RESUMEN

DESARROLLO DE UN SISTEMA PILOTO DE COMUNICACIÓN SEGURA PARA EL TRANSPORTE DE LOS DATOS EN VOTACIONES ENTRE LAS SEDES DE LA UCAB.

Martinez Monsalve, Eloy Alberto

eloym2@hotmail.com

Soto De Sousa, Marilyn Elena

marilyn.esds@gmail.com

Actualmente, el proceso de elección de representantes estudiantiles en las principales universidades del país es realizado a través del uso de papeletas físicas, las cuales son procesadas manualmente o con máquinas lectoras, lo que puede generar retardos a la hora del procesamiento en las votaciones y la posterior obtención de los resultados.

Con la finalidad de buscar una solución a la problemática anteriormente planteada, se presenta el diseño de un sistema de votaciones a través de una aplicación web. Se planteó el acceso a ésta, a través de un computador conectado a la misma red de un servidor web en el cual, se alojó la base de datos con la información necesaria para la realización de las votaciones, así como también de la totalización de resultados finales. Para la comunicación entre las sedes de la UCAB, se ofreció el diseño de un sistema seguro entre redes, el cual, permitió el acceso a dicha interfaz mediante una conexión VPN existente, a través del protocolo IPsec con alta seguridad.

Palabras Claves: sistema de votación, base de datos, servidor, VPN, IPsec.

DEDICATORIA

A mi madre, por ser mi gran apoyo en todo este camino, sin ella no podría llegar tan lejos.

A mi padre, por todo su apoyo, su educación y su enseñanza a lo largo de mis primeros años de vida.

A mis hermanos, por su apoyo y cariño, por ser mi fortaleza en los momentos que los necesitaba.

A mis amigas, Isabel, Roxana y Esthefani, por convertirse en parte de mi familia y compartir buenos y malos momentos en estos años de carrera.

Martinez Monsalve, Eloy Alberto.

A Dios, por darme toda la paciencia y fortaleza para lograr mis objetivos.

A mis padres, por haberme permitido alcanzar esta meta tan anhelada. ¡Todo esto es por ustedes!

A mis hermanos, por todo el apoyo y la compañía durante todo este tiempo. ¡Son los mejores!

Soto De Sousa, Marilyn Elena.

AGRADECIMIENTOS

A Dios, por ser mi guía en todo momento y brindarme la fortaleza en esos momentos en los que perdí el norte y la fe en lo que estaba haciendo.

A mis padres y hermanos, por todos estos años de apoyo y cariño incondicional, gracias por creer en mí, y siempre motivarme a que luchara por este sueño que se esta materializando con este Trabajo Especial de Grado.

A mi familia, por estar pendiente de mi progreso a lo largo de los años, por brindarme un hogar donde alcanzar este sueño, y siempre ayudarme con lo que estuvo a su alcance.

A mi compañera de tesis, por acompañarme a lo largo de esta difícil meta que nos puso la vida, por tener la fortaleza de seguir adelante cuando todo se nos volvía en contra, por poder ser una persona con la cual no solo compartía la carga académica, sino convertirse en una gran amiga a la que siempre tendré presente con el paso de los años. Admiro tu independencia y dedicación por las cosas que te apasionan, y sé que si te lo propones llegarás muy lejos. Nunca olvides que eres grande.

A Esthefani Machado, por ser un apoyo incondicional, siempre estar ahí cuando te necesitaba, y en la mayoría de los casos ponerte de mi lado hasta en cosas en la que no tenía razón.

A Isabel Marrero, por siempre motivarme y de una u otra forma, obligarme a dar cada día más y no rendirme a pesar de lo difíciles de las situaciones. Por tener esas palabras que a veces necesitas oír y que te impulsan a seguir adelante.

A Roxana Lara, por ser una gran amiga, por siempre saber que cuento con tu apoyo y sacarme de aprietos de vez en cuando. En conjunto con la señora Gricelida Carvajal y el resto de su familia, por brindarme un segundo hogar en los momentos

que más los necesitaba, gracias por todas las experiencias y sus consejos a lo largo de este camino.

A mis amigos, Luis Cordero, Luz Planchart y Luis Molner, por brindarme no solo su amistad, sino un especial apoyo en este TEG. A Erika Galaviz por su amistad y acompañarme a pesar de la distancia, en los últimos días de la tesis que son los más fuertes. A Alba Pinto, Daniela Soto, Andrea Fernandes, Yolmi Diaz, Josmar Salinas, Fiona Chirinos, por compartir todos estos años de camino. Y a todos los que estuvieron pendientes muchísimas gracias por el apoyo.

A nuestro tutor, José Pirrone, por siempre estar dispuesto a brindarnos sus conocimientos, además de transmitirnos la confianza y seguridad de que todo saldría bien.

A todas esas personas que sin tener nada que ver con este trabajo, nos brindaron su apoyo en los momentos que más los necesitamos, como lo son Jorge Garcia y el personal del DTI, Monica Nobrega y el personal del CIAP, los profesores de la carrera y personal de la escuela, que nos brindaron su apoyo durante todas las clases y un apoyo especial durante las pruebas.

Martinez Monsalve, Eloy Alberto.

AGRADECIMIENTOS

A Dios, por darme las fuerzas necesarias para dar lo mejor de mí en todo lo que me propongo y por no haberme rendido en esta etapa de vida que se culmina exitosamente.

A mis padres, las personas más importantes de mi vida. Gracias por darme la oportunidad y el aliento para estudiar esta carrera. Gracias papá, por todos los consejos y exigencias que me has puesto, sé que con esto he logrado ser una persona perseverante y siempre me he esforzado por alcanzar todas mis metas. Gracias mamá, por escucharme en todo momento y por estar pendiente de todo lo que me pasa, has sido el apoyo fundamental que he necesitado para lograr este objetivo.

A mis bellos hermanos. A Dani, por ser la mejor hermana del mundo, por estar ahí en todo momento, por darme toda la confianza y los mejores consejos. A Santi, por estar siempre pendiente de que terminara y por acompañarme en muchos de los trasnochos que me tocaron para poder realizar este proyecto.

A mis tías, por haber estado siempre presentes y preocuparse por mí, brindando todo el apoyo y la ayuda que necesitara.

A José Rocha, por ser mi guía en la realización de este proyecto y por poner todo el esmero para ayudarme en todo. Gracias por haberme dado fuerzas para culminar y ser el sustento que necesité para no rendirme durante los últimos meses.

A David Ruiz, quien me ayudó en todo lo que estuvo a su alcance, enseñándome muchas cosas y levantándome el ánimo cuando me veía nerviosa o desanimada. Gracias por todos los consejos especiales que me diste y por haber estado siempre pendiente.

A mi mejor amiga, Roser. Gracias por estar ahí en todo momento, por brindarme siempre tu apoyo incondicional en las buenas y en las malas.

A Oriana Valero. Gracias por haber compartido excelentes momentos desde los primeros días en la universidad y por haber estado tan pendiente. Aunque no estuvimos juntas hasta el final de la carrera, es una etapa que siempre recordaré contigo.

A mis amigos Esthefani Machado, Isabel Marrero, Bernardo Infante, Fiona Chirinos, Luis Cordero, Carlos Martins, Roxana Lara, Josmar Salinas, Carlos De Quintal y Henry Fernández por la grata compañía en este camino. Gracias por los buenos momentos que pasamos juntos. Nunca los olvidaré.

A mi compañero de tesis, Eloy. Gracias por todos los ratos que compartimos en clases, en la universidad, en salidas y en los trasnochos que nos tocaron para realizar este proyecto. Al final de todos los obstáculos que se nos presentaron, juntos logramos alcanzar esta grandiosa meta.

A José Pirrone, nuestro tutor, por todo su apoyo para la elaboración de este Trabajo Especial de Grado y por toda la paciencia que nos tuvo durante estos meses.

A Jorge García y Rafael Andara, personal del DTI, por habernos brindado toda la colaboración necesaria para la realización de las pruebas.

Soto De Sousa, Marilyn Elena.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ACRONIMOS

3DES	*Triple Data Encryption Standard*
ACL	*Access Control List*
AES	*Advanced Encryption Standard*
AH	*Authentication Header*
ASP	*Active Server Pages*
ATM	*Asynchronous Transfer Mode*
BSD	*Berkeley Software Distribution*
CEP	Colegio Electoral de Pares
CIAP	Centro de Investigación de Actualización Profesional
CNE	Centro Nacional Electoral
CRC	*Cyclic Redundancy Check*
CSP	*Cryptographic Service Provider*
CSR	*Certificate Signing Request*
DES	*Data Encryption Standard*
DH	*Diffie Hellman key Exchange*
DNS	*Domain Name System*
DTI	Dirección de Tecnología de la Información
ESP	*Encapsulating Security Payload*
FTP	*File Transfer Protocol*
HDLC	*High-level Data Link Control*
HMAC	*Hash-based message authentication code*
HTML	*Hyper Text Mark-up Language*
HTTPS	*Hyper Text Transfer Protocol*
IDEA	*International Data Encryption Algorithm*
IETF	*Internet Engineering Task Force*
IETF	*Internet Engineering Task Force*
IIS	*Internet Information Services*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPSEC	*Internet Protocol Security*
IPV4	*Internet Protocol version 4*
IPV6	*Internet Protocol version 6*
IPX	*Internetwork Packet Exchange*
ISAKMP	*Internet Security Association and Key Management Protocol*
L2F	*Layer 2 Forwarding*
L2TP	*Layer 2 Tunnelling Protocol*
LAN	*Local Area Network*

MD5	*Message Digest Algorithm 5*
MPLS	*Multiprotocol Label Switching*
NAT	*Network Address Translation*
NIC	*Network Interface Card*
NIP	Número de Identificación Personal
PDU	*Protocol Data Unit*
PHP	*Hypertext Pre-Processor*
PPP	*Point to Point Protocol*
PPTP	*Point to Point Tunneling Protocol*
PSK	*Pre-Shared Key*
RAM	*Random Access Machine*
RFC	*Request for Comments*
RSA	*Rivest, Shamir y Adleman*
SA	*Security Association*
SADB	*Security Association Database*
SDLC	*Synchronous Data Link Control*
SFTP	*SSH File Transfer Protocol*
SHA	*Secure Hash Algorithm*
SNA	*Systems Network Architecture*
SPI	*Security Parameters Index*
SQL	*Structured Query Language*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TCP	*Transmission Control Protocol*
TTL	*Time to Live*
UCAB	Universidad Católica Andrés Bello
UCV	Universidad Central de Venezuela
UNAM	Universidad Nacional Abierta de México
UNIMET	Universidad Metropolitana
USB	Universidad Simón Bolívar
VB	*Visual Basic*
WAN	*Wide Area Network*

INTRODUCCIÓN

La necesidad de comunicarse es fundamental en la vida de los seres humanos, con el objetivo de intercambiar informaciones entre sí. Con el pasar de los años, el uso de la tecnología se ha vuelto indispensable en el desarrollo de la vida diaria, lo cual ha traído como consecuencia una comunicación cada vez más impersonal.

Actualmente, es más rápido y sencillo comunicarse con otras personas así se encuentren en lugares remotos, gracias a Internet, a través de la existencia de muchas aplicaciones que nos permiten establecer comunicaciones con otras personas. No se debe olvidar que éstas están soportadas por una red pública, por lo cual, sí se intercambian informaciones privadas, algunas personas con los recursos suficientes podrían interceptar la información.

Debido a esto, surge la necesidad de crear sistemas de comunicaciones seguros entre origen y destino, para evitar posibles intrusiones en los sistemas, con el objetivo de proteger la integridad de los datos y el mensaje.

En la Universidad Católica Andrés Bello, al momento de elegir los representantes estudiantiles, se realizan elecciones anuales en las 4 sedes: Caracas, Coro, Los Teques y Guayana. Este proceso de elecciones es realizado mediante el uso de papeletas procesadas en máquinas lectoras, lo cual genera retrasos a la hora de obtener los resultados y un gasto de papel y energía considerable.

Es cada vez más común, encontrar desarrollos que permiten automatizar los procesos de elecciones, logrando reducción de tiempo al momento de la votación y obtención de resultados. Aplicar dichas experiencias al sistema de elecciones de representantes estudiantiles realizado en la UCAB, sería sumamente favorable, ya que además de los beneficios anteriormente descritos, la convertiría en una Universidad pionera en cuanto a los sistemas de votaciones se refiere.

Este Trabajo Especial de Grado propone diseñar un sistema piloto de comunicación segura, para el transporte de datos entre las distintas sedes de la UCAB, que solucione la problemática actual del sistema de votaciones, con un diseño que ofrezca confiabilidad y seguridad frente a las vulnerabilidades que pueda tener el canal de trasmisión.

A continuación, se ofrece una estructura de seis capítulos los cuales definen el proceso de elaboración y ejecución del proyecto. En el primer capítulo se describe de manera breve el problema propuesto y los objetivos planteados, demarcando los alcances e indicando las limitaciones que dan justificación al mismo.

El segundo capítulo esta compuesto por el basamento teórico que da soporte al desarrollo del sistema, planteado de forma metodológica en el tercer capítulo, en el cual se exponen detalladamente cada uno de los pasos que llevaron a obtener el producto final de este Trabajo Especial de Grado.

Los pasos anteriormente desarrollados generarán resultados plasmados en el cuarto capítulo, que conllevan a la realización de conclusiones y recomendaciones a trabajos posteriores sobre el tema, los cuales están expuestos en el último capítulo.

CAPÍTULO I

PLANTEAMIENTO DEL PROYECTO

En este capítulo se presenta de forma general una descripción del proyecto, destacando el planteamiento del problema, la justificación, los objetivos, los alcances y las limitaciones que engloban los aspectos tomados en cuenta para la realización de este Trabajo Especial de Grado.

I.1 Planteamiento del Problema

En la Universidad Católica Andrés Bello, se realiza un proceso anual de votaciones manuales en las cuatro sedes, para la elección de los representantes estudiantiles. Dichas votaciones son realizadas a través de papeletas, en las que se seleccionan los candidatos según la preferencia de cada elector, la cuales son introducidas en urnas electorales para su posterior procesamiento. En la actualidad, la Dirección de Tecnologías de Información cuenta con una sola máquina para realizar el procesamiento de las papeletas, lo que genera retrasos al momento de la totalización de resultados.

Es necesario vincular este tipo de procesos con los avances tecnológicos, en donde la digitalización es fundamental para agilizar y brindar mayor seguridad a los participantes. De esta manera, se contribuye a la reducción el gasto de papel y energía que conlleva el sistema actual de votaciones.

Este Trabajo Especial de Grado propone el desarrollo de un sistema piloto de comunicación segura, para la transmisión de datos en votaciones entre las distintas sedes de la UCAB, mediante la creación de una aplicación web y el diseño de los mecanismos necesarios que garanticen la integridad de la información que ésta genera.

I.2. Objetivos

I.2.1 Objetivo General

Desarrollar un sistema piloto de comunicación segura para el transporte de datos en votaciones entre las distintas sedes de la UCAB.

I.2.2 Objetivos Específicos

- Verificar los sistemas de votaciones desarrollados en la UCAB y otras universidades del país.
- Desarrollar un sistema de votaciones para la elección de los representantes estudiantiles en la UCAB.
- Diseñar un modelo de sistema de comunicaciones para las votaciones entre las distintas sedes de la UCAB.
- Realizar una prueba piloto del sistema de votaciones diseñado.
- Evaluar la seguridad del sistema piloto diseñado.
- Generar un instructivo de instalación del sistema.

I.3 Limitaciones y Alcances

I.3.1 Alcances

En éste Trabajo Especial de Grado se desarrolla un sistema piloto de comunicación segura para el transporte de datos de las votaciones realizadas entre diferentes sedes de la UCAB.

El tipo de comunicación segura que se plantea entre las sedes de la UCAB, para la transmisión de dichos datos, está determinada en la fase de investigación del proyecto.

La seguridad del sistema de votaciones, se comprobó mediante una serie de pruebas que se aplicaron al mismo, las cuales evaluaron la vulnerabilidad del proceso frente a las eventualidades que pudieron presentarse.

I.3.2. Limitaciones

- El sistema de votaciones creado para la elección de representantes estudiantiles, está diseñado para ser accedido desde computadoras conectadas a la misma red en la cual esté conectado el servidor.
- Las pruebas aplicadas al sistema de comunicaciones planteado, se limitó al alcance brindado por el personal de redes del DTI de la UCAB.
- La aplicación de prueba se realizó entre dos sedes de la UCAB, con un grupo de control que fue determinado y delimitado a lo largo del desarrollo de dicho sistema.
- El sistema de votaciones desarrollado, fue probado entre dos sedes de la UCAB que contaran con una conexión entre ellas, similar a la diseñada en este Trabajo Especial de Grado.
- El grupo de control que participó en la prueba realizada al sistema propuesto, estuvo conformada por un conjunto de estudiantes, profesores y personal de trabajo de las sedes que se escogieron para la verificar el funcionamiento de este proyecto.
- El servidor que se instaló contiene la base de datos con la información necesaria para la simulación del sistema y la posterior totalización de los resultados obtenidos en las votaciones.

I.4 Justificación

El avance de la tecnología ha provocado la modernización de algunos de los sistemas de votaciones en el mundo, hasta conseguir que el procesamiento de los votos y la transmisión de los mismos se realicen de forma automatizada.

Este Trabajo Especial de Grado busca optimizar el proceso actual de votaciones para la elección de los representantes estudiantiles, que se lleva a cabo en las sedes de la UCAB, ofreciendo la posibilidad de emitir el voto a través de una aplicación web, mediante un proceso rápido, seguro y confiable.

Con el desarrollo de este sistema, se plantea garantizar la integridad y seguridad de la información que se transmita en las votaciones entre una sede y otra, donde al cifrar dichos datos, se asegure la transparencia propia de los resultados finales que se obtengan en las votaciones.

CAPÍTULO II

MARCO TEORICO

Una vez planteado el proyecto a desarrollar, definidos los objetivos generales y específicos en los que se basa esta investigación, teniendo en cuenta los alcances y limitaciones de la misma, es necesario plantear los antecedentes a este proyecto, así como los sustentos teóricos e informaciones afines.

II.1. Sistema Electoral en Venezuela.

En Venezuela, el sistema de gobierno practicado es la democracia, en la cual, el poder es ejercido por todo el pueblo, o una mayoría, esta mayoría elige las personas que van a representar al colectivo mediante votaciones, dependiendo de la forma en que se realicen las mismas, definiremos la democracia como directa, indirecta o participativa, es directa cuando la elección es realizada por los miembros del pueblo, indirecta cuando la elección es realizada por personas reconocidas por el pueblo en su representación, y participativa cuando para la elección se aplica un modelo político que permite a las personas agruparse en partidos políticos u organizaciones con una serie de bases establecidas en los cuales se postulan candidatos que representen las ideologías de sus partidos y logren captar la atención de los votantes.

Todo lo concerniente al sistema electoral está a cargo del Consejo Nacional Electoral (CNE), existiendo un sistema automatizado y auditable en todas sus fases, la proveedora de esta tecnología es una empresa nacional llamada SMARTMATIC, la cual cuenta con maquinas de votación del modelo SMARTMATIC AUTOMATED ELECTION SYSTEM (SAES). El voto se realiza en dos modalidades: en la pantalla táctil, con la que viene equipada la máquina de votación o respaldándose por tarjetones electorales táctiles, todas estas al final deben recurrir a la pantalla táctil de la máquina para oprimir la opción votar y retirar un comprobante impreso para la

verificación del voto, este comprobante es depositado en una urna de resguardo para luego en caso de ser seleccionada dicha mesa, ser auditada.

Dicho voto emitido permanecerá guardado en la memoria de la máquina de forma aleatoria hasta que termine el proceso electoral, en este momento se procede a la totalización y transmisión de los datos de manera segura. Dicha transmisión consta de un paquete de votos que es enviado encriptado con una clave alfanumérica, que a su vez es encriptado con un hash o firma electrónica, esta clave está compartida por el CNE, organizaciones con fines políticos y la empresa SMARTMATIC, y se realiza por la red de la empresa de comunicaciones estatal CANTV. Esta es una red habilitada para el proceso de votación, distinta de Internet y con distintos niveles de seguridad, la información recibida es guardada en servidores. (CNE Consejo Nacional Electoral)

II.2. Elecciones Digitales en Universidades de Venezuela.

En nuestro país, actualmente no se cuenta con universidades que desarrollen sistemas que digitalicen la elección de los representantes estudiantiles. Universidades altamente reconocidas como la UCV (Universidad Central de Venezuela), la USB (Universidad Simón Bolívar) y la UNIMET (Universidad Metropolitana), realizan estas elecciones mediante papeletas y luego contabilizan los votos a través de máquinas destinadas para esto, o de manera manual.

II.2.1. Sistema actual de elecciones UCAB.

Al momento de elegir a los representantes estudiantiles se realiza una votación en las cuatro (4) sedes: Caracas, Coro, Los Teques y Guayana, se eligen los representantes estudiantiles de manera directa de los decanatos, facultades, escuelas, y los centros de estudiantes.

Actualmente este proceso se realiza utilizando una planilla, que es rellenada por cada estudiante, luego es introducida en una urna electoral para posteriormente ser procesadas por el DTI para la obtención y totalización de los resultados.

II.2.1.1. Reglamento del Sistema Actual de elecciones UCAB:

Para realizarse unas elecciones en la Universidad Católica Andrés Bello, la comisión electoral debe convocar a elecciones de los representantes estudiantiles ante el Consejo Universitario, Consejo General del Decanato de Desarrollo Estudiantil y los Consejos de Facultad y Escuela, para el siguiente año lectivo.

En ese momento se establece el programa de actividades que contiene los periodos indicados para:

- Postulaciones: se realizarán ante la comisión electoral de cada escuela. En las últimas elecciones realizadas, periodo lectivo 2011-2012, hubo 2 semanas para postularse, en un horario comprendido entre las 8:00 am y las 7:00 pm.
- Votaciones: Se realizarán en un lugar asignado por cada subcomisión electoral de Escuela, y dicho lugar será notificado previamente en la cartelera respectiva. En las últimas elecciones realizadas, periodo lectivo 2011-2012, hubo 1 día para votar, en un horario comprendido entre las 8:00 am y las 7:00 pm. (Comision Electoral Universidad Católica Andres Bello, 2011)

La Comisión Electoral también hará del conocimiento de la comunidad Ucabista las disposiciones acerca del proceso electoral, contempladas en los Reglamentos sobre Constitución de Consejos referentes a las elecciones de representantes estudiantiles ante los diferentes consejos de la universidad:

II.2.1.1.1 De la comisión Electoral Central

En esta se expresan las competencias de la Comisión electoral, entre ellas encontramos:

1. Adoptar medidas para impedir la interrupción del proceso de votación, así como también la propaganda durante el acto de votación.
2. Solicitar amonestar a quienes interfieran con las actividades docentes, de investigación o administrativas durante el proceso electoral. Así mismo, a las personas que vulneren las disposiciones que dicta la comisión electoral, tales como: la colocación de propaganda en las instalaciones universitarias.
3. Solicitar la suspensión o expulsión de las personas que incurrieren en conducta violenta que pudiere crear un peligro contra las personas o la infraestructura universitaria, o afecten el correcto funcionamiento del proceso de votación.
4. En caso de ser necesario suspender el proceso de votación si se presentan circunstancias que perjudiquen gravemente el desarrollo del proceso. (Comisión Electoral Universidad Catolica Andres Bello, 2011)

II.2.1.1.2 Del objetivo de las elecciones

En esta se expresan los cargos de representación estudiantil a elegir. Para el periodo lectivo 2011-2012 fueron los siguientes:

- Tres (3) representantes principales y tres (3) suplentes para el Consejo Universitario.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo General del Decanato de Desarrollo Estudiantil.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Facultad de Ciencias Económicas y Sociales.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Facultad de Derecho.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Facultad de Humanidades y Educación.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Facultad de Ingeniería.

- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Administración y Contaduría.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Administración y Contaduría de la extensión Guayana.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Ciencias Sociales.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Economía.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Comunicación Social.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Comunicación Social de la extensión Guayana.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Educación.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Educación de la extensión Coro.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Educación de la extensión Guayana.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Derecho de la extensión Guayana.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Filosofía.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Derecho de la extensión Guayana.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Letras.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Psicología.

- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Ingeniería Civil.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Ingeniería Civil de la extensión Guayana.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Ingeniería Industrial.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Ingeniería Industrial de la extensión Guayana.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela Ingeniería Informática.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Ingeniería Informática de la extensión Guayana.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Ingeniería de Telecomunicaciones.
- Dos (2) representantes principales y dos (2) suplentes para el Consejo de la Escuela de Ciencias Sociales de la extensión Guayana.

II.2.1.1.3 De los Electores.

Son electores todos los alumnos regulares de la Universidad siempre y cuando estén inscritos, en consecuencia, no podrán participar en el proceso electoral ningún alumno extraordinario u oyente.

II.2.1.1.4 Quienes son elegibles.

En esta se expresan las consideraciones a tener en cuenta para optar a los cargos mencionados a continuación:

1. Para el Consejo Universitario:
    a. Estar inscrito al menos en el tercer año.

b. No ser repitiente en régimen anual, ni tener aplazada en régimen semestral más de una materia en el periodo académico anterior a la elección.
c. Cursar estudios ininterrumpidamente en la universidad, durante los dos (2) últimos años académicos anteriores al del ejercicio de su representación.
d. No tener ninguna sanción disciplinaria en su expediente.

2. Para el consejo de Decanato de Desarrollo Estudiantil:
    a. Estar inscrito al menos en el tercer año, de una escuela de la facultad.
    b. Cursar estudios en la Universidad el año académico anterior a su elección.
    c. No ser repitiente en régimen anual, ni tener aplazada en régimen semestral más de una materia en el periodo académico anterior a la elección.
    d. No tener ninguna sanción disciplinaria en su expediente.
    e. Las condiciones a, b y c se deben cumplir durante el ejercicio de su representación.
3. Para el consejo de Facultad y Escuela:
    a. Estar inscrito al menos en el tercer año, de una escuela de la facultad.
    b. Cursar estudios en la Universidad el año académico anterior a su elección.
    c. No ser repitiente en régimen anual, ni tener aplazada en régimen semestral más de una materia en el periodo académico anterior a la elección.
    d. No tener ninguna sanción disciplinaria en su expediente.
    e. Las condiciones a, b y c se deben cumplir durante el ejercicio de su representación. (Comisión Electoral Universidad Catolica Andres Bello, 2011)

II.2.1.1.5 De las postulaciones.

En esta sección se expresa el lapso de postulaciones, y la forma en la cual cada uno de los representantes estudiantiles se debe postular. Cada candidato deberá postularse mediante una planilla dispuesta por la comisión electoral, en la cual, indicaran sus datos en original y copia, entregándole la segunda al candidato como comprobante de su inscripción. Este proceso se llevará a cabo en la comisión electoral de su escuela, en caso de pertenecer a más de una escuela y aspirar a Consejos de Facultad, Decanato de Desarrollo Estudiantil o Universitario, el estudiante debe postularse en solo una escuela. La lista definitiva se dará a conocer en días posteriores al cierre de las postulaciones.

II.2.1.1.6 De la propaganda electoral.

Se fija un lapso de propaganda, el cual, en el último periodo lectivo 2011-2012, fue desde el lunes 23 de mayo a las 6:00 am hasta el miércoles 25 de mayo a las 10:00 pm. Quedará prohibido utilizar colores, gráficos o slogan que hayan sido utilizados anteriormente al lapso establecido de propaganda. La propaganda escrita solo podrá ser colocada en los sitios permitidos en la normativa vigente sobre publicidad no oficial.

II.2.1.1.7 De las sub comisiones electorales de la escuela.

Esta sub comisión estará conformada por lo mínimo por un Director, que asumirá el rol del presidente de la sub comisión de la escuela, un profesor y un estudiante de la escuela en cuestión, y en caso de ser posible, por un profesor de otra escuela de la universidad. Dicha sub comisión tendrá como funciones:

1. Revisar el cumplimiento de las condiciones por cada uno de los postulados.
2. Establecer un número adecuado de mesas electorales para el correcto desarrollo del proceso electoral, y designar a miembros principales y suplentes.

3. Informar a los estudiantes acerca de la integración de la mesa, horarios y el lugar de la votación.
4. Garantizar el correcto desarrollo del proceso, haciendo énfasis en la espera de los electores.
5. Acompañar a la comisión electoral central en el proceso de escrutinio luego de terminar el proceso de votación.

II.2.1.1.8 Del procedimiento de Votación.

El proceso de votación se desarrollará de la siguiente manera:

1. Se instalarán las mesas con el material de votación dispuestas por la Sub comisión electoral de la escuela, a la hora y en el lugar designado. Tomando en cuenta que la urna no podrá ser desplazada durante el lapso de las votaciones.
2. Para iniciar el proceso de votación, se mostrará la urna totalmente vacía, para posteriormente cerrarla, sellarla y ser firmada por los miembros de las mesas y testigos.
3. Cada elector deberá mostrar su cedula de identidad, o el carnet de la universidad correspondiente al año lectivo en curso para poder ejercer su voto.
4. Será responsabilidad de los miembros de la mesa verificar si el nombre del votante se encuentra en la lista de votantes. De estar en la lista, se le entregará la papeleta de votación sellada y con el código de la escuela del votante. El votante llenara sus opciones de preferencia en privado.
5. Cada elector tendrá derecho a votar por un máximo de:
    a. Tres (3) candidatos para la elección de los Representantes al Consejo Universitario.
    b. Dos (2) candidatos para la elección de los Representantes al Consejo de Decanato de Desarrollo Estudiantil.
    c. Dos (2) candidatos para la elección de los Representantes al Consejo de Facultad.

d. Dos (2) candidatos para la elección de los Representantes a los consejos de escuela.

6. Luego del elector escoger sus candidatos, depositará la papeleta en la urna electoral y firmará la lista de electores, siendo devuelto su documento de identificación.
7. Al finalizar el acto de votación, los miembros de la mesa realizan el "acta de votación", en la cual se dejará constancia del número de votantes que han asistido al proceso, y de todas las circunstancias especiales que ocurran, tales como irregularidades.
8. A la sub comisión electoral de escuela respectiva se le hará entrega de la urna, el acta de votación, la lista de electorales y el material sobrante.
9. Las votaciones finalizarán a las 7:30 pm, siempre y cuando no haya electores en la cola esperando para votar. En caso de necesitar agilizar el proceso, se permitirá el ingreso de hasta ocho (8) alumnos.

II.2.1.1.9 Del escrutinio

Al cerrar el proceso de votación, las sub Comisión Electoral de cada escuela envía a la Comisión Electoral Central las urnas con las actas de votación para comenzar el escrutinio. El proceso se realizará de la siguiente manera:

El proceso de escrutar los votos se llevará a cabo introduciendo las papeletas en la lectora óptica, para llevar a cabo esto, deben estar presentes la Comisión Electoral Central y las sub Comisiones de la escuela. Al tener procesados todos los votos de todas las escuelas, se procede a dar el informe de todos los resultados, para luego, realizar las actas de escrutinio. En el caso de las sedes de Los Teques, Guayana y Coro, el conteo de los votos se realizará de manera manual y al obtener los resultados se realizará el llenado de las actas de escrutinio para luego enviarlas a la Comisión Central.

1. En el caso de observar alguna irregularidad, de considerarlo necesario por la Comisión Electoral Central, se colocará en el acta de escrutinio, y se procederá al conteo manual de los votos válidamente emitidos. Ocurrido esto, se procederá a levantar otra acta de escrutinio con los nuevos resultados.
2. Se considerarán como votos nulos, los que cumplan con las siguientes características:
    a. Papeletas sin sellar.
    b. Los votos en los que se señalen más de tres (3) candidatos al Consejo Universitario, y más de dos (2) Candidatos a Consejos de Decanato Estudiantil, de Facultad y de Escuela.
    c. Los votos que contengan marcas o escritos que no tengan que ver con la votación.
    d. Los votos en los que no pueda determinarse la voluntad del votante.
    e. Se consideran como votos en blanco el que no tenga mención alguna que determine la voluntad del votante.
    f. La anulación parcial de un voto para cualquiera de los Consejos, no implica que se anule en su totalidad el voto.
3. Una vez terminado el proceso de escrutinios, la Comisión Electoral Central es la encargada de hacer públicos los resultados obtenidos.

II.2.1.1.10 De la Proclamación.

Se considerarán electos para cada uno de los cargos los candidatos que cumplan con lo siguiente:

1. Para representante Principales ante el Consejo Universitario, los tres (3) candidatos que obtengan el mayor número de votos, siendo sus suplentes los que ocupen el cuarto (4to), quinto (5to) y sexto (6to) lugar respectivamente. Para dicha proclamación se debe tomar en cuenta que el reglamente sobre Constitución de Consejos dispone que los representantes principales ante el Consejo Universitario deben pertenecer a distintas facultades, por lo cual, en

caso de que resulten ganadores candidatos de la misma facultad, serán representantes principales aquellos estudiantes con mayoría de votos de otras facultades. Aplicando para los suplentes la misma norma.

2. Para representantes Principales ante el Consejo General de Desarrollo Estudiantil los dos (2) candidatos que obtengan el mayor número de votos, siendo sus suplentes los que ocupen el tercero (3ro), y cuarto (4to) lugar respectivamente. Para dicha proclamación se debe tomar en cuenta que el reglamente sobre el Decanato de Desarrollo Estudiantil dispone que los representantes principales ante el Consejo General del Desarrollo Estudiantil deben pertenecer a distintas facultades, por lo cual en caso de que resulten ganadores candidatos de la misma facultad, serán representantes principales aquellos estudiantes con mayoría de votos de otras facultades.
3. Para Representantes Principales ante el consejo de Facultad los dos (2) candidatos que obtengan el mayor número de votos, siendo los suplentes los que ocupen el tercer (3er) y cuarto (4to) lugar. Para dicha proclamación se debe tomar en cuenta que los representantes principales deben pertenecer a diferentes escuelas, con la excepción de que según el Estatuto Orgánico en el artículo 49 dice que en caso de tener escuelas iguales pero con diferentes sedes, esto no aplica.
4. Para Representantes Principales ante el Consejo de Escuela los dos (2) candidatos que obtengan el mayor número de votos, siendo los suplentes los que ocupen el tercer (3er) y cuarto (4to) lugar.
5. En caso de haber empate entre dos (2) o más candidatos, se proclamará a quien este más avanzado académicamente, y a igualdad de nivel académico a quien tenga mejor promedio de calificaciones.
6. Los alumnos, profesores o egresados, no podrán ejercer simultáneamente más de una representación electiva en los distintos organismos del sistema universitario. En caso de resultar electo para más de una opción deberá optar por una (1) y renunciar a las otras, esto según lo decidido en el Consejo

Universitario de sesión 04 de noviembre de 2004. (Comisión Electoral de la Universidad Católica Andrés Bello, 2011)

II.2.2. Diseño Sistema Electoral para la AEUCAB:

En el año 2009, se desarrolló una Tesis de Grado basada en el diseño de un sistema electoral para la Asociación de Egresados de la UCAB, donde se contempla la posibilidad de realizar las votaciones para la elección de los representantes estudiantiles mediante el uso de Internet. Con este sistema se buscaba lograr los siguientes aspectos:

- Posibilidad de realizar la votación desde cualquier computadora con acceso a Internet.
- Disminución del tiempo de obtención de los resultados.
- Reducción de la necesidad de personal encargado en la organización y desarrollo del sistema de elecciones actual.
- Eliminación de las papeletas, contribuyendo con el ahorro del papel.
- Transmisión y recuento automático de los votos.
- Alto nivel de seguridad mediante el cifrado de la información y control de acceso.
- Uso de tecnologías de bajo costo, sin necesidad de contratar a empresas especializadas en el desarrollo de estos sistemas.

Previamente, se realizó una encuesta a través de www.encuestafacil.com para que los miembros de la Asociación de Egresados de la UCAB (AEUCAB) evaluaran las ventajas y desventajas del sistema que se desarrollaba en ese momento.

Este sistema piloto diseñado por tesistas, se basó en una plataforma de telecomunicaciones, a través de un modelo cliente-servidor, con herramientas de páginas web y bases de datos que fueran compatibles con las ya existentes en la universidad, ya que el servidor desarrollado trabajó bajo el sistema operativo LINUX

al igual que el servidor que contiene la base de datos de la UCAB. Además, fue regido por las normas de la UCAB concernientes para este tipo de procesos electrónicos. El DTI (Dirección de Tecnologías de la Información) de la UCAB, es el departamento que contiene la base de datos de los estudiantes y egresados de la UCAB, el cual proporcionó la estructura de la base de datos, que sirvió para el desarrollo del sistema diseñado.

El diseño incluía dos interfaces, una administrativa y otra para el votante. La interfaz administrativa, es la usada por los administradores del sistema, una vez ingresado el nombre de usuario y contraseña, se programa la fecha y la duración de dicha jornada electoral, se cargan todos los candidatos participantes y se puede realizar todo el monitoreo del proceso, es decir, desde esta interfaz se pueden ver los resultados preliminares y se puede eliminar algún candidato que por alguna razón ya no participe en las elecciones. La interfaz del votante es más sencilla, luego de colocar el correo y la clave respectiva (Cédula de Identidad del egresado) se procedía la votación.

En este proyecto, se buscó utilizar herramientas de páginas web y bases de datos compatibles con las usadas por el DTI de la UCAB, entre las cuales se encuentran: el sistema de gestión de base datos ORACLE, el cual, es usado para crear la base de datos de la UCAB. Los diseños de las páginas web se realizaron con la herramienta DREAMWEAVER, la cual permite crear las mismas sin la necesidad de conocer el código de programación HTML, además pueden ser visualizadas en casi todos los navegadores web. Como lenguaje de programación, se empleó PHP, el cual trabaja bajo el entorno de ZEND.

Por lo tanto, para el desarrollo del diseño del sistema de votaciones que fue planteado, se usó un paquete gratuito llamado WAMPSERVER, el cual permite configurar fácilmente un servidor local que se instala sobre el servidor web de HTTP APACHE y sobre el servidor de base de datos MySQL y soporta el mismo lenguaje de programación PHP usado por el DTI.

Internamente, en el paquete WAMPSERVER se instaló la herramienta WORDPRESS, la cual es un sistema de gestión de contenido enfocado en la creación de blogs, desarrollado en PHP y MySQL y es una de las más populares por su licencia, su facilidad de uso y sus características como gestor de contenidos.

A través de la herramienta PHPMYADMIN se gestionaron dos bases de datos con MySQL, una que contenía la estructura de la base de datos de la UCAB que fue proporcionada por el DTI y otra que fue generada por WORDPRESS, con la cual, se crearon las páginas webs usando plantillas para que todas lucieran con el mismo patrón.

Desde una computadora local, el sistema se instaló bajo un servidor web para el acceso a Internet. Previamente, se adquirió el dominio www.eleccionesucab.com, usando los servicios de hospedaje de la empresa RYHOSTING.COM, cuyo contrato con la misma consistió en un plan simple, que constaba de alojamiento web básico: gestión de base de datos MySQL y cuentas FTP ilimitadas, soporte en PHP y certificados digitales. Todos estos aspectos bastaban para la compatibilidad con el sistema diseñado. La adquisición de este dominio permitía el ingreso a la página y tanto el código fuente como las bases de datos usadas, fueron exportados desde la computadora al servidor web.

Como mecanismos de seguridad en este sistema propuesto, se utilizaron las técnicas de cifrado mediante los certificados digitales. A través del método de criptografía asimétrica de clave pública, los datos transmitidos y enviados al servidor web eran cifrados bajo el sistema RSA, y se proporcionaba una conexión segura a Internet mediante el protocolo SSL.

En el panel de seguridad de Administración de SSL del dominio, se generó la llave privada, la cual, hace la petición del certificado CSR. Se contrató una prueba gratis de Autoridad de Certificación GLOBALSIGN a quienes se les suministró el CSR para que generaran un código cifrado y junto con otro certificado dado por ellos,

se enviaron al soporte de seguridad de RYHOSTING.COM para que activaran a ambos. Todo este proceso garantizó que la página de las votaciones fuera segura, usando el protocolo HTTPS en el momento en el que el votante realizaba la votación y luego de esto, confirmara la misma.

Para verificar la contraseña ingresada por el votante al momento de realizar la votación, se usó el método criptográfico MD5, el cual es un algoritmo de 128 bits que codifica el mensaje que llega al servidor y este lo compara con la contraseña registrada en la base de datos para verificar que sea la misma y darle acceso al usuario.

Entre los otros métodos de seguridad usados en este Trabajo Especial de Grado fue el de la firma digital, al momento de hacerle la solicitud a la Autoridad de Certificación para que autorizara el certificado. Asimismo, se hizo uso del control de acceso al momento de permitir el ingreso de los administradores a la interfaz de administración, para que solo estas personas estuvieran encargadas del monitoreo del dicho proceso electoral. De la misma manera, solo los egresados registrados en la base de datos podían tener acceso a dicha votación. (Montoya & Machuca, 2009)

II.3. Elecciones Digitales en el Mundo.

Para realizar unas elecciones digitales, un sistema democrático requiere certificar que las mismas sean autónomas y totalmente transparentes. Cuando se requieren hacer unas elecciones electrónicas vía Internet, es necesario que se garanticen una serie de normas que rijan el proceso electoral como el anonimato, la seguridad y la transparencia. A continuación, se describen algunos sistemas electorales desarrollados alrededor del mundo:

II.3.1. Elecciones digitales en España:

Estas elecciones fueron realizadas en Madrid, con el fin de conocer la opinión de los ciudadanos con respecto a unas mejoras para un barrio. Para la realización de

estas elecciones se instaló una urna digital, y se tenía previsto que los votantes enviaran sus respectivos votos a distancia, a través de un computador o teléfono móvil con acceso a Internet.

En dichas elecciones se verificó que el emisor del voto era una persona perteneciente a un censo previamente realizado. El voto fue secreto, ya que no debe haber relación entre el votante y el voto que ha emitido. Este el sistema contabilizó todas las opciones elegidas por cada votante.

El sistema elegido cubrió todos los requerimientos, basándose en la metodología desarrollada por la empresa catalana SYCTL. Dicho sistema funciona de la siguiente manera: el ciudadano acude con su documento de identificación a un centro de validación, donde un funcionario comprueba que esté inscrito en el censo y le entrega un sobre con un número único de dieciséis cifras, el cual es llamado numero SIM, este número no es conocido por ninguna persona. Al entregar dicho sobre, se registra para controlar que no solicite otro SIM. Este sobre tiene un código impreso en el exterior del mismo, el cual sirve para anular el SIM a petición del votante en caso de pérdida o hurto del número.

Este SIM sirve como clave secreta y el ciudadano puede mediante un teléfono móvil o computadora con acceso a Internet, realizar su voto. Al momento de la votación se comprueba que el SIM introducido es uno de los números entregados a los votantes y que no haya sido utilizado previamente. Luego de esto, realiza la votación y se culmina el proceso.

El único inconveniente con este sistema de votación es que la verificación del voto solo es por pantalla, y al no tener un comprobante físico pueden surgir dudas entre los votantes. (Gimeno, 2004)

II.3.2. Elecciones digitales en la UNAM.

Un buen ejemplo de un sistema de elecciones digitales para los representantes estudiantiles de una Universidad, se lleva a cabo en la UNAM, en la cual existe el CEP, que asegura la credibilidad y legitimidad de las elecciones electrónicas en esta universidad, además de llevar el control y la organización de las mismas. Estas elecciones están integradas por los representantes de la autoridad universitaria y representantes académicos. El CEP cuenta con un número de expertos reconocidos en informática y en telecomunicaciones para asesorar todo el proceso de las elecciones electrónicas.

Todos los procesos electorales electrónicos deben certificar que sea secreta la identidad y la preferencia de voto que tenga la persona que realice el sufragio. El CEP es el encargado de verificar que la identidad del votante no esté relacionada con el voto que éste emita. Para esto, la aplicación desarrollada para este proceso está programada bajo un código abierto, el cual está publicado en la página web de la UNAM, de esta forma, puede ser revisado en cualquier momento.

Este sistema de elecciones electrónicas consta de estrictas medidas de seguridad. Para esto, las transmisiones de datos entre las máquinas donde se realizan dichas votaciones, son encriptados bajo un protocolo SSL. Además, este sistema cuenta con una tecnología potencialmente segura y evita sistemas operativos propensos a adquirir virus y otros defectos que comprometan la seguridad del sistema. El CEP vigila todas las máquinas que se ubican físicamente en distintas sedes de la UNAM para controlar todas las políticas de acceso y la seguridad del sistema. Es de suma importancia que este sistema disponga de "*firewalls*" que protejan las votaciones. (Miramontes, 2005)

El 22 de Noviembre de 2007 se realizó un proceso para la elección de los Representantes Profesores del Área de Maestría y Posgrado y del Área de Sistema Universidad Abierta ante el Consejo Técnico de la Facultad de Economía y un

integrante para la Comisión Dictaminadora de dicha Facultad. En este proceso se hizo uso del Sistema de Votaciones Electrónicas UNAM, el cual facilitó el proceso electoral por Internet, con ventajas como la confidencialidad, seguridad y confiabilidad de la información, las cuales agilizaron la obtención de los resultados y permitieron que la votación se ejerciera debidamente, cumpliendo las siguientes características:

Universal: cuando un conjunto de personas disponen del derecho al voto, no existen discriminaciones ni exclusiones por diferentes condiciones o circunstancias.

Libre: toda persona que ejerza la votación tiene derecho y libertad de elegir al representante de su preferencia en las distintas.

Directa: todos los votantes ejercen el derecho al voto sin intermediarios, es decir, no es transferible ya que cada persona está capacitada para tomar su propia decisión.

Secreta: El voto es de libre decisión de cada uno de los votantes, por esto se debe garantizar la seguridad del mismo en todo momento.

El sistema implementado funcionó de la siguiente manera: una persona fue la encargada de habilitar el sistema para llevar a cabo el proceso de la elección a través de la página web http://www.elecciones.unam.mx., donde ingresó su respectivo número de identificación personal, el cual fue verificado en las listas nominales y es una clave, generada con la combinación de algoritmos y otros datos aleatorios, única para cada votante que validó su acceso al sistema de votación. Ésta clave es prácticamente imposible de descifrar. Luego de esto, se presentó una boleta virtual de candidatos para que el votante escogiera la opción de su preferencia a través de la página web. El sistema finalizó el proceso una vez culminada la votación electrónica.

Se garantiza que el voto sea secreto ya que en ese momento no existía asociación entre su identidad y su respectivo voto. Una vez culminado el proceso de

las votaciones, se levantó un Acta de Cierre de Casilla y una hora después una personada encargada de cada Comisión Local de Vigilancia, con un mecanismo bastante seguro de validación, descargó de una página uno de los archivos que contienen resultados particulares, donde la información estaba resguardada de todo, robo o alteración, que pudiera ocurrir. Posteriormente, se generó un certificado para cada persona a partir de esta información obtenida.

El Sistema de Votaciones Electrónicas UNAM cuenta con los siguientes mecanismos de seguridad:

- Está protegido contra diferentes tipos de ataques como: negación de servicios, verificación de puertos abiertos, envío de archivos maliciosos, etc.
- Existe un proceso de respaldo inmediato de la información.
- Utiliza protocolos seguros electrónicos.
- Mediante un certificado digital, la página web está registrada y autenticada por una autoridad conocida internacionalmente.
- Todos los archivos del sistema están protegidos bajo mecanismos de seguridad que, además, verifican el correcto funcionamiento de la página.
- El sistema verifica alguna entrada de código malicioso, envío de variables no válidas, accesos permitidos, entre otros.
- La urna electrónica está protegida a través del cifrado de datos y algoritmos de seguridad.
- El sistema bloquea el acceso al elector una vez emitido el voto, para evitar que vote nuevamente.

  El Sistema de Votaciones Electrónicas UNAM no provee los resultados parciales, o totales, en línea, mientras no se haya cerrado el proceso de votaciones. No se puede consultar, o modificar, las bases de datos, asegurando el posterior escrutinio. Tampoco se permiten nuevas asignaciones o modificaciones en el Número de Identificación Personal (NIP) de los

votantes. No se amplían ni se modifican las listas nominales para mantener el patrón de los electores. Así mismo, no se puede suspender ni reanudar.

Para controlar el sistema de votaciones electrónicas, la UNAM toma en cuenta las siguientes consideraciones:

- No se realiza un coteo preliminar de votos para no conocer las tendencias. Sin embargo, se realiza un monitoreo en el transcurso del proceso de votaciones para conocer la cantidad de personas que realizan la votación en una hora determinada.
- Este monitoreo está programado para que se actualice automáticamente cada 30 segundos mediante la pantalla.
- Para dicho monitoreo, sólo podrá ingresar en la página web la persona designada de cada Comisión de Vigilancia cuando haya ingresado su nombre de usuario y contraseña respectivamente.

Los profesores de cada Facultad que vayan a participar en dicha jornada de votaciones electrónicas. Previamente, deben verificar que se encuentren en el Padrón de Electores, en caso de no encontrarse, pero pueden solicitar acceso antes de las 48 horas previas a la votación. Los profesores procederán a ingresar en la página: www.elecciones.unam.mx en el horario comprendido entre las 8:00 a.m. y las 8 p.m. y en vez de colocar el NIP como los alumnos, ingresarán su respectivo RFC, el cual aparece en su correspondiente credencial de la UNAM o en el comprobante de pago.

Los equipos a usar en las elecciones realizadas el año 22 de Noviembre de 2007, tenían que contar con las siguientes especificaciones:

Hardware:

- Computadora PENTIUM III a 700 MHz o superior (libre de virus informático).
- 256 MB de memória RAM o superior
- Tarjeta de Red ETHERNET 10/100 Mbps. o

- MODEM de 56 Kbps de respuesta automática o superior.
- Conexión a internet, preferentemente de alta velocidad.

Software:

- WINDOWS 2000 o superior, debidamente actualizado.
- Programa antivirus
- Cualquiera de los siguientes navegadores de internet:
  - ✓ INTERNET EXPLORER V.5.0 o superior
  - ✓ FIREFOX V1.5 o superior
  - ✓ NETSCAPE V7.2 o superior. (Facultad de Economía UNAM, 2007)

Recientemente, se realizaron unas votaciones electrónicas en dicha universidad, el día 27 de Octubre de 2011, donde se publicó un Manual del Elector con todas las normas e indicaciones necesarias para participar en el sistema. Los votantes pudieron ejercer el voto desde una computadora desde su propia casa, oficina, café Internet, etc., siempre y cuando cumpliera con el horario señalado en dicha convocatoria. Para poder ingresar al Sistema de Votaciones Electrónicas UNAM, fue necesario contar con conexión a Internet, donde el tiempo de respuesta dependió del ancho de banda de la conexión.

El sistema funcionó en computadoras personales, siempre y cuando contaran con un procesador PENTIUM como mínimo y 128 de memoria de RAM. Además, pudo funcionar en algunos dispositivos móviles. Se pudo ingresar al sistema mediante los navegadores de Internet: EXPLORER 6+, MOZILLA FIREFOX, NETSCAPE, OPERA, CHROME o SAFARI. En caso de presentarse algún tipo de problema a la hora de ejercer el voto, se recomendó acceder desde un navegador diferente, o en dado caso, desde otro equipo.

De ante mano, se advirtió que era preferible realizar el sufragio desde una computadora personal, ya que, desde un dispositivo móvil había que verificar la

compatibilidad entre el proveedor de Internet, el sistema operativo y el navegador de cada dispositivo.

Una vez ingresado al portal de las elecciones electrónicas de la UNAM: http://www.jornadaelectoral.unam.mx, aparecía en pantalla lo mostrado en Figura 1.

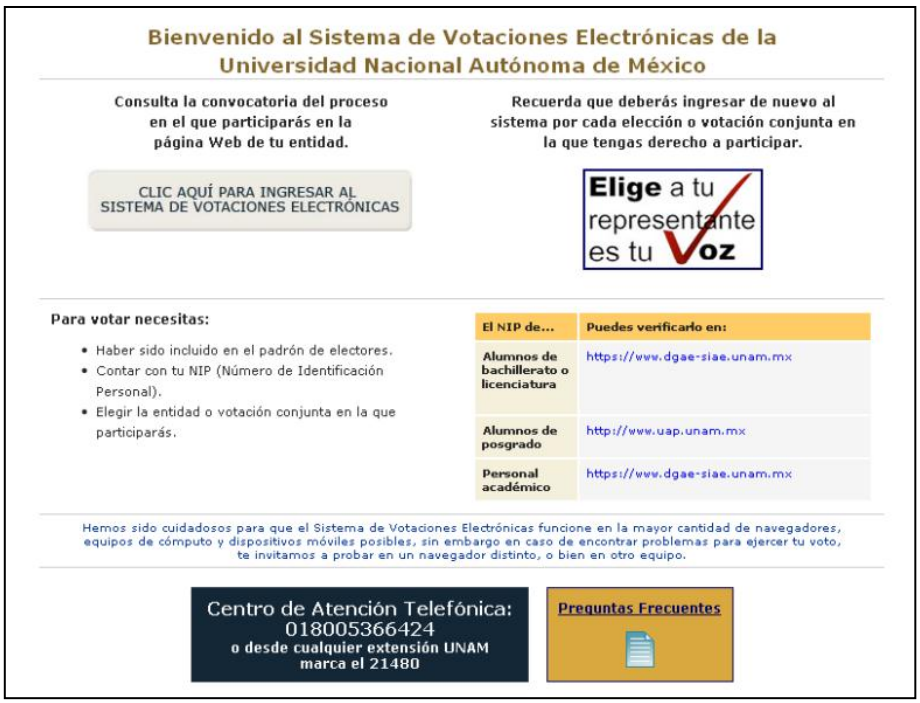

Figura 1: Página de inicio al Sistema de Votaciones UNAM

(Direccion General de Computo y de Tecnologías de Informacion y comunicación, 2011)

Luego de haber presionado el botón: “Click Aquí para ingresar al sistema de votaciones electrónicas”, se presentaba el formato que aparece en la Fiura 2 para proceder al sistema:

Figura 2: Acceso elector al Sistema de Votaciones UNAM

(Direccion General de Computo y de Tecnologías de Informacion y comunicación, 2011)

En la casilla de Identificador se colocó el Número de cuenta para alumnos y RFC para Académicos y posteriormente el NIP. Así mismo, se colocó la Entidad Universitaria, o la elección en conjunto, donde respectivamente se pueda participar.

En caso de haber ingresado algún dato incorrecto, el sistema avisa el error al votante y da derecho a colocar nuevamente los datos.

Una vez ingresado al sistema, aparecen en pantalla las opciones a la que dicho votante tiene derecho a elegir. En la parte superior de la boleta, se indican la cantidad de fórmulas a elegir, necesarias para que el voto sea considerado válido.

Si se seleccionaban más opciones de las permitidas en la boleta correspondiente, el voto era considerado Nulo y en caso de no seleccionar ninguna de las opciones que aparecen en la misma, era considerado voto en Blanco. Cualquiera de estos dos tipos de votos no fueron tomados en cuenta.

Cuando el voto se había efectuado correctamente, el votante procedía a hacer clic en el botón "URNA: Deposite aquí su voto" y posteriormente aparecía en

pantalla un resumen del sufragio realizado para que el votante confirmara su elección y el sistema notificara que el voto había sido registrado.

El tiempo permitido para realizar el voto era de cinco minutos. Si en este tiempo estipulado no se culminaba el sufragio, expiraba la sesión y había que ingresar nuevamente los datos si se deseaba volver a ingresar al sistema. (Dirección General de Computo y de Tecnologías de Información y Comunicación, 2011)

II.4 Comunicación entre las sedes.

Para establecer la comunicación entre dos lugares, se puede hacer uso de una Red Privada Virtual (RPV, en ingles VPN, Virtual Private Network) la cual, es una red que provee de una conexión segura entre 2 redes privadas. La red es virtual debido a que la información a transmitir es enviada a través de un "túnel" por una red pública, como lo es Internet, emulando una conexión punto a punto. La red es privada porque el "túnel" provee confiabilidad de la información, integridad, autenticación, y un control de acceso. El concepto del mecanismo de entunelado es simple, el cuerpo del mensaje es encapsulado con una nueva cabecera, además el cuerpo del mensaje es encriptado y autenticado. Los túneles pueden ser establecidos en diferentes tipos de redes y protocolos como IP, ATM, FRAME RELAY, y MPLS. Entre sus beneficios tenemos:

- Bajos Costos: siendo uno de los grandes beneficios de la implementación con VPN debido a que se pueden interconectar por ejemplo, sedes de compañías ubicadas geográficamente distantes, siempre y cuando en ambas se pueda acceder a internet. Ahorrando en costos de equipos, costos operacionales, y en servicio técnico de las redes en el caso de tener enlaces físicos entre las sedes.
- Escalabilidad: debido a que las VPN son fácilmente extensibles geográficamente solamente generando nuevas conexiones por parte de los proveedores de servicio.

- Flexibilidad: ofreciendo desde una conexión punto a punto, hasta una conexión con múltiples accesos. Esto lo hace cuidando la seguridad y el acceso de los usuarios a la información. (Dougligeris & Serpanos, 2007)

Una VPN debe garantizar ciertas características básicas de seguridad, como lo son:

- Autenticación y Autorización para verificar quien está al otro lado de la comunicación y que nivel de acceso tendrá.
- La integridad de la información, ya que los datos no pueden ser alterados. Para garantizar esto, se utilizan funciones de Hash como lo son *Message Digest* (MD2 y MD5) *y Secure Hash Algorithm* (SHA). (Ver Apéndice A)
- La Confidencialidad para que los datos solo puedan ser interpretados por sus destinatarios. Esto se logra mediante el uso de algoritmos de cifrado como *Data Encryption Standard* (DES), *Triple DES* (3DES) y Advanced Encryption *Standard* (AES). (Ver Apéndice B)
- El no repudio de la información, ya que los datos irán firmados por el remitente de tal forma que no pueda negar que es su autor.

Entre las arquitecturas de conexión de VPN se encuentran:

- VPN de acceso Remoto: consiste en la conexión de usuarios desde sitios remotos, usando Internet como vinculo de acceso. Los usuarios luego de la autenticación, tienen un nivel de acceso muy similar al que tienen en la red local.
- VPN punto a punto: consiste en la conexión entre 2 puntos en el cual, el servidor VPN acepta conexiones vía Internet proveniente de sitios remotos y establece el túnel VPN. Esto permite eliminar las conexiones físicas punto a punto tradicional (Por cables de cobre).
- VPN *over* LAN: es un tipo de VPN poco utilizado, es una variante de "acceso remoto" pero en lugar de utilizar Internet para realizar la conexión, emplea la

red de Área Local (LAN) de la empresa. Es utilizada para aislar zonas y servicios internos, y es de gran utilidad para mejorar la seguridad en redes inalámbricas.

- *Tunnelling*: es el tipo de VPN mas utilizado en la actualidad y consiste en encapsular un protocolo de red sobre otro, creando un túnel en la red de computadoras. El túnel se establece incluyendo un PDU (*Packet Data Unity*) dentro de otro PDU para transmitirla de un extremo a otro, así se enrutan los paquetes de datos sobre nodos intermedios, los cuales no entienden el contenido de los mismos. El túnel queda definido por los extremos y el protocolo de comunicación empleado. (CALA (CAmpus Libre y Abierto), 2006) Utiliza tres protocolos los cuales son:
  - ✓ Protocolo Portador: Este es el protocolo por el que viaja la información, como lo son *Frame Relay, ATM, MPLS*.
  - ✓ Protocolo Encapsulador o de Encapsulación: Es el protocolo que se superpone a los datos originales, como lo son *GRE, IPSEC, L2F, PPTP, L2TP*.
  - ✓ Protocolo Pasajero: Es el protocolo por donde se transportan los datos, como lo son *IPX, AppleTalk, IPv4, o IPv6*. (Vachon & Graziani, 2009)

II.4.1 Protocolos encapsuladores:

Estos protocolos se encargan de definir todo lo referente a la encriptación, seguridad, autenticación e integridad de los datos a transmitir, entre estos encontramos:

II.4.1.1 L2F (*Layer 2 Forwarding*)

Es un envió en capa 2, ya que se encarga del empaquetado y llevar a su destino cualquier datagrama local, fue creado por cisco, siendo muy similar a PPP, no es utilizado en redes WAN, provee una autenticación entre usuarios pero no encriptación de los datos. (Mañaz, 2004)

II.4.1.2 IPsec (*Internet Protocol Security*)

Es un estándar IETF (RFC 2401-2412) que se encarga de dar los lineamientos de como una VPN puede configurarse utilizando direccionamiento IP. Esta basado en algoritmos existentes para implementar encriptación, autenticación e intercambio de claves. Cuando funciona en la capa de red protege y autentica los paquetes IP entre los dispositivos que participen en la comunicación, pudiendo proteger todo el tráfico de la capa de aplicación, ya que la protección se aplica de la capa 4 al 7.

Con respecto al enrutamiento, al implementar IPsec se cuenta con un texto-plano en la cabecera de capa 3. En la capa 2 es compatible con todos los protocolos como ETHERNET, FRAME RELAY, SYNCHRONOUS DATA LINK CONTROL (SDLC) y HIGH-LEVEL DATA LINK CONTROL (HDLC).

IPsec está estructurado en 5 bloques, tal y como se muestra en la Figura 3, constituidos como se muestra a continuación:

- Un primer bloque constituye el tipo de IPsec a aplicar, siendo las opciones de ESP o AH.
- El segundo constituye la confidencialidad a aplicar utilizando algoritmos de cifrado como DES, 3DES, AES o SEAL. (Ver Apéndice B)
- El tercero constituye la integridad que se resguarda aplicando MD5 o SHA. (Ver Apéndice A)
- El cuarto constituye el establecimiento de la clave secreta compartida, la cual puede ser realizada por pre compartimiento o firma digital usando RSA. (Ver Apéndice C)
- El quinto constituye el algoritmo de DH. Encontrándose cuatro algoritmos de intercambio de clave DH, como DH grupo 1 (DH1), DH grupo 2 (DH2), DH grupo 5 (DH5), y DH grupo 7 (DH7).

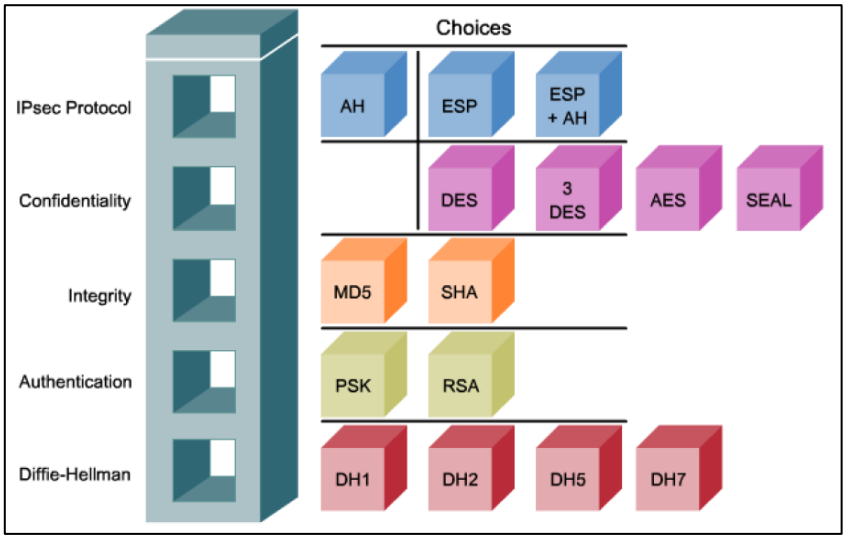

Figura 3: Estructura por Bloques de IPsec (Stewart, 2009)

Entre tantas opciones que escoger, IPsec proporciona una estructura, dejando la libertad de poder elegir los algoritmos para implementar los distintos niveles de seguridad requeridos, como lo son:

- Integridad: debido a que los datos se transportan por un medio inseguro como Internet, podrían ser interceptados y modificados, razón por la cual, hay que garantizar que el contenido no haya sido alterado. Los códigos de autenticación de mensajes HASH (HMAC) son algoritmos que se encargan de garantizar la integridad de los datos mediante un valor HASH. Este valor se origina procesando el mensaje y la clave secreta a través de un algoritmo de HASH, el mismo se añade al mensaje y se envía a través de la red. El receptor calcula nuevamente el valor del hash y lo compara con el valor de hash enviado, verificando, en el caso que coincidan, la autenticidad del mensaje. Los algoritmos HMAC mas utilizados, son *Message Digest* 5 (MD5) y *Secure Hash Algorithm 1* (SHA-1) siendo el último mas seguro. (Ver Apéndice A)
- Confidencialidad: es lograda mediante la encriptación del tráfico mientras se encuentre dentro de la VPN, dependiendo su grado de seguridad de la longitud de la clave del algoritmo de cifrado aplicado. Se utilizan para el

cifrado, en orden de menos seguro a más seguro: DES, 3DES, AES, SEAL. (Ver Apéndice B)

- Autenticación: es lograda mediante una clave privada de cifrado del remitente denominado firma digital. Entre los métodos mas utilizados para la configuración de autenticación de los pares encontramos las claves pre compartidas (PSK) y las firmas RSA, también siendo usado en menor proporción el cifrado RSA-nonce. (Ver Apéndice C)
- Intercambio seguro de claves: este intercambio es necesario para algoritmos de cifrado como DES, 3DES y AES, y algoritmos de hash como MD5 y SHA-1, compartan una clave secreta simétrica. Para esto se cuenta con Diffie-Hellman (DH) el cual plantea un intercambio de claves por un canal inseguro, creando un camino para que los miembros establezcan una clave secreta compartida conocida solo por ellos. DH tiene variaciones conocidas como grupos:
  - ✓ Grupo DH 1 y DH 2: soportan exponenciación en primer modulo con tamaños de 768 bits para DH1, 1024 bits para DH2, soporta también encriptación DES y 3DES, DH 2 adicionalmente soporta encriptación AES.
  - ✓ Grupo DH5: soportan exponenciación en primer modulo con tamaños de 1536 bits, soporta también encriptación AES.
  - ✓ Grupo DH 7: Es compatible con la criptografía de curva elíptica (ECC).

II.4.1.2.1 Estructuras del Protocolo IPsec:

Las dos principales estructuras del protocolo son la Cabecera de Autenticación (AH) y la Carga de Seguridad Encapsulada (ESP), pudiendo aplicarse en modo Transporte o modo Túnel.

- AH es el protocolo IP 51, adecuado para utilizar cuando la confidencialidad no es necesitada, Asegura que origen y destino sean correctos (Autenticación) y la integridad de los datos. No encripta los paquetes y todo el texto es transportado sin cifrar, lo cual de ser utilizado solo proporciona una protección débil. Soporta los algoritmos de HMAC-MD5 y HMAC-SHA-1, pudiendo tener problemas si se utiliza NAT, las opciones de configuración se pueden observar en la Figura 4.

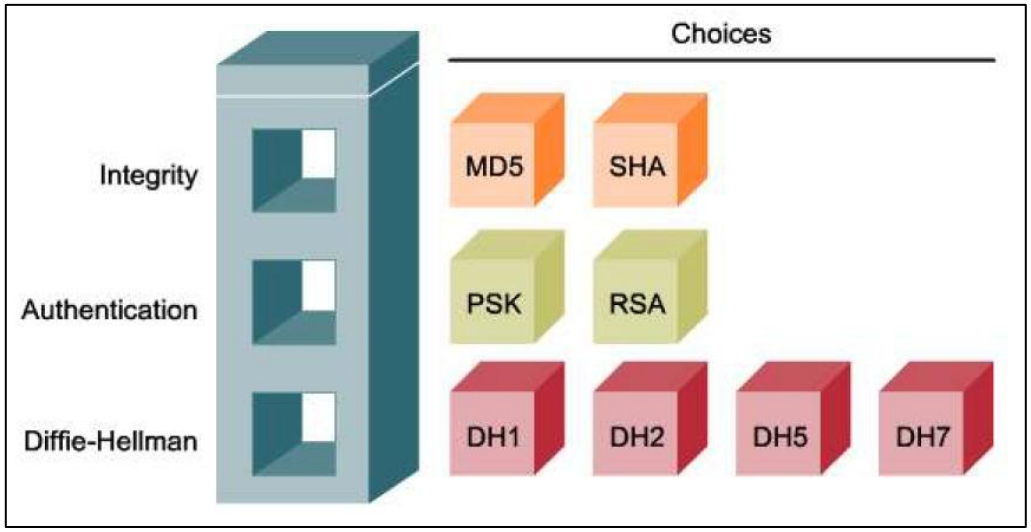

Figura 4: Opciones en AH. (Stewart, 2009)

- ESP es el protocolo IP 50, que proporciona confidencialidad y autenticación. La confidencialidad la proporciona al cifrar la carga útil, pudiendo soportar una gran variedad de cifrado simétrico, el algoritmo por defecto es el DES de 56 bits, pudiendo soportar 3DES, AES y SEAL. Dicha carga cifrada es encriptada a través de los algoritmos de hash, HMAC-MD5 o HMAC-SHA-1, proporcionando esta autenticación e integridad, las opciones de configuración se pueden observar en la Figura 5.

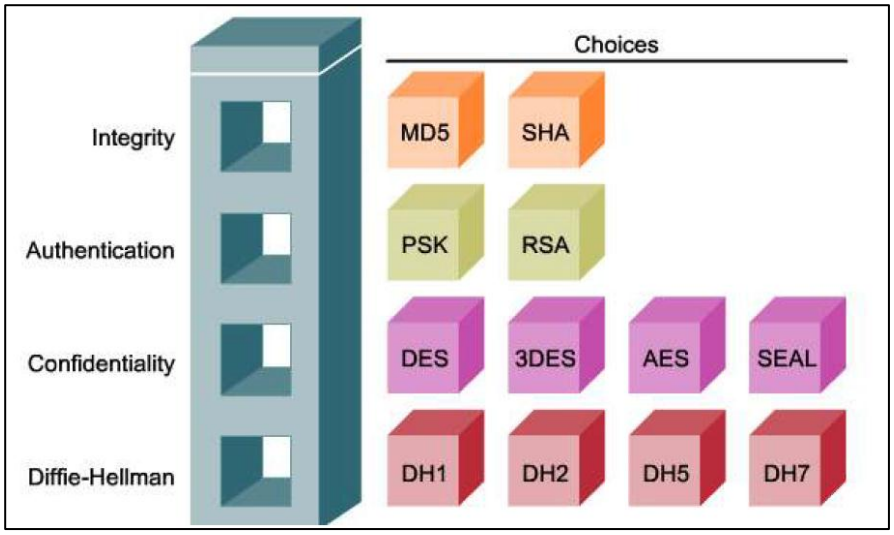

Figura 5: Opciones en ESP. (Stewart, 2009)

II.4.1.2.2 Intercambio de claves en IPsec:

Para el establecimiento de una VPN se negocian parámetros de intercambio de claves, se establece una clave compartida, se autentica el otro miembro de la comunicación, y se negocian los parámetros de codificación, realizando así una asociación de seguridad (SA).

Las asociaciones de seguridad se mantienen dentro de una base de datos SA, también llamada SADB, teniendo entradas para definir los parámetros de encriptación IPsec y parámetros para intercambios de claves. Todas estas claves no son transmitidas directamente a través de la red, se utiliza *Internet Key Exchange* (IKE) intercambiando paquetes de datos, este protocolo combina la *Internet Security Association and Key Management Protocol* (ISAKMP) con los métodos de intercambio de claves *Oakley* y *SKEME*.

ISAKMP define el formato del mensaje, la mecánica del protocolo para el intercambio de claves y el proceso de negociación para crear un SA. No define como se gestionarán ni compararán las claves entre los miembros de la comunicación. Oakley y SKEME tienen grupos principales definidos, tales como el grupo 1 con

claves de 768 bits, grupo 2 con clave de 1024 bits, y grupo 5 con claves de 1536 bits. (Stewart, 2009)

II.4.1.3 L2TP (*Layer 2 Tunnelling Protocol*)

Fue creado por CISCO y MICROSOFT para remplazar L2F y PPTP, Soporta distintos protocolos de red como IPX, SNA, IP, no provee encriptación. Permite interconectar redes cuando el túnel ofrece una conexión punto a punto orientada a paquetes. Utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son utilizados para establecer la comunicación y mantenerla, así como también el borrado de los túneles al finalizar la comunicación. Los mensajes de datos son encapsulados mediante PPP y enviados por el Túnel. (Verón, 2009) Es una extensión del protocolo PPP que permite la creación de túneles VPNs a nivel 2 o de enlace de datos, tiene un protocolo de entunelamiento basado en L2F permitiendo transportar medios de empaquetamiento tales como FRAME RELAY, X.25 y ATM. (Andreu, Pellejero, & Amaia, 2006)

En la mayoría de los casos, L2TP utiliza IPsec para cifrar los datos, siendo uno independiente del otro, pero al usarse por separado ya el túnel no será cifrado. L2TP por medio de IPsec, permite autenticar al usuario que desea establecer la sesión, y autenticar la cuenta de equipo mediante un certificado, intercambiando claves cifradas.

Las ventajas que ofrece son las siguientes:

- Permite la compresión de los encabezados (4 bytes por 6 para PPTP).
- Permite la autenticación en el túnel.
- Utiliza IPsec para el cifrado de los datos, logrando un gran nivel de seguridad. (Mathon, 2004)

II.4.1.4 SSH (*Secure Shell*)

Se encarga de cubrir la autenticación, encriptación y la integridad de la data transmitida en la red. Determina un puerto arbitrario para enviar la información, dirige el tráfico recibido del puerto de salida al puerto de llegada. La autenticación se realiza para establecer la comunicación, se utiliza normalmente para acceder a computadores remotos, busca una prueba digital para verificar la identidad. La encriptación la realiza revolviendo la data para que sea inentendible excepto para los recipientes, y la integridad la garantiza ya que si otra persona modifica los datos en tránsito por la red, SSH detectaría este hecho. (Barret, Silverman, & Byrnes, 2005)

II.4.1.4.1 *Open SSH*

De sus siglas en ingles *Open Secure Shell*, es una versión libre de comunicación segura, del paquete de herramientas del protocolo SSH para redes, se encarga de cifrar todo el tráfico de los datos, incluyendo las contraseñas, evitando así intromisiones externas, y otros ataques a nivel de red. Ofrece distintas posibilidades para la implementación de túneles con distintos métodos de autenticación.

Es un proyecto que ha venido desarrollando el proyecto OpenBSD, el cual produce un sistema operativo libre de tipo UNIX, multiplataforma, desarrollado en su totalidad por voluntarios, que se enfoca en la portabilidad, estandarización, corrección, seguridad proactiva y criptografía integrada. En dicho sistema operativo están integrados los programas SSH sustituyendo a RLOGIN y TELNET, CSP sustituyendo a RCP, y SFTP sustituyendo a FTP. (OpenBSD 4.8, 2011)

Existen dos variedades del protocolo SSH, las cuales son incompatibles, estos son SSH 1 y SSH 2 descritos a continuación:

- SSH 1: en el encontramos el protocolo 1.3 y 1.5, las dos utilizan clave asimétrica RSA para negociar claves y luego, utilizan 3DES y *Blowfish* para

esconder los datos. Para la integridad de los datos se utiliza un CRC simple, que gracias a las ayudas de banda dificultan la efectividad de los ataques.

- SSH 2: fue inventado para evitar los problemas con las patentes de RSA, y a su vez, para mejorar el problema de integridad de los datos de SSH 1. Utiliza algoritmos asimétricos DSA y DH, y para la integridad de los datos usa un algoritmo real HMAC. (SSH, 2004)

Entre las características de OPENSSH encontramos:

- Proyecto de código abierto.
- Licencia libre.
- Fuerte cifrado utilizando 3DES, *Blowfish*, AES, o *Arcfour*. Todos estos algoritmos de cifrado están libres de patentes. El cifrado comienza antes de la autenticación, y ninguna contraseña ni otro tipo de información se transmite sin cifrar. El cifrado también se utiliza como protección contra falsificación de paquetes.
- Fuerte autenticación contra varios inconvenientes de seguridad, como lo son la suplantación de identidad (*IP spoofing*), rutas falsas (*fake roots*) y suplantación de DNS (*DNS spoofing*). La autenticación se realiza mediante *rhosts* (el cual solo permite acceso a usuarios determinados y considerados seguros) (Martínez D. D., 2002) junto con un sistema propio de autenticación basado en RSA, contraseñas para uso de una sola vez y autenticación mediante *Kerberos*.

> *Kerberos:* es un sistema de autenticación de red, que actúa como un tercero de confianza que mantiene todas las claves secretas de todos los usuarios y servicios. Al iniciarse sesión le provee al usuario una

concesión que le permitirá acceder a otros servicios sin volver a introducir su contraseña. (OpenBSD, 2000)

- Renvío por puertos de conexiones de TCP/IP a una maquina remota por un canal cifrado, pudiendo asegurar aplicaciones típicas de internet como POP de esta manera.

- Interoperabilidad con versiones de SSH, todas las versiones de OPENSSH contienen soporte para los protocolos SSH 1.3 y SSH 1.5. A partir de la versión 2.0 de OPENSSH, también se cuenta con el soporte para el protocolo SSH 2.0.

- La compresión de datos es una característica clave en redes lentas, ya que mejora los resultados comprimiendo los datos antes del cifrado. (OPEN SSH, 2004)

OPENSSH ha sido sometido a distintas pruebas demostrando su nivel de seguridad, demostrando no ser vulnerable ante los siguientes acontecimientos:

- Ataques *Password Cracking, Replay o Modification* sobre el cifrado CR4, debido a que se eliminó el soporte de CR4.

- Ataques a clientes de renvío en conexiones no cifradas, ya que todas las conexiones son cifradas.

- Ataques en el último paquete del algoritmo de cifrado IDEA, debido a que no hay soporte para el mismo.

- Ataque de circunvalación de las autenticaciones de la clave anfitriona, debido a que al anfitrión local también se le verifican las claves.

- Ataque de inserción, en el caso del protocolo SSH 1 este ataque si puede ser llevado a cabo pudiendo tener éxito.

- Ataque de vulnerabilidad en contraseñas por fuerza bruta, demostrado desde la versión SSH 1. (Open SSH, 2004)

CAPÍTULO III

METODOLOGÍA Y DESARROLLO

A continuación se describen los diversos procedimientos realizados en este Trabajo Especial de Grado para el desarrollo de un sistema piloto para el transporte de datos en votaciones, entre las sedes de la UCAB:

III.1 Recopilación de información sobre votaciones actuales.

Se efectuó un estudio sobre los diferentes sistemas de votaciones existentes para poder realizar con base el diseño del sistema piloto que se plantea. Se investigó el proceso electoral en Venezuela, el cual está a cargo del Consejo Nacional Electoral (CNE), que ha desarrollado un sistema automatizado y auditable en todas sus fases para diversas elecciones.

Para el caso de la elección de los representantes estudiantiles en las universidades del país, se obtuvo información acerca de sus procedimientos electorales, en donde se pudo constatar que son de forma manual, en algunos casos utilizando una máquina lectora para procesar las boletas de los votantes. Entre las universidades estudiadas encontramos la Universidad Central de Venezuela (UCV), Universidad Simón Bolívar (USB), Universidad Metropolitana (UNIMET) y la Universidad Católica Andrés Bellos (UCAB).

Centrando la investigación en la UCAB, se obtuvo información acerca del proceso de votación basada en comunicados emanados por la Comisión Electoral. Se pudo acceder al "*Reglamentos sobre constitución de Consejos referente a las elecciones de los Representantes Estudiantiles ante los diferentes Consejos de la Universidad*" el cual contiene las disposiciones acerca del proceso electoral, entre las disposiciones se encontraron:

- Atribuciones de la comisión electoral.
- Objetivo de las elecciones, el cual contiene los cargos a elegir.
- Estudiantes considerados Electores.
- Estudiantes elegibles para los cargos.
- Postulaciones.
- Propaganda Electoral.
- Procedimiento de Votación.
- Escrutinio.
- Proclamación

Se consultó un Trabajo Especial de Grado, realizado en el año 2009, titulado "*Diseño de un Sistema Electoral para la Asociación de Egresados de la UCAB utilizando la plataforma de telecomunicaciones existente*", publicada en la Biblioteca de dicha universidad. En esta se realizaron un sistema de elecciones estudiantiles vía web, utilizando cualquier computadora con acceso a Internet, esto con el fin de disminuir el tiempo de obtención de resultados, ahorrar papel y facilitar el derecho al voto a los egresados que no podían ir hasta la sede de la universidad.

A través de Internet, se estudiaron también algunos sistemas de votaciones digitales en otras partes del mundo, en donde se encontraron unas votaciones electrónicas realizadas en Madrid para reunir opiniones respecto a ciertas mejoras de un barrio de la zona. En dichas elecciones se verificó que el emisor del voto estuviera autorizado para votar, que no existiera relación entre el votante y el voto, lo cual, garantiza el secreto del mismo y que no realizara su votación más de una vez.

Así mismo, se obtuvo información acerca de un sistema electrónico de votaciones en la Universidad Nacional de México (UNAM), utilizado para las elecciones de los representantes estudiantiles de la misma. Este sistema contaba con las características:

- La identidad y la preferencia del voto de la persona son secretos.

- Garantía de la universalidad del voto.
- Uso de protocolos de seguridad electrónicos.
- Los votos son registrados en una urna electrónica protegida a través de un cifrado de datos y algoritmos de seguridad.
- El sistema no permite votar dos veces a un usuario, entre otras.

Para finalizar este estudio sobre procesos de votaciones actuales, es realizaron encuestas sobre las opiniones y consideraciones de los estudiantes de la UCAB en el proceso de elecciones para los representantes estudiantiles del día 31 de Mayo de 2012, en la misma se evaluó el sistema actual con respecto a uno sistematizado, evaluando ítems como:

- Rapidez en el proceso de votación.
- Seguridad y confiabilidad.
- Impresión del voto.

Una vez diseñada la encuesta, fue revisada por la Profesora Mayra Narváez, revisora de este Trabajo Especial de Grado, quedando estructurada como se muestra en la Figura 6.

ENCUESTA ELECCIONES REPRESENTANTES ESTUDIANTILES

UCAB 31 DE MAYO DE 2012

A continuación se le plantean diferentes preguntas relacionadas con las elecciones de representantes estudiantiles de la UCAB, con el fin de sondear la opinión que tienen los estudiantes sobre el mecanismo de votación actual. Marque con una X la opción que más se corresponda con sus consideraciones: **1: MUY EN DESACUERDO, 2: DESACUERDO, 3: INDIFERENTE, 4: ACUERDO, 5: MUY DE ACUERDO.**

	1	2	3	4	5
Estoy conforme con la forma en la que se realizan estas votaciones.					
Considero que son seguras y confiables.					
Opino que el proceso es lento.					
Pienso que implica un gasto excesivo de papel.					
Estoy de acuerdo con que estas elecciones deberían ser en formato digital.					
Considero que serían más seguras y confiables que las tradicionales.					
Creo necesaria la impresión de un comprobante de mi voto.					
Estoy dispuesto en participar en una prueba piloto de Elecciones Digitales.					

Si estás dispuesto, por favor escríbenos tu e-mail para invitarte a participar en un simulacro de Elecciones Digitales en la UCAB para validar un sistema propuesto en nuestra Tesis de Grado: _____

Figura 6: Encuesta Realizada. (Elaboración Propia)

En el Apéndice D se muestran los resultados y análisis obtenidos en cada una de las sentencias realizadas.

III.2 Diseño de un sistema piloto de votaciones para la elección de representantes estudiantiles de la UCAB.

El diseño de este sistema piloto se basó en el proceso para la elección de representantes estudiantiles que se realiza actualmente. Dicha información fue suministrada por Yanira Hernández, Secretaria de la Comisión Electoral de la UCAB, sobre las Elecciones de Representantes Estudiantiles realizadas en el año 2011, en las cuales, cada estudiante tuvo derecho a realizar la votación para escoger tres candidatos para el Consejo Universitario, dos candidatos para el Consejo de Decanato de Desarrollo Estudiantil, dos candidatos para el Consejo de Facultad y dos candidatos para el Consejo de Escuela.

Asimismo, se tomaron en cuenta para este diseño, las opiniones plasmadas en las encuestas realizadas a los participantes de las votaciones del día 31 de Mayo de 2012, en donde se concluyó que los estudiantes están conformes con las características actuales del sistema pero están de acuerdo con que se realicen en formato digital.

La prueba del sistema se realizó entre dos sedes de la UCAB, simulando las votaciones que se realizaron en dicha jornada electoral en la Escuela de Educación de Coro y Caracas, de manera que el sistema diseñado fuera lo más cercano a la realidad.

Los candidatos postulados en el año 2011 para la Escuela de Educación en la UCAB de Caracas y Coro fueron los siguientes:

Postulados para Consejo Universitario:

1. Aguilera del Llano, Gonzalo (Psicología)
2. Antonorsi García, Carlos Felipe (Economía)
3. Correia Carballo, Cristofer Javier (Administración y Contaduría)
4. Gutiérrez Vivas, Gabriel Hernández (Ingeniería en Telecomunicaciones)
5. Martínez Fernández, Jorge Luis (Comunicación Social)
6. Pérez, Edward Jesús (Derecho)

Postulados para Consejo General del Decanato de Desarrollo Estudiantil:

1. Del Castillo, Mercedes (Comunicación Social)
2. García Martínez, Ana Karina (Derecho)
3. Hernández Coronel, Mariana Andrea (Comunicación Social)
4. Pérez Muñoz, Ligia Cristina (Derecho)
5. Sfeir Malavé, Ghesn Daniel (Ingeniería Informática)

Postulados para Consejo de Facultad de Humanidades y Educación:

1. Bastidas Parra, Gabriel Andrés (Comunicación Social)
2. Saim Hostos, Jorge Roberto (Letras)
3. Suarez Ortega, Andrés Rafael (Educación)

Postulados para Consejo de Escuela de Educación Caracas:

1. Cubides Goncalves, Marcos Andrés
2. Flores Padrón, Adolfo.
3. Jiménez Oquendo, Marco Alejandro.
4. Rodríguez Alvarado, Karla Daniela.
5. Travieso Trigo, Natacha.

Postulados para Consejo de Escuela de Educación Coro:

1. Montes, Rolando Alberto.
2. Naveda Sirit, Lilia Yuleima.

La UCAB está registrada en el Sistema en línea de MICROSOFT, el cual le permite realizar a sus estudiantes la descarga de una serie de *software* de manera gratuita. Por esta razón, para el montaje del sistema piloto de votaciones planteado en este Trabajo Especial de Grado, se utilizaron las herramientas de servidores, bases de datos y programas de desarrollo web disponibles en este sistema.

En primer lugar, se instaló el servidor MICROSOFT WINDOWS SERVER 2008 R2, en una máquina virtual de ORACLE VM *Virtual Box*. Este servidor se encarga de alojar la aplicación web y la base de datos que contiene la información pertinente a la prueba piloto de votaciones. (Para más información, ver Apéndice E)

Para el modelo de sistema de votaciones, fue necesario la configuración de dos roles en específico, ofrecidos en este servidor:

- *Domain Name System Server (DNS Server):* es un servicio de resolución de nombres para redes TCP/IP. Su función es traducir una dirección IP a un nombre más sencillo de interpretar. Para este caso se configuró el nombre de dominio: **eleciones-ucab.com** para el ingreso a la aplicación web.

- *Internet Information Server 7.0 (IIS 7.0):* es una infraestructura de un servidor web, el cual integra ASP.NET, que permite tener todas las características necesarias para hospedar contenido web en entornos de producción, ideal para cuando se desea probar aplicaciones web como en el caso de este Trabajo Especial de Grado.

Una vez configurados los roles nombrados anteriormente, se procedió a hacer la instalación de MICROSOFT SQL *Server 2008*, el cual es un sistema de gestión de base de datos. Además, la versión *Express* de esta herramienta se encuentra disponible para descargarla gratuitamente desde la página oficial de MICROSOFT y ésta cumple con los requerimientos necesarios para este tipo de sistemas.

Para el acceso, configuración, administración, y manejo de la base de datos, se utilizó el software SQL *Server Management Studio 2008*. Esta herramienta permite la edición del motor de base de datos que es MICROSOFT SQL *Server 2008*. (Para más información, ver Apéndice E)

Con este software se crearon una serie de tablas que contienen los datos necesarios para realizar las votaciones, mostrados en la Tabla 1.

Nombre de la Tabla	Descripción	Nombre del campos y tipo de dato
Administrador	Contiene el id del lector de resultados y su contraseña correspondiente.	id: nchar(10)
		password: int
Candidato	Contiene los datos de todos los candidatos postulados que se tomaron en cuenta para la simulación.	cédula: int
		nombre: nvarchar(50)
		plancha: nvarchar(50)
		id_cargo: int
		escuela: nvarchar(50)
Cargo	Contiene el nombre y el id del cargo de cada una de las candidaturas propuestas.	id_cargo: int
		descripcion: nvarchar(50)
Claves_AleatoriasCaracas	Contiene claves aleatorias creadas para la sede de Caracas, las cuales son únicas e irrepetibles.	clave: nchar (10)
		status: nchar(10)
		idclave: nchar(10)
Claves_AleatoriasCoro	Contiene claves aleatorias creadas para la sede de Coro, las cuales son únicas e irrepetibles.	clave: nchar (10)
		status: nchar(10)
		idclave: nchar(10)

Tabla 1: Tablas para el Sistema de Votaciones (Elaboración Propia)

Las opciones seleccionadas por cada votante, son insertadas en tablas con campos inicialmente vacíos, estos campos se encuentran en la Tabla 2.

Nombre de la tabla	Descripción	Nombre del campo y tipo de dato
Consejo_Universitario	Contiene el registro de las opciones elegidas por los votantes para cada cargo.	id: int
		opcion11: int
		opcion12: int
		opcion13: int
Consejo_Decanato	Contiene el registro de las opciones elegidas por los votantes para cada cargo.	id: int
		opcion21: int
		opcion22: int
Consejo_Facultad	Contiene el registro de las opciones elegidas por los votantes para cada cargo.	id: int
		opcion31: int
		opcion32: int
Consejo_EscuelaCaracas	Contiene el registro de las opciones elegidas por los votantes para cada cargo en la sede de Caracas.	id: int
		opcion41: int
		opcion42: int
Consejo_EscuelaCoro	Contiene el registro de las opciones elegidas por los votantes para cada cargo en la sede de Coro.	id: int
		opcion51: int
		opcion52: int

Tabla 2: Tablas de registro de votos. (Elaboración propia)

La creación de vistas en SQL *Server Management Studio 2008* son fundamentales para relacionar los datos entre las distintas tablas creadas y de esta forma, se pueden hacer sumatorias de los votos para la posterior totalización de los resultados.

Para el diseño de la aplicación web se hizo uso del programa *Visual Studio 2012*, con la ayuda de una serie de herramientas y controles, se originaron dos interfaces para el sistema de votaciones: una para el votante y otra para el lector de los resultados. (Para más información, ver Apéndice E)

La interfaz del votante consistió en una serie de páginas, donde el usuario pudo procesar su votación de manera rápida y sencilla. En la primera página se le da la bienvenida al participante al sistema y luego procede a seleccionar la sede donde estudia.

En principio, se planeaba que el estudiante para entrar al sistema de votación, ingresara su cédula y una clave para autenticar su identidad, la cual se le haría llegar a cada estudiante vía correo días antes de la jornada electoral. Como este proceso iba a ser algo tedioso y no se tenían definidos previamente los participantes que iban a colaborar en la prueba del sistema, se cambió esta propuesta por la de generar una serie de claves aleatorias que se les entregó a cada participante en el momento de la votación para ingresar al sistema.

Se generaron claves a través de la página: http://www.clavesegura.org/, el cual, es un sitio web que genera, fácilmente, contraseñas seguras para usar en cualquier sitio que se requiera. Para la sede de Caracas, se crearon 105 claves y 27 para la sede simulada de Coro, donde cada una está formada por 8 caracteres, en los que se incluyen letras (mayúsculas y/o minúsculas) y números, lo que le da seguridad al sistema.

De esta manera, se logra que cada participante vote solo una vez, ya que en las tablas en donde se guardan dichas claves, existe un campo llamado status asignado a cada una de éstas. Este campo se encuentra inicialmente en cero y cambia a uno, una vez se haya realizado el voto, negando la posibilidad de usar nuevamente dicha clave. Además, este sistema de claves únicas trae como beneficio que no exista relación alguna entre el votante y las opciones escogidas.

Una vez el participante ingrese a la interfaz de votación, para cada uno de los cargos, se presentan un número de casillas igual a la cantidad de opciones que el votante puede escoger. Estas casillas se muestran en forma de pestañas, en las que se despliegan las opciones a elegir y no se podrá seleccionar a un mismo candidato más de una vez.

En el caso de no tener preferencia por algún candidato en alguna de las casillas destinada para la votación, se deberá seleccionar la opción “Voto Nulo” para que el voto sea procesado correctamente.

Por otra parte, se creó una interfaz para el lector de los resultados, la cual tiene dos funciones. Antes de dar inicio a la jornada electoral, el lector de resultados verifica que la base de datos se encuentra vacía al comprobar que en dicha página no existe registro de voto alguno. Al finalizar el proceso de votación, esta interfaz se utilizó para ver la totalización de los resultados para cada uno de los cargos de la jornada electoral.

En la Figura 7 y 8, se muestran dos diagramas de flujo que representan la funcionabilidad de cada una de las dos interfaces creadas para el sistema piloto de votaciones.

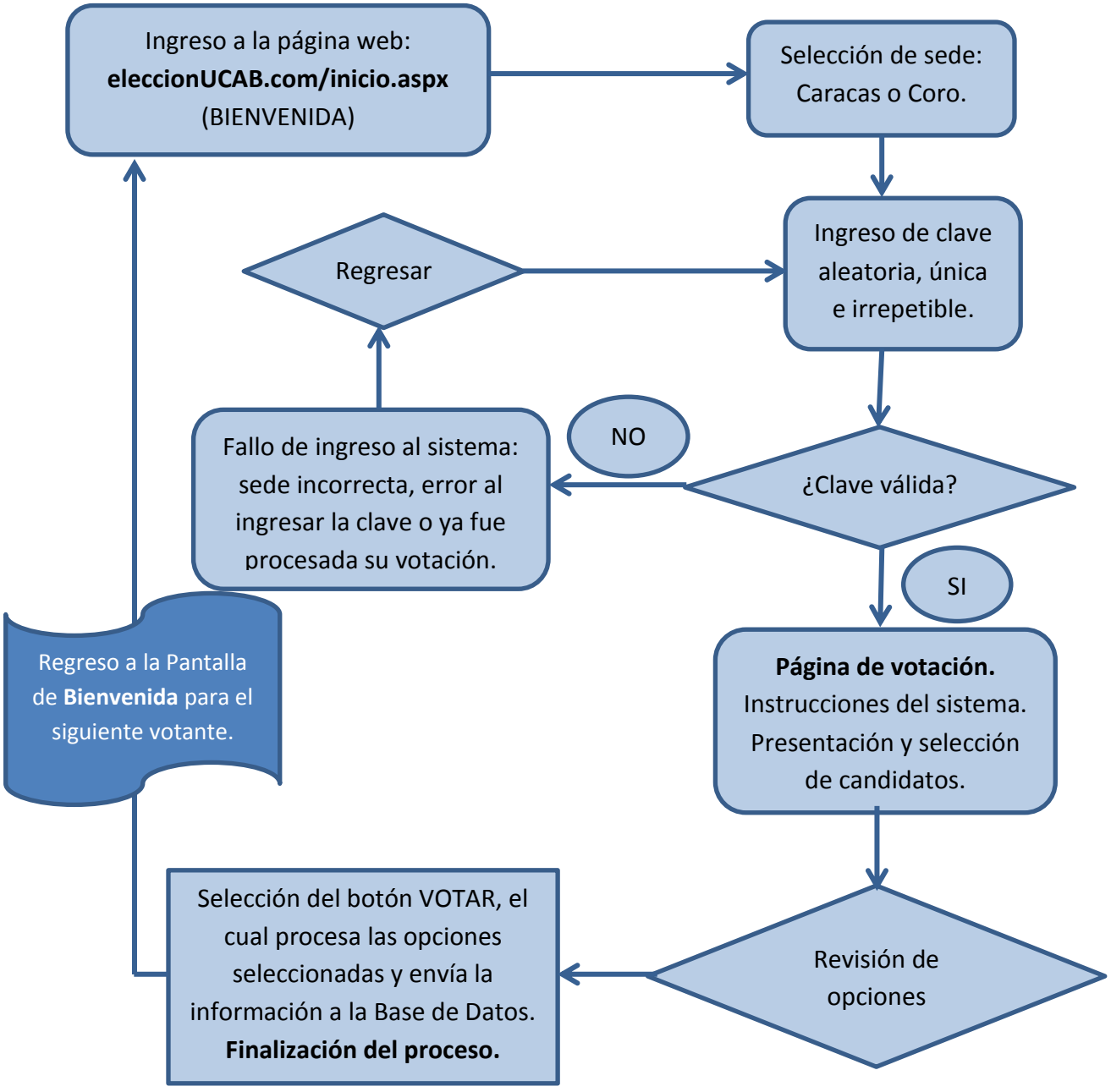

Figura 7: Diagrama de flujo de interfaz de votación (Elaboración propia)

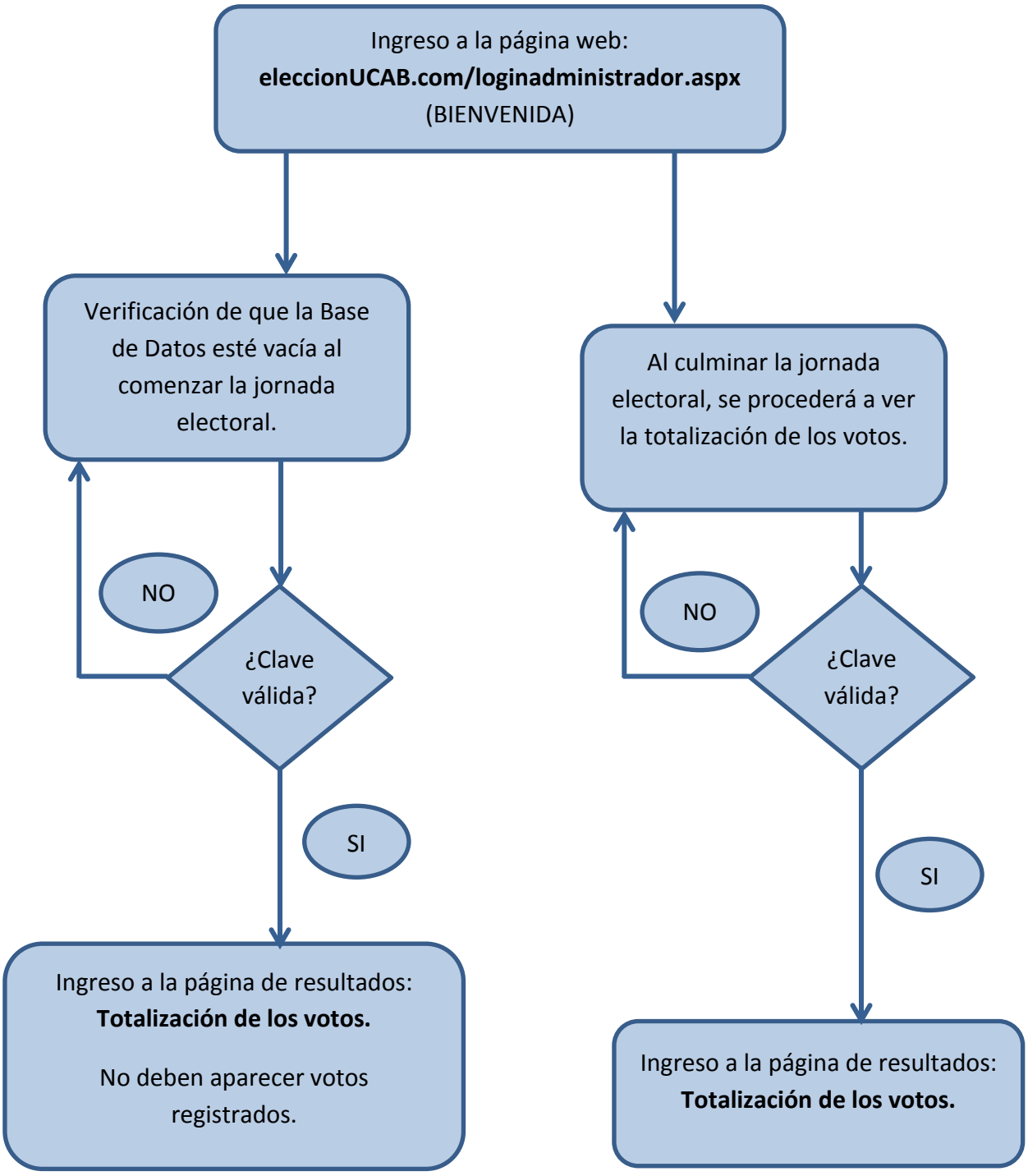

Figura 8: Diagrama de flujo de interfaz del lector de resultados (Elaboración propia)

Cada una de las páginas creadas para el sistema de votación cumple con ciertas funciones, las cuales son las siguientes:

Para la interfaz del votante:

- Inicio: es la pantalla inicial de bienvenida al votante para el sistema de votaciones.
- Sede: en esta página el votante selecciona la sede donde estudia.
- LoginCaracas: se presentan los cargos para la sede de Caracas y el votante ingresa su respectiva clave.
- LoginCoro: se presentan los cargos para la sede de Coro y el votante ingresa su respectiva clave.
- EleccionCaracas: se dan instrucciones del proceso de votación, se muestran fotos de los candidatos postulados para la sede de Caracas y se procede a realizar la votación.
- ElecciónCoro: se dan instrucciones del proceso de votación, se muestran fotos de los candidatos postulados para la sede de Coro y se procede a realizar la votación.
- Fallo: es una pantalla de error al ingresar al sistema debido a alguna de las siguientes razones: el votante seleccionó la sede equivocada, ingresó la clave incorrecta o ya fue procesada su votación.

Para la interfaz del lector de resultados:

- LoginAdministrador: sirve para el ingreso de usuario y contraseña por parte del lector de resultados.
- Resultados: es la página que refleja la totalización de resultados de votación por cargo con sus respectivos candidatos.

III.3 Estudio de los protocolos de seguridad en redes.

Se realizó un estudio acerca de los diferentes protocolos de seguridad existentes, centrando la investigación en aquellos que refieren al uso e implementación de Redes Privadas Virtuales (RPV, de sus siglas en Inglés VPN), siendo este el medio de conexión entre las sedes de la UCAB.

Se eligió el uso de VPN para el diseño del sistema de comunicaciones seguro, debido a sus múltiples beneficios como bajos costos, escalabilidad, flexibilidad y fácil aplicabilidad. Además, garantiza beneficios de seguridad como autenticación, autorización, integridad de la información, confidencialidad y el no repudio de la información.

Entre las arquitecturas de conexión existentes, se encuentran VPN de acceso remoto, VPN punto a punto, VPN *over* LAN y *Tunnelling*. De estos se eligió el *Tunnelling*, que es el tipo de VPN más utilizado, el cual se basa en la utilización de tres protocolos, uno portador en el que viaja la información, uno encapsulador que se superpone a los datos y uno pasajero que se encarga de transportar los datos.

Todo el proceso de *Tunnelling* se centra en el protocolo encapsulador, el cual se va a encargar de la encriptación, seguridad, autenticación, e integridad de los datos. En la tabla 4 se muestran la comparación de las características de los protocolos encapsuladores.

Protocolo	Autenticación	Integridad	Encriptación
L2F	✓	✗	✗
L2TP	✓	✗	✗
SSH	✓	✓	✓
IPSEC	✓	✓	✓

Tabla 3: Comparación protocolos encapsuladores (Elaboración propia)

III.4 Diseño de un sistema piloto de seguridad entre las sedes de la UCAB.

Realizado el estudio anterior, se concluyó que los protocolos encapsuladores que cumplen con los parámetros de seguridad requeridos a la hora de transmitir los datos por un medio no seguro, como lo es el Internet, fueron SSH e IPsec, y se procedió a realizar la comparación entre sus diferentes protocolos, plasmada en la Tabla 4.

SSH	**IPsec**
SSH 1 • Integridad: CRC. • Autenticación: claves asimétricas RSA. • Confidencialidad: 3DES y *Blowfish*.	**AH** • Integridad: MD5 y SHA. • Autenticación: PSK y RSA. • Confidencialidad: No tiene. • DH: DH1, DH2, DH5, DH7.
SSH 2 • DSA Y DH para intercambio de claves. • Integridad: HMAC. • Autenticación: Kerberos.	**ESP** • Integridad: MD5 y SHA. • Autenticación: PSK y RSA. • Confidencialidad: DES, 3DES, AES, SEAL • DH: DH1, DH2, DH5, DH7.

Tabla 4: Comparación SSH y IPSEC (Elaboración propia)

Contrastando las ventajas ofrecidas por cada uno de ellos, se seleccionó IPsec sobre SSL, ya que no está obligado a ningún tipo de cifrado, autenticación, algoritmos de seguridad o intercambio seguro de claves específico, con lo cual, se adapta de manera más adecuada a cualquier tipo de sistema en el que se quiera implementar.

Respecto a la confidencialidad, se logra mediante la encriptación del tráfico mientras viaja a través de la VPN, y depende de la longitud de la clave de algoritmo del cifrado.

La integridad se logra mediante los códigos de autenticación de mensajes *HASH*, en el cual un miembro de la comunicación toma el mensaje y una clave secreta y los procesa a través de un algoritmo hash, generando un valor que se añade al mensaje y se envía a través de la red. En miembro receptor, se vuelve a calcular el valor de hash y se compara con el recibido, quedando verificada la integridad del mensaje en el caso que sean iguales.

Para autenticar, el remitente hace uso de una clave privada de cifrado llamada firma digital, que es autenticada en el receptor haciendo uso de la clave pública del remitente.

El intercambio de claves es necesario para algoritmos de cifrado que exigen una clave compartida secreta simétrica, como lo son DES, 3DES, AES, y algoritmos de *hash* MD5 y SHA-1. Para hacerlo, IPsec se basa en el uso de *Diffie-Hellman* que es un método de intercambio de claves que proporciona los mecanismos necesarios para que los miembros establezcan una clave secreta compartida que solo ellos conocen, a pesar de estar comunicados por un canal inseguro.

Entre las dos opciones de IPsec se decidió aplicar el ESP, ya que el AH no ofrece confidencialidad. ESP proporciona confidencialidad al realizar el cifrado del paquete IP, ocultando la carga de datos y la identidad de la fuente y destino. Con esto, proporciona autenticación al paquete interno IP y genera una cabecera ESP, como se muestra en la Figura 9.

<table>
<tr><th>0-7 bit</th><th>8-15 bit</th><th>16-23 bit</th><th>24-31 bit</th></tr>
<tr><td colspan="4">Security Parameters Index (SPI)</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Payload data (Variable)</td></tr>
<tr><td colspan="4">Padding (0-255 bytes)</td></tr>
<tr><td colspan="2"></td><td>Pad Length</td><td>Next Header</td></tr>
<tr><td colspan="4">Authentication Data (Variable)</td></tr>
</table>

Figura 9: Diagrama de Paquete ESP (Elaboración propia)

En el cual *SPI* identifica los parámetros de seguridad en combinación con la dirección IP, *Sequence number* es un número creciente utilizado para evitar ataques de repetición, *payload data* contiene los datos a transferir, *padding* es utilizado para rellenar por completo los bloques, *pad length* es un tamaño de relleno en *bytes*, *Next header* identifica el protocolo de los datos transferidos, y *Authentication data* contiene los datos utilizados para autenticar el paquete.

El proceso de establecimiento de un túnel IPsec comienza cuando uno de los miembros de la comunicación envía un tráfico interesante a otro miembro. Para que un tráfico sea considerado interesante, debe viajar entre dos miembros que utilicen IPsec y estar dentro de los criterios de la lista de acceso de la VPN.

El intercambio de claves se realiza por medio de una red pública, donde se deben negociar parámetros entre ambos miembros de la comunicación, conocidos como asociaciones de seguridad (SA). Las SA negocian el establecimiento de las políticas de seguridad IKE, la cual, combina protocolos de intercambio de claves con ISAKMP. Esta última, se encarga de definir el formato del mensaje, los protocolos de intercambio de claves y el proceso de negociación para la creación de SA.

Para establecer un canal de comunicación seguro, el protocolo IKE se ejecuta en dos fases:

En la primera fase, se realizan las negociaciones iniciales de las SA, pudiendo ser implementado en el modo principal (antes del contacto inicial) o de modo agresivo (después de iniciar el contacto). En el modo principal se realiza en tres intercambios:

- En el primer intercambio se establecen las políticas de seguridad básicas, negociando y acordando los algoritmos *hash* que se utilizan para proteger las comunicaciones IKE. Luego se transmiten las opciones de encriptación y autenticación a utilizar del emisor, buscando el receptor las políticas de ISAKMP coincidentes. Una coincidencia se logra cuando tienen la misma encriptación, hash, autenticación y valores de parámetros DH. El parámetro de tiempo de vida puede ser diferente entre ambos miembros y se utilizará el que tenga el tiempo de vida más corto. Sí una política coincide entre los pares, la fase 1 IKE continua. En la Tabla 5, se presentan los parámetros de la política ISAKMP establecidos en ambos enrutadores. La configuración completa de ambos se encuentra en el Apéndice F.

Numero de Política	10
Autenticación	Claves Pre compartidas
Encriptación	AES 256
Grupo DH	2
Hash	MD5
Tiempo de Vida	3600 segundos

Tabla 5: Directivas ISAKMP (Elaboración Propia)

- En el segundo intercambio, se ejecuta el protocolo de intercambio de claves DH para adquirir las claves necesarias para algoritmos de *hashing* y encriptación.
- En el tercer intercambio, se autentican los dispositivos finales, para luego considerar la ruta de comunicación segura. Culminando la fase 1 IKE.

En modo agresivo, las negociaciones se realizan de forma más rápida que la principal debido a que se comprimen las fases de negociación en tres paquetes, el primer paquete es enviado por el emisor y contiene todos los paquetes para la negociación SA, incluyendo su clave DH pública. Para el segundo paquete, el emisor recibe la información, compara con sus políticas de seguridad, y responde con los parámetros aceptables, información de autenticación y su clave DH pública. En un tercer paquete, el emisor envía una confirmación de que ha recibido la información, y verifica la identidad del otro miembro. Al recibir esta información el miembro receptor, auténtica el otro miembro y culmina la fase IKE 1.

La fase 2 IKE se encarga de negociar los parámetros de seguridad IPsec, IPsec *transform set*, que serán aplicados al tráfico que circule por la interfaz y finalmente establecer el IPsec. En el caso de los *transform set* se seleccionaron en ambos enrutadores: *aes 256 esp-md5-hmac*. Cada cierto tiempo son renegociados los SA IPsec para garantizar la seguridad del sistema o cuando el tiempo de vida de una SA IPsec expira.

Todo este proceso de intercambio de claves y establecimiento del túnel IPsec es explicado gráficamente en la Figura 10.

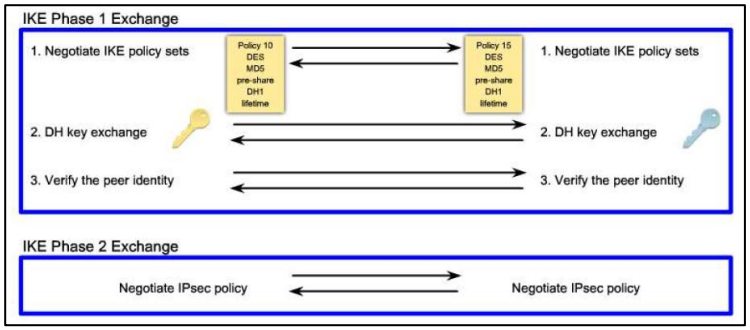

Figura 10: Fase IKE modo principal. (Stewart, 2009)

III.5 Aplicación de la prueba del sistema de votaciones.

En conversaciones con el Ingeniero Jorge García, Jefe de Redes y Seguridad de la Dirección de Tecnologías de Información de la UCAB, se constató que existen conexiones VPN establecidas entre la sede de UCAB Montalbán con UCAB Coro, UCAB Los Teques y el Centro Internacional de Actualización Profesional (CIAP), ubicado en La Castellana.

Se optó por realizar la prueba al sistema de votaciones diseñado, usando la conexión VPN existente entre las sedes de UCAB Montalbán y CIAP La Castellana, debido a que ambas se encuentran ubicadas en Caracas. Dicha conexión se establece mediante el protocolo IPsec, tal y como se diseñó para el sistema de comunicaciones planteado.

El servidor web fue alojado en la red interna de la UCAB Montalbán para proceder a la realización de las pruebas pertinentes. En primer lugar, se logró conectar el mismo en una de las oficinas de la Escuela de Ingeniería en Telecomunicaciones, logrando acceder desde cualquier computador perteneciente a la red interna de dicha sede, registrándose algunos votos. En la sede de La Castellana no se logró realizar una prueba simultánea al sistema, debido a políticas de seguridad en las redes internas, establecidas por el DTI.

Por el motivo expuesto anteriormente, hubo la necesidad de realizar una segunda prueba, en la cual se conectó el servidor web en las oficinas del DTI, logrando acceder al sistema de votación en ambas sedes. En la UCAB de Montalbán, las votaciones se realizaron desde computadores ubicados en la Escuela de Ingeniería en Telecomunicaciones y en la sede del CIAP La Castellana, Mónica Nobrega, Analista de Logística y Ejecución, suministró un espacio físico para realizar dichas pruebas.

Es importante resaltar que el sistema mantuvo el registro de los votos realizados en la primera prueba en la sede de UCAB Montalbán.

Estando en funcionamiento el sistema, las votaciones estuvieron basadas en los siguientes parámetros:

- **Inicialización del proceso de votación:** se verificó que estuviera vacía la tabla que contienen el registro de los votos en la base de datos.
- **Requerimientos para la prueba piloto:** por ser una prueba piloto, se solicitó la colaboración por parte de estudiantes, profesores y personal de trabajo de cada una de las sedes. Dichos participantes colocaron su respectivo nombre, número de cédula y firma en el Listado de Electores. (Ver Apéndice G)
- **Acceso al sistema:** luego de registrarse en el Listado de Electores, el votante retiró una de las claves contenidas en un recipiente para proceder a ingresar al sistema de votaciones.
- **Selección de candidatos:** una vez el votante haya introducido correctamente su clave, se le desplegará en pantalla las instrucciones del sistema y las opciones a las que tiene derecho a votar.
- **Registro del voto en el sistema:** cuando el votante haya verificado todas las opciones escogidas, deberá presionar el botón VOTAR para que quede registrado el voto en la base de datos. La clave utilizada para ingresar al

sistema, debe ser introducida por el estudiante en la urna electoral destinada para este fin.

- **Finalización del proceso de votación:** al culminar el tiempo pautado para la prueba piloto, se realizó el cierre de la votación, para proceder con la generación de resultados y la auditoría del sistema.
- **Generación de Resultados:** el lector de resultados introdujo el nombre de usuario y contraseña respectivamente para acceder a la totalización del sistema, el cual mostró en pantalla los votos obtenidos por cada candidato en su respectivo cargo.
- **Auditoria del sistema:** al finalizar el proceso, se abrió la urna electoral que contuvo las claves utilizadas y se verificó que coincidía con la cantidad de personas registradas en el Listado de Electores y en la totalización de resultados del sistema.

III.6 Generación de instructivo de instalación del sistema.

Una vez desarrollado el sistema piloto de comunicación segura para votaciones entre las sedes de la UCAB, se realizaron dos instructivos de cada una de las fases necesarias para la obtención del producto final planteado en este Trabajo Especial de Grado.

En primera instancia, se describieron todos los pasos que dieron lugar a la creación del sistema de votaciones, conformado por la instalación del servidor WINDOWS *Server 2008*, el manejo de bases de datos en SQL *Server Management Studio 2008* y el desarrollo de una aplicación web usando la herramienta *Visual Studio 2012*, la cual englobó las interfaces para la elección de los representantes estudiantiles.

En segunda instancia, se describieron los pasos a seguir para la configuración de cada uno de los parámetros de interés, que conllevan al correcto establecimiento de

un túnel IPsec en enrutadores Cisco, los cuales son utilizados para establecer las conexiones entre las sedes de la UCAB.

III.7 Generación de conclusiones y recomendaciones.

Se recolectaron los resultados globales obtenidos en el desarrollo de un sistema piloto de comunicación segura para el transporte de datos en votaciones entres las sedes de la UCAB, para su análisis y generación de conclusiones.

Por otra parte, se generaron las recomendaciones de acuerdo a las experiencias obtenidas para posteriores estudios relacionados con el tema tratado en este Trabajo Especial de Grado.

III.8 Realización del Tomo.

Se unieron todas las fases anteriores en un tomo que dio por finalizado el Trabajo Especial de Grado.

CAPITULO IV

RESULTADOS

En este capítulo se describen los productos que se obtuvieron al realizar cada una de las fases planificadas, las cuales dieron lugar al cumplimiento de todos objetivos planteados.

El conjunto de logros alcanzados, permitió la obtención de un sistema piloto de comunicación segura para el transporte de datos en votaciones entre las sedes de la UCAB, el cual fue comprobado a través de un sistema de votaciones para la elección de representantes estudiantiles.

Para esto, se instaló un servidor web en la sede de UCAB Montalbán, el cual alojaba una base de datos que contuvo todos los datos necesarios para realizar dichas votaciones y se verificó que la información se transmitió desde la sede del CIAP a dicho servidor de manera segura a través del túnel VPN existente entre ambas localidades.

A continuación, se detallan los resultados obtenidos a partir de cada objetivo específico planteado:

IV.1 Verificar los sistemas de votaciones desarrollados en la UCAB y otras universidades del país.

Fueron verificados los sistemas de votación desarrollados en la UCAB y en otras universidades del país, así como también los sistemas electrónicos de votación desarrollados en Venezuela y alrededor del mundo para lograr obtener y aplicar estos conocimientos de experiencias anteriores al sistema diseñado.

Del sistema de la UCAB se tomaron en cuenta todas las normativas y parámetros que se tienen al momento de realizar unas elecciones estudiantiles, para realizar un sistema con características lo más cercanas posible al del sistema actual.

Por otra parte, se realizaron encuestas a 194 estudiantes participantes en las votaciones para los representantes estudiantiles de la UCAB en la sede Montalbán, con el objetivo de recolectar opiniones sobre el sistema actual y las consideraciones que tendrían si se digitalizara dicho proceso.

Entre los resultados obtenidos en estas encuestas, se pudo observar que un porcentaje del 77,83% de los participantes están conformes en la forma en la que se realizan estas encuestas y un 74,23% del total de los encuestados considera que son seguras y confiables. Sin embargo, un 13,92% piensa que el proceso de votación se torna lento.

Un porcentaje del 55,67% de los participantes de las encuestas realizadas, consideraron que el sistema actual implica un gasto excesivo de papel, ya que estas votaciones se realizan de forma física, a través de papeletas.

Otra de las observaciones que se obtuvo al realizar estas encuestas, fue que el 74,75% de los encuestados estarían de acuerdo con realizar estas elecciones en formato digital. Sin embargo, un 57,73% del total de los participantes, opinaron que serían más seguras y confiables que las tradicionales.

Con respecto a la impresión del comprobante de voto, en caso de usar un formato digital en estas votaciones, una porción del 43,81% de los encuestados lo consideraron necesario y un 35,05% opinó lo contrario, por lo que no se vio una tendencia concluyente en la evaluación de este ítem.

Todos los resultados obtenidos al evaluar las diferentes características del sistema actual y compararlo con uno en formato digital, fueron usados al diseñar el sistema de

votaciones que se plantea en este Trabajo Especial de Grado. Para información más detallada sobre las encuestas realizadas, ver Apéndice D.

Del sistema de votaciones realizadas en Madrid se tomó en cuenta la forma en que se realizaba el proceso de claves aleatorias para el ingreso al sistema, adaptándolo al modelo que se desarrolló.

El sistema de votaciones implementado por la UNAM y el diseñado en el Trabajo Especial de Grado titulado "*Diseño de un sistema electoral para la Asociación de Egresados de la UCAB utilizando la plataforma de telecomunicaciones existente*", sirvieron de base para el diseño, planificación y configuración del sistema propuesto para la elección de representantes estudiantiles.

IV.2 Desarrollar un sistema de votaciones para la elección de los representantes estudiantiles en la UCAB.

Se diseñó una aplicación con el uso del lenguaje de programación *Visual Basic* .NET y las diversas herramientas que ofrece el *software Visual Studio*, dando lugar a dos interfaces: una para el votante y una para el lector de los resultados. (Para sobre los códigos de las interfaces, ver Apéndice H)

Cada una de las interfaces creadas para el sistema de votación cumple con ciertas funciones, las cuales se describen a continuación con su respectiva representación gráfica:

IV.2.1 Interfaz del votante

- Inicio: es la pantalla inicial de bienvenida al votante para el sistema de votaciones, como se muestra en la figura 11.

Figura 11: Interfaz Inicial sistema de votaciones (Elaboración propia)

- Sede: en esta página el votante selecciona la sede donde estudia, como se puede observar en la figura 12, teniendo entre las opciones Caracas y Coro.

Figura 12: Interfaz de selección de sedes (Elaboración propia)

- LoginCaracas: se presentan los cargos a elegir para los votantes de la sede de Caracas, y el campo donde el votante ingresa su respectiva clave, como se puede apreciar en la figura 13.

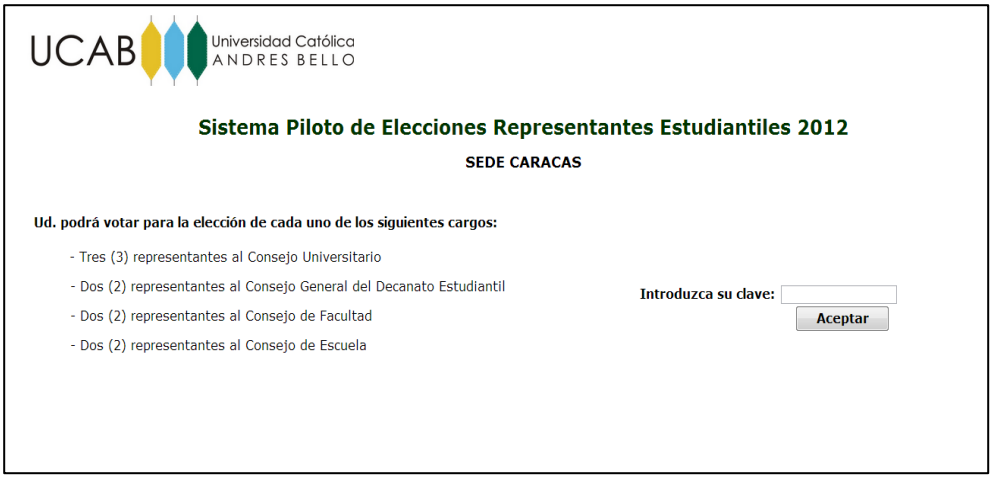

Figura 13: Interfaz de acceso al sistema sede Caracas (Elaboración propia)

- LoginCoro: se presentan los cargos a elegir para los votantes de la sede de Coro, y el campo donde el votante ingresa su respectiva clave, como se puede apreciar en la figura 14.

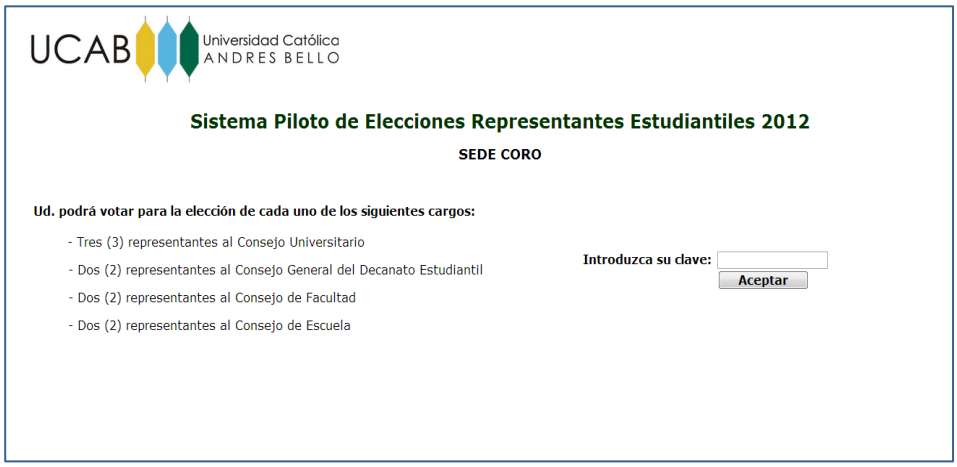

Figura 14: Interfaz de acceso al sistema sede Coro (Elaboración propia)

- EleccionCaracas: se suministran instrucciones del proceso de votación, información de los candidatos postulados para la sede de Caracas y se encuentra el botón con el que se realiza la votación, como se muestra en la figura 15.

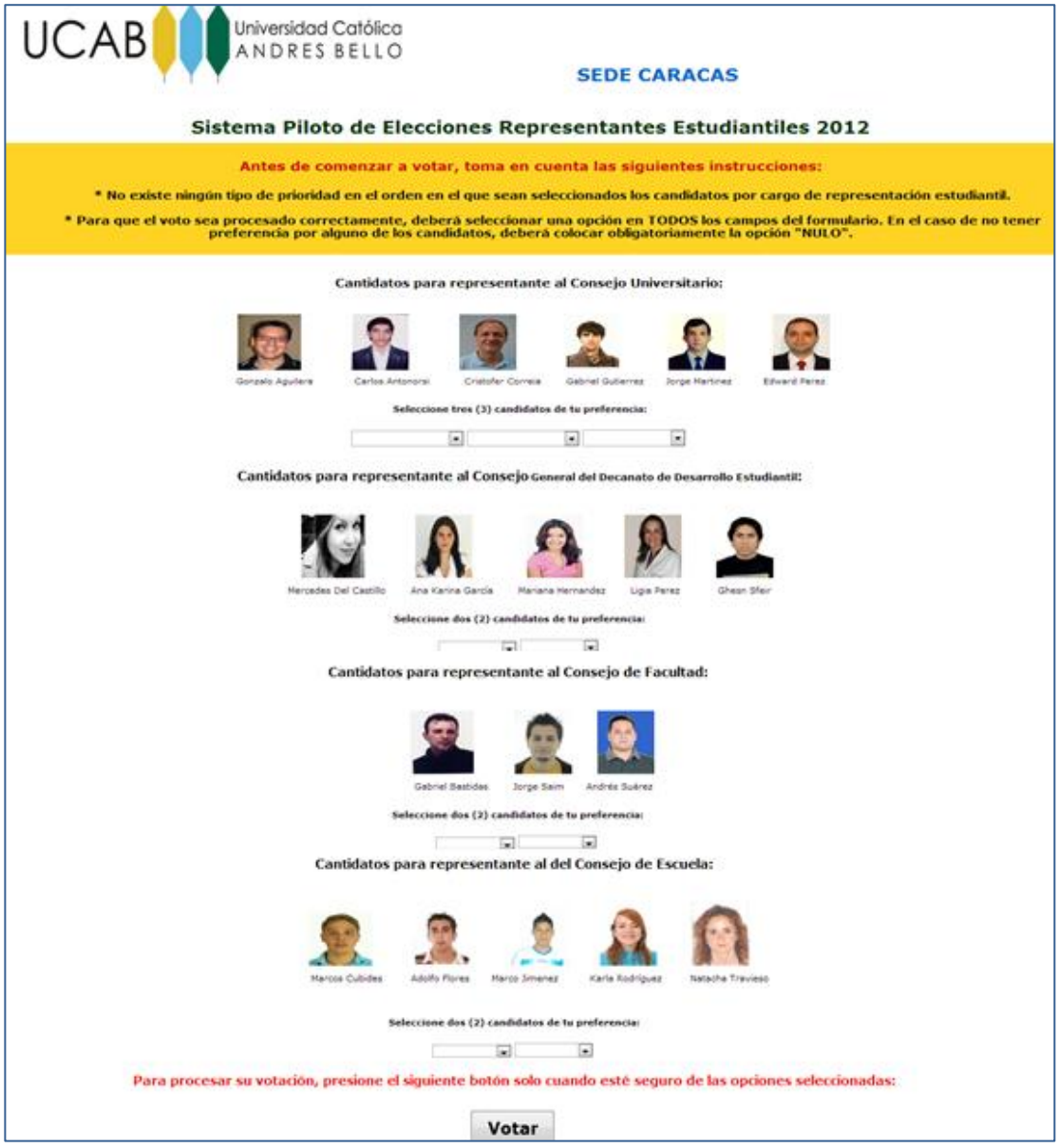

Figura 15: Candidatos a la Representación Estudiantil sede Caracas (Elaboración propia)

- ElecciónCoro: se suministran instrucciones del proceso de votación, información de los candidatos postulados para la sede de Caracas y se encuentra el botón con el que se realiza la votación, como se muestra en la figura 16.

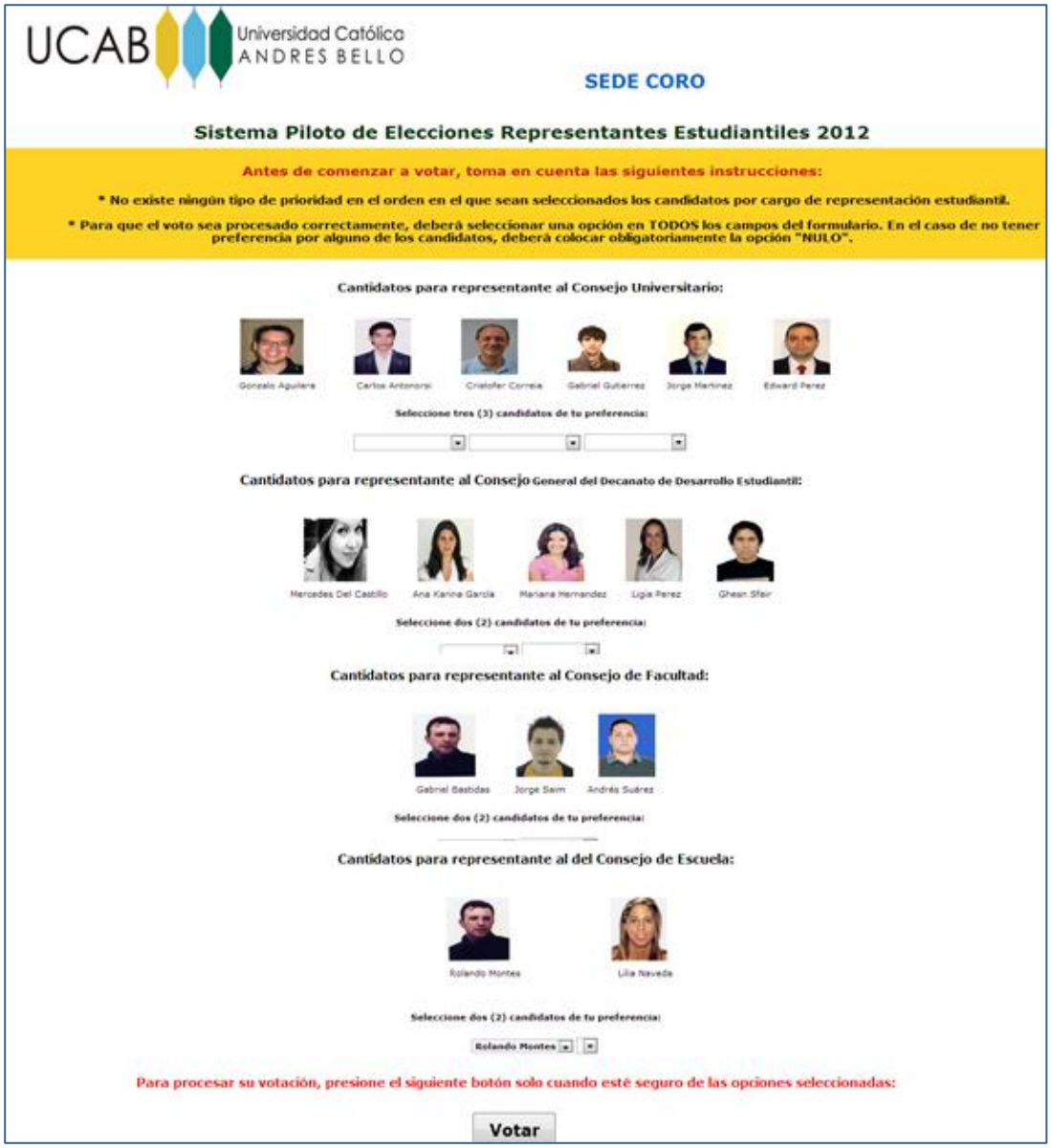

Figura 16: Candidatos a la Representación Estudiantil sede Coro (Elaboración propia)

- Fallo: es una pantalla de error al ingresar al sistema debido a alguna de las siguientes razones: el votante seleccionó la sede equivocada, ingresó la clave incorrecta o ya fue procesada su votación, mostrada en la figura 17.

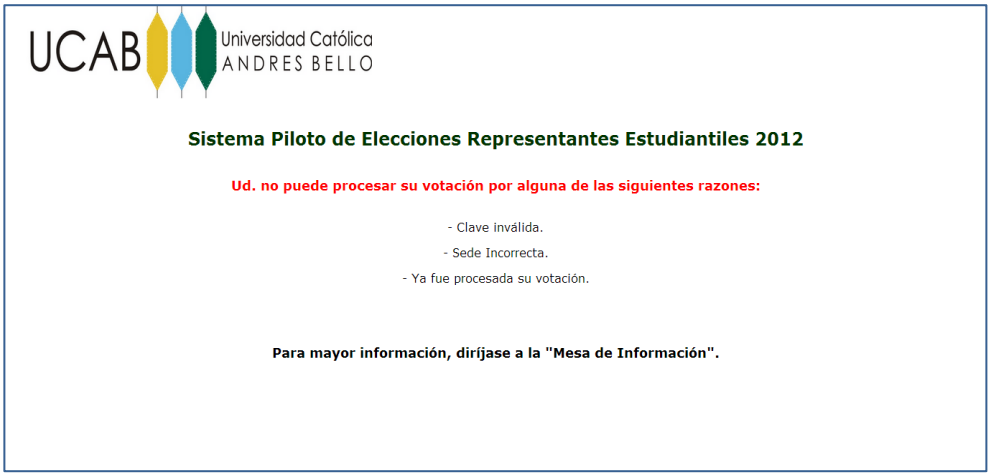

Figura 17: Interfaz de fallo al ingresar al sistema (Elaboración propia)

V.2.2 Interfaz del lector de resultados

- LoginAdministrador: sirve para el ingreso de usuario y contraseña por parte del lector de resultados, dicha interfaz se muestra en la figura 16.

Figura 18: Interfaz Inicial lector de resultados (Elaboración propia)

- Resultados: es la página que refleja la totalización de resultados de votación por cargo con sus respectivos candidatos, como se observa en la figura 19.

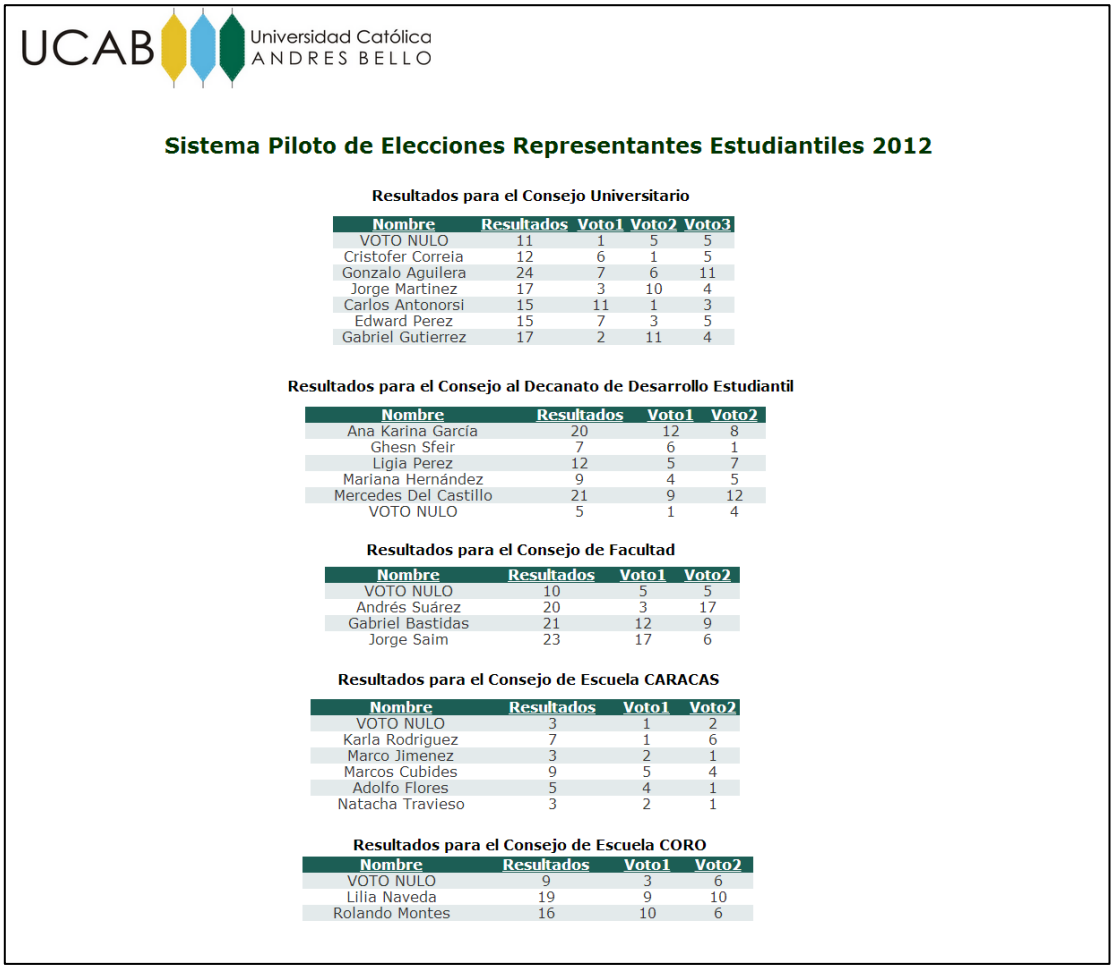

Figura 19: Interfaz de Totalización de resultados (Elaboración Propia)

Para hospedaje de la aplicación web creada, se realizó la instalación de un servidor que integró características de servicio web y DNS. Además, dicho servidor actuó como recolector de la información usada en la votación y de los resultados obtenidos en la misma, a través de la configuración de una base de datos.

IV.3 Diseñar un modelo de sistema de comunicaciones para las votaciones entre las distintas sedes de la UCAB.

Luego de estudiar los protocolos de seguridad en redes existentes en la actualidad, se decidió diseñar una conexión VPN con otras sedes utilizando IPsec, dicha conexión fue simulada en el programa *Cisco Packet Tracer*, como se muestra en la figura 20.

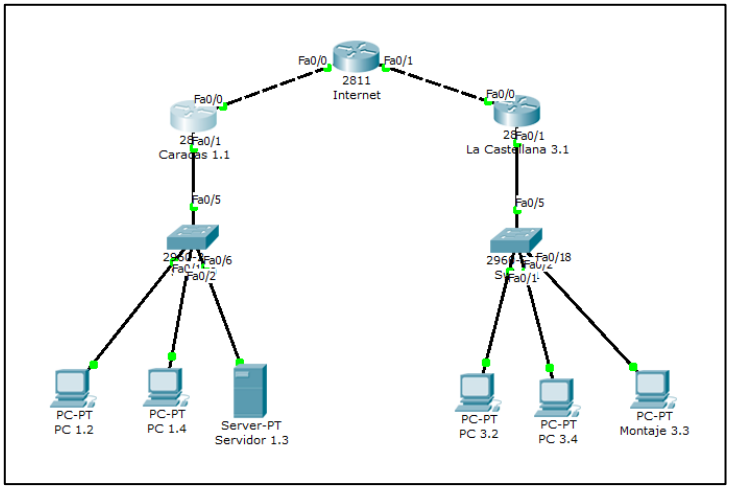

Figura 20: Topología de Diseño. (Elaboración Propia)

La configuración IP de los equipos, se encuentra en la tabla 6.

Dispositivo	Interfaz	Dirección IP	Máscara
Caracas 1.1	Fa 0/0	10.1.1.1	255.255.255.252
	Fa 0/1	192.168.1.1	255.255.255.0
PC 1.2	NIC	192.168.1.2	255.255.255.0
Servidor 1.3	NIC	192.168.1.3	255.255.255.0
PC 1.4	NIC	192.168.1.4	255.255.255.0
Internet	Fa 0/0	10.1.1.2	255.255.255.252
	Fa 0/1	10.2.2.2	255.255.255.252
Los Teques 2.1	Fa 0/0	10.2.2.1	255.255.255.252
	Fa 0/1	192.168.3.1	255.255.255.0

PC 3.2	NIC	192.168.3.2	255.255.255.0
Montaje 3.3	NIC	192.168.3.3	255.255.255.0
PC 3.4	NIC	192.168.3.4	255.255.255.0

Tabla 6: Direcciones IP de Diseño. (Elaboración propia)

Se realizaron cuatro demostraciones del establecimiento y funcionamiento del túnel IPsec:

1. Se realizó un *tracert* o rastreo de la ruta entre el servidor (servidor 1.3) de la red de Caracas y uno de los computadores (Montaje 3.3) ubicado en la red de la castellana, sin el túnel IPsec, para observar cuales fueron los saltos a realizar por el paquete para llegar a su destino, como se muestra en la figura 21.

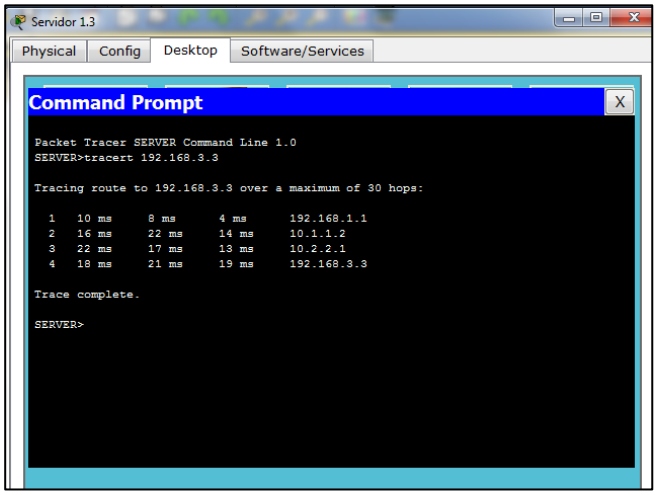

Figura 21: Tracert red Caracas a red La Castellana sin IPsec (Elaboración Propia)

Se observó como el paquete de datos para llegar al destino, pasa por el enrutador de la red de origen, luego da distintos saltos en su paso por Internet (representado por un enrutador), y finalmente llega al enrutador de la red de destino, el cual se encarga de entregar el paquete al dispositivo final ubicado en la castellana. En su recorrido realiza un total de tres saltos.

La simulación se desarrolló en una red pequeña, pero cuando se hace un *tracert* en una red operativa con acceso a Internet, este número de saltos aumenta considerablemente.

En el caso de utilizar un túnel IPsec, el rastreo de la ruta cambia, y todos los saltos que el paquete de datos realice entre el enrutador de origen y destino son transparentes para el dispositivo final, realizando solamente dos saltos, como se observa en la figura 22.

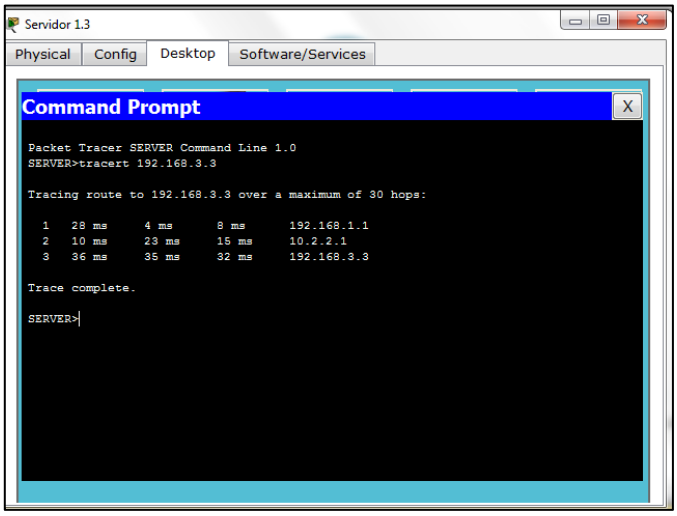

Figura 22: Tracert red Caracas a red La Castellana con IPsec. (Elaboración Propia)

2. Se observaron los pasos que realiza el enrutador de Caracas una vez que verifica que esta en presencia de un tráfico interesante para IPsec. como se muestra en la figura 23.

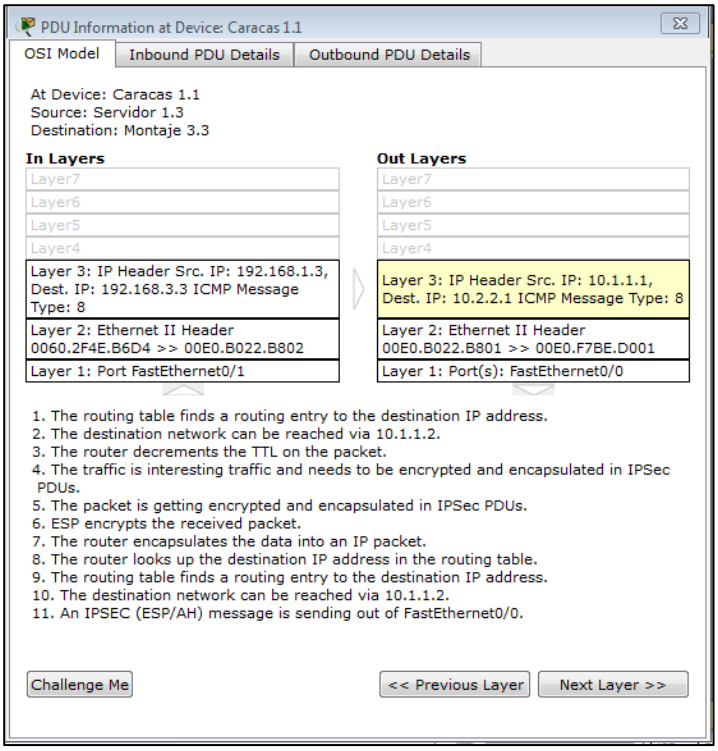

Figura 23: Información del PDU del enrutador sede Caracas (Elaboración propia)

Entre los puntos 1 y 3, el enrutador ejecuta el proceso de búsqueda de destino del paquete de datos en su tabla de enrutamiento, una vez conseguida la red de destino, decrementa el tiempo de vida del paquete para que sea enviado por la interfaz correspondiente.

Luego, entre los puntos 4 y 7, se detecta que el tráfico es interesante por lo que es necesario encriptarlo y encapsularlo en una PDU de IPsec. El protocolo ESP encripta el paquete recibido y lo encapsula en un paquete IP.

Finalmente, entre los puntos 8 y 11, se realiza el proceso de búsqueda en la tabla de enrutamiento hasta encontrar la dirección IP de destino, como la red puede ser alcanzada, el paquete es enviado.

3. Se verificó el establecimiento de las políticas de seguridad *isakmp*, con el comando *show crypto isakmp sa*, como no se ha enviado ningún tráfico

interesante, en la figura 24 no se muestra información como origen y destino del intercambio de claves, estado, identificador de la conexión (*conn-id*) y estatus.

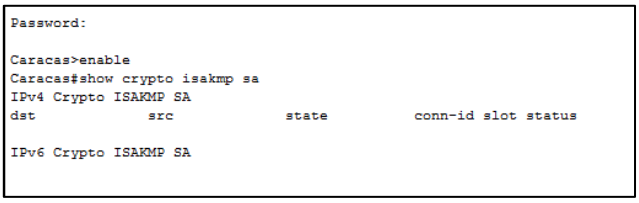

Figura 24: show crypto isakmp sa antes de tráfico interesante (Elaboración propia)

Al realizar un *ping* entre las dos redes definidas en la lista de acceso, una asociación de seguridad (SA) es establecida, la información de su establecimiento es mostrado en la figura 25. Se muestra la información de las direcciones IP de origen y destino, el indicador de conexión (*con-id*) en "*QM_IDLE*" que nos indica que las fases 1 y 2 IKE se han completado con éxito, y el *status* en *ACTIVE* nos indica que la conexión se encuentra activa.

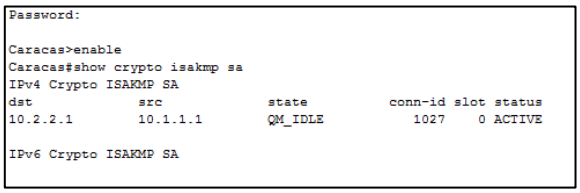

Figura 25: show crypto isakmp sa luego de tráfico interesante (Elaboración propia)

4. Mediante el *show crypto IPsec sa*, se pueden observar las políticas IPsec establecidas, tal como se muestra en la figura 26.

```
Caracas>enable
Caracas#show crypto ipsec sa

interface: FastEthernet0/0                                                    (1)
    Crypto map tag: MYMAP, local addr 10.1.1.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)         (2)
  remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer 10.2.2.1 port 500
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0                          (3)
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

    local crypto endpt.: 10.1.1.1, remote crypto endpt.:10.2.2.1              (4)
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
    current outbound spi: 0x0(0)

    inbound esp sas:                                                          (5)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:

    outbound ah sas:

    outbound pcp sas:
```

Figura 26: Show crypto IPsec sa en enrutador Caracas (Elaboración Propia)

En (1) se muestra la interfaz a la que corresponde establecer la comunicación, el *crypto map* llamado *MYMAP* que se encuentra habilitado, y la dirección IP que utilizó el enrutador local para establecer la conexión.

En (2) se pueden observar las redes involucradas en la comunicación y el enrutador de destino.

En (3) si la conexión es establecida correctamente, entre otras informaciones, se muestra el número de paquetes que han sido encriptados, desencriptados, encapsulados y desencapsulados, así como también los que han tenido errores, enviados y recibidos. En este caso como no se ha enviado

un tráfico interesante entre las redes involucradas todos los valores anteriormente mencionados se encuentran en cero.

En (4) están los puntos finales locales y remotos para la conexión IPsec, así como el MTU utilizado.

Finalmente en (5), se muestran los 2 grupos de asociaciones de seguridad para cada túnel, uno de entrada y uno de salida. Ambos tienen dos secciones, una para tráfico ESP y otra para tráfico AH.

Se realiza un *ping* entre las 2 redes consideradas en las listas de acceso, y se introduce nuevamente el comando *show crypto IPsec sa*, generando la figura 27, se observó que los valores de paquetes encapsulados, encriptados, y desencapsulados han cambiado, así como también se muestra que ocurrió un error en uno de los paquetes, esto se debe a que es el primer *ping* que se envía y los enrutadores están construyendo sus tablas de enrutamiento y se pierden paquetes.

También se pudo observar en detalle las características del tráfico ESP entrante y saliente, mostrando los valores aplicados para el encriptado como lo son los c*rypto map*, los protocolos de transformada IPsec y el estatus de la conexión.

```
Caracas>enable
Caracas#show crypto ipsec sa

interface: FastEthernet0/0                                              (1)
    Crypto map tag: MYMAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)  (2)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0                   (3)
   #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.:10.2.2.1       (4)
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x65BA0E42(1706692162)

     inbound esp sas:                                                   (5)
      spi: 0x4B9D21F9(1268589049)
        transform: esp-aes 256 esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: FPGA:1, crypto map: MYMAP
        sa timing: remaining key lifetime (k/sec): (4525504/626)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     outbound esp sas:
      spi: 0x65BA0E42(1706692162)
        transform: esp-aes 256 esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: FPGA:1, crypto map: MYMAP
        sa timing: remaining key lifetime (k/sec): (4525504/626)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Figura 27: Show crypto IPsec sa en el enrutador Caracas (Elaboración propia)

IV.4 Realizar una prueba piloto del sistema de votaciones diseñado

Una vez realizada la prueba al sistema piloto para la elección de representantes estudiantiles, se ingresó a la interfaz del lector de resultados, en donde se obtuvieron las cifras mostradas en las Tablas 7, 8, 9, 10 y 11.

Nombre del candidato	Cantidad de votos
Gonzalo Aguilera	24
Gabriel Gutierrez	17
Jorge Martínez	17
Carlos Antonorsi	15
Edward Pérez	15
Cristofer Correia	12
Votos Nulos	11
Total de Votos	**111**

Tabla 7: Resultados para el cargo al Consejo Universitario (Elaboración propia)

Nombre del candidato	Cantidad de votos
Mercedes del Castillo	21
Ana Karina García	20
Ligia Pérez	12
Mariana Hernández	9
Ghesn Sfeir	7
Votos Nulos	5
Total Votos	**74**

Tabla 8: Resultados para el cargo al Consejo al Decanato de Desarrollo Estudiantil (Elaboración propia)

Nombre del candidato	Cantidad de votos
Jorge Saim	23
Gabriel Bastidas	21
Andrés Suárez	20
Votos Nulos	10
Total Votos	**74**

Tabla 9: Resultados para el cargo al Consejo de Facultad de Humanidades y Educación

(Elaboración propia)

Nombre del candidato	Cantidad de votos
Marcos Cubides	9
Karla Rodríguez	7
Adolfo Flores	5
Marco Jiménez	3
Natacha Travieso	3
Votos Nulos	3
Total Votos	**30**

Tabla 10: Resultados para el cargo al Consejo de Escuela de Educación - Caracas

(Elaboración propia)

Nombre del candidato	Cantidad de votos
Lilia Naveda	19
Rolando Montes	16
Votos Nulos	9
Total Votos	**44**

Tabla 11: Resultados para el cargo al Consejo de Escuela de Educación - Coro (Elaboración propia)

Al finalizar el proceso de votación, se comprobó que los votantes registrados en el Listado de Electores de cada sede, era igual al número de claves contenidas en la urna electoral.

Para evaluar los resultados obtenidos, se procedió por realizar una auditoría al comprobar que la cantidad total de votos registrados para cada cargo, era igual al número de votantes.

Según los Listados de Electores, que se encuentra en el Apéndice G, en la sede de UCAB Montalbán votaron 15 personas, mientras que en el CIAP de La Castellana votaron 22 personas.

El número de votantes para el cargo al Consejo Universitario fue de 37 personas, ya que participaron los electores de ambas sedes. Cada uno tuvo la oportunidad de escoger a tres candidatos, por esta razón, la cantidad de personas que votaron para este cargo por el número de oportunidades de selección que tenía cada una fue de 111 votos (37 votantes x 3 opciones= 111 votos), que coinciden con la sumatoria total de votos registrados que se muestra en la Tabla 7.

Para el cargo al Consejo al Decanato de Desarrollo Estudiantil y al Consejo de Facultad, la cantidad de votantes fue de 37 personas, ya que, de igual manera, participaron los electores de ambas sedes. En esta ocasión, cada uno tuvo la oportunidad de escoger a dos candidatos, por lo que la cantidad de personas que votaron para este cargo por el número de oportunidades de selección que tenía cada una fue de 72 votos, que coinciden con la sumatoria total de votos registrados que se muestra en la Tabla 8 y 9.

En el caso del cargo al Consejo de Escuela de la sede de UCAB Caracas, el número de votantes fue de 15 personas ya que solo participaron los votantes de dicha sede. Para esta oportunidad, los electores tenían la posibilidad de escoger a dos candidatos, por esta razón, el número de personas que votaron por el número de

opciones de voto que tenía cada una fue de 30 votos, los cuales coinciden con el total de votos registrados en la Tabla 10.

Para el cargo al Consejo de Escuela de la sede simulada de Coro, en el CIAP de La Castellana, la cantidad de participantes fue de 22 personas, que fueron los registrados en dicha sede. De igual manera que para la sede de Caracas, los electores podían escoger a dos candidatos, por lo que el número de personas que votaron para esta cargo por la cantidad de oportunidades de selección que tenía cada una fue de 44 votos, que coincidió con la sumatoria total de votos registrados que se muestran en la Tabla 11.

Con los resultados expresados anteriormente, se verificó que la transmisión de la información se realizó correctamente y se cumplió con el objetivo establecido, al haber sido un simulacro en el que se utilizó el reglamento establecido por la Comisión Electoral de la UCAB. Además, para el diseño de este sistema propuesto, se usaron mismos candidatos postulados en las elecciones de representantes estudiantiles para la Escuela de Educación en las sedes de la UCAB de Caracas y Coro en el año 2011, lo que dio lugar a un simulacro real del proceso que realiza un participante en dichas votaciones.

Durante esta prueba, se capturaron vídeos de algunos participantes, una vez finalizaron el proceso de votación, expresando sus opiniones en donde consideraron al sistema con las siguientes características:

- Interfaz amigable.
- Proceso de votación rápido.
- Sencillo de utilizar.
- Seguro.

Además, se tomaron una serie de fotografías de dichos participantes realizando la prueba en las sedes de UCAB Montalbán y CIAP, las cuales se muestran en el Apéndice J.

IV.5 Evaluar la seguridad del sistema piloto de votaciones diseñado

Se aplicaron un conjunto de pruebas al sistema desarrollado para verificar la seguridad de cada una de las interfaces creadas en la aplicación web. Para la interfaz del votante, se realizaron las siguientes pruebas:

1. Se comprobó que al introducir nuevamente una clave ya usada en el sistema de votaciones, no se permitiera el ingreso, mostrándose así la página de fallo. De esta manera, el participante solo puede realizar la votación una sola vez.
2. Se verificó en la Base de Datos que al utilizar una clave para realizar una votación, el campo status de la misma, el cual se encuentra inicialmente en cero, se colocara efectivamente en uno. La aplicación web no permite el acceso a la página de selección de candidatos cuando este campo se encuentra en uno.
3. Se confirmó que una clave destinada para una de las sede, no fuera utilizable en la otra localidad, para evitar así el registro de votos por participantes no pertenecientes a la sede seleccionada.
4. Se realizaron pruebas de votación en el sistema, y se constató que se registraran respectivamente los votos en las casillas de las tablas correspondientes.
5. Se comprobó que cuando se intenta acceder a la página en la que se seleccionan a los candidatos, esta redirecciona automáticamente a la página de inicio del sistema de votación, prohibiendo al participante votar sin previo ingreso de una clave.
6. Se corroboró que al ingresar una clave inválida, no se podía ingresar al sistema de votación.

7. La clave debe ser escrita correctamente en el espacio destinado para esto, incluyendo la distinción entre mayúsculas y minúsculas.

Para la interfaz del lector de resultados finales de la votación, se procedió a realizar las siguientes pruebas:

1. Se verificó que cuando se intenta acceder a la página de resultados directamente, esta redirecciona automáticamente a la página de inicio de sesión del administrador o lector de resultados.
2. Se comprobó que cualquier persona que ingrese a la interfaz de lector de resultados, solo será capaz de visualizar los mismos, más no podrá modificarlos o alterarlos. Es importante destacar que solo el que tenga acceso a la base de datos podrá cambiar alguna característica del sistema, incluyendo los resultados. Por esta razón, esta persona debe ser de un ente diferente al lector de resultados ya que es la única que conoce el nombre de usuario y contraseña necesarios para acceder a la base de datos.
3. Se corroboró que la página de resultados reflejara exactamente los mismos resultados registrados en la base de datos.

Por cada uno de los puntos mencionados anteriormente, se puede afirmar que la evaluación de seguridad realizada al sistema resultó favorable, ya que refleja el correcto funcionamiento de cada una de las interfaces, comprobando la obtención de un sistema eficaz y seguro de votaciones para la elección de representantes estudiantiles.

IV.6 Generar un instructivo de instalación del sistema

Se realizó un conjunto de instructivos que describen, a través de una serie de pasos, el proceso necesario para la instalación del sistema de votaciones planteado, el cual consiste en la configuración del servidor, la base de datos y la aplicación web respectivamente.

Por otra parte, para llevar a cabo el establecimiento de la comunicación VPN entre las sedes, se deben realizar ciertas configuraciones en cada uno de los enrutadores. Todos los instructivos nombrados anteriormente, se encuentran detallados en el Apéndice I.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se reflejan todas las ideas obtenidas luego de haber realizado cada una de las fases que conformaron este proyecto. Además, se expresan las recomendaciones en base a las experiencias adquiridas durante la elaboración de este Trabajo Especial de Grado.

V.1 Conclusiones

En los últimos años, la proliferación de aplicaciones web que acceden a un servidor a través de Internet, ha generado un crecimiento exponencial en las tecnologías de seguridad en redes, ya que existe la necesidad de que la información se transmita de forma íntegra y confiable, autenticando los miembros de la comunicación.

Para el desarrollo del sistema de votaciones que se plantea en este Trabajo Especial de Grado, fue fundamental la información obtenida en la investigación previa acerca de distintos procesos electorales desarrollados en varios países y universidades del mundo. El sistema de votaciones que se diseñó, cumplió con los parámetros establecidos por la Comisión Electoral de la UCAB y estuvo ajustado a las características con la cual estuviera familiarizado el alumnado que participó.

Se comprobó que el servidor WINDOWS *Server* implementado en el sistema de votaciones es totalmente utilizable para este proceso, dado que se verificó la funcionalidad del sistema entre dos sedes de la UCAB. Este servidor pudo ser instalado fácilmente en la red interna de la universidad y el acceso a la aplicación web para la votación se realizó a través de los computadores conectados a las redes pertenecientes a ambas sedes, a través de la conexión VPN.

La seguridad del control de acceso al sistema fue verificada por el mecanismo de ingreso a través de claves aleatorias entregadas a los participantes al momento de realizar la votación. De esta manera, se garantizó que el elector no realizara el voto más de una vez.

La comunicación entre las sedes de la UCAB es factible mediante el uso de una conexión VPN, ya que se comprobó en el desarrollo de este Trabajo Especial de Grado, la utilización de un túnel con protocolo IPsec que conecta a dos sedes de la UCAB, brindando integridad, confidencialidad, y autenticación de los miembros de la comunicación.

Se pudo comprobar el establecimiento de un túnel IPsec, mediante el uso del simulador *Cisco Packet Tracer,* realizando verificaciones de protocolos utilizados para el intercambio de claves, políticas de seguridad establecidas y el procedimiento de encapsulación de un paquete IP cuando contiene un tráfico interesante para la VPN.

Se verificó la disminución de tiempo del proceso de votaciones en comparación con el sistema actual, al haber realizado pruebas reales del sistema, en el cual, se obtuvieron comentarios por parte de los estudiantes y profesores participantes, donde afirmaron la rapidez al momento de realizar la votación y la totalización de los resultados finales.

La implementación del sistema de votaciones para futuras elecciones de representantes estudiantiles en la UCAB, utilizando los elementos de seguridad verificados en el presente trabajo de grado, es viable y relativamente sencillo de implementar debido a la facilidad de la base de datos y de las interfaces creadas en la aplicación web.

Finalmente, con la digitalización de este tipo de procesos, se contribuye con el ahorro de papel al eliminar, en gran parte, el uso de las papeletas necesarias para realizar las votaciones actuales.

V.2 Recomendaciones

A continuación, se describen un conjunto de sugerencias a tomar en cuenta para la implementación del sistema propuesto y como aporte a futuras investigaciones relacionadas con el tema planteado en este Trabajo Especial de Grado:

- Generar una interfaz de administrador en la aplicación web, la cual sea capaz de modificar desde ésta la base de datos creada, sin la necesidad de ingresar a la misma, como por ejemplo la posibilidad de inclusión o exclusión de los candidatos postulados para votaciones.
- Para el ingreso al sistema de votaciones, se recomienda utilizar los correos electrónicos y claves registrados en las bases de datos del DTI, que asigna la UCAB para el acceso al correo interno a cada uno de los estudiantes.
- Se plantea que para la implementación de este tipo de sistemas, por cada participante se imprima un comprobante del voto, que sirva para cotejar que la cantidad de votos obtenidos en la posterior auditoría del proceso sea igual al totalizado por el sistema.
- Para que los votantes conozcan el proceso de votación, se sugiere que antes del proceso electoral, se promueva toda la información necesaria para la utilización de dicho sistema.

BIBLIOGRAFÍA

OpenBSD. (1 de Septiembre de 2000). Recuperado el 17 de Julio de 2012, de Manual Pages: http://www.openbsd.org/cgi-bin/man.cgi?query=kerberos&sektion=8

Open SSH. (03 de Septiembre de 2004). Recuperado el 20 de Julio de 2012, de Seguridad: http://www.openssh.com/es/security.html

OPEN SSH. (05 de Septiembre de 2004). Recuperado el 18 de Julio de 2012, de Caracteristica: http://www.openssh.com/es/features.html

CALA (CAmpus Libre y Abierto). (8 de Mayo de 2006). Recuperado el 30 de Julio de 2012, de http://campusvirtual.unex.es/cala/cala/mod/resource/view.php?id=1875

OpenBSD 4.8. (27 de Marzo de 2011). Recuperado el 15 de Julio de 2012, de http://www.openbsd.org/es/

Andreu, F., Pellejero, I., & Amaia, L. (2006). Fundamentos y Aplicaciones de Seguridad en Redes WLAN. Barcelona, España: Marcombo.

Barret, D., Silverman, R., & Byrnes, R. (2005). SSH, the secure shell: the definitive guide. (M. Loukies, Ed.) Estados Unidos: O'reilly.

Cisco. (17 de Marzo de 2008). Manual Cisco CCNA Protocolos de Enrutamiento. (Cisco) Recuperado el 07 de Febrero de 2011, de http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx.

Cisco. (2010). Voz sobre IP. Recuperado el 05 de Junio de 2011, de http://www.cisco.com/web/ES/solutions/es/voice_over_ip/index.html.

Cisco. (2010). VPN. Recuperado el 02 de Junio de 2011, de http://www.cisco.com/web/ES/solutions/es/vpn/index.html

CNE Consejo Nacional Electoral. (s.f.). Consejo Nacional Electoral. Obtenido de Tecnología Electoral en Venezuela: www.cne.gov.ve/web/sistema_electoral/tecnologia_electoral_descripcion.php

Comisión Electoral Universidad Catolica Andres Bello. (28 de abril de 2011). Comunicado Nº 2. Eleccion de los Representantes Estudiantiles ante los Consejos de la Universidad para el año 2011-2012. Caracas, Distrito Capital, Venezuela.

Direccion General de Computo y de Tecnologías de Informacion y comunicación. (2011). Sistema de Votacione Electrónicas. Recuperado el 19 de Diciembre de 2011, de http://www.unam.mx/elecciones2011/pdf/SVE_ManualUsuarioElector.pdf

Dougligeris, C., & Serpanos, D. (2007). Network Security: Current status and future directions. Canada: IEEE.

Facultad de Economía UNAM. (2007). Elecciones Electrónicas en la facultad de Economía. Entre Tanto, 1-4.

Gimeno, J. M. (24 de Junio de 2004). La Flecha. Recuperado el 26 de Febrero de 2012, de Diario de Ciencia y Tecnología: http://www.laflecha.net/articulos/e-administracion/e-voto/

Mañaz, J. A. (2004). Mundo IP. (S. Rodriguez, Ed.) Madrid, España: Ediciones Nowtilus, S.L.

Martínez, D. D. (14 de Julio de 2002). Sistemas Operativos plan 1999 y plan 2009. Recuperado el 18 de Julio de 2012, de http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm

Martínez, M. J. (s.f.). Protocolos de Enrutamiento Simulador de Tráfico de Redes. Universidad Nacional de Nordeste.

Mathon, P. (2004). VPN Implementacion en Windows Server 2003. Barcelona: Ediciones ENI.

Microsoft. (2010). Authentication of VPN clients. Recuperado el 02 de Junio de 2011, de http://technet.microsoft.com/en-us/library/cc782786(WS.10).aspx

Microsoft. (2010). VPN Tunneling Protocols. Recuperado el 02 de Junio de 2011, de http://technet.microsoft.com/en-us/library/cc782786(v=ws.10).aspx.

Miramontes, O. (2005). Reflexiones en torno a los procedimientos y normas para las elecciones electronicas vía Internet en la UNAM. Recuperado el 12 de

diciembre de 2011, de http://scifunam.fisica.unam.mx/mir/voto_electronico.pdf

Montoya, Z., & Machuca, E. (05 de Marzo de 2009). Diseño de un sistema electoral para la Asociación de Egresados de la UCAB. Caracas, Distrito Capital, Venezuela.

SSH, O. (05 de Septiembre de 2004). Objetivos del Proyecto. Recuperado el 17 de Julio de 2012, de http://www.openssh.com/es/goals.html

Stewart, E. (2009). CCNA Security 640-553. Pearson Education.

Vachon, B., & Graziani, R. (2009). Acceso a la WAN. (J. Domínguez, Ed.) Ribera del Loira: Pearson Edicación.

Verón, J. (2009). Práctica de Redes. Zaragosa, España.