Universidad Autónoma del Estado de México

Centro Universitario UAEM Valle de Chalco

DESARROLLO DE UNA APLICACIÓN SEGURA PARA VOTO ELECTRÓNICO EN UN ESPACIO ACADÉMICO

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A

MACARIO GALICIA NEGRETE

ASESORA:
DRA. MARÍA DE LOURDES LÓPEZ GARCÍA

Revisor:
Dr. en C. Juvenal Rueda Paz

Revisor:
Mtro. Iván Fabián Luna

VALLE DE CHALCO SOLIDARIDAD, MÉXICO SEPTIEMBRE 2020.

CENTRO UNIVERSITARIO XICO VALLE DE CHALCO
CUVCH

DESARROLLO DE UNA APLICACIÓN SEGURA PARA VOTO ELECTRÓNICO EN UN ESPACIO ACADÉMICO

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO 1. INTRODUCCIÓN

En México, la mayoría de las elecciones electorales a cualquier candidatura son realizadas de manera tradicional; esto requiere una gran cantidad de material de apoyo y tiempo en la planeación. Al ser realizadas de la misma manera una y otra vez, se pueden encontrar factores de vulnerabilidad permitiendo el incumplimiento de los servicios de seguridad de la información alterando el resultado electoral.

Este proyecto propone utilizar la red local del espacio académico para automatizar el proceso de elección de director del Centro Universitario, donde la comunidad universitaria pueda emitir su voto a través de un sistema confiable, cumpliendo los lineamientos de la Legislación Universitaria [1]. El sistema propuesto se tiene como nombre SEVS por sus siglas “Sistema Electrónico de Votación Segura” y fue desarrollado usando la metodología del Proceso Unificado de Desarrollo de Software [2] y su Lenguaje Unificado de Modelado (UML) [3].

1.1 Planteamiento del problema

Las elecciones electorales en México, son realizadas en su mayor parte de forma tradicional, esto con lleva que en el cumplimiento de sus procesos se requiera el uso de una gran cantidad de personal, uso de planillas electorales, casillas electorales, entre otras cosas. Todo lo mencionado anteriormente genera un gran costo y grandes demoras de tiempo.

Un aspecto importante, es la autenticación del elector para poder expresar su derecho electoral. La forma tradicional consiste en presentar una identificación y ser revisado si pertenece al patrón electoral vigente. Este proceso puede prestarse para llevar a cabo un fraude electoral, por suplantación de identidad,

como, por ejemplo, presentarse con una identificación ajena, que incluso puede estar muerta y realizar el derecho de manifestación ciudadana.

El conteo de los votos por cada casilla electoral es otro aspecto que se puede mejorar, el cual se realiza de forma manual, boleta por boleta. Es realizado por personal encargado, el cual demora una cantidad de tiempo considerable, este proceso puede contener fallas, o contar votos no existentes a favor de un candidato.

Por lo anterior, se presentan las siguientes preguntas de investigación. ¿Cuáles son las herramientas digitales que en las votaciones ayudarán a reducir los altos índices de fraude electoral?, ¿Cuáles son los algoritmos óptimos para proteger el valor del voto y evitar los problemas de seguridad informática conocidos? y ¿Cuál es el proceso para proteger la información electoral, ante futuros problemas que se puedan presentar?

1.2 Objetivos

Los objetivos a planificar en este trabajo son los siguientes:

General

Desarrollar una aplicación en línea de votación electrónica segura aplicando herramientas criptográficas de llave pública.

Específicos

- Diseñar el modelo del sistema informático adecuado que utilizará el usuario final para realizar su voto, proporcionando una interfaz gráfica amigable.
- Implementar medidas de seguridad informática eficientes en el sistema a desarrollar para evitar alteraciones al sistema.

- Gestionar los posibles riesgos que afrontan los medios de comunicación empleados en el sistema de votación electrónica.
- Comprobar las ventajas del proceso electoral implementado el voto electrónico.

1.3 Hipótesis

La importancia de utilizar protocolos criptográficos en un sistema informático donde se gestionan grandes cantidades de información debe ser obligatoria para proveer los servicios de seguridad de la información los que son: integridad de la información, confidencialidad, no repudio, disponibilidad, autenticación.

El uso de protocolos criptográficos ofrece la certeza de proteger la información electoral ante ataques contra la autenticación del votante y la confidencialidad e integridad del voto.

1.4 Metodología

Para alcanzar el objetivo propuesto de este trabajo, dado que se va a desarrollar un sistema informático, se utilizará la metodología de Proceso Unificado de Desarrollo de Software (PUDS) en donde nos basaremos de Lenguaje Unificado de Modelado (UML).

En el caso de consulta de información y análisis de los requerimientos se utilizará la investigación documental.

- Recopilación de información: se realizará una investigación documental de las principales características y el funcionamiento sobre los sistemas que se encuentren en la red que tienen la función de gestionar un proceso electoral.

- Analizar los requerimientos: se realizarán esquemas para cubrir los requisitos requeridos mediante los diagramas UML proporcionado una idea clara de cómo el sistema deberá interactuar con el usuario, como se desarrollan las actividades a llevar acabo.

En el caso del diseño e implantación del sistema se utilizará la investigación experimental.

- Diseñar un sistema: en esta acción se diseñarán los prototipos de la interfaz, también se llevará acabo el esquema de la base de datos utilizando el modelo entidad relación.
- Implementar el sistema: aquí se montará la base de datos, se programarán las interfaces y la parte lógica del sistema, una vez hecho eso se procederá a la instalación de las aplicaciones necesarias, su configuración y el montaje del sistema.

  Para las pruebas del sistema se utilizará una investigación de campo.

- Pruebas de sistema: En esta parte se realizan las pruebas que corroboraran el correcto funcionamiento del sistema haciendo una pequeña prueba piloto.

1.5 Alcances

El desarrollo del sistema intentara cubrir los servicios de seguridad necesarios para cumplir con las características de un proceso electoral como son: la democracia, la transparencia, el anonimato del ciudadano y la integridad del voto.

1.6 Organización del documento

El presente escrito cuenta con la siguiente estructura:

En el Capítulo 2, se describe de manera rápida el campo de la criptografía y una breve clasificación de sus algoritmos, describiendo brevemente el protocolo de seguridad que utilizara el sistema propuesto SEVS.

En el Capítulo 3, se expresarán los requerimientos de una elección académica manual en México, como sus respectivas fases. Se partirá de la forma más general, y finalmente manifestar los requerimientos específicos dictados por la legislación correspondiente a la UAEM, con el objetivo de poder realizar la elección de director del Centro Universitario.

En el Capítulo 4, se describe la estructura y el funcionamiento de SEVS como sus respectivos módulos, representados de manera clara con la ayuda de los diagramas UML.

En el Capítulo 5, se describe la implementación de SEVS con un uso ideal y cualquier percance conocido que pueda citarse, con el fin de ilustrar el funcionamiento al usuario final, es importante mencionar que los datos colocados como ejemplo son ficticios con la intención de cuidar la información personal de los usuarios reales.

En el Capítulo 6, se presentarán las conclusiones de este trabajo y se expone un trabajo futuro relacionado a SEVS.

CAPÍTULO 2. HERRAMIENTAS CRIPTOGRÁFICAS UTILIZADAS

En este capítulo se presenta un pequeño enfoque en el campo de la criptografía, posteriormente se mencionarán algunos ejemplos de protocolos criptográficos para realizar una votación electrónica confiable, cuidando la integridad del voto emitido y el anonimato del votante.

2.1 Criptografía y criptografía de llave simétrica

La criptografía surgió conforme a la necesidad del ser humano con la finalidad de proteger información sensible de terceras personas [4]. Sus inicios remontan desde las primeras civilizaciones, mediante técnicas artesanales, sustituciones de símbolos, o algoritmos sencillos; lo cual se realizaban a mano o con aparatos mecánicos de la época, esto conoce como criptografía clásica.

Las técnicas empleadas se podían descifrar mediante un análisis frecuente de secuencias, dejando expuesta la confidencialidad e integridad de la información, esto produjo a la realización de técnicas más complejas, donde surge la criptografía moderna; usando algoritmos matemáticos de cifrado, facilitando otras características como la firma digital y certificados digitales.

A partir de estos cimientos surgieron nuevos y complejos sistemas criptográficos, pudiéndolos clasificar en dos maneras:

- Clave simétrica: los algoritmos simétricos utilizan una única clave de cifrado y descifrado, por lo que se tiene que proteger su difusión, solo debe ser conocida por el emisor y receptor. Es posible hacer una nueva clasificación de acuerdo como trata la información en su proceso de

cifrado, distinguiéndose entre sistemas de cifra de flujo y sistemas de cifra en bloque [4].

- Clave asimétrica: en este caso cada entidad dispone de dos claves, privada y pública, inversas entre sí, cuando la clave pública es usada para cifrar, el descifrado del criptograma debe ser realizado con la clave privada [4].

En la Figura 2.1, se muestra una clasificación de la criptografía de acuerdo al manejo de algoritmos utilizados.

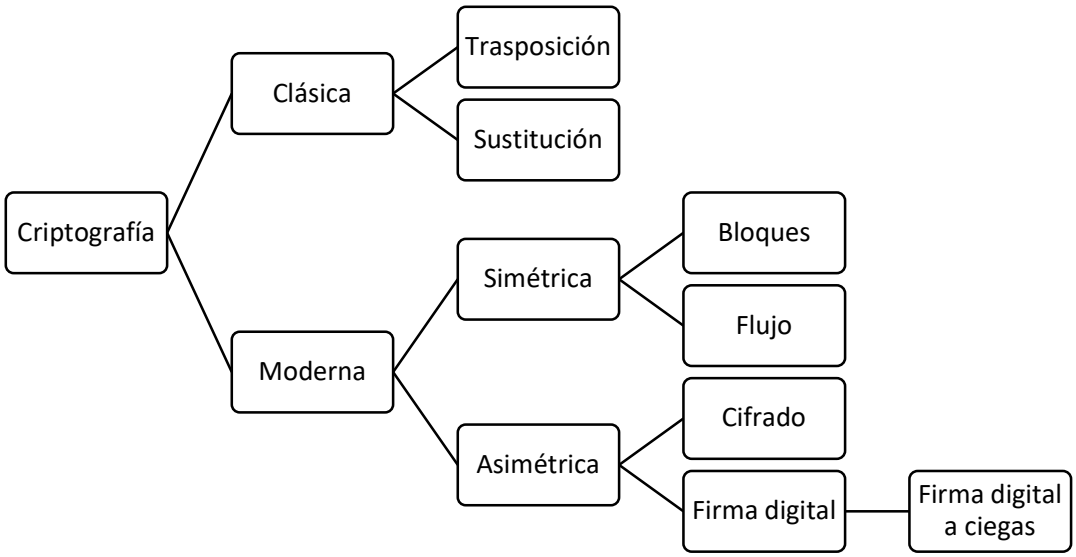

Figura 2.1 Clasificación de la criptografía (Fuente: Propia, 2020).

Como se observó en la Figura 2.1, la criptografía asimétrica facilita la realización de cifrado, firma digital y una variación de estas denominadas firmas a ciegas, del que se hablara más adelante.

2.2 Criptografía de llave asimétrica

La criptografía asimétrica también conocida de clave pública utiliza un par de llaves relacionadas matemáticamente: las claves públicas que pueden ser difundidas ampliamente, y las claves privadas que solo la debe conocer el propietario y mantenerla en secreto, de esto depende la seguridad del sistema.

Cada participante en un sistema de claves públicas como se mencionó anteriormente dispone de un par de claves. Un mensaje cifrado con la primera clave debe descifrarse con la segunda clave y un mensaje cifrado con la segunda clave debe descifrarse con la primera clave [5], permitiendo la implementación de firmas digitales impidiendo modificaciones de la información mediante un canal inseguro.

Otra característica del sistema de clave pública, consiste en el proceso de distribución de claves en un medio inseguro, no impide que la llave publica sea conocida por terceras personas, así pues, era un importante problema en los criptosistemas simétricos o de clave privada del cual la llave acordada se debe mantener en todo momento oculta solo conocida por los participantes de la comunicación. El criptosistema más conocido e importante de la criptografía de clave pública hoy en día es el RSA.

2.2.1 Cifrador RSA

Su nombre se deriva por sus tres inventores: Ronald Rivest, Adi Shamir y Leonard Adleman, que publicaron por primera vez el método RSA en 1979 y es válido tanto para cifrar como para realizar firmas digitales [6], su funcionamiento consiste en la exponenciación modular y su fortaleza se basa en la complejidad del problema de la factorización de números enteros grandes.

A continuación, se muestra los pasos para generar el par de claves del criptosistema RSA:

1. Generar dos números primos de manera aleatoria, p y q (lo suficientemente grandes, que sean diferentes), los valores p y q no deben ser públicos.
2. Calcular el valor público de cifra n, y el indicador de Euler $\varphi(n)$

$$n = pq$$

$$\varphi(n) = (p-1)\,(q-1)$$

3. Elegir una clave pública e, de forma que:

$$1 < e < \varphi(n)$$

y que cumpla la condición:

$$mcd[e, \varphi(n)] = 1$$

4. Elegir una clave privada d; se conoce como d por la primera letra de la palabra decrypt, de forma que:

$$1 < d < \Phi(n)$$

y que cumpla la condición:

$$d = e^{-1}\, mod\, \varphi(n)$$

5. Posteriormente se da a conocer la clave pública (e, n) y se protege la clave privada (d, n). Para cifrar un mensaje m, este debe estar dentro del intervalo $[0,\ n-1]$. Si m cumple esta característica, se calcula donde, c es el mensaje cifrado:

$$c = m^e\, mod\, n$$

6. Para poder recuperar el mensaje original, se debe calcular:

$$m = c^d\, mod\, n$$

2.2.2 Funciones HASH

Las funciones hash son algoritmos que, al aplicarlos sobre una entrada m, donde m representa un (texto, mensaje, archivo o una contraseña, por ejemplo); entregan un resumen de x bits de longitud fija, conocido como $h(m)$ formando una salida alfanumérica. Se trata de un número que a modo de huella digital representara a dicha entrada de forma supuestamente única [4].

El tamaño de $h(m)$ dependerá del algoritmo utilizado, independiente del tamaño de la entrada m, como se muestra en la Figura 2.2, por ejemplo, SHA-1 produce como salida un resumen de 160 bits.

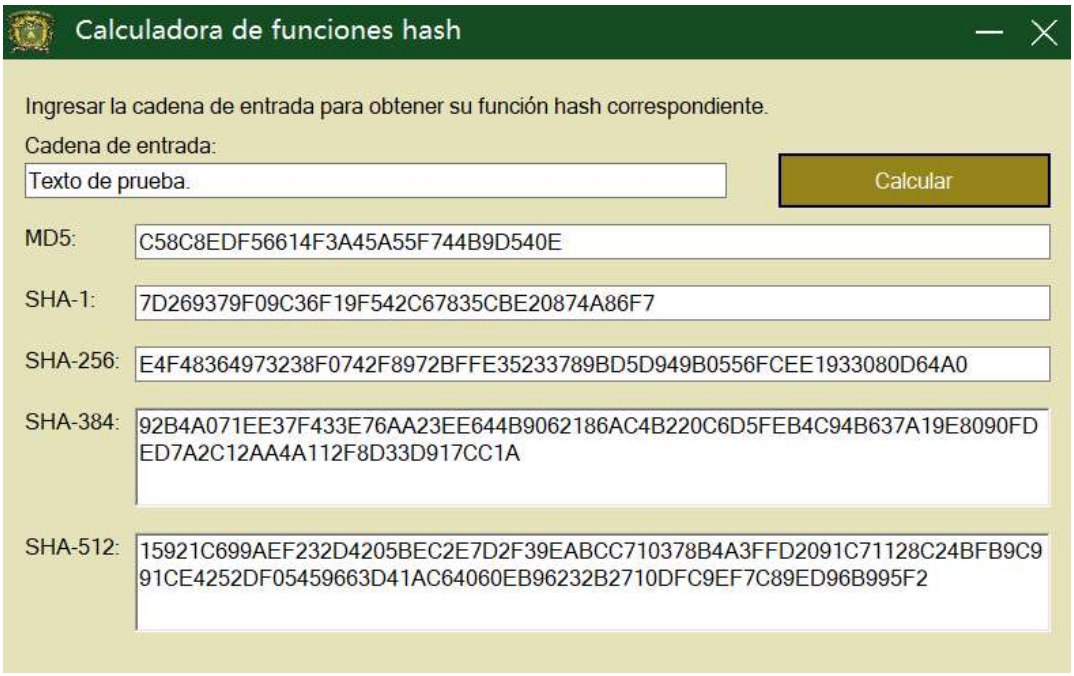

Figura 2.2 Diferentes algoritmos de funciones hash. (Fuente: Propia, 2020).

Una de las propiedades de estas funciones es que, si se altera algún bit de la cadena de entrada, accidentalmente o bien de forma consiente, el resumen de este será completamente distinto.

2.2.3 Firma digital RSA

Una firma digital es un número que se adjunta a un documento [7]. La firma digital se basa en la combinación de dos técnicas distintas, que es la utilización de las funciones hash para obtener un número de salida fijo de bits, posteriormente a este resultado se cifrara con la llave privada de la entidad certificadora o el creador del documento. De esta manera se puede acreditar quien es el emisor o autor del mismo y que nadie ha manipulado o modificado el contenido.

La firma digital equivale a la firma autógrafa en cuanto a la identificación del autor del que procede el mensaje [8].

En el apartado 2.3.1, se dan a conocer los pasos para generar un par de claves del criptosistema RSA. Partiendo de la creación de las claves de la entidad A que es la entidad certificadora, se mostrará los pasos de creación para una firma digital RSA:

1. Calcular el hash del mensaje $h(m)$, las entidades deben de llegar a un acuerdo, para la utilización de una única función hash.
2. Con la clave privada de A: $[dA, nA]$, se genera la firma s.

$$\mathrm{s} = h(m)^{dA} \bmod \mathrm{nA}$$

3. Los valores $[m, s]$ se envían a la entidad que solicito la firma.

La entidad que solicito la firma la cual ya conoce la llave pública de A $[Ea, nA]$, realizara la verificación de la firma, debe seguir los pasos siguientes:

1. Aplicar la función hash acordada anteriormente al mensaje recibido para obtener $h(m)$.
2. Calcular el hash del mensaje firmado, conociendo la llave pública de A

$$h1(m) = s^{eA}\ mod\ nA$$

3. Finalmente se realiza la comparación de: $h1(m) = h(m)$. Si son iguales la firmará será tomada como valida, de lo contrario este se rechazará.

2.2.4 Firma a ciegas RSA

Los esquemas de firmas a ciegas son protocolos criptográficos bipartidos entre un cliente V y un firmante U, de tal forma que U firma digitalmente una serie de datos enviados por V, sin conocer el contenido de los mismos. El concepto de firma ciega fue propuesto por Chaum [9] y las dos implementaciones que mencionaba en su artículo eran el voto electrónico y el dinero electrónico.

Un protocolo de firma a ciega requiere de la presencia de los siguientes componentes [10]:

1. Un protocolo de firma digital que sea desarrollado por el prestador del servicio o firmante U, de tal forma que $S(m)$ represente la firma digital del mensaje m.
2. La implementación de dos funciones, f y g, conocidas solo por el usuario V

$$g(S(f(m))) = S(m)$$

El protocolo de firmas a ciegas RSA está constituido por cuatro fases, además el firmante U y el cliente V deben contar con su par de claves pública y privada, ver el apartado 2.3.1, donde se muestra la creación de estas, las fases para realizar el protocolo son las siguientes:

Fase de inicialización: propuesto el mensaje m originado por V y que debe ser firmado por U, debe cumplir la siguiente:

$$0 \leq m \leq n - 1$$

La entidad V genera k, donde k es número entero que cumple las siguientes condiciones:

$$0 \leq k \leq n - 1$$

$$mcd(k, n) = 1$$

Fase de ocultación o de opacidad: La entidad V calcula la opacidad del mensaje, esta debe conocer la llave pública de U (e_U, n_U):

$$h = H(m)$$

$$h' \equiv hk^{e_U} \, mod \, n_U$$

El mensaje oculto será enviado a U, donde h' es el mensaje oculto.

Fase de firma: La entidad U firma el mensaje oculto con ayuda de su llave privada (d_U, n_U), calculando:

$$s' \equiv (h')^{d_U} \equiv (hk^{e_U})^{d_U} \, mod \, n_U$$

Se obtiene s', constituyendo al mensaje oculto firmado por la entidad U, posteriormente se enviará al cliente V.

Fase de recuperación: el cliente V quitara el factor de opacidad al mensaje oculto firmado con la ayuda de su llave privada (d_U, n_U), calculando:

$$s \equiv s'k^{-1} \equiv (h^{d_U})kk^{-1} \, mod \, n_U$$

que es la firma digital del mensaje m por U.

La utilización del cifrado, firmas digitales y firmas a ciegas, facilitan la implementación de los servicios de seguridad, que todo sistema informático debe contar.

2.3 Servicios de seguridad

Ayudan a controlar riesgos de pérdida o modificaciones no autorizadas de la información, hace referencia al conjunto de procedimientos y técnicas de seguridad que lleva a cabo una institución para proteger y asegurar los medios para tratarla, distribuirla o almacenarla. Estos servicios deben implementarse de

manera óptima, su incumplimiento le ocasionaría una pérdida de confianza sobre sus colaboradores.

Elementos de un buen sistema de seguridad:

a) Confidencialidad: consiste en garantizar que la información almacenada o distribuida por la red, no tenga acceso a terceras personas, implica la ocultación de información, esta solo puede ser accesible por aquellas personas que estén autorizadas. Existen diferentes modos para efectuar el mencionado servicio, podría ser de manera física o la implementación de complejos algoritmos matemáticos.

b) **Autenticación**: se refiere al proceso de verificar una supuesta identidad. Consiste en obtener la información de autenticación de una entidad, posteriormente se analizan los datos y determina si la información de autenticación es efectivamente asociada a la entidad. La autenticación se puede realizar de las siguientes formas:

   i. Algo que se tiene
   ii. Algo que se sabe
   iii. Algo que se es

c) Integridad de información: se refiere a la garantía que la información no ha sufrido alteraciones desde su creación sin autorización, la información por lo tanto es válida. Corresponde a que la información no hay sido sufrido modificaciones de intrusos o por cualquier otro medio ajeno sin previa autorización.

d) No repudio: garantiza la participación en la comunicación de las dos partes. En toda comunicación existe un emisor y receptor, por lo que se puede presentar en dos maneras:

   i. No repudio de origen: garantiza que la entidad que envía el mensaje no pueda negar que es el emisor de este, ya que el receptor tendrá pruebas del envió.

ii. No repudio en destino: el receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de este.

e) **Control de acceso**: es el proceso de conceder permisos a usuarios o grupos para acceder a información asignada, permite o niega el acceso a una entidad. Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos, lógicos y digitales.

2.4 Sistemas de reconocimiento biométrico

Un sistema de identificación personal, es utilizado al realizar un proceso de autenticación, consiste en utilizar algún medio que le brinde al usuario la posibilidad de demostrar que es quien dice ser y no ser una entidad no autorizada como lo demuestra la Figura 2.3, a través de: algo que la persona sabe (una contraseña, un PIN, etc.), por algo que la persona tiene (una llave, una tarjeta de identificación, tarjetas inteligentes, etc.) o por medio de la ayuda de un sistema biométrico de reconocimiento en el que la entidad de un individuo es autorizada a partir de alguna de sus características fisiológicas o de comportamiento [11]. Un sistema biométrico se realiza por la utilización de medio de algo que la persona es (una característica fisiológica), o algo que la persona genera (un patrón de comportamiento).

Las características fisiológicas en las que se basan los sistemas de reconocimiento biométrico son: la huella dactilar, la geometría de la mano, el iris, los patrones faciales, etc. Entre las características de comportamiento están: la voz, la firma escrita, el modo de caminar, la forma de escritura por teclado, etc.

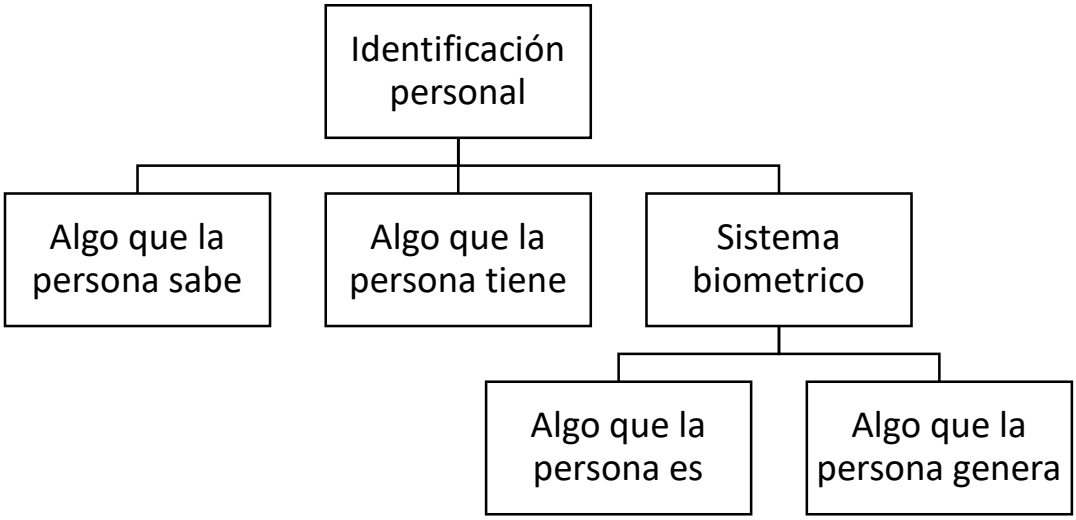

Figura 2.3 Medios para realizar el proceso de autenticación (Fuente: Propia, 2020).

Un sistema biométrico en general está formado de componentes tanto de hardware como de software necesarios para el reconocimiento de una característica exclusiva de una persona, las más utilizada y conocida en la actualidad es el reconocimiento de la huella dactilar por su sencilla implementación y su bajo costo beneficio. La huella dactilar es un rasgo particular de cada individuo, cuyo origen tiene lugar en la etapa fetal y no presenta cambios durante el tiempo de vida del poseedor.

2.4.1 Sistema biométrico de huella dactilar

Un sistema de huella dactilar es capaz de autenticar, registrar e identificar la entidad perteneciente a la persona asociada. Una huella digital normalmente está compuesta por una serie de líneas oscuras que representa las crestas y una serie de espacios en blanco que representa los valles.

Sus cimientos están relacionados con la traducción de la información contenida en la huella digital (utilizando un mapa de puntos clave encontrados

dentro de la huella dactilar) a algoritmos únicos y personales con el objetivo de identificar al usuario y relacionar esta información con sus datos personales.

2.4.2 Arquitectura de un sistema biométrico de huella dactilar

Para realizar un análisis biométrico se debe cumplir los siguientes requisitos [12]:

- Universalidad: el rasgo biométrico está presente para todos los individuos
- Unicidad: el rasgo identifica unívocamente a cada individuo
- Permanencia: la característica es prácticamente estática, no debe modificarse al paso del tiempo
- Cuantificación: la característica puede medirse en forma cuantitativa

Un sistema biométrico de huella dactilar posee tres primordiales módulos. El conjunto de estos módulos realiza las funciones necesarias para reconocer a un individuo que accede al sistema [12].

a) Módulo de inscripción

Está formado por un sistema de adquisición encargado de proporcionar la señal biométrica obtenida del lector biométrico. Las tareas realizadas en este apartado son posibles gracias al lector biométrico y el extractor de características.

Teniendo la señal biométrica resultante de la acción anterior del lector biométrico, se procede a la extracción de las características del rasgo biométrico del individuo. Las características expresan de forma clara y compacta la identidad del individuo y constituyen su llamado patrón biométrico (template) formado por las coordenadas espaciales de los puntos característicos de la imagen, mostrado en la Figura 2.4. Dichos puntos reciben el nombre de minucias.

Figura 2.4 Puntos característicos de una huella dactilar, [13].

b) Base de datos

El patrón biométrico extraído por el módulo de inscripción es almacenado en la base de datos del sistema de reconocimiento. La base de datos contendrá, por tanto, todos los patrones biométricos de los individuos que sean usuarios legítimos del sistema. También dichos patrones dependiendo la finalidad de la aplicación, podrían almacenarse sobre otros soportes como, por ejemplo, una tarjeta magnética o una tarjeta inteligente; en estos casos los datos del individuo se almacenan exclusivamente sobre la tarjeta, dejando a un lado la base de datos centralizada.

c) Módulo de reconocimiento

El módulo de reconocimiento se encarga del reconocimiento de individuos. El proceso de identificación inicia cuando el lector biométrico captura la característica del individuo a ser verificado y la transforma a formato digital, con la finalidad que el extractor de características entregue una representación compacta del patrón biométrico (templates) la representación resultante se le denomina query y se envía al reconocimiento de patrones que se encarga de confrontar un query con uno o varios templates almacenados en la base de datos.

En la Figura 2.5, se observa la interacción de los módulos antes mencionados, de esta forma funciona un sistema biométrico de huella dactilar.

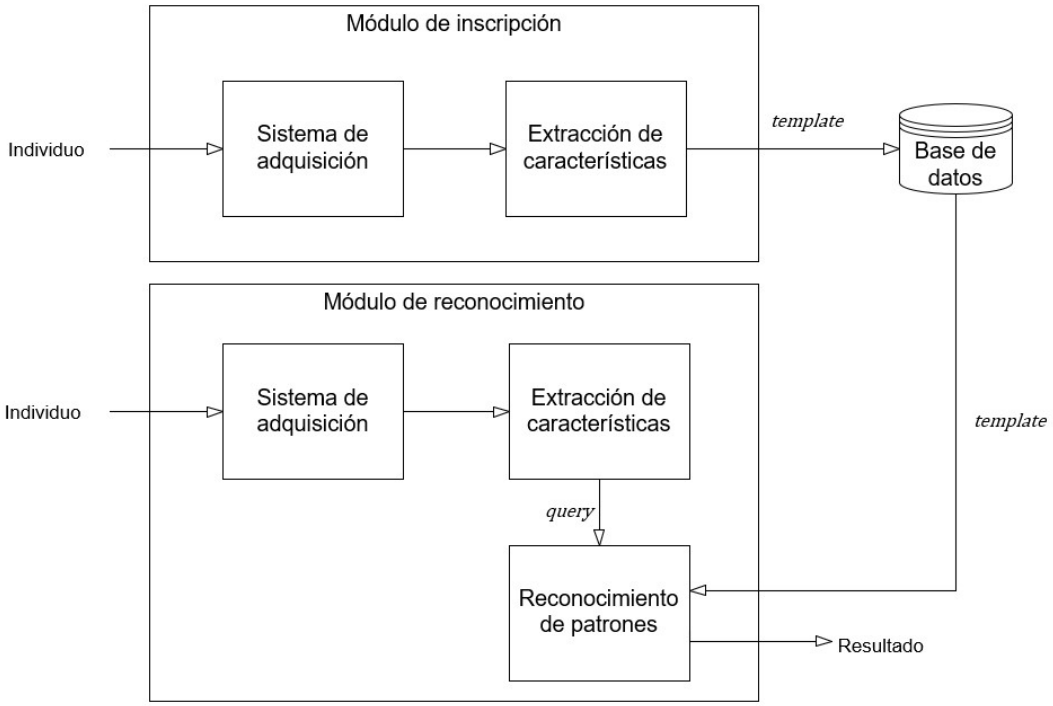

Figura 2.5 Arquitectura de un sistema biométrico de huella dactilar. (Fuente: Propia, 2020).

2.5 Protocolos de votación electrónica

El avance de la tecnología facilita la realización de las actividades cotidianas, permitiendo pasar de sistemas de elección manual a esquemas automatizados de votación electrónica, por medio de dispositivos electrónicos o de Internet. De forma que las entidades electorales, como los votantes pueden desplegar una elección de manera competente, con una simplicidad alta en la emisión del voto o la contabilidad de los mismos en pequeño tiempo.

Un Sistema de Votación Electrónica sostiene su funcionalidad y seguridad en protocolos criptográficos por mencionar algunos ejemplos: firmas a ciegas, cifrado homomórfico y redes combinadas también conocidas como mixing [10].

Las firmas digitales a ciegas: son protocolos bipartidos entre un cliente V y un firmante U, de forma que U firma digitalmente una serie de datos enviados por V sin conocer el contenido de los mismos. El principal propósito es la obtención de una serie de datos firmados cuyo contenido solo sea conocido por el cliente.[14].

Cifrado homomórfico: se basa en la propiedad de ser homomórfico. Lo que se busca es una función $E: M \rightarrow C$, donde M es el espacio de posibles mensajes, y C el espacio de posibles mensajes cifrados, junto con dos opciones binarias, $\oplus$ definida en M y $\otimes$ definida en C, tales que para cualquier mensaje $v1, v2 \in M$, se satisface que $E(v1) \otimes E(v2) = E(v1 \oplus v2)$ [].

La idea es que cada voto sea cifrado individualmente y que la suma de votos se pueda computar sin que sea necesario descifrar cada voto. Una vez que todos los votos sean sumados el total es descifrado. Cramer, Gennaro y Schoenmakers en 1997, proponen un protocolo para voto electrónico basado en una función homomórfica, haciendo uso de una variante del esquema de cifrado de llave pública ElGamal [15].

Protocolo de mezcla o mixing: esto protocolo actúa en la fase de recuento. Trata de imitar las elecciones convencionales, cuando finaliza la elección la urna se agita para romper el orden en que los votos se han depositado.

Los votos emitidos por los votantes, cifrados y firmados previamente al servidor de votación, se almacenan. Cuando acaba la elección, los votos verificados por la firma digital, entran al proceso de mixing para desordenados según la permutación secreta, de esta manera se pierde su relación entre los votos y sus firmas, esto da como resultado la desvinculación de los votantes y el voto emitido, finalmente se procede a su descifrado para obtener el resultado final [16].

Para realizar este proceso se usa una red de mezcla denominados Mix-nodes como se muestra en la Figura 2.6 que, por turnos, van recibiendo los votos

de salida del nodo anterior y se permutan conforme a unos valores secretos para que el orden inicial no pueda ser restablecido una vez terminado el proceso.

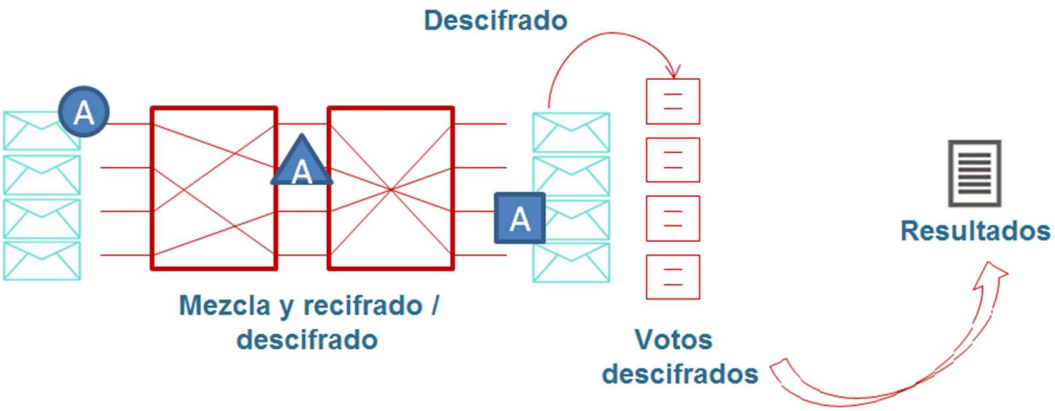

Figura 2.6 Esquema de recuento basado en una Mixnet [16].

Cada protocolo de votación electrónica genera especulaciones por el grado de seguridad que proporciona cada uno de ellos y su funcionamiento que en ocasiones para el votante se le es desconocido. Particularmente, un protocolo satisface la problemática detectada anteriormente por esta razón puede haber amenazas que no sean conocidas burlando su seguridad.

CAPÍTULO 3. REQUERIMIENTOS DE UNA ELECCIÓN ACADÉMICA MANUAL

Mediante esta sección se analizarán los requerimientos y procedimientos para realizar una elección electoral en México, posteriormente nos centraremos en los requisitos para poder llevar a cabo una elección académica en el Centro Universitario UAEM Valle Chalco.

3.1 Elección electoral en México

En México las elecciones electorales federales y locales se organizan a cargo del Instituto Nacional Electoral INE, que es un organismo público e independiente en sus decisiones y funcionamiento.

En la Tabla 3.1, se definen las entidades que actúan dentro del proceso electoral establecido por el INE.

Tabla 3.1 Entidades participantes en el proceso electoral. (Fuente: Propia, 2020).

Elector	Persona con capacidad de votar y que se encuentra inscrita en el censo electoral.
Candidato	Persona que aspira a acceder a determinado cargo. Dicha candidatura pude ser propuesta por ella misma o terceros.
Partido político	Son asociaciones de interés público que representan y transmiten las solicitudes de los ciudadanos y promueven su participación en el ámbito democrático.
Casilla	Es el lugar físico donde los funcionarios de casilla reciben la

	votación de los electores según la sección y el distrito federal electoral que corresponda.
Urna	Es el recipiente que se utiliza durante el proceso electoral con la finalidad que los electores depositen las papeletas en las que han expresado su voluntad, de esta manera se conservan hasta el momento de escrutarlos al final de la votación.
Representante de partido político	Son ciudadanos acreditados ante los organismos electorales que actúan, defienden y representan los intereses del partido político al que pertenecen.
Observadores electorales	Son ciudadanos mexicanos facultados interesados por la ley en conocer el desarrollo y las actividades que se realizan antes y durante las elecciones [17].

El INE propone una serie de tres etapas que dividen el proceso electoral. Si se trata de una elección donde solo se eligen diputados federales. la Figura 3.1 se muestra las etapas antes mencionadas.

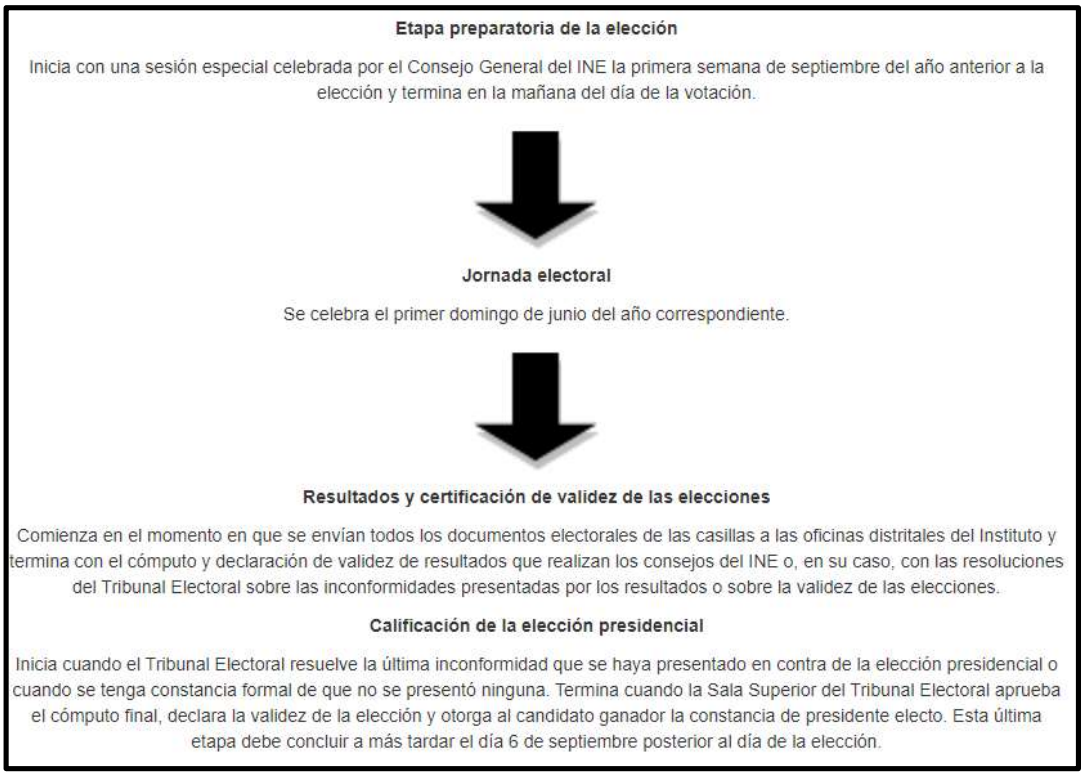

Figura 3.1 Etapas que comprende un proceso electoral federal [18].

Para la realización del proceso electoral se sigue el procedimiento general de votación dirigido por el INE [18], que se describe de esta manera.

- El día de la elección, las casillas deben instalarse en los lugares asignados y la votación se empieza a recibir después de las 08:00 horas. Las personas deben votar en el orden en que llegan a la ubicación de casilla correspondiente.
- Los votantes deben de presentar su credencial para votar ante la mesa directiva de la casilla. La credencial es comparada con la lista nominal de electores que poseen tanto la mesa directiva como los representantes de los partidos políticos.
- Después de verificar su inscripción a en la lista nominal, el votante recibe la papeleta o papeletas de votación.

- Dentro de las mamparas, debe marcar con un crayón el recuadro de su candidato de su preferencia o el logotipo del partido político al que pertenece.
- Una vez que el elector ha marcado su papeleta o papeletas, debe depositarlas en la urna o urnas correspondientes.
- Después de cerrar la casilla, los funcionarios de la misma comenzaran el conteo inicial de los votos en presencia de los representantes de los partidos políticos y de los observadores electorales acreditados.

En la Tabla 3.2 se muestra otra manera de representar las etapas del proceso electoral en fases-

Tabla 3.2 Fases de una elección federal en México

Registro	Autenticación	Votación	Conteo
Inscripción en el Registro Federal de Electores.	El elector acredita pertenecer al listado electoral, ante la mesa directiva de la casilla. Se le entrega su papeleta.	Dentro de las mamparas, debe marcar con un crayón el recuadro del candidato de su preferencia o el partido político al que pertenece.	Después de cerrar la casilla, los funcionarios, representantes de partidos y observadores electorales; contaran los sufragios.

Para poder participar en el proceso electoral dirigido por el INE, debe cumplir con las siguientes características [18]:

- Todos los mexicanos mayores de edad y que disfruten un modo honesto de vivir. Sin embargo, para que disfruten de ese derecho es necesario. Además, que estén inscritos el Registro Federal de Electores.

- Los ciudadanos que hayan sido rehabilitados en sus derechos político-electorales.
- Los ciudadanos que cuenten con una resolución del Tribunal Electoral del Poder Judicial de la Federación, que en sus resolutivos ordene que se les permita ejercer su derecho.

3.2 Elección académica en el Centro Universitario UAEM Valle de Chalco

Para la recopilación de los requerimientos para efectuar una votación electoral en un Centro Universitario perteneciente a la UAEM, nos orientamos de los Lineamientos que regulan el proceso de elección de director de Organismo Académico, Centro Universitario UAEM y plantel de la Escuela Preparatoria de la Universidad Autónoma del Estado de México [3], que siembran los cimientos de como regular una jornada electoral académica perteneciente, estos se encuentran publicados en la Gaceta Universitaria. .

Los presentes lineamientos son reglamentarios del artículo 117 del Estatuto Universitario; y tienen por objetivo establecer las bases que deberán observarse en la sustentación de las fases de publicación de convocatoria; inscripción, calificación y registro de aspirantes; jornadas de promoción; auscultaciones cualitativa y cuantitativa y opinión del Consejo de Gobierno, para la apelación y toma de protesta de los directores de Organismos Académicos, Centro Universitario UAEM o plantel de la Escuela Preparatoria.

Nota: Para facilitar la lectura y no agrandar la extensión de dicho documento, el Centro Universitario UAEM y plantel de la Escuela Preparatoria, estará contenido en la entidad Organismo Académico.

La vigilancia y conducción del proceso de elección de Director de Organismo Académico, estará a cargo de la Comisión de Procesos Electorales del Consejo Universitario o CPECU.

La CPECU tendrá por finalidad, dictaminar sobre la aceptación o rechazo del registro de aspirantes y resolver otros aspectos no previstos en los presentes Lineamientos.

Además de los miembros designados como permanentes, con el objeto de ampliarla, se integrarán a la CPECU.

a) El director que se encuentre en funciones del Organismo Académico
b) Cuatro consejeros: dos alumnos y dos integrantes del personal académico, integrantes del Consejo de Gobierno del Organismo Académico, y designados por ese órgano.
c) A esta comisión se integrarán, en su caso, los representantes de los aspirantes que solicitaron y obtuvieron su registro. El representante será integrante del personal académico del Organismo Académico de que se trate, además de la representación que detenta, funciones exclusivas de observador, con voz y sin derecho a voto en el seno de la Comisión.

La publicación de convocatoria para el proceso de elección de Director de Organismo Académico, será expedida en términos de lo dispuesto por el Estatuto Universitario y publicado con al menos 15 días naturales de anticipación.

Las solicitantes de registro de aspirantes a director, deberán presentarse ante el director que se encuentre en funciones, al tercer día hábil posterior a la publicación de la convocatoria. El director que se encuentre en funciones turnara las solicitudes recibidas a la Comisión Ampliada de Procesos Electorales del Consejo Universitario o CAPECU.

Las solicitudes de registro de aspirantes se presentarán por escrito, acompañadas de los documentos que acrediten el cumplimiento de los requisitos que señala el artículo 116 del Estatuto Universitario para ocupar el cargo.

En caso de que exista inconformidad por parte del aspirante respecto a la negativa de su registro, podrá interponer el día y hora que se fije en la convocatoria, a través de su representante, recursos que consideren ante la CAPECU, la comisión resolverá la inconformidad en un plazo no mayor a doce horas entregando su resolución por escrito al interesado; la resolución que emita la Comisión, no admitirá recurso alguno.

Para poder participar en las jornadas de promoción y consecuentemente en la fase de auscultación, el aspirante requiere haber obtenido constancia de registro emitida por la CAPECU.

Los aspirantes con registro deberán realizar jornadas de promoción en que demuestren su calidad académica y espíritu universitario, obligándose a preservar la vida institucional, no alterar el orden ni la dignidad de los otros aspirantes.

Es obligación de los aspirantes con registro suspender su jornada de promoción y retirar su propaganda 24 horas antes de iniciar el proceso de auscultación cuantitativa de los sectores correspondientes.

Durante el tiempo previsto para la realización de las jornadas de promoción, la CAPECU llevara a cabo la auscultación cualitativa.

Terminada la fase de promoción, la CAPECU, procederá a realizar la auscultación cuantitativa, con el objeto de que los Consejeros Universitarios puedan orientar su criterio al emitir su voto.

El proceso de auscultación cuantitativa es el mecanismo que permite recoger opiniones de los integrantes de la comunidad universitaria correspondiente a cada Organismo Académico.

La opinión del Consejo de gobierno corresponde a cada Organismo Académico, contendrá elementos cuantitativos de los aspirantes, sin realizar juicios o argumentos valorativos en beneficio o demerito de uno o más de ellos.

En el proceso de auscultación cuantitativa correspondiente a cada Organismo Académico, solo podrán participar:

a) Los alumnos inscritos en las listas oficiales expedidas por el Departamento, Jefatura o dependencia similar de Control Escolar del Organismo Académico de que se trate.
b) El personal académico ordinario y administrativo adscrito al Organismo Académico de que se trate; según la relación que emita la Dirección de Recursos Humanos de la Universidad.
c) El personal académico definitivo que imparta docencia en semestres alternados, se encuentre de goce de año sabático, de una beca, de un permiso de estudios de una licencia o permiso expedido por la Universidad en términos de la legislación Universitaria.

En el caso de personas que detentan simultáneamente las calidades de personal académico, personal administrativo y/o alumno, emitirán única y exclusivamente su opinión en la calidad como se presentó su primera vinculación con la Universidad.

En el proceso de elección, designación, y toma de protesta de Director de Organismo Académico, consiste en la serie de antecedentes y actos que permiten al Rector de la Universidad la presentación de o los candidatos a ocupar el cargo ante el Consejo Universitario, a fin de que este proceda a celebrar la elección mediante voto personal, nominal, discreto y secreto.

El Consejo Universitario elegirá por mayoría de votos al director del Organismo Académico, para un periodo ordinario de cuatro años.

La presentación del o los candidatos a ocupar el cargo de director de Organismo Académico, la realizara el Rector de la Universidad, conforme lo establecido en la fracción IX del artículo 24 de la Ley Universitaria.

En la presentación se dará lectura al acta de auscultación cuantitativa y se informará sobre la síntesis del Curriculum Vitae, resumen del programa de trabajo

y la calificación prevista en el artículo 8 de los Presentes Lineamientos y las opiniones vertidas por el Consejo de Gobierno, correspondiente al Organismo Académico.

Finalmente teniendo presentes los requisitos para efectuar un proceso de votación electoral en un Centro Académico, como siguiente paso es plasmar los diseños con los requerimientos solicitados.

CAPÍTULO 4. DISEÑO DEL SISTEMA PROPUESTO

Una vez realizado el análisis pertinente para el desarrollo de un sistema de votación electrónico, en este capítulo se presenta el diseño de SEVS que tiene como objeto principal identificar las funciones primordiales del sistema con el enfoque particular de reducir la cantidad posible ataques conocidos durante la realización del proceso electoral. Para tal efecto, el diseño del software planteado se basa en el Proceso Unificado de Desarrollo de Software, particularmente con los diagramas de Lenguaje Unificado de Modelado (UML).

4.1 Casos de Uso

El diseño del sistema comienza con el diagrama general de casos de uso, donde se aprecian los requerimientos funcionales del sistema, aquel se presenta en la Figura 4.1, que muestra la interacción de todos los actores principales, como el Aspirante a Director, la Comisión de Procesos Electorales y el Integrante del Centro Universitario; lo subsistemas o módulos que lo integran, que son, los Módulos de registro, de votación y de conteo.

En la Figura 4.2, se observa cómo está conformado en un nivel menos abstracto el caso de uso *Generar Padrón Electoral*, presente en el Módulo de registro, que tiene como objetivo gestionar el listado del padrón electoral; en el cual se guarda la información de los candidatos y votantes en la base de datos que corresponde al listado nominal.

De este caso de uso, se desprenden los casos de uso *Registrar candidato, Registrar votante, Registrar huella digital y Generar información criptográfica*. La Tabla 4.1 detalla lo realizado por el caso de uso Registrar votante, que se puede considerar la actividad más importante para el Módulo de Registro.

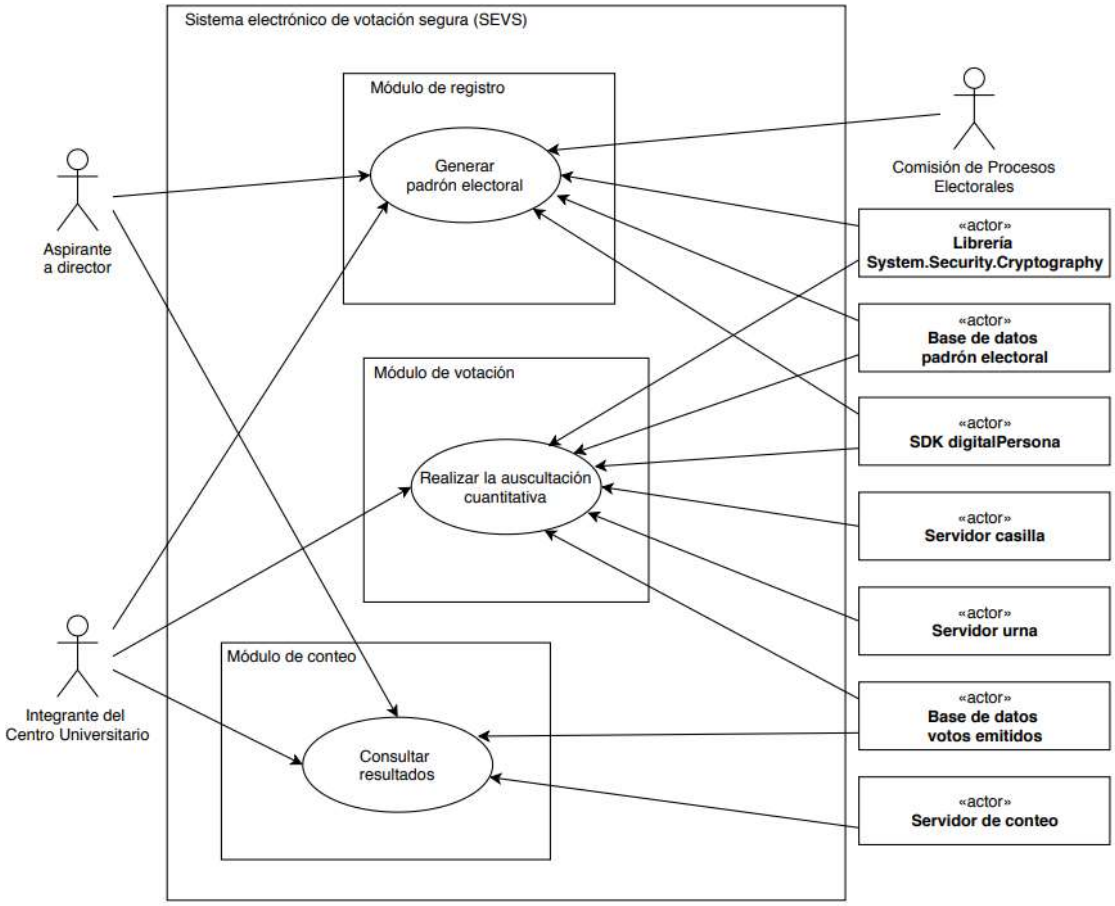

Figura 4.1 Diagrama de casos de uso general (Fuente: Propia, 2020).

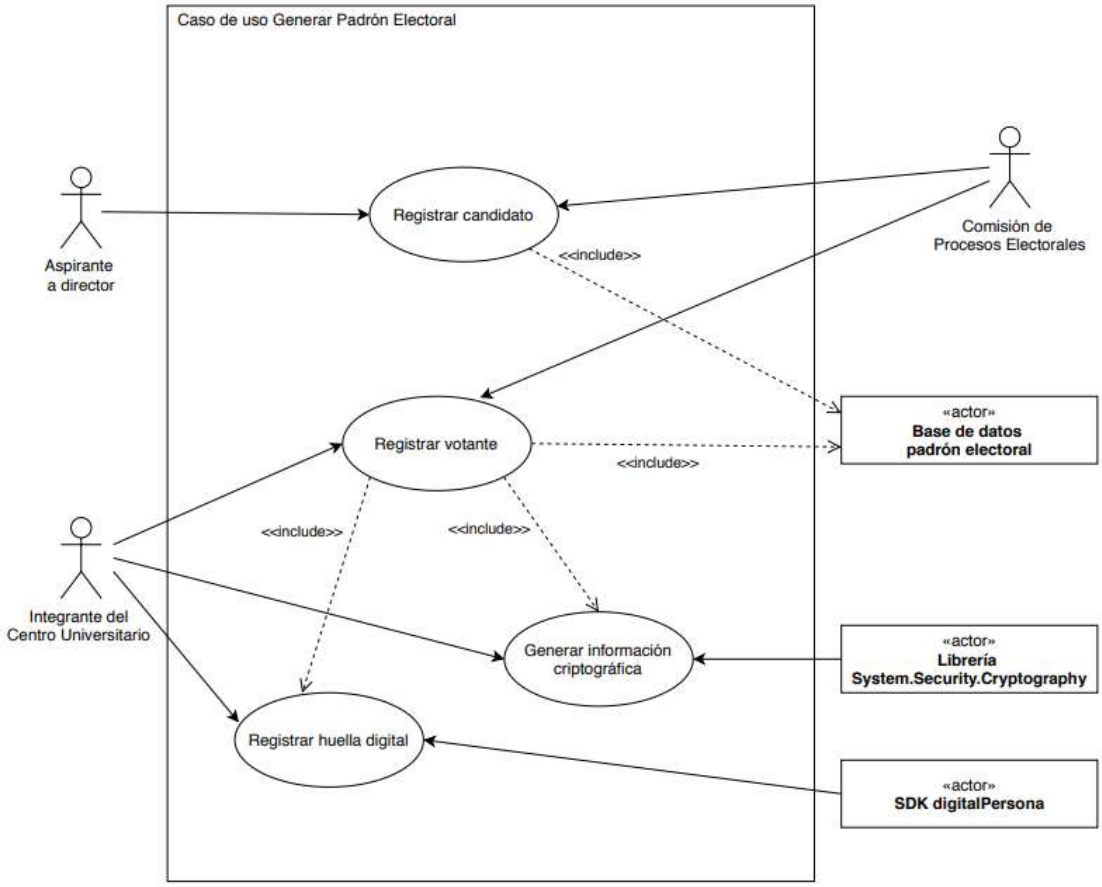

Figura 4.2 Diagrama de caso de uso Generar Padrón Electoral (Fuente: Propia, 2020).

Tabla 4.1 Caso de uso Registrar votante (Fuente: Propia, 2020).

Nombre: Registrar votante
Actores: Comisión de Procesos Electorales, Integrante del Centro Universitario, Base de datos padrón electoral, Librería System.Security.Cryptography y SDK digitalPersona.
Descripción: Alta de un Integrante del Centro Universitario en el Padrón Electoral.
Disparador: Click en el elemento “Registrar” que se encuentra dentro del submenú “Votante”.
Precondiciones:

1. El Integrante del Centro Universitario debe ser personal activo.
2. El Integrante del Centro Universitario debe solicitar su registro y estar presente durante el proceso.

Postcondiciones:

1. El Integrante del Centro Universitario:
    a. Se integra al padrón electoral.
    b. Se obtiene su información criptográfica
    c. Se genera su información biométrica.

Flujo normal:

1. El Integrante del Centro Universitario solicita su registro.
2. Un Integrante de la Comisión de Procesos Electorales verifica si el Integrante del Centro Universitario se encuentra activo. E1
3. Un Integrante de la Comisión de Procesos Electorales solicita dar de alta al votante.
4. El sistema despliega un formulario para registrar al votante.
    a) Categoría (*).
    b) Matricula (*).
    c) Nombre (*).
    d) Apellido paterno (*).
    e) Apellido materno.
    f) Patrón biométrico (*). El sistema llama al caso de uso Registrar huella digital
    g) NIP (*).
    h) Confirmar NIP (*).
5. El integrante de la Comisión de Procesos Electorales completa los campos con la ayuda del Integrante del Centro Académico, con excepción de los campos NIP, Confirmar NIP, Patrón Biométrico, los cuales, solo serán ingresados por el Integrante del Centro Universitario.

6. El sistema valida los campos. S1, E2. 7. El sistema llama al caso de uso Generar información criptográfica. 8. El sistema cifra la llave privada tomando como llave simétrica al NIP. 9. El sistema guarda los datos en la base de datos.
Flujos alternativos: S1 No se cargaron todos los campos requeridos.
Excepciones: E1. El Integrante del Centro Universitario no se encuentra activo. E1.1 El integrante de la Comisión de Procesos Electorales no procede a realizar el registro y le da a saber su situación. E.1.2 Termina el Caso de Uso E2. El formulario se encuentra incompleto. E2.1 Se despliega el aviso “Favor de ingresar los elementos necesarios”. E.2.2 Termina el Caso de Uso
Prioridad: Alta
Frecuencia de uso: Alta
Reglas: Todos los campos deben ser validados para proceder con el registro en el padrón electoral.

Otro caso de uso importante por mencionar es *Realizar la auscultación cuantitativa* presente en el Módulo de votación, ilustrado en la Figura 4.3. En él, se realiza el proceso de selección del candidato en el caso de uso *Emitir voto*, en el cual se deberá solicitar la boleta electoral ante el servidor casilla, aquel pedirá que se identifique para demostrar que verdaderamente es la entidad correspondiente. El voto emitido debe ser ocultado para que el servidor casilla verifique su integridad, este proceso debe ser necesario para ser enviado al

servidor urna, el cual se encargara de guardar el voto en la base de datos votos emitidos.

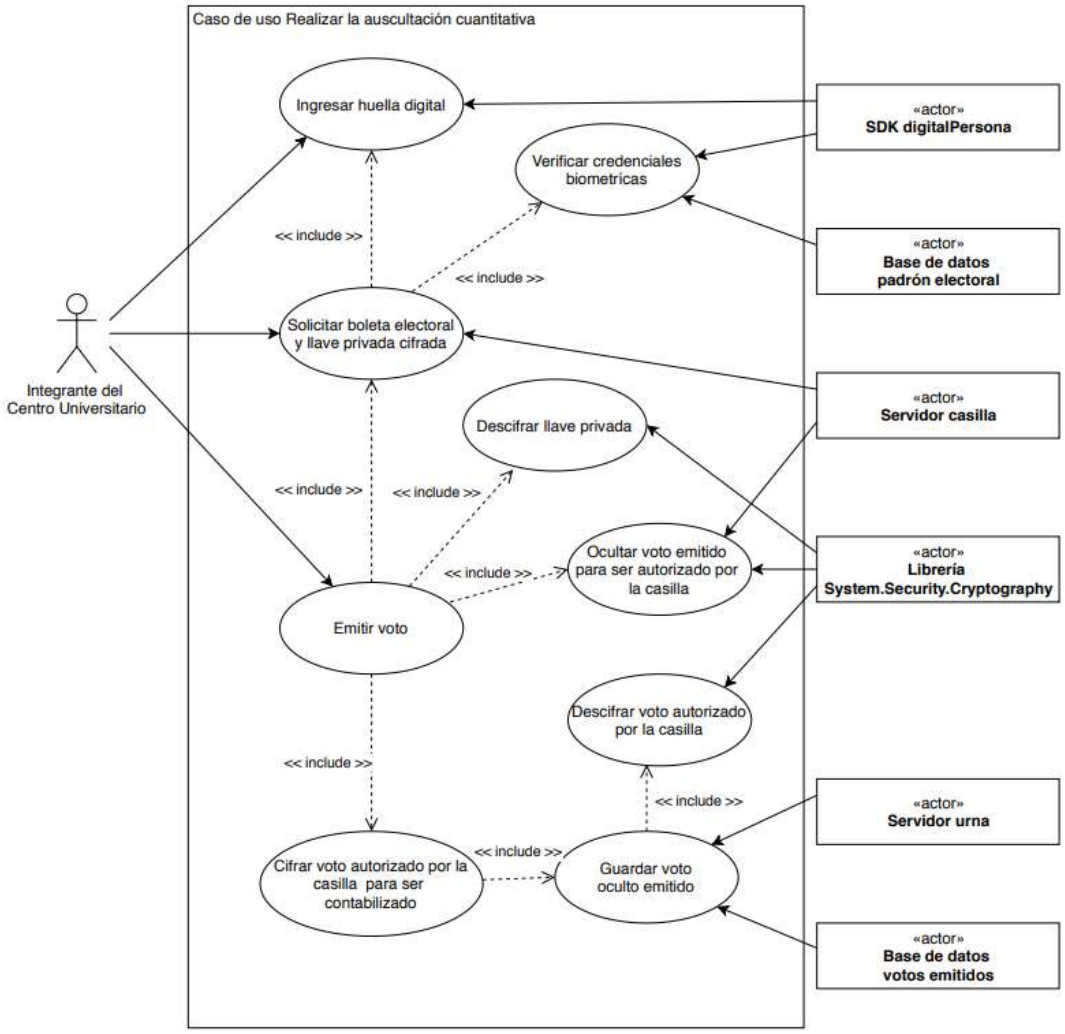

Figura 4.3 Diagrama de caso de uso Realizar la auscultación cuantitativa (Fuente: Propia, 2020).

En la Tabla 4.2 se detallan las características y el flujo para el caso de uso *Solicitar boleta electoral y llave privada cifrada*. Este caso de uso tiene como objetivo obtener la boleta electoral y su respectiva llave privada esta se encuentra cifrada, proporcionadas por el servidor casilla estas se obtienen demostrando que el Integrante del Centro Universitario es quien dice ser, validando sus credenciales biométricas registradas en la base de datos padrón electoral.

Tabla 4.2 Caso de uso Realizar la Auscultación Cuantitativa (Fuente: Propia, 2020).

Nombre: Solicitar boleta electoral y llave privada cifrada
Actor: Integrante del Centro Universitario, Servidor casilla, Base de datos padrón electoral y SDK digital Persona.
Descripción: Obtener boleta electoral por parte de la casilla y la llave privada cifrada correspondiente del Integrante del Centro Universitario demostrando ser parte del padrón electoral.
Disparador: Finalizar el llenado del formulario de autenticación para el acceso a la fase de Auscultación cuantitativa.
Precondiciones: 1. El Integrante del Centro Universitario: a. Debe estar inscrito en el padrón electoral. b. No debe haber solicitado la boleta electoral al Servidor casilla y la llave privada cifrada previamente.
Postcondiciones: 1. El Integrante del Centro Universitario obtendrá la boleta electoral y su llave privada cifrada para continuar con emitir su voto.
Flujo normal: 1. El módulo de votación despliega el formulario para ingresar al sistema: a) Matricula (*). b) Leer huella digital (*). Se llama al caso de uso Ingresar huella digital. S1. 2. El sistema llama al caso de uso *Verificar credenciales biométricas*. E1, E2. 3. Se muestra la boleta obtenida proporcionada por la casilla.
Flujos alternativos: S1 No se obtuvo la huella digital.

S1.1 El votante abandono el sistema o no se encontró el lector biométrico y se termina el caso de uso.
Excepciones: E1. El Integrante del Centro Universitario no se encuentra inscrito en el padrón electoral o sus credenciales no coinciden. E1.1 El sistema desplegara el aviso adecuado a su situación. E.1.2 Termina el Caso de Uso E2. El servidor casilla no se encuentra activo, fin del proceso electoral. E2.1 Se despliega el aviso “El servidor casilla se encuentra inhabilitado”. E.2.2 Termina el Caso de Uso
Prioridad: Alta
Frecuencia de uso: Alta
Reglas: Para solicitar la boleta electoral y la llave privada cifrada debe estar vigente el periodo del proceso electoral.

En la Tabla 4.3 se muestran las características y el flujo del caso de uso *Emitir voto*. El cual debe realizar lo siguiente: elegir el candidato preferido por el votante; demostrar ante el Servidor casilla la integridad del voto sin que conozca el contenido de éste, ocupando una función de ocultamiento; enviar el voto cifrado validado por la casilla hacia el Servidor urna para que verifique la integridad del voto descifrándolo; y finalmente guardar en la base de datos el voto emitido.

Tabla 4.3 Caso de uso Solicitar boleta electoral y llave privada cifrada (Fuente: Propia, 2020).

Nombre: Emitir voto
Actor: Integrante del Centro Universitario, Servidor casilla, Servidor urna, Base de datos padrón electoral y SDK digitalPersona.

Descripción: Emitir el voto por parte del votante.
Disparador: Seleccionar el candidato preferido por el Integrante del Centro Universitario en la boleta digital.
Precondiciones: 1. El Integrante del Centro Académico: a. Debe contar con su boleta electoral. b. Debe de recordar el NIP proporcionado en el Módulo de registro.
Postcondiciones: 2. El Integrante del Centro Universitario emitirá su voto el cual será contabilizado finalizando el tiempo electoral 3. El Integrante del Centro Universitario no podrá volver a emitir nuevamente su voto.
Flujo normal: 1. El Módulo de auscultación cualitativa despliega el formulario contenedor de la boleta electoral obtenida en el caso de uso *Solicitar boleta electoral y llave privada cifrada*, donde se muestran los candidatos registrados y la opción de generar un voto nulo. 2. El Integrante del Centro Universitario selecciona a su candidato preferido, realizando la acción de click sobre su respectiva foto. 3. El sistema le pedirá que compruebe su candidato elegido. S1. 4. El sistema despliega un formulario donde solicita que ingrese su NIP proporcionado en el Módulo de registro. E1. 5. El sistema llama al caso de uso *Descifrar llave privada*, utilizando el NIP solicitado anteriormente. E2. 6. El sistema llama al caso de uso *Ocultar voto* emitido para ser autorizado por la casilla. 7. El sistema llama el caso de uso *Cifrar voto* autorizado por la casilla para ser contabilizado.

Flujos alternativos: S1 El Integrante del Centro Universitario no comprueba su candidato elegido. S1.1 El votante abandono el sistema y el voto no es almacenado.
Excepciones: E1. El Integrante del Centro Universitario no se acuerda de su NIP. E1.1 El sistema desplegara el aviso adecuado a su situación. E.1.2 Termina el Caso de Uso E2. El Integrante del Centro Universitario ha emitido su voto anteriormente. E2.1 Se despliega el aviso “No se puede votar más de una vez”. E.2.2 Termina el Caso de Uso
Prioridad: Alta
Frecuencia de uso: Alta
Reglas: Para emitir el sufragio, el Integrante del Centro Universitario: a) No haber votado antes. b) Recordar su NIP c) En caso de no recordar el NIP, no podrá recuperarlo.

4.2 Diagrama de Clases

En este apartado se describen las partes y componentes del sistema propuesto, en especial, los módulos de registro y de votación, mostrando de forma detallada, las clases más importantes. El módulo de conteo es omitido en este apartado por su sencillo entendimiento.

En la Figura 4.4 se muestran las relaciones que existen entre las clases del módulo de registro del sistema propuesto.

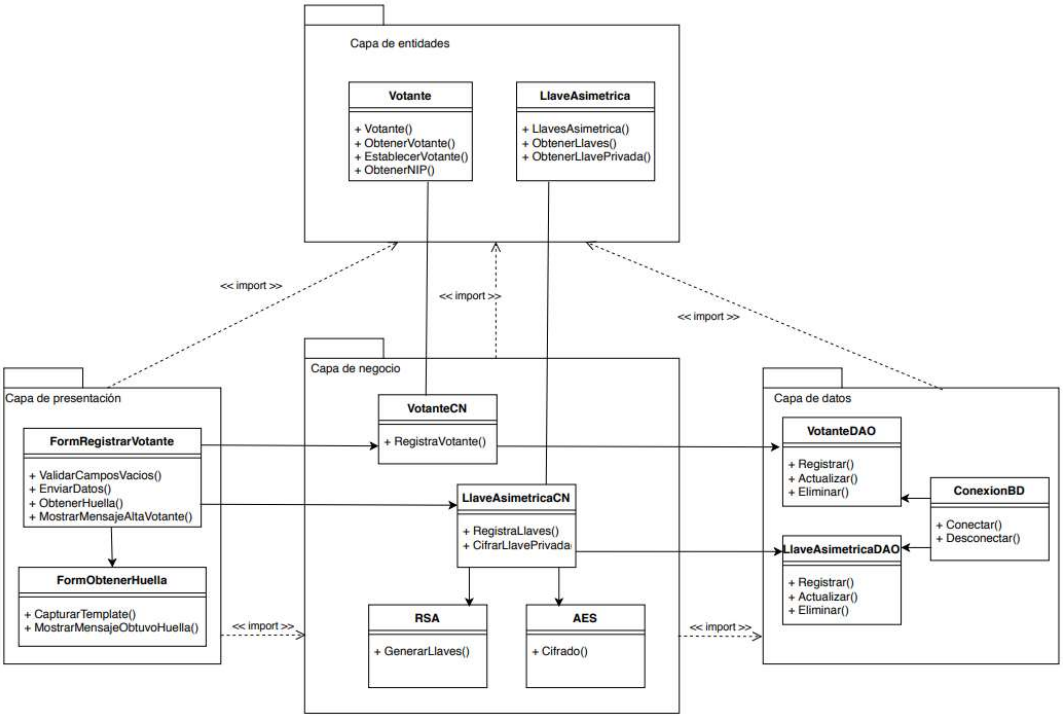

Figura 4.4 Diagrama de clases del módulo registro (Fuente: Propia, 2020).

Finalmente, en la Figura 4.5 se muestran las relaciones que existen en el Módulo de votación y la comunicación con el Servidor casilla y Servidor Urna.

4.3 Diagrama de Secuencia

Los diagramas de secuencia permiten conocer cómo trabaja el sistema y la manera de que el usuario interactúa con el sistema [3]. Así mismo, se muestran las relaciones que hay entre las clases y sus métodos que fueron descritos por los diagramas de clases. En las Figuras 4.6 y 4.7 se describen los casos de uso *Registrar votante* y *Realizar la auscultación cuantitativa*.

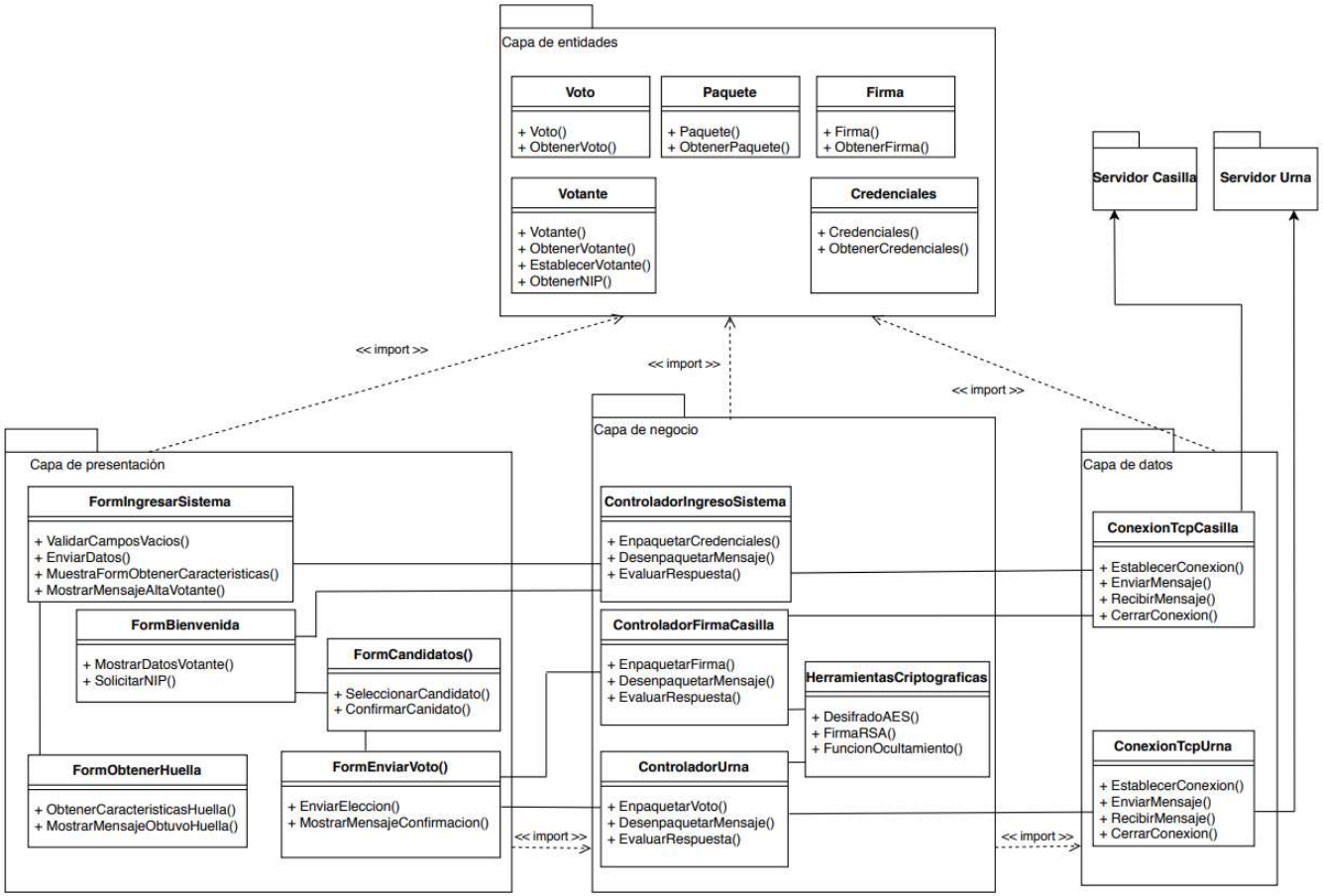

Figura 4.5 Diagrama de clases del módulo votación (Fuente: Propia, 2020).

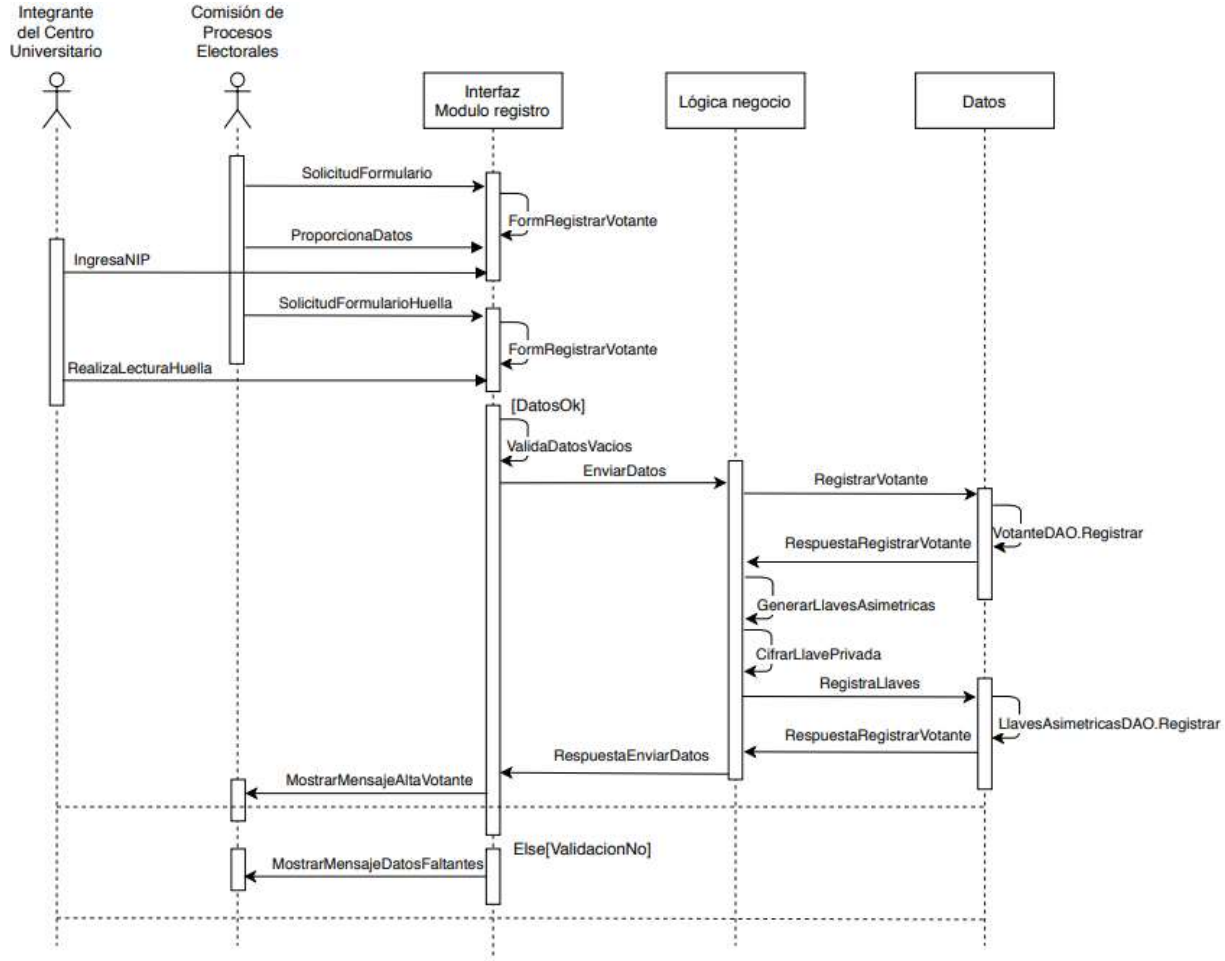

Figura 4.6 Diagrama de secuencia de Registro de votante. (Fuente: Propia, 2020).

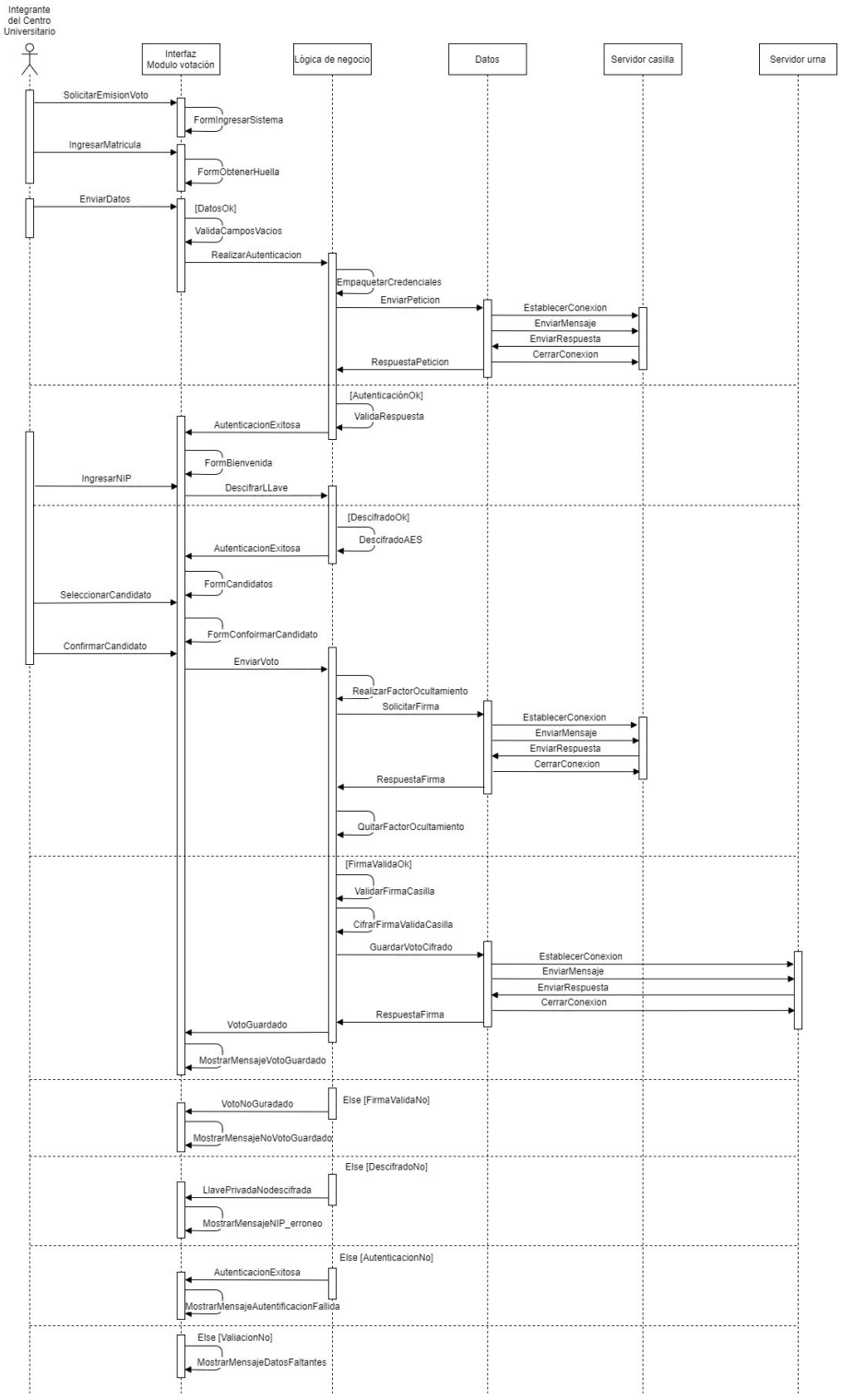

Figura 4.7 Diagrama de secuencia de Realizar la auscultación cuantitativa. (Fuente: Propia, 2020).

CAPÍTULO 5. IMPLEMENTACIÓN Y PRUEBAS DE SEVS

En este capítulo se presenta la interfaz de los módulos correspondientes del sistema, proporcionado en cada uno de ellos un ejemplo sin desacierto por parte del usuario, es decir, suponiendo que el actor pertinente ingresa toda la información como lo establece el proceso correspondiente al módulo anfitrión.

a) Modulo de registro

En el primer acercamiento, se presenta el diagrama de bloques mostrando la ruta para cada una de las opciones contenidas en la interfaz del módulo en la Figura 5.1.

Como puede observarse, el módulo se compone de dos principales tareas y a partir de ellas se desprenden las diferentes opciones que permitirán al usuario interactuar de forma amigable con el sistema.

La implementación del módulo se realizó en un equipo de cómputo con un procesador Intel(R) Celeron(R) CPU N2840 @ 2.16 GHz 2.16 GHz, memoria RAM 4.00 GB, 500 GB en disco duro y sistema operativo Windows 10 Pro de 64 bits. Además, la incorporación del lector de huellas dactilares DigitalPersona 4500.

Respecto al software, se utilizó lo siguiente:

- Lenguaje de programación C#
- IDE Visual Studio 2019
- Draw.io para la realización de los diagramas UML
- Gestor de base de datos MySQL Server 5.5.5-10.4.8-MariaDB
- SDK DigitalPersona para configuración de la parte biométrica

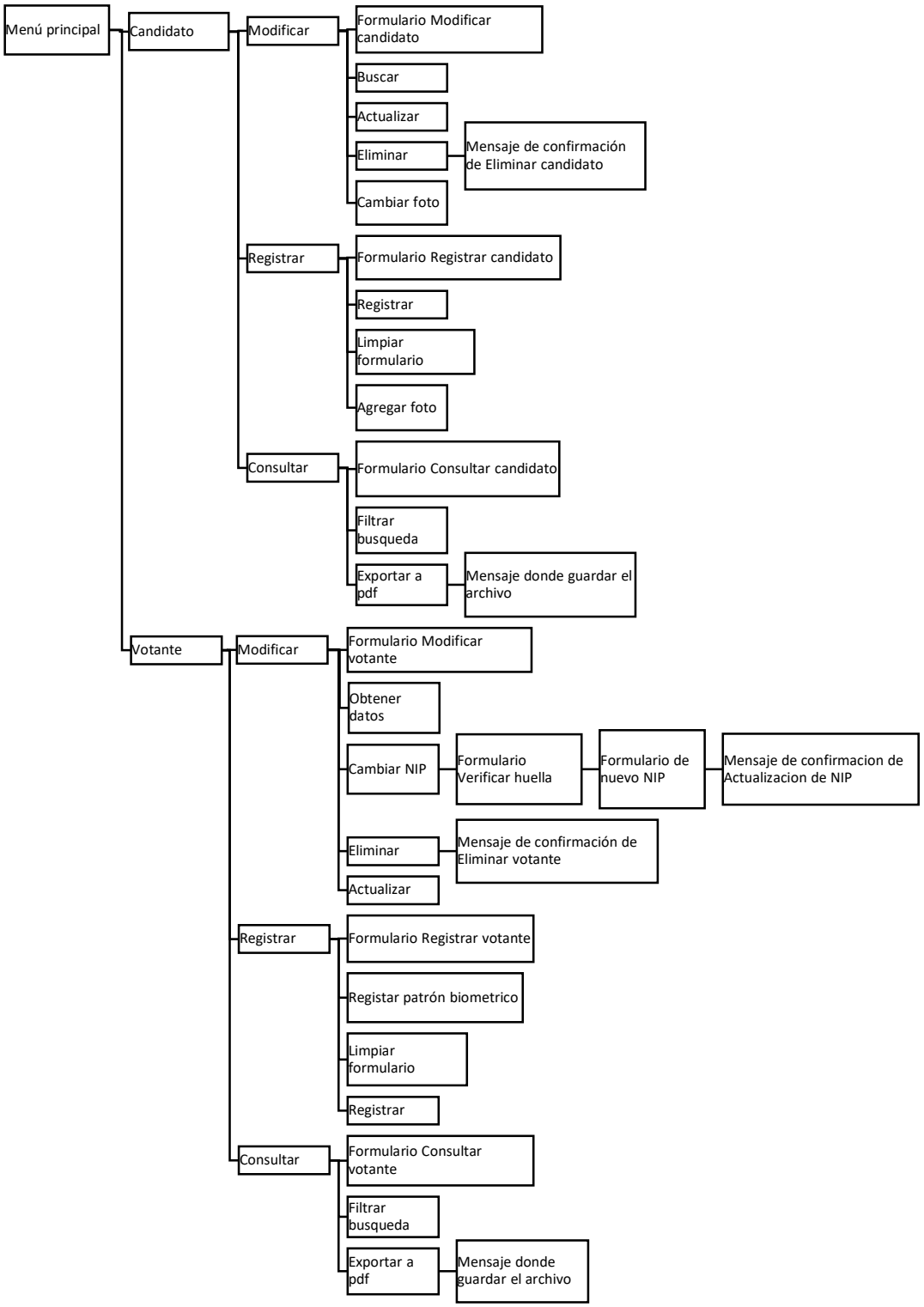

Figura 5.1 Diagrama de bloques del Módulo de Registro. (Fuente: Propia, 2020).

b) Módulo Casilla y Módulo Votación

Como se observa en la Figura 5.2, el módulo tiene como tarea principal la emisión del voto en forma secuencial, la interfaz del módulo es amigable con el usuario.

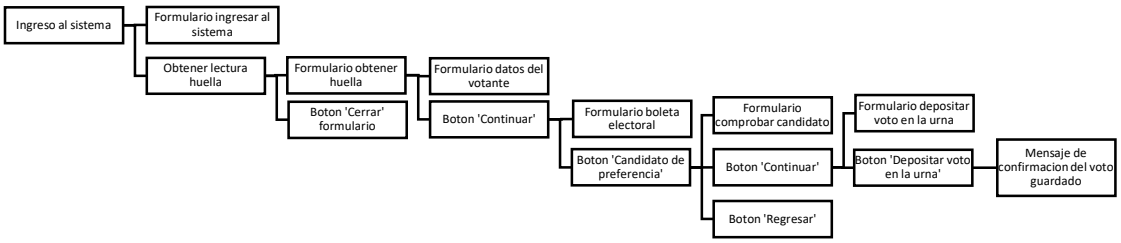

Figura 5.2 Diagrama de bloques del módulo de votación. (Fuente: Propia, 2020).

La implementación se realizó en un equipo de cómputo con un procesador Intel(R) Core (TM) i7-9750H CPU @ 2.6 GHz. Memoria RAM 16 GB, 1 TB en disco duro y sistema operativo Windows 10 Pro de 64 bits. Respecto al software se utilizó lo siguiente:

- Lenguaje de programación C#
- IDE Visual Studio 2019
- Draw.io para la realización de los diagramas UML
- SDK DigitalPersona para configuración de la parte biométrica.

c) Módulo de conteo

Siguiendo con el proceso, en la Figura 5.3, se muestra el diagrama de bloques del módulo del conteo, en el cual los usuarios podrán consultar los resultados de la elección cuando esta termine.

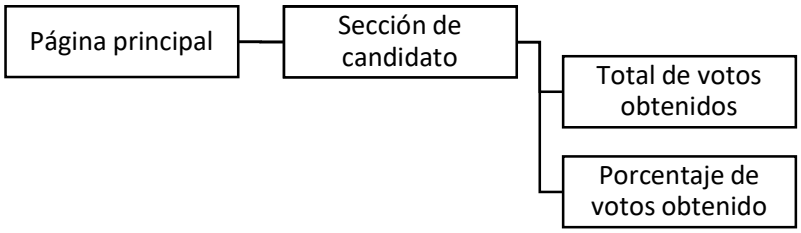

Figura 5.3 Diagrama de bloques del módulo de conteo. (Fuente: Propia, 2020).

La implementación se realizó en un equipo de cómputo con un procesador Intel(R) Core (TM) i7-8750H CPU @ 2.2 GHz. Memoria RAM 16 GB, 1 TB en disco duro y sistema operativo Windows 10 Pro de 64 bits. Respecto al software se utilizó lo siguiente:

- Lenguaje de programación PHP 7
- IDE Visual Studio Code
- Draw.io para la realización de los diagramas UML
- Bootstrap
- HTML 5
- Gestor de base de datos MySQL Server 5.5.5-10.4.8-MariaDB

5.1 Caso de prueba

En este apartado se presenta un caso de prueba que se inicia con el alta de un candidato. Es importante mencionar que todos los datos colocados en el ejemplo son ficticios para proteger la información de los usuarios reales que utilizaron SEVS. Como primer paso se selecciona la opción Candidato ubicada en el Menú principal del módulo se puede observar en la Figura 5.4.

Figura 5.4 Menú principal del módulo de registro. (Fuente: Propia, 2020).

Procediendo con el proceso se despliega el menú desplegable, se debe seleccionar la opción Registrar, realizando este paso se mostrará el formulario para registrar el candidato, en la Figura 5.5 se puede observar el formulario correspondiente.

Figura 5.5 Formulario para registrar un candidato. (Fuente: Propia, 2020).

Se continua el registro del candidato ingresando los datos del mismo, así como su foto personalizada, la cual debe tener un tamaño recomendado de 500px x 500px. Finalmente, se elige la opción de Registrar para salvar los datos capturados, si la acción se realiza con éxito se muestra un mensaje que el Candidato se registró satisfactoriamente, como se visualiza en la Figura 5.6.

Siguiendo con la demostración de funcionalidad del sistema, se muestra los pasos para registrar a un votante, iniciando con elegir la opción de Votante ubicada en el menú principal, se desplegará un menú desplegable y se elegirá la opción de Registrar obteniendo el formulario de registro de votante, como se muestra en la Figura 5.7.

Figura 5.6 Registro del candidato en el Módulo de registro (Fuente: Propia, 2020).

Figura 5.7 Formulario para realizar el registro de un votante. (Fuente: Propia, 2020).

Con la ayuda del Integrante del Centro Universitario se llena el formulario, el cual tendrá que ingresar sus datos confidenciales estos son NIP y las lecturas biométricas que permiten generación de su patrón biométrico. En la Figura 5.8 se puede apreciar el llenado de los campos del formulario anfitrión.

Figura 5.8 Llenado del formulario para poder registrar al votante. (Fuente: Propia, 2020).

Cuando el usuario selecciona la opción de Generar patrón biométrico dactilar emerge un nuevo formulario, mostrado en la Figura 5.9. Este formulario tiene el objetivo principal de recolectar las lecturas del dedo índice y generar el patrón biométrico para poder continuar con el registro del votante.

Para finalizar con el registro del votante y teniendo el formulario con los datos correspondientes, se elegirá la opción Registrar para guradar los datos en la base de datos correspondiente, si todo se realiza correctamente se desplegara un aviso con la siguiente leyenda “Votante registrado satisfactoriamente.”, como se observa en la Figura 5.10.

Figura 5.9 Formulario para obtener el patrón biométrico. (Fuente: Propia, 2020).

Figura 5.10 Registro de votante. (Fuente: Propia, 2020).

Para realizar la emisión del voto, se ingresará al sistema por medio de la interfaz mostrada en la Figura 5.11, la cual solicita la matrícula correspondiente del votante que se quiere identificar ante el servidor casilla.

Una vez ingresada la matrícula asociada el votante, se elegirá la opción Obtener huella la cual se observa en la Figura 5.12, realizando este procedimiento se mostrará una nueva interfaz en la cual solicitará la lectura del dedo índice para obtener los datos correspondientes del votante que se encuentran guardados en el servidor casilla.

En la Figura 5.13 se muestra el formulario por el cual se realiza la autenticación biométrica con el servidor casilla, si la autenticación se realiza de manera correcta se mostrará un nuevo formulario mostrando los datos públicos del votante.

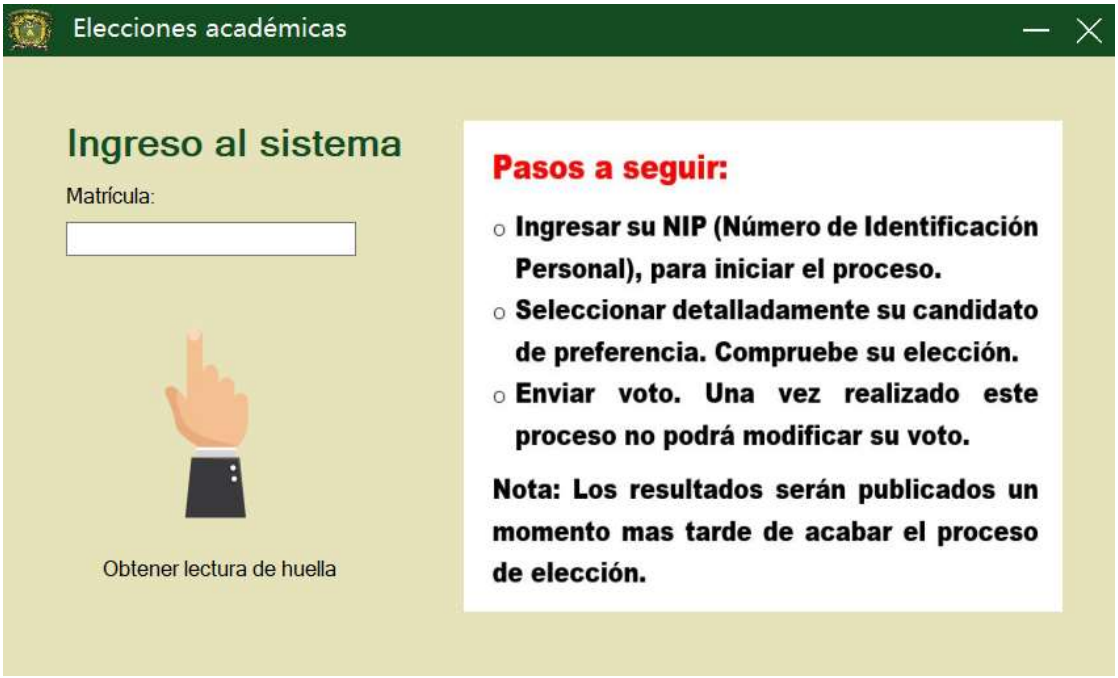

Figura 5.11 Formulario para ingresar al sistema. (Fuente: Propia, 2020).

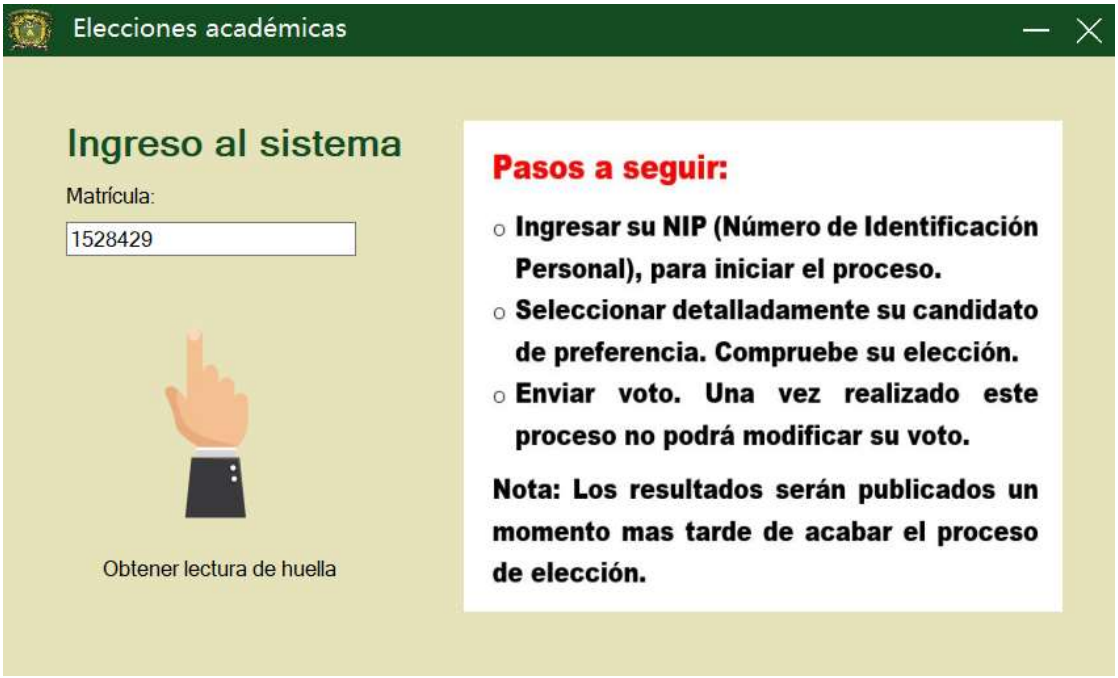

Figura 5.12 Llenado del formulario para ingresar al sistema. (Fuente: Propia, 2020).

Figura 5.13 Verificar credenciales. (Fuente: Propia, 2020).

Continuando con el proceso de la emisión del voto, el votante deberá ingresar en el formulario de datos del votante, mostrado en la Figura 5.14, el NIP que el mismo proporciono en la fase de registro, con el objetivo de descifrar la llave privada del votante. Si esta acción se lleva a cabo de manera óptima se mostrará un nuevo formulario donde se desplegará la boleta electoral.

Figura 5.14 Formulario de bienvenida, solicita NIP para descifrar la llave privada. Fuente (Propia: 2020).

En la Figura 5.15 se muestra el formulario contenedor de la boleta electoral, donde se puede observar el folio único asignado a la boleta electoral que no es conocido por otra entidad. En este formulario el usuario debe elegir la opción de su preferencia, en este caso como ejemplo el votante eligió al candidato Luis Camacho López, recordando que todos los ejemplos mostrados son datos ficticios solo sirven como ilustración del funcionamiento de cada uno de los módulos del sistema.

Una vez seleccionando su candidato preferente se desplegará un nuevo formulario de confirmación, el cual cuenta con dos opciones el de Regresar en el caso de que quieras cambiar al candidato elegido, y la opción continuar en el caso de que el usuario este seguro de su elección, como se observa en la Figura 5.16.

Figura 5.15 Formulario de boleta electoral. (Fuente: Propia, 2020).

Figura 5.16 Despliegue de aviso para confirmar el candidato elegido. (Fuente: Propia, 2020).

Finalmente, si el usuario confirmo su elección se mostrará un nuevo formulario con la opción de enviar voto al servidor urna, como se observa en la Figura 5.17.

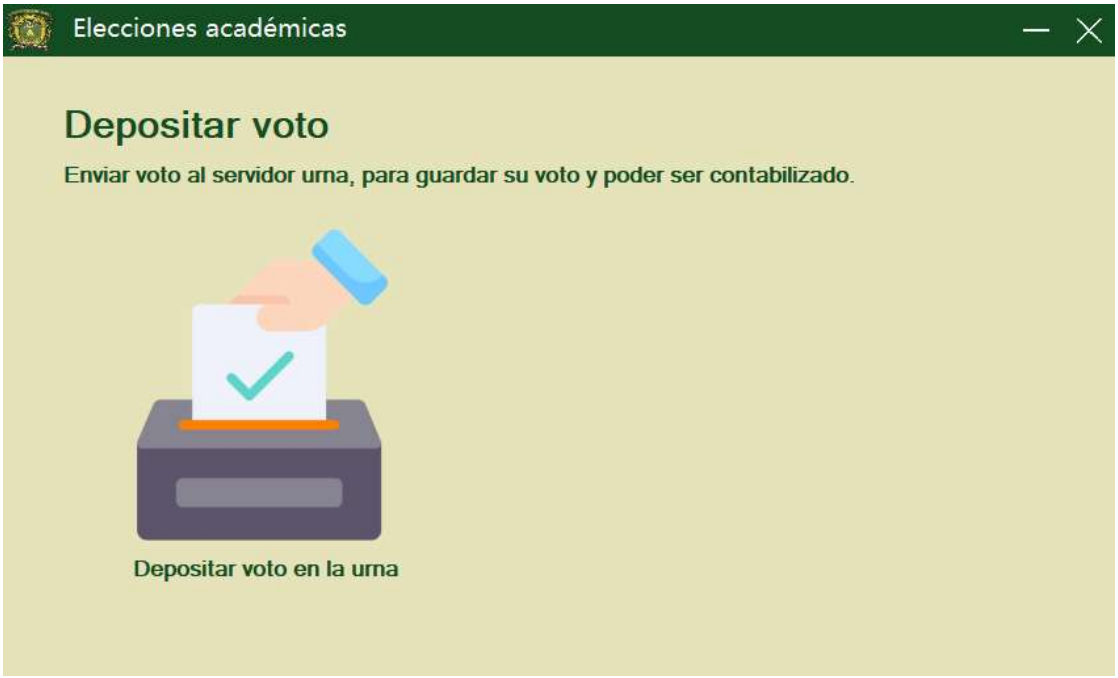

Figura 5.17 Formulario para enviar voto y que sea guardado por el servidor urna. (Fuente: Propia, 2020).

Finalmente, cuando se elige la opción de Depositar voto en la urna, esta opción cumple la tarea de solicitar firma sobre el voto por el servidor casilla, finalmente se envía el voto cifrado al servidor urna, el cual lo descifrará y verificará la firma emitida por la casilla, si el proceso se concluye con éxito se desplegará un aviso con la siguiente leyenda “Voto guardado en la urna”, como se aprecia en la Figura 5.18.

En el módulo de conteo se refleja el resultado final, en documento HTML con la finalidad que pueda ser consultado desde cualquier dispositivo conectado a la red local. En el documento se puede observar información detallada como el número de votos válidos obtenidos por el candidato y su correspondiente porcentaje, mostrado en la Figura 5.19.

Figura 5.18 Despliega de la respuesta del servidor casilla. (Fuente: Propia, 2020).

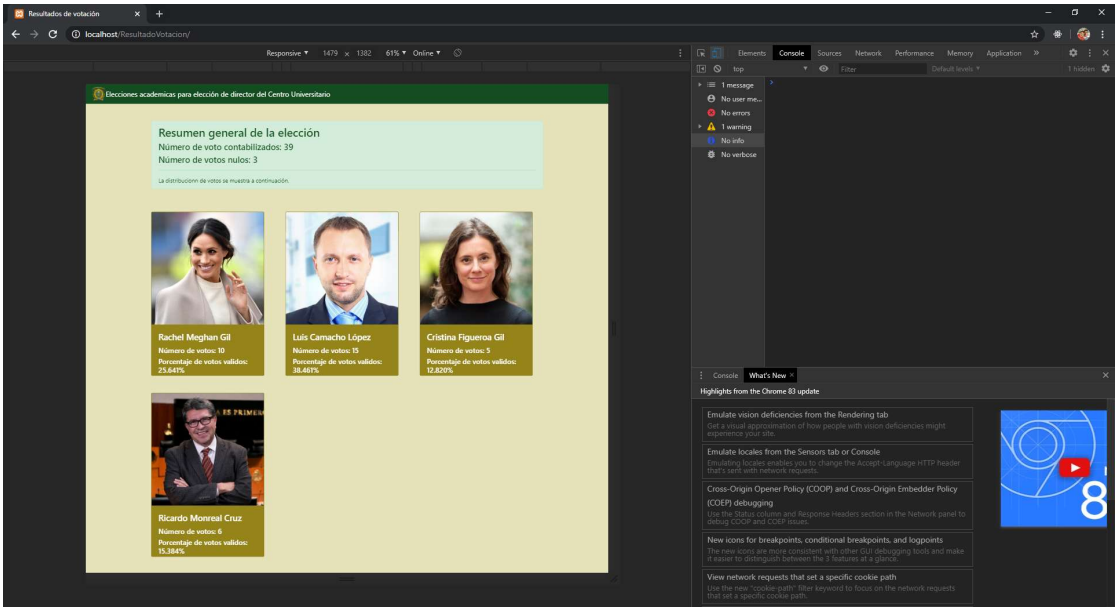

Figura 5.19 Visualización de la página de resultados. (Fuente: Propia, 2020).

5.2 Comprobación de funcionalidad

El siguiente punto de este capítulo, estipula las validaciones que se establecen en cada proceso del módulo pertinente, cada una de ellas es importante para gestionar la interacción del usuario y el sistema, a continuación, se describen cada una de ellas.

a) Generación de patrón biométrico erróneo

Cuando se está llevando a cabo el registro de un votante y se requiere generar el patrón biométrico y no se siguen las recomendaciones, o el sensor se encuentra leyendo las huellas de múltiples dedos, se despliega un aviso de error. El ejemplo demostrativo se puede apreciar en la Figura 5.20.

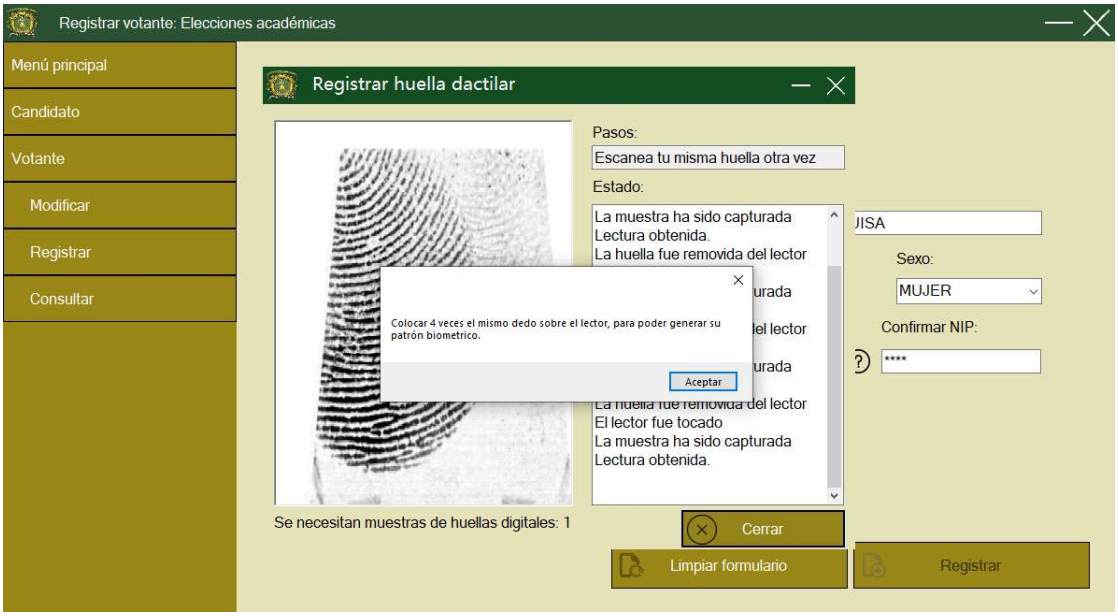

Figura 5.20 Mensaje de error al no poder generar correctamente el patrón biométrico. (Fuente: Propia, 2020).

b) Registro de votante con matrícula ya registrada

Se activa esta excepción, cuando se pretende registrar un votante con un matrícula o número de plaza previamente registrado en la base de datos, como

se observa en la Figura 5.21, donde se muestra el despliega el aviso sobre el error correspondiente.

Figura 5.21 Despliegue del aviso correspondiente a tratar de registrar un votante con la matrícula registrada con anterioridad. (Fuente: Propia, 2020).

c) Enviar el voto más de una vez de manera intencionada

Se cita cuando, el votante vuelve a ejercer su voto más de una vez, con el objetivo de que su candidato preferente obtenga una cantidad mayor de votos. La excepción se controla gracias a un parámetro del tipo booleano, este solo se modifica cuando se ejerce por primera vez el voto. En la Figura 5.22, se observa el despliegue consecuente de esta característica.

Figura 5.22 Despliegue del aviso que el voto ha sido emitido anteriormente. (Fuente: Propia, 2020).

d) Enviar el voto más de una vez de manera involuntaria

Esta excepción se cita, cuando por razones desconocidas o problemas técnicos se pierde la conexión con alguno de los servidores, que permiten la realización de la auscultación cuantitativa. Este problema no es reflejado en el resultado final.

Figura 5.23 Problema de conexión con el servidor casilla. (Fuente: Propia, 2020).

5.3 Funciones adicionales

En esta sección se mencionan algunas funcionalidades necesarias en el sistema propuesto.

a) Impresión de reporte de votantes

SEVS en su módulo de registro tiene la función de exportar reportes que la Comisión de Procesos Electorales puede utilizar para dar informes, la consulta del reporte puede ser filtrada para obtener datos más detallados. En la Figura 5.24 se observa la opción de exportar a pdf, la cual solicitará una ruta en donde se guardará el archivo resultante.

En la Figura 5.25 se observa, el archivo generado por la exportación de los votantes registrados, en la cual se pueden observar los campos: matrícula, nombre, apellidos, sexo, categoría, fecha de registro, fecha de actualización.

Figura 5.24 Formulario de consulta de votantes del módulo de registro. (Fuente: Propia, 2020).

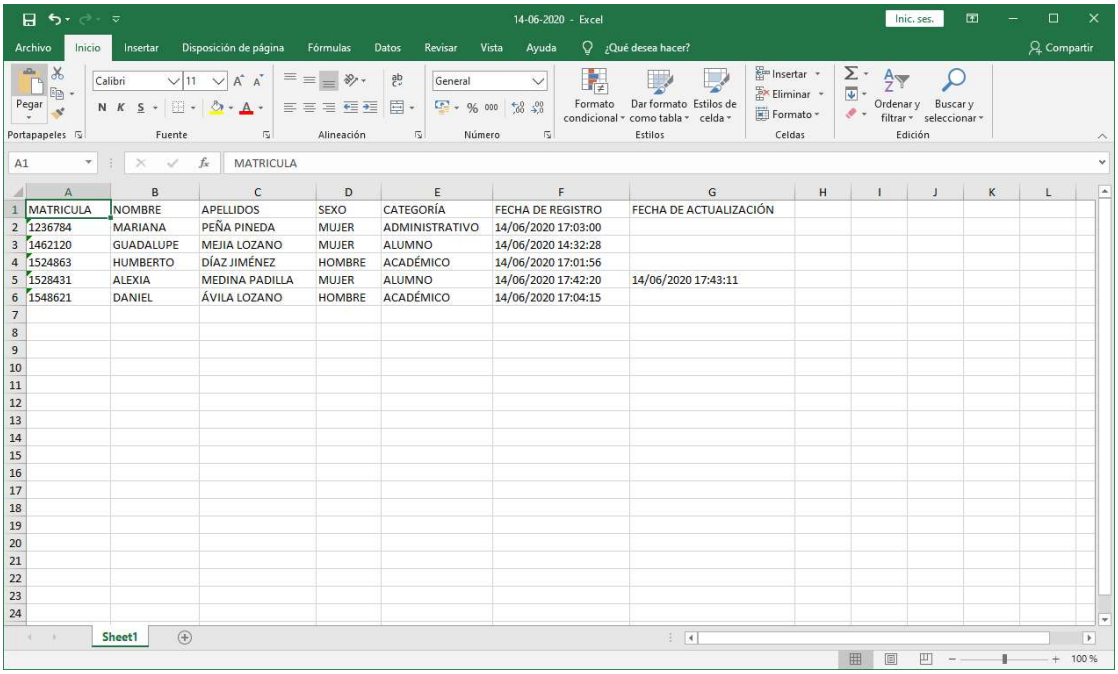

Figura 5.25 Archivo resultante de la exportación de la consulta de votantes registrados. (Fuente: Propia, 2020).

b) 5.3.2 Página de resultados adaptable responsivo

El contenido del módulo de conteo se adapta al tamaño de la pantalla del dispositivo que está consumiendo el recurso, de esta manera la información expuesta es de fácil digestión para usuarios con dispositivos, móviles o Smart tv.

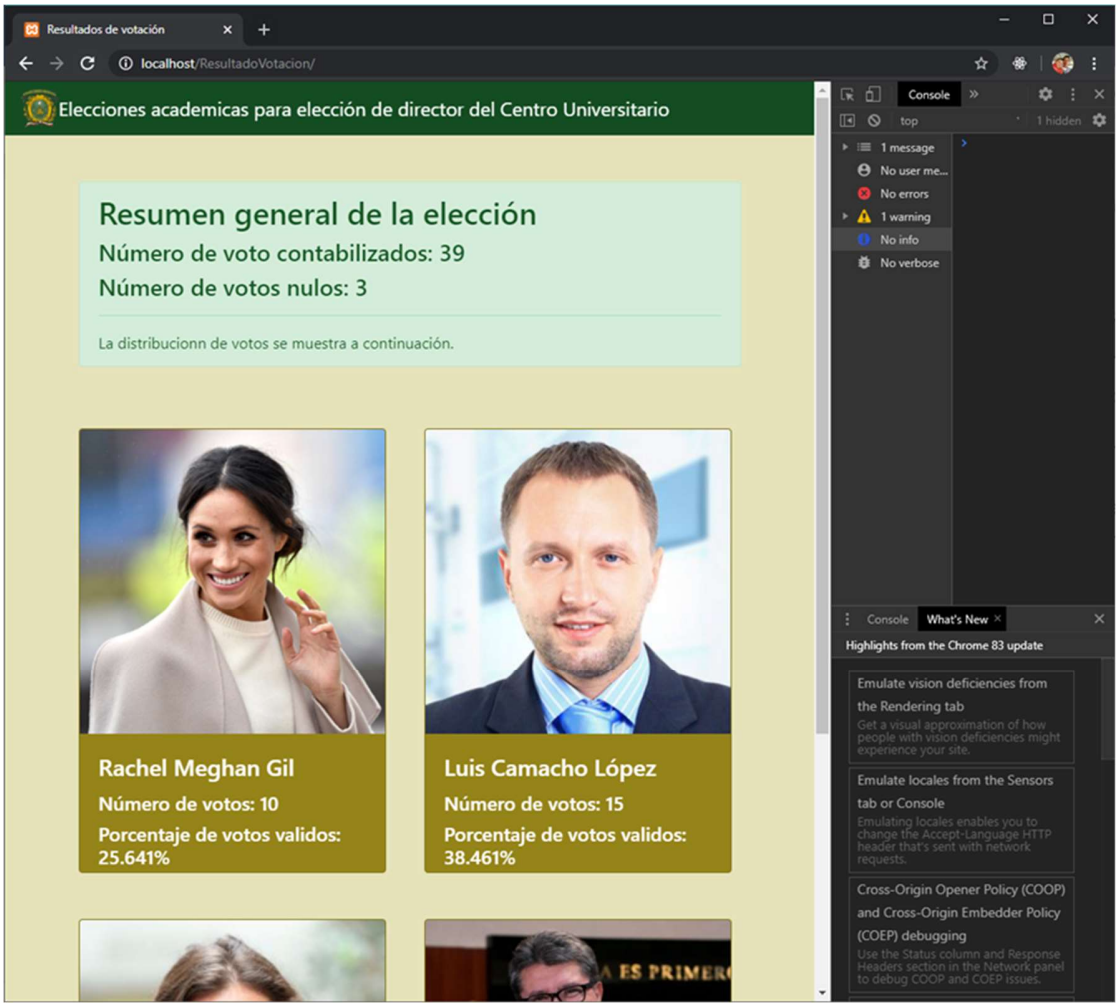

Figura 5.26 Pagina de resultados adaptable al tamaño de la pantalla del dispositivo. (Fuente: Propia, 2020).

c) Cambiar NIP del votante

Si por razones ajenas el votante necesita cambiar su NIP, el módulo de registro puede realizar esta acción solo debe seleccionar el apartado de Votante

encontrada en el menú principal, esta acción desplegará el menú desplegable con la opción de Modificar, esta acción tendrá como resultado la visualización del formulario de Modificar votante, como se observa en la Figura 5.27.

Figura 5.27 Formulario para modificar el registro de un votante. (Fuente: Propia, 2020).

Como se observó en la Figura 5.27 las opciones Cambiar NIP, Eliminar y Actualizar se encuentran inactivas, para poder activarlas se necesita realizar una búsqueda del votante son la matrícula con la que fue asociada en la fase de registro, si la búsqueda se fue encontrada en la base de datos estas opciones serán habilitadas como se observa en la Figura 5.28, donde se efectuó una búsqueda de un votante con la matricula “1462120”.

Una vez realizada la búsqueda seleccionar la opción de Cambiar NIP, la cual desplegara un formulario para poder realizar la autenticación biométrica, el cual se muestra en la Figura 5.29.

Figura 5.28 Realización de una búsqueda del votante utilizado como ejemplo. (Fuente: Propia, 2020).

Figura 5.29 Realización de autenticación biométrica para modificar el NIP asociado al votante. (Fuente: Propia, 2020).

Si la autenticación biométrica se realizó con éxito se visualizará el formulario para poder modificar el NIP, mostrado en la Figura 5.30 Este formulario cuenta con

dos campos en el cual se deberá ingresar el NIP nuevo, posteriormente se elegirá la opción Continuar para poder guardar los cambios.

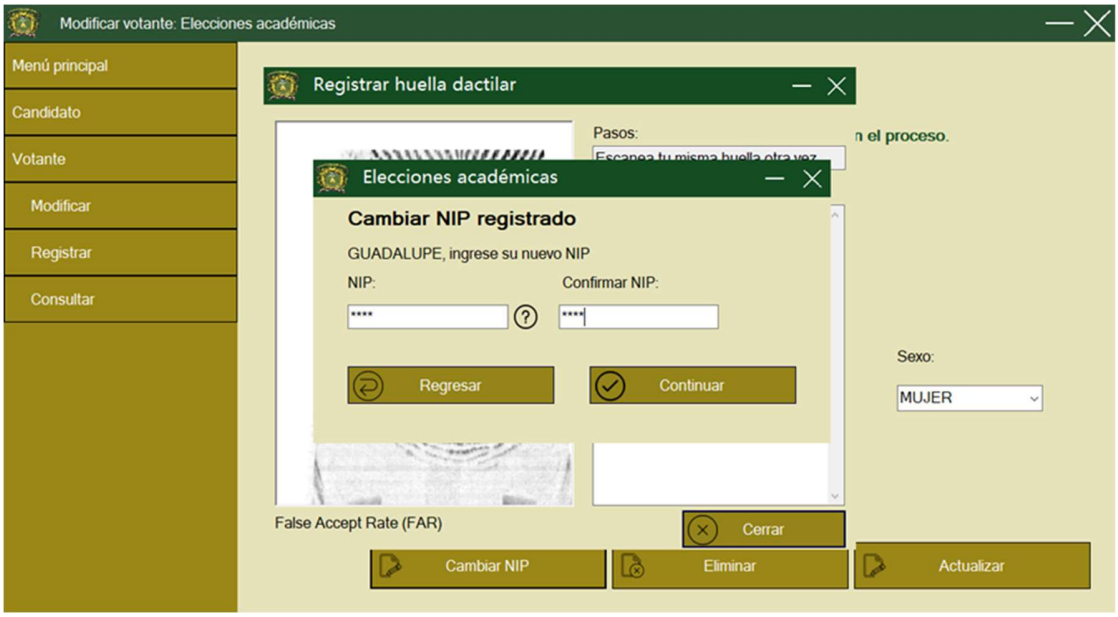

Figura 5.30 Visualización del formulario para poder modificar el NIP. (Fuente: Propia, 2020).

Cuando se selecciona la opción Continuar, se realiza el siguiente proceso, se generan nuevas llaves criptográficas asimétricas RSA, la llave privada es cifrada por el algoritmo AES, como clave de cifrado se toma el nuevo NIP.

Finalmente se sustituyen las llaves almacenadas en la base de datos asociadas con la clave del votante por las nuevas llaves generadas. Si este proceso se realiza correctamente se despliega un nuevo aviso con la leyenda “NIP actualizado satisfactoriamente”, como se observa en la Figura 5.31.

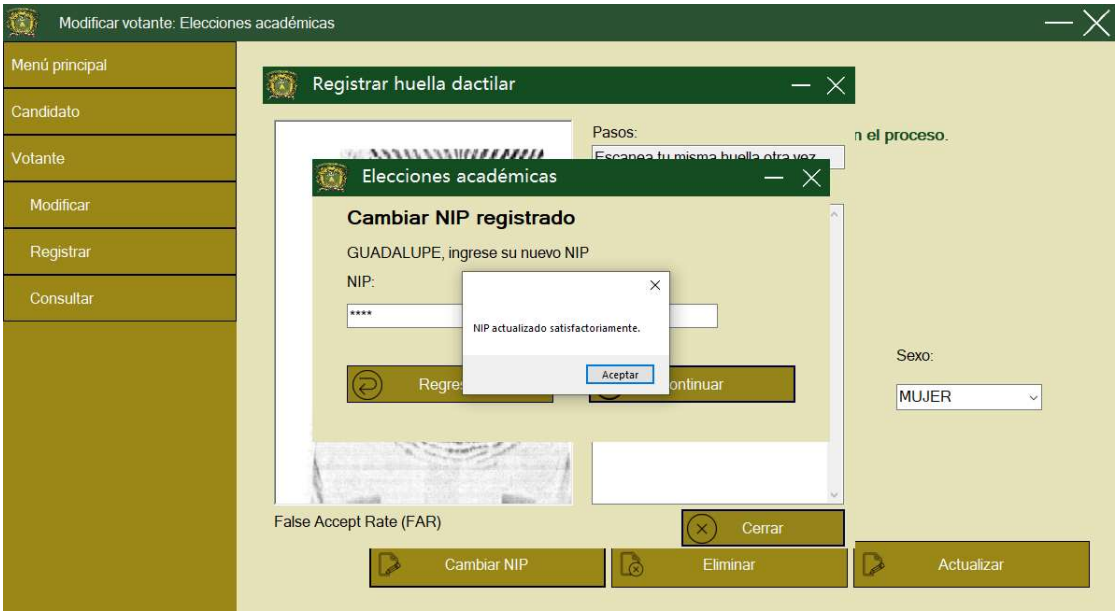

Figura 5.31 Modificación del NIP realizada con éxito. (Fuente: Propia, 2020).

5.4 Experimentación

Para el ejercicio de prueba mencionada anteriormente, se registraron 4 candidatos y 40 votantes, el numero total de votos obtenidos fueron 39, los cuales los 39 fueron válidos, no se presentó algún intento de votación invalida. Los votos se distribuyeron de la siguiente manera:

- Rachel Meghan Gil: 10 votos válidos con un porcentaje obtenido de: 25.64%
- Luis Camacho López: 15 votos válidos con un porcentaje obtenido de: 38.46%
- Cristina Figueroa Gil: 5 votos válidos con un porcentaje obtenido de: 12.82%
- Ricardo Monreal Cruz: 6 votos válidos con un porcentaje obtenido de: 15.38%
- Votos nulos presentados: 3

En el ejercicio de prueba el ganador fue Luis Camacho López con 5 votos más de ventaja sobre su competidor mas cercano Rachel Meghan Gil.

Finalizando el ejercicio de prueba se realizó una pequeña encuesta de 5 preguntas sobre la utilización de SEVS y sobre la confianza generada al participar en una votación electrónica. La cual los resultados se observan en las Figuras 5.32, 5.33 y 5.34.

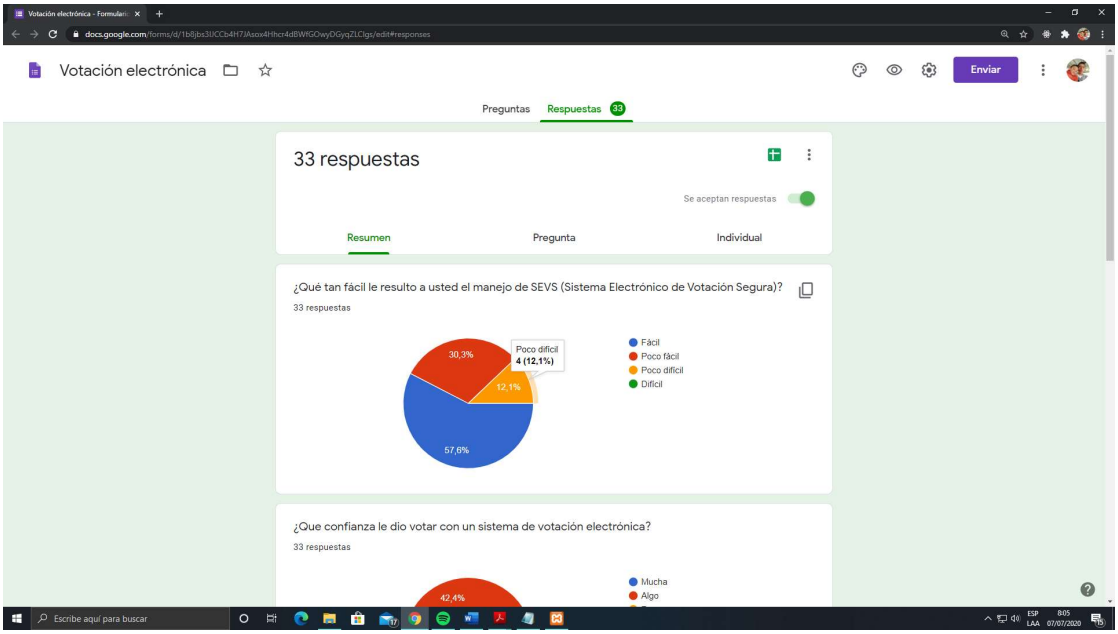

Figura 5.32 Encuesta de satisfacción sobre votación electrónica parte 1. (Fuente: Propia, 2020).

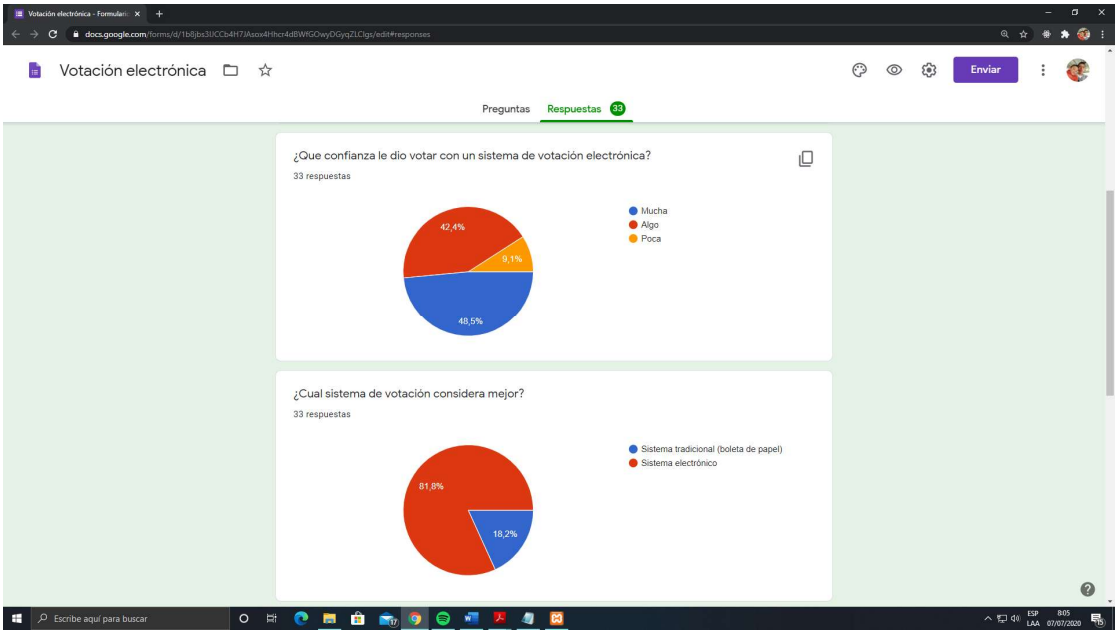

Figura 5.33 Encuesta de satisfacción sobre votación electrónica parte 2. (Fuente: Propia, 2020).

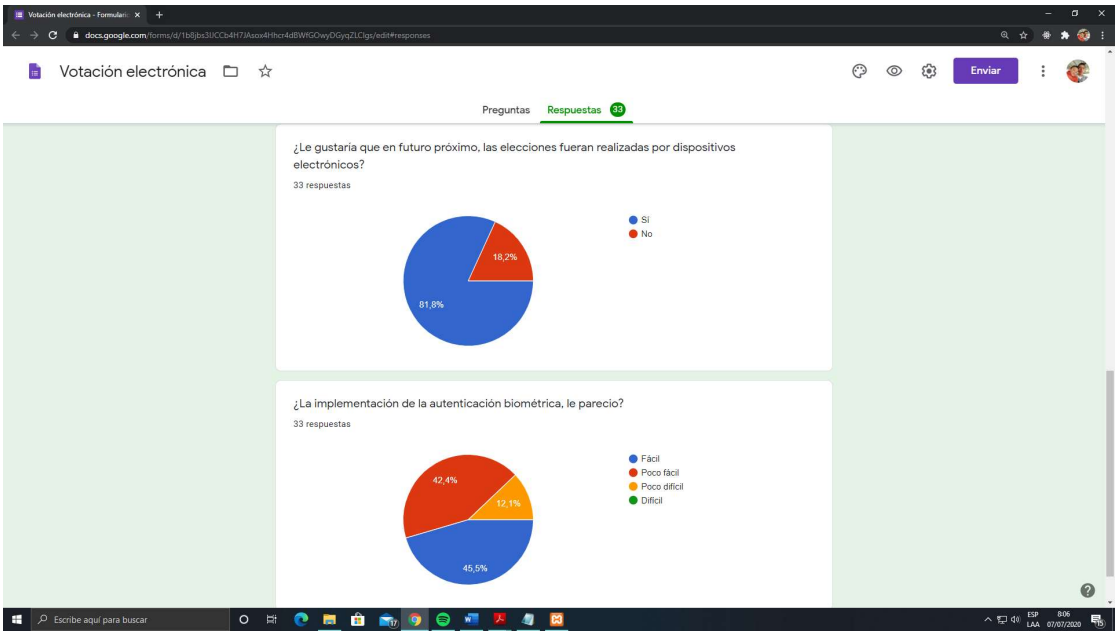

Figura 5.34 Encuesta de satisfacción sobre votación electrónica parte 3. (Fuente: Propia, 2020).

CAPÍTULO 6. CONCLUSIONES Y TRABAJO FUTURO

Esta tesis presenta el desarrollo del Sistema Electrónico de Votación Segura (SEVS), que permite a la Comunidad Universitaria ejercer su derecho de votación con la finalidad de elegir al director de un espacio académico de forma electrónica, por lo cual, en todo momento se procura salvaguardar la información y el anonimato del votante, con la finalidad que no sea vinculado con su correspondiente voto.

Para lograr su implementación, primero se realizó un análisis de los lineamientos que regulan el proceso de elección de Director de Organismo Académico, Centro Universitario UAEM y plantel de la Escuela Preparatoria de la Universidad Autónoma del Estado de México, los cuales se encuentran publicados en la “Gaceta Universitaria”, con un contenido de 36 artículos.

Como se mencionó, la finalidad del software propuesto es un sistema de votación electrónica, se investigaron los distintos protocolos que cumplen el propósito, tomando como base el protocolo de firma digital a ciega creado por David Chaum, que permite a una persona obtener un mensaje firmado por otra entidad, sin revelarle información contenida del mismo, el proceso de votación se realiza en tres fases: Autenticación, Votación y Conteo y es capaz de no permitir la acción que un votante ejerza su derecho electoral más de una vez, gracias al uso de la información biométrica del votante.

La metodología utilizada para el desarrollo de sistema fue el Proceso Unificado de Desarrollo de Software, construyendo con el Lenguaje Unificado de Modelado (UML) los modelos de Casos de Uso, Diagramas de Clase y Diagramas de Secuencia.

SEVS consta de tres módulos que cubren los servicios fundamentales de Registro, Votación y Conteo. Además, realizan peticiones con dos servidores ubicados dentro de la red local Casilla y Urna. El servidor Casilla realiza la tarea

de autenticar al votante, y firmar digitalmente el voto oculto emitido por el votante, otra tarea que cumple es llevar un registro correspondiente de acuerdo si el votante ejerció su derecho electoral. El servidor Urna recibirá el voto oculto firmado por el servidor casilla previamente cifrado y lo almacenará, terminado el tiempo electoral se descifrará y se realizará el conteo final.

Los protocolos de seguridad aplicados en SEVS son el protocolo de votación electrónica basado en firmas a ciegas RSA, más el uso de cifrado AES y la autenticación biométrica estática de huella dactilar.

6.1 Trabajo futuro

Trasladar el sistema hacia el sector móvil, actualmente la mayoría de las personas cuentan con un celular y su interacción con él, es amplia. Lo mencionado anteriormente ayudara al realizar el ejercicio electoral de manera sencilla y dinámica, utilizando un dispositivo que la mayoría de los votantes se trasladan con él, emitiendo su derecho electoral desde cualquier punto del globo terráqueo, teniendo en cuenta una conexión a internet.

Realizar la autenticación biométrica con ayuda del lector de huellas que algunos dispositivos móviles cuentan de esta manera se podría realizar el proceso de votación desde cualquier lugar, el problema del lector biométrico se soluciona. Finalmente se utilizarán conexiones seguras HTTPS, para que el voto viaje en un canal inseguro como lo es Internet.

REFERENCIAS

[1] Oficina del abogado general (2006). *Lineamientos que regulan el proceso de elección de Director de Organismo Académico, Centro Universitario UAEM y plantel de la Escuela Preparatoria de la Universidad Autónoma del Estado de México*, Consultado el 29 de marzo del 2020, de http://web.uaemex.mx/abogado/doc/0061%20LinDirectores.pdf

[2] I. Jacobson, G. Booch y Rumbaugh J. (2000). *El Proceso Unificado de Desarrollo de Software*, Addison Wesley.

[3] I. Jacobson, G. Booch y Rumbaugh J. (2000). *El Lenguaje Unificado de Modelado*, Addison Wesley.

[4] Ramió A. (2018). *Curso de Criptografía Aplicada*. Consultado el 30 de marzo del 2020, de http://www.criptored.upm.es/descarga/CursoCriptografiaAplicada2018.pdf

[5] IBM (2014). *Criptografía de clave pública*. Consultado el 30 de marzo del 2020, de https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm

[6] Rivest R.L., Shamir A. y Adleman L. (1978). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Recuperado de: https://people.csail.mit.edu/rivest/Rsapaper.pdf

[7] Roa J. (2013). *Seguridad informática*. McGraw-Hill Interamericana de España

[8] García C. (2005). *Diseño y Desarrollo de un Sistema para Elecciones Electrónicas Seguras (SELES) (tesis de maestría),* Unidad Zacatenco departamento de Ingeniería Eléctrica sección de Computación, México, D.F., Recuperado de: http://delta.cs.cinvestav.mx/~francisco/Repository/tesisCPGZ.pdf

[9] D. Chaum. *Blind Signatures for Untraceable Payments*. En Proc. CRYPTO ’82, 199–203, ISBN 978-1-4757-0602-4. Springer, 1983.

[10] Satizábal I. (2015), *Seguridad de los protocolos de voto electrónico a través de internet: una comparación*, Revista Colombiana de Tecnologías de Avanzada, 2(26), 61-67.

[11] Simón D. (2003). *Reconocimiento automático mediante patrones biométricos de huella dactilar* (Tesis doctoral). Universidad Politécnica de Madrid, Madrid, España.

[12] Cortés J., Medina A. y Escobar J. (2010) *Sistemas de seguridad basados en biometría*, Scientia Et Technica, 4(46), 98-102.

[13] Biometrics. (2020). *Identificación biométrica a través de las huellas dactilares*, Consultado el 15 de mayo de 2020, de https://biometrics-on.com/identificacion-biometrica-huellas-dactilares/#site-header

[14] Cabello A., Hernández A., Hoya S., Martín del Rey A., Rodríguez G., (24-28 de septiembre de 2007). *Un protocolo de votación electrónica basado en firmas digitales ciegas.* Congreso de Ecuaciones Diferenciales y Aplicaciones. Congreso llevado a cabo en la Universidad de Salamanca. Recuperado de: http://congreso.us.es/cedya2007/actas/textos/144.pdf

[15] Cabarcas D. (2015). *El voto electrónico y retos criptográficos relacionados*, Revista Facultad de Ciencias Universidad Nacional de Colombia, 4(2), 83-102.

[16] Villar J. (Sin fecha). *Protocolos criptográficos para sistemas de voto electrónico*, Consultado el 13 de abril de 2020, de https://web.mat.upc.edu/jorge.villar/esamcid/rep/evot/reportevotingse2.html

[17] INE. (Sin fecha). *Observadores Electorales*, Consultado el 13 de abril de 2020, de https://www.ine.mx/voto-y-elecciones/observadores-electorales/

[18] INE. (Sin fecha). *Información Básica Sistema Electoral Mexicano*, Consultado el 13 de abril de 2020, de https://portalanterior.ine.mx/archivos3/portal/historico/contenido/Informacion_Electoral/