING: no stonith devices and stonith-enabled is not
false

Last updated: Tue Dec 16 16:15:29

Last change: Tue Dec 16 15:49:47

Stack: cman

Current DC: cluster1 - partition WITHOUT quorum

Version:

2 Nodes configured

0 Resources configured

Online: [ cluster1 cluster2 ]
```

La configuración del clúster de Pacemaker puede observarse como un archivo *xml* con el comando:

```
[root@cluster1 ~]# pcs cluster cib
<cib crm_feature_set="3.0.9" validate-with="pacemaker-2.3" epoch="5" num_updates="8"
admin_epoch="0" cib-last-written="Tue Dec 16 15:49:47 2014" have-quorum="1" dc-
uuid="2">
  <configuration>
    <crm_config>
      <cluster_property_set id="cib-bootstrap-options">
        <nvpair id="cib-bootstrap-options-have-watchdog" name="have-watchdog"
value="false"/>
        <nvpair id="cib-bootstrap-options-dc-version" name="dc-version" value="1.1.12-
a14efad"/>
        <nvpair id="cib-bootstrap-options-cluster-infrastructure" name="cluster-
infrastructure" value="corosync"/>
        <nvpair id="cib-bootstrap-options-cluster-name" name="cluster-name"
value="mycluster"/>
      </cluster_property_set>
    </crm_config>
    <nodes>
      <node id="1" uname="cluster1"/>
      <node id="2" uname="cluster2"/>
    </nodes>
    <resources/>
    <constraints/>
  </configuration>
  <status>
    <node_state id="2" uname="cluster2" in_ccm="true" crmd="online" crm-debug-
origin="do_state_transition" join="member" expected="member">
      <lrm id="2">
        <lrm_resources/>
      </lrm>
      <transient_attributes id="2">
        <instance_attributes id="status-2">
          <nvpair id="status-2-shutdown" name="shutdown" value="0"/>
          <nvpair id="status-2-probe_complete" name="probe_complete" value="true"/>
        </instance_attributes>
      </transient_attributes>
    </node_state>
    <node_state id="1" uname="cluster1" in_ccm="true" crmd="online" crm-debug-
origin="do_state_transition" join="member" expected="member">
      <lrm id="1">
        <lrm_resources/>
      </lrm>
      <transient_attributes id="1">
        <instance_attributes id="status-1">
          <nvpair id="status-1-shutdown" name="shutdown" value="0"/>
          <nvpair id="status-1-probe_complete" name="probe_complete" value="true"/>
        </instance_attributes>
      </transient_attributes>
    </node_state>
  </status>
</cib>
```

9. En los log (`/var/log/messages`) y en el resultado del estatus del clúster se observó un mensaje de advertencia acerca de los *Fence Agents*. Para evitar que esta parte influya en el funcionamiento del clúster se desactivó la opción de STONITH.

```
[root@cluster1 ~]# pcs property set stonith-enabled=false
```

10. Para que el clúster sea accesible al resto de los equipos en la red, es necesario configurar una dirección IP virtual (VIP), lo cual es entendido por Pacemaker como un recurso. En este documento se usará la IP `192.168.1.100` para referirse a la VIP. Su configuración se ejecuta por medio de:

```
[root@cluster1 ~]# pcs resource create ClusterIP
ocf:heartbeat:IPaddr2 ip=192.168.1.100 cidr_netmask=32 op
monitor interval=1s
```

Con este comando se le indica a Pacemaker que genere un recurso llamado `ClusterIP` que será la definición de la dirección IP virtual, la cual revisará cada segundo (`op monitor interval=0`) que se encuentre funcionando. Recordando la arquitectura para la capa de clúster, cada nodo tiene varias interfaces de red; en este caso, Pacemaker asigna la VIP a la interfaz que coincida con la misma dirección de red que la suministrada por el parámetro `ip=192.168.1.100`.

11. Tomando en cuenta que el modo de funcionamiento del clúster es Activo-Activo, Pacemaker usa los llamados *clones* —una copia de un recurso previamente definido que funcionará en dos o más nodos con la misma configuración que el original, salvo en los parámetros que requieran ser modificados con los propios de la máquina en donde se alojará—. Así, el servicio `ClusterIP` se clonó en todos los nodos del clúster, lo que significa que cada uno de ellos responderá a cualquier solicitud enviada.

La distribución de los paquetes corre por cuenta de `IPaddr2` (configurado en el punto anterior), el cual utiliza una *dirección MAC multicast* para que la infraestructura de comunicaciones envíe a todos los nodos del clúster los

mismos paquetes, los cuales serán tomados por un único nodo con ayuda de reglas de *iptables* hechas a la medida por el propio Pacemaker.

```
[root@cluster1 ~]# pcs cluster cib loadbalance_cfg

[root@cluster1 ~]# pcs -f loadbalance_cfg resource clone
ClusterIP clone-max=2 clone-node-max=2 globally-
unique=true
```

- clone-max=2 indica al agente del recurso (IPaddr2) que divide los paquetes en 2, donde el número representa la cantidad de nodos que podrán albergar el servicio.
- clone-node-max=2 se refiere a que un nodo puede hospedar como máximo 2 instancias del servicio clonado, es decir, el mismo número de nodos de los que se compone el clúster. Si un miembro falla, todas sus peticiones serán atendidas por los nodos en funcionamiento; de lo contrario, las peticiones serían descartadas.
- globally-unique=true le indica al clúster que los clones no son cien por ciento idénticos (cada clon debe manejar distintas peticiones), por lo que el agente del recurso inserta reglas de *iptables* para que cada nodo procese los paquetes que le corresponden.

12. Después de los comandos anteriores, fue necesario indicarle al agente de recurso cómo decidir acerca de cuáles paquetes serán procesados por cada nodo. Lo anterior se implementa de la siguiente manera:

```
[root@cluster1 ~]# pcs -f loadbalance_cfg resource update
ClusterIP clusterip_hash=sourceip-sourceport
```

IPaddr2 asignará los paquetes de acuerdo a la dirección IP y puerto del cliente, creando un hash con esos datos, para que cada nodo procese cierto rango de hashes.

A continuación se carga la configuración al clúster y se verifica su funcionamiento por medio del estatus.

```
[root@cluster1 ~]# pcs cluster cib-push loadbalance_cfg
CIB updated

[root@cluster1 ~]# pcs status
Cluster name: hsm-cluster
Last updated: Fri Aug 14 11:32:07
Last change: Fri Aug 14 11:32:04
Stack: cman
Current DC: cluster1 - partition WITHOUT quorum
Version:
2 Nodes configured
2 Resources configured

Online: [ cluster1 cluster2 ]

Full list of resources:

Clone Set: ClusterIP-clone [ClusterIP] (unique)
     ClusterIP:0        (ocf::heartbeat:IPaddr2):
Started cluster1
     ClusterIP:1        (ocf::heartbeat:IPaddr2):
Started cluster2
```

En el *status* anterior se observa que el recurso `ClusterIP` está corriendo en ambos nodos del clúster. Si algún nodo dejara de funcionar, su clon sería transferido al nodo funcional. Para probar lo antes dicho, se pone en `standby`[22] al cluster2, posteriormente se verifica que los recursos hayan sido transferidos al cluster1:

[22] Pacemaker es capaz de simular la falla de un nodo del clúster sin necesidad de detener los servicios asociados, de esta manera, el comando standby pone a *dormir* al nodo especificado para que el clúster lo considere como un nodo no funcional.

```
[root@cluster1 ~]# pcs cluster standby cluster2
[root@cluster1 ~]# pcs status
Cluster name: hsm-cluster
Last updated: Fri Aug 14 11:32:07
Last change: Fri Aug 14 11:32:04
Stack: cman
Current DC: cluster1 - partition WITHOUT quorum
Version:
2 Nodes configured
2 Resources configured


Online: [ cluster1 ]
OFFLINE: [ cluster2 ]

Full list of resources:

Clone Set: ClusterIP-clone [ClusterIP] (unique)
     ClusterIP:0        (ocf::heartbeat:IPaddr2):
Started cluster1
     ClusterIP:1        (ocf::heartbeat:IPaddr2):
Started cluster1
```

Ya comprobada la funcionalidad esperada, se vuelve a activar el cluster2, con lo que el servicio vuelve a operar correctamente en ambos nodos.

13. Una vez configurada una dirección IP virtual que permita la entrada de peticiones al clúster, se continuó con la configuración de un nuevo recurso. Esta vez se agregó el servidor Apache en modo proxy. Para ello se siguieron pasos similares a los usados para la VIP. El agente de recurso de Apache necesita la configuración de una página de estatus que le indique si el servidor web está en funcionamiento, en consecuencia se cambió su configuración en `httpd.conf`:

```
<VirtualHost 127.0.0.1:80>
    <Location /server-status>
        SetHandler server-status
        Order deny,allow
        Deny from all
        Allow from 127.0.0.1
    </Location>
</VirtualHost>
```

Fig. 25 Configuración del módulo de estatus en Apache

Fuente: Elaboración propia, 2015

14. En el clúster se agrega el recurso con los parámetros correctos:

```
[root@cluster1 ~]# pcs resource create ClusterApache
ocf:heartbeat:apache configfile=/etc/httpd/conf/httpd.conf
statusurl="http://localhost/server-status" op monitor
interval=1s
```

15. Con esta configuración, Pacemaker tratará de repartir la carga entre todos los nodos e iniciará sus recursos configurados en el orden que sea más conveniente para asegurar un óptimo servicio. Sin embargo, esto puede provocar ciertos problemas con la VIP y Apache, para solucionarlo, se crearon restricciones sobre los recursos:

    La VIP y Apache deben correr en el mismo nodo.

```
[root@cluster1 ~]# pcs constraint colocation add
ClusterApache with ClusterIP INFINITY
```

    Para que Apache pueda conectarse al Puerto 54321 de la dirección IP de la VIP, necesariamente, este servicio debe ser iniciado con anterioridad.

```
[root@cluster1 ~]# pcs constraint order ClusterIP then
ClusterApache
Adding ClusterIP ClusterApache (kind: Mandatory) (Options:
first-action=start then-actio=start)
[root@cluster1 ~]# pcs constraint
Location Constraints:
Ordering Constraints:
  start ClusterIP then start ClusterApache (kind:Mandatory)
Colocation Constraints:
  ClusterApache with ClusterIP (score:INFINITY)
```

16. Definidas las restricciones es posible clonar el servicio de Apache del mismo modo en que se realizó con la VIP.

```
[root@cluster1 ~]# pcs cluster cib active_cfg
[root@cluster1 ~]# pcs –f active_cfg resource clone
ClusterApache
[root@cluster1 ~]# pcs cluster cib-push active_cfg
```

Finalmente, el estado del clúster fue el siguiente:

```
[root@cluster1 ~]# pcs status
Cluster name: hsm-cluster
Last updated: Fri Aug 14 12:05:37
Last change: Fri Aug 14 11:49:29
Stack: cman
Current DC: cluster1 - partition WITHOUT quorum
Version:
2 Nodes configured
4 Resources configured

Online: [ cluster1 cluster2 ]
Full list of resources:
 Clone Set: ClusterIP-clone [ClusterIP] (unique)
     ClusterIP:0        (ocf::heartbeat:IPaddr2):       Started
cluster2
     ClusterIP:1        (ocf::heartbeat:IPaddr2):       Started
cluster1
Clone Set: ClusterApache-clone [ClusterApache]
     Started: [ cluster1 cluster2 ]
```