Universidad Nacional Autónoma de Nicaragua

Recinto Universitario Rubén Darío

Facultad de Ciencias e Ingeniería

Trabajo Monográfico

Para Optar al Título de Licenciatura en Ciencias de la Computación

Tema: Voto Electrónico E-Vote

Sub-tema:

Propuesta Estratégica para la Aplicación de un Sistema de Votos Electrónicos remotos en los Procesos Electorales Presidenciales de Nicaragua

Integrantes:

- ✓ Br. Xiomara Bermúdez Moreno
- ✓ Br. Heidy Castellón Muñoz
- ✓ Br. Joaquín Torres Tenorio

Tutor: Lic. Edgard Monge Cardoza

Managua, Nicaragua Diciembre 2012

Índice

Dedicatoria

Dedico este trabajo monográfico a:

Primeramente a Dios por haberme permitido llegar hasta este punto y haberme dado salud, ser el manantial de vida y darme lo necesario para seguir adelante día a día para lograr mis objetivos, además de su infinita bondad y amor.

A mi madre por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor. A mi padre por los ejemplos de perseverancia y constancia que lo caracterizaron y que me infundo siempre, y por su amor. A mi pareja por permanecer a mi lado y enseñarme que hay que luchar en momentos difíciles para salir adelante y a todos aquellos que ayudaron directa o indirectamente a realizar este documento.

A mi maestro por su gran apoyo y motivación para la culminación de nuestros estudios profesionales, por su apoyo ofrecido en este trabajo, por haberme transmitidos los conocimientos obtenidos y haberme llevado pasó a paso en el aprendizaje

Xiomara Bermúdez Moreno

Dedico este trabajo monográfico a:

A Dios primeramente por ser el pilar fundamental de mi vida y la inspiración a seguir adelante en medio de luchas y retos que se enfrentan en este camino. Por darme salud y fuerzas, por ser mi consolador y mí amigo fiel en los momentos buenos y en los momentos malos, por todo su gran amor hacia mí y toda su misericordia.

A mi madre que ha sido mi gran apoyo en la realización de mis sueños, por todos sus consejos y por creer en mí en todo momento, por todas sus oraciones y sus buenas enseñanzas, así como a Humberto Villalobos Ruiz quien ha sido uno de los grandes regalos que la vida me ha dado y que con todo su amor y cariño me motiva a no rendirme ante nada, a ser fuerte y luchar por mis sueños y alcanzarlos sin dudar en ningún momento.

A mis maestros que con paciencia y dedicación formaron una educación integral y motivaron a la culminación de este trabajo.

Y finalmente a todas aquellas personas que de una u otra forma estuvieron prestas a ayudarme y aportar sus preciados conocimientos para llevar a cabo este estudio.

Heidy Castellón Muñoz

Dedico este trabajo monográfico a:

A Dios, por brindarme la dicha de salud, bienestar espiritual.

A mi madre, forjadora de mi camino debido a su incansable esfuerzo y apoyo incondicional lleno de amor y paciencia tanto en lo personal como en lo profesional.

A mi esposa, por apoyarme en esta travesía con sus consejos y dedicación, siempre a la par mía dándome fuerzas para no desfallecer.

A mi hija, por ser el motor que me impulso para iniciarme en esta carrera.

A mis maestros, que con sus enseñanzas y consejos aportaron directamente a la culminación de esta etapa.

A nuestro tutor, que tuvo la paciencia para orientarnos en cada etapa de este trabajo.

Joaquín Torres Tenorio

Agradecimientos

Al momento de haber llevado a cabo nuestros deseos de forjarnos agradecemos con mucha sinceridad:

A Dios por proveernos de sabiduría y perseverancia en este camino.

A nuestros padres, esposos y esposa por ser nuestra fuerza, motivación e inspiración para ser cada día mejores, por sus grandes apoyos incondicionales y que gracias a ellos hoy somos lo que somos.

A nuestro tutor el Lic. Edgard Monge Cardoza por brindarnos el conocimiento y la guía en el desarrollo de este trabajo, por creer en nosotros, por su paciencia y apoyo incondicional muchas gracias por todo.

A los docentes del Departamento de computación de la Unan Managua, quienes nos enseñaron todo lo que hoy podemos aplicar en el área laboral, sin sus enseñanzas no lo hubiéramos podido lograr. Muchas Gracias por toda su gran labor en nuestra formación.

Capítulo 1

1. Introducción

Hoy en día el avance tecnológico ha dado un gran impacto en la sociedad y su entorno y el internet como parte de este cambio ha mejorado la comunicación y ha facilitado el acceso de información a lugares aun remotos en el mundo. Los diferentes ámbitos sociales, culturales, e incluso políticos no han quedado atrás en estas transformaciones tecnológicas.

El proceso de voto electoral como parte del ámbito político no es un asunto de ayer sino de hace muchos tiempo, en Europa hasta después de la Revolución Industrial (antes solo existían monarquías y, por tanto, traspaso de poderes) y en América (por su condición colonial) hace aproximadamente dos siglos. Nació con el fin de fortalecer la democracia en los países del mundo y a través de las facilidades que brinda la tecnología este proceso ha comenzado a realizarse a través del Sistema de voto electrónico, para referendos y elecciones.

Existen diferentes tipos de voto electrónico como: El Sistema de Reconocimiento Óptico de Marcas (OMR), Sistema de Registro Electrónico Directo (DRE), Sistema de Voto Electrónico Remoto, los cuales se han implementado en diferentes países desarrollados como Austria, Suiza y Reino Unido para sus procesos de votaciones. Latinoamérica no ha sido ajena a esta tendencia países como: Venezuela, México y Chile han adoptado estos tipos de sistemas, los que han tenido gran éxito, ya que la adopción de cualquier sistema de votación ha traído ventajas evidentes como el ahorro en los costos de la elección, y el ahorro en tiempo, mayor seguridad y garantías de transparencia, pues el escrutinio de los votos se realiza de manera rápida y los resultados son casi inmediatos.

En Nicaragua no existe una implementación que realice estos procesos electorales como se ha venido ejerciendo en otros países del mundo, tampoco existe una implementación que permita a los ciudadanos nicaragüenses en el extranjero que puedan ejercer su derecho al voto, ya que aún la ley electoral no lo prevé.

Por esta razón se hace necesaria la creación de un sistema que permita realizar el voto desde distintos lugares, la necesidad de garantizar el servicio de internet (gratuito de ser posible) en las zonas donde no hay redes de conexión.

El presente trabajo se enfoca en los sistemas electrónicos remotos que proporcionan un medio de votación a aquellos ciudadanos aptos a ejercer su derecho que no tienen la posibilidad de acudir a un recinto de votación el día de las elecciones por diferentes razones, ya sea que estos se encuentren fuera del país o se encuentren en zonas alejadas con dificultad de acceso a las urnas.

2. Planteamiento del problema

En la actualidad, Nicaragua aun realiza los procesos electorales de forma manual, en donde los ciudadanos una vez verificados, marcan su voto sobre el candidato de su preferencia en la boleta, depositándola en una urna que las almacena físicamente y una vez cerrados los comicios, estos son contados y recontados de forma manual.

Una de las grandes desventajas que trae consigo este proceso es el tiempo que se lleva en entregar los resultados finales, como se ha podido observar, pasan hasta cinco días para conocer con exactitud los resultados de cualquier elección, y en el peor de los casos, solo se queda con las preliminares de conteo. Todo este proceso pudiera ocasionar inconformidad y desconfianza en la población.

Además, se puede observar que nicaragüenses con cédula activa ,que aparecen en un padrón electoral y que se encuentran fuera del país en el tiempo que se realizan elecciones, no pueden participar de estos comicios, ya que no existe una alternativa que les permita a ellos ejercer su derecho al voto desde cualquier lugar del mundo.

Por esta razón, surge la necesidad de utilizar la tecnología en estos procesos electorales, ya que un sistema automatizado que reemplace este mecanismo manual ayudaría a reducir considerablemente los costos y a incrementar la participación de los nicaragüenses en elecciones no importando el lugar donde se encuentren.

El sistema automatizado de votación electrónica remota tiene su base sobre la mayor red de redes: Internet, que permite establecer prioridades de seguridad para cerciorar que los datos que serán almacenados en el sistema, no sean violentados por terceros y que a la misma vez, se aproveche la infinidad de recursos que brinda la web para la implementación del sistema.

Este estará hospedado en un proveedor de servicios hosting, en donde se establecerán controles y políticas de seguridad, para garantizar la pureza del proceso.

¿Qué opción de voto tienen las personas que no pueden usar servicios electrónicos?

¿Con qué garantía se cuenta para acceder a internet desde las zonas más alejadas de las redes de conexión?

¿De qué manera se fiscalizaría la participación transparente sobre quienes no cuentan con los niveles de instrucción para usar los medios electrónicos?

¿Qué políticas de seguridad del voto se aplicarían mediante las redes de conexión a internet?

¿Cómo funcionaría un sistema electrónico de votación en Nicaragua?

3. Antecedentes

Los intentos de utilizar tecnologías de la información y de la comunicación en los diversos aspectos del voto electrónico pueden parecer recientes, pero estos ya se han implementado en otros sitios de América Latina. Las primeras aplicaciones de las tecnologías electromecánicas para uso del ejercicio del voto electrónico y del posterior recuento de papeletas. Pero quien concreto su primera parte fue Thomas Alva Edison a finales del siglo XIX, para un sistema de grabación de voto electrónico.

Con la aparición de los primeros computadores a mediados de la década de 1940 se retomó la posibilidad de utilizar las máquinas para el voto electrónico. En la actualidad, muchos países han intentado desarrollar pruebas de voto electrónico con diversos tipos de soluciones y tecnologías; no menos Nicaragua, quiere incursionar en la implementación de dicha tecnología permitiendo con premura, agilidad y eficiencia la recopilación, obtención y procesamiento de los votos emitidos en los diferentes comicios para su posterior presentación en los distintos medios de comunicación y la respectiva proclamación de las nuevas autoridades del país.

La mayoría de los países en el mundo han considerado el uso del voto electrónico. De ellos, una buena parte ha realizado pruebas y algunos ya lo utilizan de forma vinculante. En varias repúblicas de Europa se han implementado diversos esquemas con sus respectivas pruebas. En otros lugares, varios Estados de Estados Unidos, en Brasil, seguido de cerca por México, el empleo del voto electrónico está ampliamente desarrollado. Asimismo, está siendo considerado en buena parte de los países de América Central y del Sur.

Para que el ejercicio sea efectivo se debe satisfacer las siguientes condiciones básicas:

- ✓ Infraestructura instalada que permita el debido funcionamiento del sistema.
- ✓ Un padrón electoral actualizado y depurado.
- ✓ Cedulación masiva de la población.
- ✓ Capacitación masiva de los electores mediante campañas informativas.
- ✓ Aprobación de parte de la Asamblea Nacional de una reforma electoral que permita el voto de los nicaragüenses residentes en el extranjero.

Esta propuesta beneficiará a una pequeña pero no menos importante población nicaragüense, las poblaciones indígenas y étnicas de la RAAN y la RAAS, así como un sector de individuos con incapacidades visuales, móviles o analfabetas, que son marginados o privados del uso de su derecho universal al sufragio en los distintos comicios electorales.[1] También se incluiría a la población migrante de nicaragüenses.

[1]Observaciones finales del Comité de Derechos Humanos en Nicaragua CCPR/NIC/CO/3 30 de octubre de 2008

4. Justificación

Considerando los avances tecnológicos que día a día se desarrollan, y tomando en cuenta las debilidades que presenta el mecanismo actual del proceso electoral en Nicaragua, es necesario realizar una propuesta que ayude al mejoramiento y de este.

Nicaragua no es ajena a la tecnología de punta, se puede observar que las inversiones en estas áreas han aumentado, y esto permite sustentar la viabilidad de un sistema de voto electrónico remoto en los procesos electorales.

Actualmente este proceso se hace de forma manual, donde la población que cumple con las condiciones para participar se verifica en un padrón electoral y ejerce su derecho en una junta receptora y marca su voto en boletas donde aparece el candidato de su preferencia. En seguida este es depositado en una urna física donde luego estas son contadas y recontadas de forma manual. En el caso de los nicaragüenses que se encuentran fuera del país, lamentablemente no existe un medio que les permita ser partícipes de los comicios.

Todo esto conlleva a realizar una aplicación que almacene el voto de aquellos nicaragüenses con cédula activa y que aparecen en el padrón electoral y que además se encuentran en cualquier lugar del mundo, de esta manera, ellos tendrán la oportunidad de ejercer su derecho a través de urnas digitales,

Esta aplicación web permite recoger el voto de aquellos nicaragüenses que se encuentran en cualquier lugar del mundo, para que de esta manera, ellos puedan participar de los comicios que se celebran en su país natal. Reforzando así mayor participación sin importar las fronteras.

Con el sistema VER2012 (voto electrónico remoto) se pretende demostrar que si se cumplen normas, procedimientos y niveles de seguridad tanto en el sistema como en el lugar de la red en la que se implementara, se estaría realizando una reingeniería al proceso electoral, la cual redundaría en el fortalecimiento de la democracia en el país.

El tiempo necesario para que gran parte de la población pueda apropiarse y ser capacitada en el correcto uso del sistema automatizado, depende en parte del desarrollo de una interfaz

amigable, la existencia de la infraestructura necesaria de soporte y de la capacitación que el ente electoral debería realizar tanto en zonas alejadas de la ciudad como en el extranjero.

Esto nos lleva a considerar que aun cuando se deba realizar una alta inversión inicial a largo plazo su existencia disminuirá considerablemente los costos de votación y mejorará la percepción de seguridad, eficacia, eficiencia y credibilidad de los electores en el sistema.

5. Tema:

VOTO ELECTRÓNICO

6. Subtema:

PROPUESTA ESTRATEGICA PARA LA APLICACIÓN DE UN SISTEMA DE VOTOS ELECTRONICOS REMOTOS EN LOS PROCESOS ELECTORALES PRESIDENCIALES DE NICARAGUA.

7. Objetivo General

- Proponer un sistema automatizado para la realización de votación electrónica remota en las elecciones presidenciales de Nicaragua.

8. Objetivos Específicos

1. Facilitar la oportunidad de ejercer el derecho a elegir libremente las autoridades gubernamentales a las personas que viven en el extranjero o zonas alejadas de Nicaragua mediante un sistema de voto electrónico.

2. Desarrollar un mecanismo electrónico que permita agilizar la obtención de los resultados electorales y la transparencia de los mismos.

3. Enumerar las ventajas que proporcionará el sistema de votación electrónica remota.

4. Contribuir a la optimización de tiempo, disminución de gastos y garantización de la seguridad del proceso electoral a través del sistema electrónico remoto.

9. Hipótesis

Un sistema Automatizado de Voto Electrónico Remoto permite mayor participación ciudadana dentro y fuera del país en elecciones electorales.

Capítulo 2

1. Marco Teórico

Elementos que conforman el proceso electoral actual

Plantearemos el caso específico de Nicaragua, Ley No. 331 de la Ley electoral, que establece en su Arto. 2 que el poder electoral se encargará de organizar, dirigir y supervisar las elecciones de las distintas autoridades.

En cuanto a la emisión del voto el Arto. 109 plantea que los ciudadanos concurrirán a depositar el voto en la Junta Receptora de Votos en cuya lista se encuentren registrados.

Arto. 116 establece que para el acto de votación se procederá de la siguiente forma:

1) Cada elector acudirá personalmente ante la Junta Receptora de Votos presentando su Cédula de Identidad Ciudadana o su Documento Supletorio de Votación.
2) La Junta Receptora de Votos verificará la validez de la Cédula de Identidad o del Documento supletorio de Votación y si esta corresponde a su portador, se comprobará si el elector se encuentra registrado en la lista del Padrón Electoral o de los Catálogos de Electores según el caso para entregarle las boletas electorales correspondientes.
3) Si debidamente identificado como residente de esa circunscripción electoral, el elector con su Cédula de Identidad Ciudadana o su Documento Supletorio de Votación y su nombre no apareciera en el listado del Padrón Electoral o del Catálogo de Electores o apareciera escrito en forma distinta de la que contiene el documento de identidad, los miembros de la Junta Receptora de Votos deberán aceptar el ejercicio del sufragio, haciendo constar dicha circunstancia en el acta de cierre.
4) El presidente de la Junta Receptora de Votos le explicará al elector la forma de emitir el voto.
5) El votante marcará en cada boleta electoral con una <<X>> o cualquier otro signo en el círculo de su preferencia y la introducirá debidamente doblada en la urna electoral correspondiente.
6) Si la <<X>> o cualquier otro signo hubiese sido marcada en la boleta fuera del círculo, pero se pueda entender la intención del votante, el voto se consignará válido.

7) Previo al ejercicio del derecho al voto, en el caso que el lector portare el Documento Supletorio de votación, este quedará retenido en la Junta Receptora de Votos, salvo en el derecho al voto en la segunda convocatoria si la hubiere.

El Arto. 118 determina que una vez concluido el acto de votación el elector previa limpieza deberá introducir el dedo pulgar de la mano derecha en tinta indeleble procurando que el dedo se impregne hasta la base de la uña. En defecto de ese dedo el elector introducirá el dedo de la mano izquierda o cualquier otro dedo de sus manos si le faltaren los pulgares. La tinta deberá estar en la misma mesa en que opera la Junta Receptora de Votos.

El Arto. 119 plantea que las personas que tuvieren impedimento físico podrán hacerse acompañar de una persona de su confianza para ejercer su derecho al voto. Esto se hará constar en el acta respectiva. Cuando el impedimento físico sea de las extremidades superiores la impregnación de la tinta indeleble podrá hacérsele en cualquier parte visible del cuerpo, esto se hará constar en el acta respectiva.

Con respecto al escrutinio Arto. 123. Terminadas las votaciones y firmada el Acta de cierre, la Junta Receptora de Votos procederá a realizar el escrutinio en el mismo local de la votación y a la vista de los fiscales. Para tal efecto se abrirán las urnas, previa constatación de su estado. Se contarán y examinarán las boletas electorales para verificar si su cantidad corresponde al de las personas que votaron.

De acuerdo al Arto. 124. Se considerará voto válido únicamente el que se realice en la boleta electoral oficial y esté marcado con una <<X>> o cualquier otro signo, en uno de los círculos que tendrá el efecto y que demuestre claramente la voluntad del elector.

En caso que el signo se encuentre fuera del círculo pero se pueda aún interpretar la intención del votante el voto se deberá consignar válido.

Arto. 125. Serán nulas las boletas en que no pueda determinarse la voluntad del elector y las depositadas sin marcar.

Arto. 126. Los votos válidos se clasificarán y contarán de acuerdo con las clasificaciones del Reglamento que dicte el Consejo Supremo Electoral.

Arto. 127. El Acta de escrutinio se levantará en la forma y copias que determine el Consejo Supremo Electoral, de conformidad con la presente Ley, incluidas las que deberá recibir cada uno de los fiscales y los órganos electorales y deberá consignar:

1) El número total de votos depositados.
2) El número de votos válidos.
3) El número de votos nulos.
4) El número de boletas recibidas y las que no se utilizaron.
5) Los votos válidos obtenidos por cada partido político o alianza de partidos, para la elección correspondiente. Las cantidades de votos se consignarán en el acta en números y letras.

Los reclamos o impugnaciones hechos por los fiscales sobre la validez o invalidez de los votos y sobre cualquier otro incidente.

2. Modelo básico de elecciones

En un modelo básico de elecciones participan principalmente dos tipos de agentes: autoridades de la elección y votantes. Estos pueden ser definidos como sigue:

Autoridad de la elección: Es la persona o grupo de personas a cargo del proceso de elección. Dicha autoridad establece los parámetros del proceso, los requisitos de los participantes, el objetivo de la elección.

Votante: Es cualquier persona que tiene derecho a participar en un proceso de elección emitiendo un voto. Una persona es un votante legítimo si cumple con los requisitos definidos por la autoridad de la elección.
Fases en las que se desenvuelve un modelo básico de elecciones. Estas fases son:

Preparación

- Registro de votantes para definir el censo electoral
- Anuncio de la elección

- Definición de parámetros de la elección
- Preparación técnica y configuración de la elección

Votación

- Autenticación
- Envío del voto

Consolidación de resultados

- Recolección de votos
- Escrutinio y determinación de resultados
- Publicación de resultados

Tipos de elección: Existen una gran variedad de tipos de elección. Se describen a continuación las más comunes:

- Si / No. El votante debe escoger la respuesta a una pregunta cerrada. Las consultas ciudadanas o referendos entran en esta clasificación.
- 1 de N. El votante debe escoger una entre N opciones posibles.
- K de N. El votante debe escoger K (K>1) entre N opciones posibles.
- K de N con orden de preferencia. El votante debe escoger en orden de preferencia K (K>1) entre N opciones posibles.
- N de N ordenados por preferencia. El votante selecciona el total de las opciones en orden de preferencia.
- Abierta. El votante plantea su propia opción de voto. Este tipo de elección puede ser combinado con otros, por ejemplo con “1 de N”, de forma que el votante puede escoger una entre N opciones posibles, o bien, proponer su propia opción.

Entornos de elección: Existen diferentes entornos en los cuales se llevan a cabo procesos de elección. Los más conocidos son los entornos gubernamentales (elecciones presidenciales, parlamentarias, municipales,), sin embargo también se llevan a cabo

elecciones en entornos a menor escala como son asociaciones estudiantiles, juntas de accionistas y sindicatos.

3. Conceptos básicos y evolución de los sistemas de voto electrónico

Análisis y Diseño de Sistemas: Proceso de examinar la situación de una organización con el propósito de mejorarla con métodos y procedimientos adecuados.

Sistema: Conjunto de componentes que interactúan entre sí, con el propósito de alcanzar un objetivo común.

Sistema de información: Medio por el cual los datos fluyen de una persona o departamento hacia otros y puede ser cualquier cosa, desde la comunicación interna entre los diferentes componentes de la organización y líneas telefónicas hasta sistemas de cómputos que generan reportes periódicos para varios usuarios; por tanto los sistemas de información proporcionan servicios a todos los demás sistemas de una organización y enlazan todos los componentes de forma tal que estos trabajen con eficiencia para alcanzar el mismo objetivo.[2]

Los sistemas de información son desarrollados con propósitos diferentes dependiendo de las necesidades de la organización. Los sistemas de procesamiento de transacciones (TPS, Transaction Processing Systems) funcionan al nivel operacional de la organización, los sistemas de automatización de oficina (OAS, Office Automation Systems) y los sistemas de trabajo de conocimiento (KWS, Knowledge Work Systems) que dan cabida al trabajo a nivel de conocimiento. Los sistemas de más alto nivel incluyen a los sistemas de apoyo a decisiones (DSS, Decision – Support Systems) así como a los sistemas de información gerencial (MIS, Management Information Systems). Los sistemas expertos aplican a la experiencia de los tomadores de decisiones para resolver problemas específicos estructurados. Al nivel estratégico de la administración encontramos sistemas de apoyo a ejecutivos (ESS, Executive Support Systems) y los sistemas de apoyo a decisiones de grupo (GDSS, Group Decision – Support Systems) ayudan a la toma de decisiones al mismo nivel, en una forma sin estructura o semi estructurada.

[2]Seen James A. Análisis y Diseño de Sistemas de Información. México: McGraw Hill, 1992. Pp. 11, 12, 19, 20

4. Necesidad del Análisis y Diseño de Sistemas

El análisis y el diseño de sistemas, tal como lo realizan los analistas de sistemas, pretenden estudiar sistemáticamente la operación de ingreso de los datos, el flujo de los mismos y las salidas de la información; todo ello dentro del contexto de una empresa en particular. En general el análisis y diseño de sistemas sirve, para fomentar mejoras en la operación de la empresa, lo cual puede realizarse mediante el uso de sistemas de información computarizada. Si un sistema se instala sin planeación adecuada es muy probable que no sea satisfactorio y después quede en el olvido.

El análisis y el diseño del sistema, permite estructurar el costoso esfuerzo de la implantación de los sistemas de información. El diseño y el análisis de sistemas se conforman por una serie de procesos, que al ejecutarse sistemáticamente mejoran la operación mediante el uso de los sistemas de información computarizados. Una buena parte del análisis y el diseño de sistemas involucran el trabajo en colaboración con los usuarios actuales o eventuales de tales sistemas de información.[3]

5. Ciclo de desarrollo de los sistemas

El SDLC (System Development Life Cycle) es un enfoque por etapas de análisis y diseño, el cual postula que el desarrollo de los sistemas mejora cuando existe un ciclo específico de actividades del analista y de los usuarios.

El ciclo se divide en siete etapas y aunque cada etapa se presenta de manera discreta, nunca se lleva a cabo como un elemento independiente, sino que se realizan al mismo tiempo diversas actividades, y estas llegan a repetirse.[4]

5.1. Identificación de problemas oportunidades y objetivos

En esta primera etapa, el analista se involucra en la identificación de los problemas, de las oportunidades y los objetivos. Esta fase es crucial para el éxito del resto del proyecto. Esta

[3] Kendall & Kendall. Análisis y diseño de sistemas. México: Prentice Hall, 1997. pp. 2,5
[4] Kendall & Kendall. Análisis y diseño de sistemas. México: Prentice Hall, 1997. pp. 8

etapa requiere que el analista observe de forma objetiva lo que ocurre en una empresa y luego en conjunto con los otros miembros de la organización los hará notar.

Las oportunidades, son aquellas situaciones que el analista considera que pueden perfeccionarse mediante el uso de los sistemas de información computarizados. Al aprovechar las oportunidades la empresa puede lograr una ventaja competitiva o llegar a establecer un estándar industrial.

5.2. Determinación de los requerimientos de información

En esta etapa el analista aborda los requerimientos de información a partir de los usuarios particularmente involucrados. Para identificar los requerimientos de información dentro de la empresa, pueden utilizarse diversos instrumentos, los cuales incluyen: el muestreo, el estudio de los datos y formas usadas para la organización, la entrevista, los cuestionarios; la observación de la conducta de quien toma las decisiones así como su ambiente.

El analista hace todo lo posible por identificar que información requiere el usuario para desempeñar sus tareas. Esta etapa sirve para que el analista se cree una imagen de la organización y de sus objetivos.

5.3. Análisis de las necesidades del sistema

Esta etapa consiste en analizar las necesidades propias del sistema. Una vez más existen técnicas y herramientas especiales que facilitan al analista la realización de las determinaciones requeridas. Estas incluyen el uso de los diagramas de flujo de datos, que cuentan con una técnica estructurada para representar en forma gráfica la entrada de datos de la empresa, los procesos y la salida de la información.

A estas alturas del ciclo de desarrollo del sistema el analista prepara una propuesta del sistema que resume todo lo que ha encontrado, presenta un análisis costo/beneficio de las alternativas y plantea las recomendaciones (si es que existen) de lo que deberá realizarse. Si la dirección acepta alguna de las recomendaciones, el analista procederá de acuerdo con ella. En sistemas cada problema es único y en consecuencia nunca habrá una sola solución

correcta. La manera como se plantea una recomendación depende de las características individuales de cada analista.

5.3.1. Diseño del sistema recomendado

En esta etapa del ciclo de desarrollo de los sistemas, el analista de sistemas usa la información que recolectó con anterioridad y elabora el diseño lógico del sistema de información. El analista diseña procedimientos precisos de captura de datos, con el fin de que los datos que se introducen al sistema sean correctos. También diseña accesos efectivos al sistema de información mediante el uso de las técnicas de diseño de formas y de pantallas.

Parte de la elaboración del sistema de información es la interfaz con el usuario. Esta etapa también incluye el diseño de la base de datos que almacenará aquellos datos requeridos por el sistema. La buena estructura de la base de datos es fundamental para cualquier sistema de información. En esta etapa también se preparan la interfaces graficas del usuario.

5.3.2. Desarrollo de documentación del software

En esta etapa se desarrolla la documentación indispensable del software, incluyendo los manuales de procedimientos para administradores y usuarios. Contiene las indicaciones para resolver cualquier problema del sistema.

5.3.3. Prueba y mantenimiento del sistema

En un principio se hacen una serie de pruebas para identificar las posibles fallas del sistema, el costo es menor si se detectan los problemas antes de la entrega. El programador realiza algunas pruebas por su cuenta, otras se llevan a cabo en colaboración con el analista de sistemas y otras en colaboración con los usuarios.

El mantenimiento del sistema se realizará de forma rutinaria a lo largo de la vida de este, el mantenimiento implica para la empresa un alto costo, pero este disminuye de forma considerable si el analista aplica procedimientos sistemáticos en el desarrollo de los sistemas.

5.3.4. Implantación y evaluación de sistema

En esta última etapa del desarrollo del sistema el analista ayuda a implantar el sistema de información. Esto incluye el adiestramiento que el usuario requerirá. Si bien es cierto, la capacitación la dan las casas comerciales, la supervisión del adiestramiento es una responsabilidad del analista de sistemas.

Aunque la evaluación del sistema se plantea como parte integrante de la última etapa del ciclo de desarrollo de los sistemas; realmente la evaluación toma parte en cada una de las etapas.

5.4. La importancia del mantenimiento

Después que el sistema está instalado se le debe dar mantenimiento, esto significa que los programas de computadora deben ser modificados y mantenidos actualizados. Generalmente en mantenimiento se consume un promedio que oscila entre un 48 – 60% del tiempo total empleado en el desarrollo de sistemas, quedando muy poco tiempo para el desarrollo de nuevos sistemas. Conforme aumenta la cantidad de programas escritos aumenta la cantidad de mantenimiento que requieren.

El mantenimiento se realiza por dos razones. Primero para corregir errores de software y para mejorar la capacidad del software en respuesta a las necesidades organizacionales cambiantes, que generalmente involucran algunas de las siguientes acciones:

- Los usuarios frecuentemente solicitan características adicionales después de que se familiarizan con el sistema.
- El negocio cambia a través del tiempo. El software debe ser modificado para abarcar tales cambios.
- El hardware y el software están cambiando a un ritmo acelerado. Un sistema que utiliza tecnología antigua puede ser modificado para usar las capacidades de una tecnología nueva.

6. Normalización

La normalización es un proceso que consiste en comprobar que las tablas que componen la base de datos cumplan con determinadas condiciones. Estas condiciones permiten garantizar la no existencia de redundancia (duplicidad de datos) y una cierta coherencia en su representación mediante un esquema relacional de entidades y relaciones del modelo conceptual (diagrama de E-R), además permite que la base de datos se simplifique y minimicen los problemas de lógica.

El modelo de datos relacional hace una representación del mundo real por medio de un conjunto de estructuras que son llamadas relaciones, las cuales se constituyen de dominios y de atributos. Sin embargo en la mayoría de los casos estas relaciones iníciales tienen dentro de su constitución, inconsistencias semánticas que provocan anomalías de manipulación (pérdida de información, actualización redundante, inserción múltiple) pueden dejar las bases de datos en un estado no deseado y no necesariamente va a reflejar los requerimientos de información de la organización.

El proceso de normalización es un método propio del modelo relacional y consiste en descomponer las relaciones originales en otras más pequeñas con el fin de eliminar una serie de anomalías de almacenamiento y manipulación que se pueden dar en las relaciones iníciales y que conformarían la futura base de datos relacional.

Entre los beneficios que se pueden dar en una base de datos correctamente normalizada se encuentran las siguientes:

- ✓ Reducir los problemas asociados con la supresión e inserción de registros.
- ✓ Reducir el tiempo asociado con modificaciones de los registros.
- ✓ Identificar problemas potenciales que puedan requerir de un análisis adicional.
- ✓ Mejorar la información para la forma de decisiones referentes a la organización física de los datos.

El proceso de normalización se compone de una serie de seis etapas llamadas formas normales.

6.1 Primera forma normal (1FN): Es la primera etapa del proceso e incluye la eliminación de todos los grupos repetidos y la identificación de la llave primaria. Para hacer esto la relación necesita ser dividida en dos o más relaciones. En este momento, las relaciones ya pueden estar sin anomalías de manipulación, pero es muy probable que se necesiten más pasos para transformar las relaciones y estas se encuentren sin anomalías**.**

La regla de la primera forma normal dice que:

- ✓ Se debe eliminar grupos repetidos en las tablas individuales.
- ✓ Crear una tabla diferente para cada conjunto de datos relacionados.
- ✓ Identificar cada conjunto de datos relacionados mediante una clave principal.

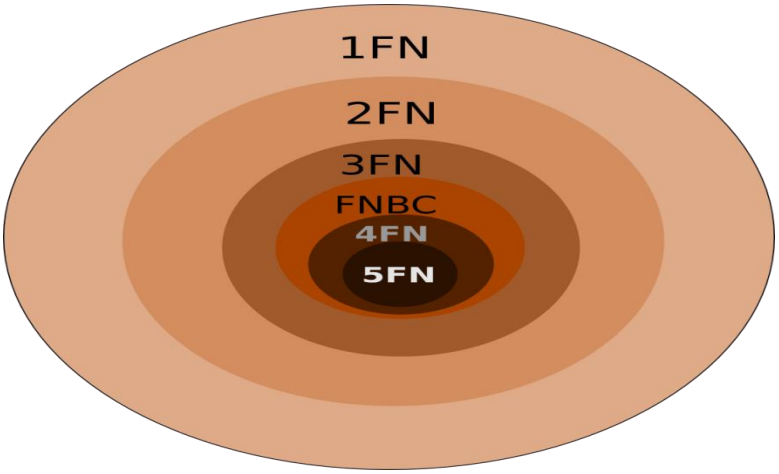
6.2. Segunda forma normal (2FN): Asegura que todos los atributos que no son llave sean completamente dependientes de la llave primaria, es decir que una afinidad se encuentra en segunda forma normal, si todos sus atributos que no son claves dependen por completo de la clave.

6.3. Tercera forma normal (3FN): Una tabla está normalizada si todas las columnas que no son llave son completamente dependientes de la llave primaria. Cuando no se encuentran datos repetitivos y contienen una llave única como primaria provee un esquema limpio y elegante, el cual es fácil de trabajar y expandir; aquí se está alcanzado la tercera forma normal**.**

6.4. Tercera forma normal de Boyce – Codd (3FNBC): Una relación se encuentra en tercera forma normal de Boyce – Codd (3FNBC), si todos los atributos son determinados solo por llaves.

6.5. Cuarta forma normal o dependencias multivaluadas (4FN): Una relación se encuentra en cuarta forma normal si se encuentra en 3FNBC y no tiene dependencias de valores múltiples. Esto se hace construyendo dos afinidades, donde cada una almacena datos para solamente uno de los atributos de valores múltiples.

6.6. Quinta forma normal (5FN): La quinta forma normal se refiere a las llamadas dependencias producto que garantizan la descomposición de una relación en tres o más relaciones, manteniendo el contenido original y con menor redundancia.



En el caso de nuestra base de datos se manejará con MySQL esto ayudará a hacer que el código PHP sea más fácil de comprender, de ampliar, y en determinados casos hacer que la aplicación sea más rápida; mediante una adecuada normalización se podrán extraer los datos y hacer relaciones eficientes.

Dependencia Funcional: Una dependencia funcional, denotada por X->Y, entre dos conjuntos de atributos X y Y que son subconjuntos de R(R={A1,A2,…A3}) específica una restricción sobre las posibles tuplas que podrían formar un ejemplar de relación r de R. La restricción dice que, para cualquier dos tuplas t1 y t2 de r tales que t1[X]=t2[X], debemos tener también t1[Y]=t2[Y]. Esto significa que los valores componentes de Y de una tupla de r dependen de los valores del componente X, o están determinados por ellos. También se dice que hay una dependencia funcional de X a Y o qué Y depende funcionalmente de X.

Los procesos de votación datan de hace más de 2500 años y han sido parte fundamental en los procesos democráticos. El voto constituye un derecho de los ciudadanos y en algunos casos también una obligación. Los procesos de votación determinan los destinos de pueblos completos. Por esta razón, dichos procesos captan la atención de masas. En las democracias actuales se busca que los resultados de una elección representen la voluntad del pueblo, por lo cual existe gran interés en que dichos resultados sean precisos y confiables.

7. Evolución del voto electrónico

El objetivo de los sistemas de votación electrónica es tratar de automatizar los diferentes procesos de la elección a fin de lograr una mayor eficiencia. Los primeros sistemas automatizados han estado enfocados al escrutinio de los votos. Sin embargo, también se han estado llevando a la práctica sistemas electrónicos para cada una de las fases de una elección, por ejemplo para el registro de los votantes y para la fase de votación.

La justificación teórica está compuesta de conceptos importantes dentro del análisis y diseño de sistemas y de redes informáticas que sirven de apoyo en la elaboración de este trabajo.

A continuación se describe una breve reseña de la evolución de los sistemas de voto electrónico más importantes.

7.1. Tipos de Sistemas Electrónicos

7.1.1. Sistemas de Reconocimiento Óptico de Marcas (OMR)

Estos sistemas emplean papeletas de votación en las cuales los candidatos u opciones de votación están impresos junto con viñetas que pueden rellenarse. Los votantes escogen su opción rellenando la viñeta anexa a su preferencia. Al finalizar el proceso de votación, el votante coloca la papeleta en un dispositivo para que sea escaneada y de esta manera se confeccione en paralelo un registro electrónico de los votos. El votante también puede depositar la papeleta en una urna física, y en este caso sería un oficial de la elección (por ejemplo; el presidente de la mesa electoral). Quien coloque el conjunto de papeletas de votación en el dispositivo de escaneo al final de la elección. Utilizando esta tecnología se pueden obtener automáticamente los resultados locales de una elección. Para un escrutinio global, algunos de los dispositivos tienen la posibilidad de conectarse remotamente a un servidor central para realizar el envío de sus resultados locales. De otro modo, se emplean otros medios para llevar a cabo la recolección de los votos.

El dispositivo de escaneo utiliza técnicas de reconocimiento de marcas, en donde se tienen en cuenta las partes más oscuras del área destinada para rellenar los votos, deduciendo de

esta manera las preferencias del votante. Esta es una tecnología ampliamente utilizada en otras áreas por lo que su correcta funcionalidad ha sido suficientemente probada.

7.1.2. Sistemas de Registro Electrónico Directo (DRE)

Estos sistemas de votación utilizan medios digitales para la selección del voto, por ejemplo, por medio de botones o pantalla táctil incluidos en el terminal de votación. El registro del voto se almacena localmente en formato electrónico. Los sistemas DRE previenen a los votantes de errores involuntarios, ya que el terminal de votación conduce al votante paso a paso hasta que un voto válido es registrado. Una variante de los sistemas DRE son los que imprimen la papeleta para que sea depositada en una urna, teniendo de esa manera un registro electrónico y otro impreso.

Los terminales DRE suelen contar con una interfaz de red, por lo que los resultados generados localmente pueden enviarse a un servidor central por medio de una red de comunicación. Otra opción es almacenar una copia de los resultados locales en un medio de almacenamiento removible y entonces enviar dicho registro a un centro de escrutinio para la consolidación de los resultados.

7.1.3. Sistemas de Voto Electrónico Remoto

La tendencia de los últimos años en los procesos electorales ha sido utilizar medios electrónicos para automatizar y hacer más eficientes los diferentes procesos de una elección. Aún cuando esta automatización se ha presentado de manera gradual, el propósito final es utilizar medios electrónicos para el registro de votantes, autenticación de los votantes registrados, emisión del voto, y desde luego para el escrutinio y publicación de resultados.

Los sistemas de voto electrónico remoto surgen especialmente para tratar de dar al votante una mayor facilidad para emitir su voto al no tener que acudir a un lugar específico para emitir su voto.

Si bien las características de los sistemas de voto remoto son atractivas, resultan más complejos que los sistemas de voto presencial debido a los riesgos de seguridad inherentes a un ambiente de votación remoto, en el cual la autoridad de la elección no puede tener control.

Existen diversos canales de comunicación en los cuales se puede llevar a cabo el voto remoto, entre los que se puede destacar: Internet (Web o e-mail), SMS, IVR, etc. En el capítulo 3 se presenta una comparativa de los sistemas de voto remoto más utilizados, incluyendo voto postal.

El propósito principal de los sistemas de voto remoto es proporcionar un medio de votación a los votantes que no tienen la posibilidad de acudir a un recinto de votación el día de la elección. Las razones de no poder acudir al recinto de votación pueden ser variadas, por ejemplo los votantes que residen en el extranjero, o votantes que viven en zonas muy alejadas a un recinto de votación.

Algunos países han implementado el uso del voto postal para permitir a los votantes emitir su voto de una manera remota. Sin embargo, debido a problemas comunes en los servicios postales para enviar el material a los votantes así como para recibir el voto, las autoridades electorales se han visto en la necesidad de estudiar vías alternas de votación remota, especialmente a través de medios electrónicos. En algunos casos ya se han estado implementando sistemas electrónicos de votación remota.

En general, el voto electrónico remoto puede resultar más conveniente que el voto postal. Los votantes tienen menos restricciones en cuanto al tiempo en que deben enviar su voto. Además, un votante puede verificar de una manera rápida, incluso en tiempo real, si su voto ha sido recibido por la autoridad electoral. Por otro lado, en algunos sistemas como el voto por Internet, el votante es alertado si no completa de manera correcta la selección de un voto, lo cual evita errores involuntarios que en el caso del voto en papel anularían.

Es importante hacer notar que los sistemas de voto electrónico remoto deben satisfacer al menos los mismos requisitos de seguridad propios de los sistemas electrónicos presenciales y aun los de los sistemas de voto convencional basado en papel. Los requerimientos que debe cumplir un sistema de voto electrónico remoto son los siguientes:

- **Legitimidad del votante:** En un proceso de elección, solamente pueden participar votantes autorizados y además sólo se puede tomar en cuenta un voto por votante. Tanto en los procesos de elección convencionales, como en los procesos que se utilizan sistemas de voto electrónico presencial, este requisito se cumple cuando el

participante muestra una identificación que lo acredite como votante autorizado. La autoridad de la elección comprueba la legitimidad del votante verificando que su registro se encuentra en las listas del censo electoral. En el voto electrónico remoto es más complejo realizar dicha autenticación del votante.

Comúnmente se han estado utilizando técnicas de identificación remota: por ejemplo un nombre de usuario y contraseña o certificados digitales.

- **Privacidad:** La relación entre votante y voto no debe ser conocida ni deducida. En un proceso de voto convencional se logra ocultar fácilmente la opción elegida por un votante, ya que una vez que el votante ha sido identificado como legítimo para votar, éste emite su voto de manera privada y lo deposita en la urna. Esta separación entre voto e identidad del votante es una tarea compleja en el voto electrónico remoto.

- **Precisión:** El resultado de la elección debe proceder exactamente de los votos emitidos de manera legítima. Es decir, solamente los votos válidos provenientes de votantes legítimos deben ser tomados en cuenta. Por lo tanto, los votos duplicados o no válidos deben ser excluidos del escrutinio. Además, debe prevenirse cualquier alteración de los votos. Cualquier intento de quebrantar la integridad de los resultados de la elección debe ser detectado oportunamente.

- **Equidad:** No se deben conocer resultados parciales durante la fase de votación, de lo contrario dicho conocimiento podría influir en la decisión de los votantes que aún no han emitido su voto.

- **Verificación individual:** En un sistema de voto electrónico remoto, cada votante debería poder verificar:

  - ✓ que su voto ha sido recibido correctamente por el servidor de votación (verificación de registro correcto),
  - ✓ que su voto ha sido incluido correctamente en el escrutinio (verificación de escrutinio correcto).

- **Verificación universal:** Un elemento importante para dar fiabilidad a un sistema de voto electrónico remoto es que este sea públicamente verificable, de tal manera que cualquier participante u observador pueda verificar la integridad de los resultados.

- **Incoercibilidad:** Un votante no debería tener la posibilidad de probar a un tercero la opción o candidato que ha elegido en una elección, ya que el poder probarlo facilitaría la coerción o venta de votos.

- **Robustez:** Un sistema de voto electrónico remoto debería ser tolerante a fallos tecnológicos, así como prevenir ataques de denegación de servicio. Por otro lado, un sistema de voto electrónico remoto debería ser resistente a ataques derivados de confabulaciones de autoridades deshonestas que intenten llevar a cabo una ataque contra el sistema de votación, por ejemplo violar la privacidad de los votantes o alterar los resultados de la elección.

7.2. Amenazas de seguridad en los sistemas de voto remoto

La mayoría de los requisitos de seguridad en los sistemas de voto electrónico son necesarios en parte debido a las diferentes amenazas que se pueden presentar en dichos sistemas. Las amenazas son eventos inesperados que pueden suponer un peligro a uno o más de los elementos de la elección, por ejemplo a votos individuales, al resultado de la elección. Una amenaza puede ser deliberada o accidental (por ejemplo a causa de un error o incluso un evento ambiental o natural). Por su parte, un ataque es la realización de una amenaza.

En todo sistema de información existen tres áreas básicas de seguridad que pueden ser afectadas por un ataque: confidencialidad, integridad y disponibilidad [ISO27002].

Aplicando estas áreas de seguridad a los sistemas de votación, las principales amenazas son aquellas que podrían llegar a comprometer alguno de los siguientes objetivos:

- privacidad del votante (confidencialidad).
- precisión de los resultados (integridad).
- continuidad hasta completar el proceso de elección (disponibilidad).

7.3. Vulnerabilidades en un sistema de votación

Un atacante tratará de explotar alguna vulnerabilidad del sistema de votación a fin de comprometer alguno de los objetivos generales de la elección. A continuación se describen algunos ejemplos de vulnerabilidades en un sistema de voto electrónico remoto:

7.3.1. Deficiente sistema de registro de votantes: El sistema de registro es el medio por el cual se recaba la información de los votantes para formar un censo electoral. Si dicha recolección de datos es ineficiente, no se puede garantizar la correcta verificación de la legitimidad de los votantes durante la fase de votación. Por ejemplo, un votante legítimo podría ser erróneamente rechazado para votar por un error en la constitución del censo electoral.

7.3.2. Deficiente diseño de los mecanismos criptográficos empleados: Un aspecto esencial en la seguridad de los sistemas de voto electrónico remoto es la criptografía utilizada. Un diseño inapropiado del mecanismo criptográfico podría causar un riesgo importante a la integridad de la elección. El diseño comprende el protocolo, el algoritmo utilizado, la longitud de las claves, el medio de almacenamiento de las claves privadas.

7.3.3. Proceso de autenticación débil: Un proceso robusto de autenticación aceptará solamente votantes legítimos para emitir un voto. Por el contrario, un esquema de autenticación débil afronta el riesgo de aceptar votantes no legítimos, por lo tanto representa una vulnerabilidad que puede ser aprovechada por un atacante.

7.3.4. Control de acceso débil a elementos del sistema de votación: Los elementos lógicos tales como ficheros, bases de datos, claves de cifrado, así como los elementos físicos como son los servidores, terminales de votación, deben ser protegidos de accesos no autorizados. De lo contrario, un atacante podría hacer un uso indebido de los mismos.

7.3.5. Terminales de votación inseguros: Debido a que en un sistema de voto electrónico remoto los terminales de votación están fuera del control de la autoridad de la

elección, existe la posibilidad de que dichos terminales tengan problemas propios de seguridad. Ésta es una de las principales vulnerabilidades de un sistema de voto electrónico remoto y podría ser ampliamente aprovechada por un atacante, por ejemplo insertando algún software malicioso que pretenda conocer el contenido del voto o bien, modificarlo antes de ser emitido.

7.3.6. Canales de comunicación inseguros: Debido a que algunas de las transacciones llevadas a cabo durante el proceso de elección se llevan a cabo a través de una red telemática, un canal de comunicación inseguro representa una vulnerabilidad que puede afectar a los objetivos de la elección.

7.3.7. Sistema de logs deficiente: Un registro deficiente de las transacciones llevadas a cabo durante la elección podría ser un punto de debilidad que no garantiza la detección de manipulaciones en la información. Por lo tanto, si no se cuenta con un registro eficiente de las transacciones existe una probabilidad mayor de ataques sin detección.

7.3.8. Procesos deficientes en la verificación de elementos: Durante la configuración de una elección se debe llevar a cabo algunos procesos de verificación. Estos procesos tienen el propósito de determinar la correcta configuración y operación de los elementos que participarán en la elección. Por lo tanto, un proceso de verificación deficiente podría resultar en una situación de vulnerabilidad.

El diseño de un sistema de voto electrónico remoto debe considerar las posibles vulnerabilidades para tratar de evitar que alguno de los objetivos críticos del proceso de elección se vea afectado. Adicionalmente, se debe considerar que en un entorno de votación pueden existir distintos tipos de atacantes, por ejemplo un votante, un oficial de la elección, un miembro del personal técnico, o bien una persona externa, es decir, aquella que no tiene ningún rol dentro de un proceso de elección.

8. Auditoría del sistema de voto electrónico remoto

Uno de los desafíos de los sistemas de voto electrónico es ofrecer mecanismos de transparencia que permitan al votante, o a cualquier parte implicada directa o indirectamente en un proceso de elección, verificar la integridad de los resultados. Las propiedades de verificación del votante, forman parte de la auditoría. Si cada votante verifica el correcto tratamiento de su voto se logra un alto grado de auditoría. Sin embargo hay elementos que quedan fuera del alcance de los votantes. Un ejemplo de esto es la práctica de adición de votos ilegítimos en la base de datos de votos recibidos. En este caso, aún cuando cada votante puede verificar la gestión de su propio voto, ningún votante se percataría de la adición de votos ilegítimos.

En un sistema de voto electrónico la auditoria pretende:

- Comprobar que los votos fueron registrados en el servidor de votación de acuerdo a la elección hecha por los votantes.
- Comprobar que todos los votos registrados fueron correctamente contemplados en el escrutinio final.
- Detectar manipulaciones en cualquiera de los procesos en los que el sistema de votación esté involucrado.
- Detectar errores de funcionamiento en el sistema de votación, los cuales podrían haber afectado el resultado de la elección.

En los procesos de elección llevados a cabo con sistemas de voto electrónico podemos distinguir dos tipos de auditoría, la que se lleva a cabo antes de la elección y la auditoría posterior a la elección. Además, durante la elección también se llevan a cabo algunas tareas de auditoría por parte del votante. Sin embargo, podemos clasificar dichas tareas como parte de la verificación individual.

8.1. Auditoría previa a la elección

El objetivo de la auditoría previa a la elección es asegurar que todos los elementos que se usarán en los diferentes procesos funcionan de acuerdo a las especificaciones. Se llevan a cabo verificaciones que a su vez servirán para llevar a cabo auditorías posteriores. De

manera más específica, las tareas realizadas en una auditoría previa a la elección son las siguientes:

- **Auditoria de la seguridad:** Se lleva a cabo un análisis exhaustivo de la arquitectura y funcionalidad del sistema de votación con el fin de determinar su seguridad. Este análisis puede incluir una estimación de riesgos y la manera en que el sistema utilizado puede afrontarlos.

- **Verificación de componentes:** Se verifica la integridad de los componentes físicos y lógicos que se utilizarán en la elección.

- **Validación de la configuración de la elección:** Por una parte, se valida que la información que se utilizará para la configuración de la elección (por ejemplo nombres de candidatos, partidos.) corresponde al objetivo de la elección.

  Además, se verifica que los componentes que se utilizarán corresponden a los que se han validado previamente.

- **Certificación del código fuente:** En la mayoría de los países con legislación en materia electoral se requiere certificar el software que se utilizará en una elección.

  Después de la certificación, la autoridad de la elección está a cargo de custodiar el software certificado y de vigilar la instalación de dicho software. Sin embargo, se han presentado diversas ocasiones en las que el software utilizado es diferente al que ha sido certificado. La certificación del software es un problema crítico tanto para la autoridad de la elección como para los proveedores del software de votación. Por ejemplo, si una vez que el software ha sido certificado el proveedor detecta algún error de funcionamiento, tendría que volver a certificar el software corregido. Esto tiene como consecuencia costos adicionales para el proveedor del software.

Este tipo de auditoría se puede aplicar tanto a los sistemas de voto electrónico presencial como a los sistemas de voto electrónico remoto.

8.2. Auditoría posterior a la elección

En este caso se pretende verificar el correcto funcionamiento de todas las fases de la elección una vez que esta ha finalizado y en algunos casos incluso durante el proceso de votación.

Uno de los propósitos de los sistemas de verificación independiente es tener un registro adicional que permite llevar a cabo una auditoría del proceso de votación. Sin embargo, dichos sistemas de verificación son adecuados principalmente para los sistemas de voto electrónico presencial, por lo que podemos descartar su viabilidad para un proceso de auditoría en una elección llevada a cabo a través de un sistema de voto electrónico remoto.

Se pueden llevar a cabo auditorias posteriores a la elección como las que se describen a continuación.

8.3. Recuento total de votos

En el voto electrónico, como es bien sabido, el escrutinio de los votos se lleva a cabo de manera automática como parte de las funciones que lleva a cabo el software del sistema de votación. Por lo tanto, un recuento total de los votos por el mismo medio en principio ofrecerá el mismo resultado que el inicial, ya que el cómputo será invariable.

La auditoria posterior a la elección en un sistema de voto electrónico se puede llevar a cabo siguiendo alguno de los métodos de verificación independiente, los cuáles aplican tanto a la verificación individual así como para fines de auditoría (sistemas de verificación directa, sistemas de procesos separados, sistemas de testigos, o sistemas de verificación de cifrado extremo a extremo).

Los recuentos de votos a través de los registros originados en el sistema de verificación independiente constituyen un mecanismo común para llevar a cabo auditorías de la elección. Sin embargo, los recuentos presentan una seria deficiencia. Un recuento a través de un medio independiente puede dar diferentes resultados a los obtenidos en el escrutinio inicial y usualmente el resultado que se tomaría en cuenta sería el del recuento. Sin embargo, los errores o manipulaciones se pueden presentar tanto en el escrutinio inicial como en el recuento, por lo que no podemos considerar que éste sea un método fiable de auditoría.

De hecho, un atacante que desee cambiar el resultado de la elección, tendrá más información para llevarlo a cabo con éxito cuando se realizará un recuento. Supongamos que en el escrutinio de una elección el candidato A tiene 2500 votos más que el candidato B. El atacante (probablemente con privilegios de acceso) sabrá entonces cuantos votos debe agregar antes de que se lleve a cabo el recuento si desea que el ganador sea el candidato B.

Un recuento que ofrezca un resultado diferente pero que conserve al mismo ganador del escrutinio inicial, generalmente no será discutible aún cuando la diferencia en el resultado sea significativa. Por otro lado, un recuento que arroje un ganador diferente al del escrutinio inicial y para el cual no se pueda dar una explicación de la razón de las diferencias entre ambos conteos, causará un alto grado de desconfianza entre los votantes.

Los sistemas de verificación independiente afrontan el desafío de escoger acertadamente el registro que será considerado como correcto en caso de discrepancias.

8.4. Recuento de una muestra de los votos

Unas consideraciones importantes para llevar a cabo un recuento parcial como parte de una auditoría, es que por un lado un recuento total de los votos es muy costoso y por otro lado, existe un riesgo muy alto de que se encuentren diferencias entre el escrutinio original y el recuento, con el impacto que eso puede tener.

En cambio, en un recuento menor en dónde se han seleccionado apropiadamente los parámetros para determinar la muestra, se podría tener una idea clara de la fiabilidad del escrutinio original o de la posibilidad de que haya existido fraude. Esto, sin tener que llegar a un nivel alto de precisión requerido en los recuentos totales.

Existen diferentes trabajos basados en procesos estadísticos o probabilísticos que hacen un análisis del porcentaje de votos, de máquinas de votación o de los recintos que deberían ser auditados a fin de detectar con una probabilidad alta si han existido alteraciones en los resultados de la elección. Usualmente se toman como variables el número total de recintos o máquinas de votación, el margen de diferencia de votos entre el candidato presumiblemente ganador y el segundo lugar y el tamaño de los recintos.

El problema de determinar el número de recintos es menor si consideramos que el problema principal de los recuentos parciales se encuentra en la decisión de cuáles recintos formarán parte del recuento. Si un atacante sabe en cuáles recintos o de cuáles máquinas de votación o conjunto de votos se llevará a cabo el recuento, y consigue acceso a dichos elementos entonces podrá tomar ventaja añadiendo o eliminando votos de acuerdo con su interés. Si a esta situación añadimos que la decisión de los recintos que serán auditados se puede conocer antes del cierre de la elección, un atacante podrá manipular uno o más recintos de los que no se han considerado para ser auditados y esto no será detectado.

Ventajas que ofrecería un sistema de voto electrónico remoto de aplicarse en el futuro:

- Eliminación de las boletas de votación
- Eliminación del padrón electoral impreso en papel (reduciendo la tala de árboles)
- Eliminación del acta electoral (y sus copias)
- Eliminación de la urna o ánfora electoral
- Reducción del números de mesas y de locales de votación, aumento de números de votantes
- Reducción del número de miembros de mesa
- Eliminación de los votos por error
- Eliminación del llamado error material
- No habría actas de impugnación, solo reportes de resultados
- Disminución del tiempo de entrega de los resultados

A diferencia de la votación tradicional basada en papel, el voto electrónico es grabado almacenado y procesado en una computadora.

En suma, el voto electrónico facilita los pasos del proceso de votación, así como reduce tiempos.

Desventajas:

¿Cómo garantizo la inviolabilidad del voto? En ese sentido, los datos de ambos módulos (identificación y votación) son almacenados en bases de datos distintas, que no se relacionan

una con la otra. La posibilidad de identificar que un elector votó, por ejemplo, a las 3 de la tarde, y que a esa hora se dio un voto por un determinado partido, es nula. La máquina de votación registra votos, pero no el momento en que fue emitido ni en qué cabina.

¿Qué mecanismos se están considerando? Antes, durante el proceso piloto y al final de la recolección de información de los votos emitidos, se podrán realizar auditorías por las entidades respectivas y competentes en cuanto a Ley electoral.

¿Cómo se llegaría a las ciudades donde no hay energía eléctrica? En este caso se proveería de baterías para su grabación en CD los cuales deberán ser llevados a un centro de transmisión más cercano para trasladar la información.

¿Considerando el índice de analfabetismo en el país cómo ejercerían su derecho estas personas analfabetas? El sistema se desarrollará de tal manera que ninguna persona (independientemente de su posición geográfica, idiomas, instrucción o pobreza) quedará sin ejercer el uso del sufragio universal. Es decir, como se mencionó antes, los migrantes podrán hacer valer sus derechos de elegir a sus gobernantes independientemente de donde se encuentren, solamente requerirán de una conexión de red (PC, móvil,) con acceso a internet.

Ventajas de los sistemas de voto electrónico

Las ventajas de los sistemas de votación electrónica sobre los sistemas tradicionales de votación en papel se destacan a continuación:

- Rapidez en el escrutinio de los votos
- Accesibilidad para votantes con discapacidades físicas
- Prevención de errores en el proceso de votación, lo cual evita que se tengan que anular votos
- Menores costos de implementación (en elecciones a gran escala y/o con el paso del tiempo)
- Posibilidad de que el votante pueda verificar el correcto tratamiento de su voto

Por su parte, con el uso de un sistema de voto electrónico remoto existen algunas ventajas adicionales:

- Conveniencia para el votante, al no tener que desplazarse a un recinto de votación específico
- Horario más amplio del período de votación, que puede ser de varios días o incluso semanas
- Gestión centralizada del proceso de elección

Principales aspectos de una elección que presenta vulnerabilidades importantes y que han impedido el uso extensivo del voto electrónico:

- Si bien la mayoría de las propuestas de esquemas de voto electrónico se concentran en la fase de votación, es importante considerar que existe una fase previa en la que se constituye el censo electoral. Si la recopilación de dicho censo no se lleva a cabo de una manera eficiente y segura, puede haber consecuencias negativas en las fases posteriores. Este proceso de recolección de datos de votantes le denominamos registro de votantes y es parte de la preparación de una elección. En los últimos años, en algunos países, se han empezado a utilizar medios remotos para llevar a cabo este proceso de una manera más eficiente. Sin embargo, los sistemas actuales de registro remoto de votantes presentan algunos riesgos de seguridad que pueden resultar en un censo electoral deficiente.

- Tradicionalmente en unas elecciones gubernamentales que utilizan un sistema de votación basado en papel, el votante marca su opción de voto, deposita la papeleta en una urna y ahí termina su función. El votante no tiene forma de verificar que en el escrutinio su voto se ha incluido correctamente, aun cuando al final de la elección se publique una lista con los nombres de los votantes que ejercieron su derecho al voto. Por lo tanto, los votantes tienen que confiar en la autoridad de la elección cuando se publican los resultados de la elección. Por su parte, en muchos de los esquemas de voto electrónico propuestos a la fecha no se considera la verificación por parte del votante como parte fundamental de la seguridad, es decir, el votante no cuenta con mecanismos eficientes que le permitan verificar que su voto se ha registrado correctamente y que en el escrutinio, dicho voto se ha incluido apropiadamente. Estos esquemas asumen que las autoridades de la elección y administradores de sistemas actuarán honestamente y que los votantes confían en dichas autoridades. En un

ambiente real no podemos suponer eso, por lo que el votante necesita un medio de confianza tangible para que un sistema de voto sea fiable y por tanto factible para su implementación. Por lo tanto, tendríamos que dividir la seguridad de un sistema de voto electrónico en dos aspectos. Por una parte, la seguridad que es auditada y validada por expertos en seguridad y que pueden constatar que cierto esquema cumple con los requerimientos de seguridad críticos. Por otro lado, se debe considerar la seguridad desde el punto de vista de los votantes, o dicho de otro modo, la percepción de seguridad y por lo tanto la fiabilidad que tienen los votantes en un sistema. Para lograr este segundo aspecto de seguridad, el sistema debe ser capaz de proporcionar al votante mecanismos de verificación que proporcionen dicha confianza.

- Además se presenta el problema de consolidar los resultados de una elección para llevar a cabo el escrutinio, especialmente cuando la elección se lleva a cabo utilizando distintos canales de votación. Por ejemplo, en una elección se podrían utilizar simultáneamente máquinas de votación de registro directo (DRE's), voto convencional en papel, voto postal y voto por Internet. A la hora de consolidar los resultados a partir de los distintos canales de votación se presentan serias complicaciones de seguridad que podrían llegar a alterar los resultados reales.

- Un problema adicional de los esquemas de voto electrónico, y de alguna manera paralelo al de la falta de mecanismos que permitan la verificación por parte del votante, es la falta de transparencia en la mayoría de los sistemas actualmente utilizados. Por esta razón, se requiere implementar técnicas que proporcionen elementos suficientes para llevar a cabo auditorías, dando de esta manera mayor transparencia y por lo tanto mayor confianza a los votantes.

Existe aún mucho por resolver entre los aspectos que proporcionan seguridad y eficiencia en los esquemas de voto electrónico remoto para que estos sean fiables ante la ciudadanía en general.

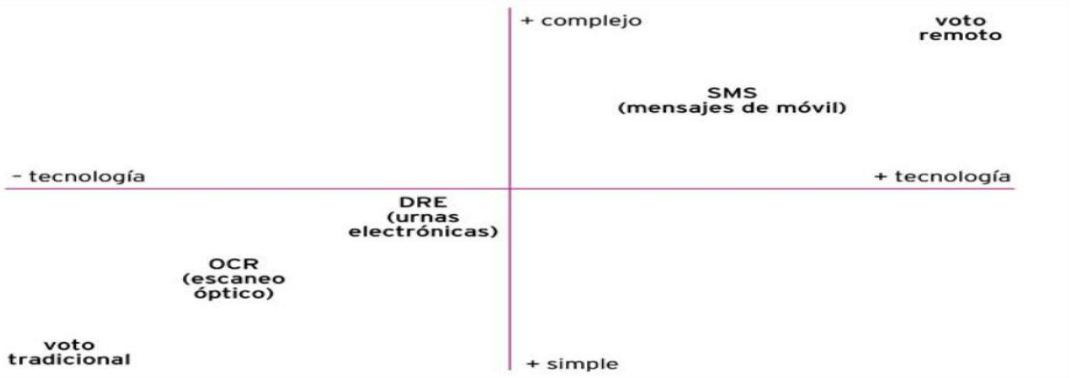
8.5. Ocho dudas razonables sobre la necesidad del voto electrónico

En un momento en que se generaliza el uso de las diferentes soluciones de voto electrónico, se trata de hacer balance sobre cuáles son los principales obstáculos que esta

revolución electoral debe superar. Antes, sin embargo, consideramos necesario discutir los principales malentendidos que se han creado en torno al voto electrónico, así como intentar aclarar cuáles son los motivos que se aducen para su implementación. A partir de aquí, se presentan ocho grandes dudas a las que todavía no se ha dado una respuesta satisfactoria en su conjunto, si bien una buena parte de estos aspectos han sido objeto de especial atención en algunas experiencias de voto electrónico.

8.5.1. Algunos malentendidos

8.5.1.1. El voto electrónico es solo por Internet: El primer malentendido hace referencia a la vinculación automática que se establece entre el voto electrónico y la utilización de Internet como único canal para la emisión del voto. Desde esta concepción, exclusivamente centrada en el voto electrónico remoto, se critican sus efectos negativos en cuanto a la profundización de la brecha digital, como mínimo en el corto plazo. Se dirá que el voto electrónico remoto sólo podrá ser empleado por aquellos ciudadanos con acceso a la Red y, por lo tanto, con unos niveles socioeconómicos y culturales por encima de la media del conjunto de la población. Dicha afirmación, válida en gran medida para este tipo de voto electrónico, parte de un error. El voto electrónico no sólo se ha desarrollado como una solución remota, sino que también puede tener una configuración local mediante el desarrollo de urnas electrónicas así como también pueden considerarse dentro de este tipo de voto las tecnologías de reconocimiento óptico de caracteres (OCR).[5]



[5] Josep Reniu Vilamala, Ocho dudas razonables sobre la necesidad del voto electrónico www.uoc.edu/idp/6/dt/esp/reniu.pdf

8.5.1.2. El voto electrónico es solo para entornos no controlados: Ausencia de controles y de garantías jurídicas en el momento de la emisión del voto. A partir de la premisa del voto electrónico remoto, se critican las altas posibilidades de coacción que puede sufrir el votante al tener que ejercer su derecho de sufragio en un entorno en el que ninguna autoridad electoral vela por sus derechos.

Si bien es cierto que la posible coacción es uno de los principales peligros de la votación electrónica remota, este tipo de voto no es el único escenario posible y/o deseable. Así, la práctica más habitual en estos momentos de implantación del voto electrónico es la que aprovecha los entornos controlados vinculados a los colegios electorales para la ubicación de urnas electrónicas o máquinas de votación.

Más allá de la estrategia global adoptada (sustitución total del voto tradicional o bien coexistencia de las urnas electrónicas con las urnas tradicionales), lo interesante de la utilización de entornos controlados radica precisamente en el mantenimiento de idénticos o similares procedimientos de identificación y registro del votante.

8.5.1.3. El voto electrónico es sólo para elecciones políticas: Si anteriormente considerábamos los equívocos en la definición teórica del voto electrónico, en esta ocasión nos hallamos frente a equívocos en su concreción práctica.

Probablemente fruto de concepciones democráticas reduccionistas, se ha venido vinculando el voto electrónico única y exclusivamente a los procesos electorales públicos, limitando por tanto el alcance de su desarrollo.

Las consideraciones sobre la generalización de las **NTIC** (Nuevas Tecnologías de Información y Comunicación) en el ámbito político electoral no pueden limitarse únicamente a procesos públicos vinculantes. Es más, la gran mayoría de los ejercicios mundiales de voto electrónico corresponden no sólo a procesos diferentes, sino que además no revisten carácter vinculante. Nos encontramos así con que las pruebas pilotos, los experimentos no vinculantes son el principal activo en el total de votaciones electrónicas.

Efectivamente, el voto electrónico, en cualquiera de sus modalidades, debe entenderse como un mecanismo para la extensión de la cultura democrática en todo el entramado social.

Procesos electorales en el seno de instituciones universitarias, asociaciones de estudiantes, asociaciones profesionales, partidos políticos. Constituyen espacios especialmente indicados en los que mejorar y facilitar la participación electoral. Si a el lo unimos la utilización de dichas soluciones tecnológicas para la realización de consultas ciudadanas, vinculantes o no, conseguiremos avanzar en la profundización de las prácticas democráticas más allá de los procesos electorales institucionales.

8.5.1.4. El voto electrónico es solo para países ricos: Referencia a la capacidad económica de las sociedades que desarrollan y/o aplican procesos de voto electrónico. Dicha afirmación pudiera parecer cierta, debido a los altos costos económicos vinculados al desarrollo o adquisición de equipos de votación electrónica, lo cierto es que un simple repaso a la distribución geográfica nos muestra lo erróneo de esta consideración. Además de buena parte de los condados de EE.UU. o de diferentes aplicaciones en la Unión Europea (Francia, Bélgica, Holanda, Suiza), lo cierto es que encontramos procesos de votación electrónica en países tan distintos como Argentina, México, Brasil, Nueva Zelanda, Australia, Singapur, España, Estonia o Kazajstán, por citar algunos. En cualquier caso, esta variedad geográfica contradice en buena medida el determinismo económico del voto electrónico, siendo posible su implementación más allá del potencial socio económico del país en cuestión.

8.6. Motivos que justifican la introducción del voto electrónico

Tras haber intentando deshacer los malentendidos existentes sobre la definición y características del voto electrónico, es preciso abordar cuáles son las razones que están detrás de la adopción de dichos sistemas. En este sentido, consideramos que el conjunto de experiencias hasta la fecha pueden agruparse bajo cuatro grandes motivaciones vinculadas con:

1. Desarrollo tecnológico.
2. Profundización en los mecanismos de democracia participativa.
3. Búsqueda de mayor legitimación democrática.
4. Complejidad del proceso electoral.

En el primer caso hacemos referencia a aquellas sociedades en las que se ha producido un elevado desarrollo tecnológico y que, por lo tanto, observan el ámbito electoral como una etapa más en ese crecimiento. Caracterizados por su elevada producción tecnológica, países

como Japón o Suecia han iniciado procesos de desarrollo de aplicaciones tecnológicas vinculadas al voto electrónico, si bien aún no han incorporado dichas soluciones a sus respectivos sistemas electorales.

En segundo lugar, se encuentran aquellos países cuya cultura política democrática está plenamente consolidada y, además, utilizan de manera habitual mecanismos de participación ciudadana para el diseño de políticas públicas. El caso paradigmático en este sentido es Suiza, con elevados índices de voto postal para multitud de consultas y referendos sobre las más variadas cuestiones sociopolíticas. No es raro, entonces, que algunos cantones suizos sean líderes en la adopción de soluciones de voto electrónico remoto para facilitar la participación ciudadana en dichos procesos, así como para seguir profundizando en el ejercicio de estos mecanismos de democracia participativa.

Otra de las razones, no aducidas en este sentido de forma directa pero sí claramente perceptible en su desarrollo, es la que vincula la adopción de las **NTIC** (Nuevas Tecnologías de Información y Comunicación) con los procesos de legitimación democrática del sistema político. Si bien ésta es una cuestión problemática y que no podríamos abordar aquí, lo cierto es que el análisis de algunos de los países que han adoptado migrado completamente, para ser más exactos al voto electrónico no destacan precisamente por sus altos niveles de consolidación democrática. Seguramente, los dos ejemplos paradigmáticos en este sentido son Venezuela y la India, aunque por motivos diferentes. En el caso del subcontinente asiático, la estratificación social imperante basada en el sistema de castas hace realmente difícil su clasificación dentro de los estándares democráticos habituales. Es por ello por lo que, junto con los motivos que a continuación se mencionan respecto a la complejidad del proceso electoral, todo parece indicar que la adopción de un sistema de voto electrónico esté operando también como mecanismo legitimador de las diferentes correlaciones de fuerzas existentes en el país.

Finalmente, con toda probabilidad la razón más poderosa para justificar los procesos de introducción o migración al voto electrónico es la primera de las citadas. Así, aquellos países cuyos sistemas electorales presentan diferentes grados de complejidad procedimental plantean la necesidad de simplificar el proceso de emisión del voto por parte de los ciudadanos. Básicamente, podríamos establecer dos grandes tipos de dificultades en el proceso electoral:

- Las problemáticas derivadas de la forma de expresión del voto.
- Aquellas vinculadas con el tamaño del proceso electoral.

Dudas

- Conveniencia político – electoral + optimismo tecnológico.
- Reducción de los costos generales.
- Capacidad de generar más y mejor participación.
- Eliminación de los votos nulos.
- Brecha democrática.
- Seguridad y garantía del sufragio (libre, igual, universal y secreto).
- Verificabilidad individual y colectiva.
- Aceptación ciudadana.

Certezas

- Modernización de los procesos político – electorales.
- Reducción de gastos puntuales.
- Incremento de la participación de determinados sectores sociales.
- Múltiples aplicaciones participativas.
- Necesidad de autoridades electorales específicas.
- Coexistencia con el voto tradicional.
- Implementación gradual y real.

9. Sistemas Biométricos

Algunos sistemas de registro de votantes se basan en el uso de biometría. Los oficiales de registro usualmente verifican alguna característica intrínseca al votante que le identifica de manera única, por ejemplo, una identificación con fotografía (reconocimiento facial) o una firma manuscrita (caligrafía). Sin embargo, la precisión en la identificación de tales características personales se dificulta si consideramos que los oficiales de registro no son expertos en reconocimiento de características biométricas.

Los sistemas biométricos se especializan en la identificación de usuarios a partir del procesamiento de características únicas, ya sea físicas o de comportamiento. Dichos

sistemas se clasifican en base a la característica del usuario utilizada para llevar a cabo la identificación, ya sea el ADN, huella dactilar, retina, escritura, voz. Sin embargo, la precisión en los diferentes sistemas biométricos es variada y cada uno de ellos presenta ventajas y desventajas.

Requisitos de un sistema biométrico

- **Universalidad:** Todos los usuarios deben poseer la característica biométrica en la que se basa la identificación.
- **Unicidad:** La característica debe distinguir a cada individuo de forma única.
- **Permanencia:** La característica biométrica debe permanecer en el individuo con el paso del tiempo.
- **Obtención:** El sistema biométrico debe proporcionar un medio o interfaz para obtener la característica fácilmente.
- **Rendimiento:** Se refiere a la rapidez y precisión en la identificación a través de la característica biométrica, así como a los recursos requeridos para llevar a cabo dicha identificación.
- **Aceptación:** Indica el nivel de aceptación entre las personas que deben aportar su característica biométrica para llevar a cabo la identificación.
- **Robustez:** Este requisito refleja el nivel de resistencia contra métodos fraudulentos que traten de engañar al sistema biométrico.

En el caso de un sistema de registro remoto de votantes debemos considerar un requisito adicional, el sistema biométrico debe estar disponible remotamente para la mayoría de los votantes hacia los que está dirigido el uso del sistema. Por lo tanto, la adquisición de la información biométrica debe ser llevada a cabo utilizando medios o dispositivos estándares que estén al alcance de los votantes remotos. Esta restricción reduce el número de candidatos a las características de firmas manuscritas y de voz. La firma manuscrita puede ser adquirida remotamente a través de la digitalización (escaneo) del formulario de registro en donde se incluye la firma del votante. Por su parte, la voz puede ser adquirida remotamente a través de un teléfono estándar.

10. LA RED y sus Protocolos

La suites de protocolos son colecciones de protocolos que habilitan la comunicación entre dos host a través de una red, Un Protocolo de red es una descripción formal de un conjunto de reglas y convenciones que gobiernan el modo en que se comunican los dispositivos en una red.los protocolos determinan el formato, al temporización, la secuenciación y el control de errores en la comunicación de datos. Sin los protocolos la computadora no puede crear o reconstruir el flujo de bits entrante desde otra computadora a fin de obtener los datos originales.

Los protocolos controlan los aspectos de la comunicación de datos, determinan como se construyen la red física, como se conectan las computadoras a la red, como se formatean los datos para la transmisión y como se envían los datos. Esas reglas sobre redes la crean y mantienen diferentes organizaciones y comités:

- IEEE (Institute of electrical and Electronic Engineers) Instituto de Ingenieros Eléctricos y Electrónicos.
- ANSI (American NacionalEstándar Institute) Instituto Nacional Americano de Normalización.
- TIA (Telecomunication Industries Association) Asociación de la industrias de telecomunicaciones.
- EIA (Electronic Industries Alliance) Asociación de industrias Electrónicas.
- ITU (Internacional Communication Union) Unión internacional de telecomunicaciones, antiguamente conocido como CCIT (Comité de consultoría internacional para telegrafía y comunicación.

10.1. Redes LAN: Es un sistema de comunicación entre computadores donde la distancia debe ser pequeña para pode compartir información y recurso; ejemplo: Ethernet y la (CSMS-CD), ésta última utiliza un mecanismo denominado Call Sense Múltiple Access- Colisión Detect esto quiere decir que el cable solo puede ser utilizado por el equipo que esté usando hasta que lo deje libre.

Están constituidas por computadoras, tarjetas de interfaz de red, dispositivos periféricos, medios de red y dispositivos de red. Las LAN´s permiten a las empresas que emplean

tecnología de computación compartir local y eficazmente ficheros e impresoras y posibilitar las comunicaciones internas, como el correo electrónico. Unen entre sí datos, comunicaciones locales y equipos de computación.

Las LAN´s están diseñadas para hacer lo siguientes:

- Operar dentro de una zona geográfica limitada.
- permitir a muchos usuarios acceder a medios de gran ancho de banda.
- proporcionar conectividad a tiempo completo a los servicios locales.
- conectar físicamente dispositivos adyacentes.

Algunas tecnologías LAN´s comunes son:

- Ethernet.
- Token ring.
- FDDI.

10.2. Redes MAN: Es una red de banda ancha que puede cubrir un área extensa geográficamente con capacidad de prestar múltiples servicios mediante la transmisión de datos, de voz y video hace uso de medios como la fibra óptica y par trenzado de cobre a gran velocidad. Tiene muchas aplicaciones:

- Interconexión de redes de área local (RAL).
- Interconexión de centralitas telefónicas digitales (PBX y PABX).
- Transmisión de imagen y video.
- Pasarelas para redes de áreas extensas (WAN).

10.3. Redes WAN: se prevé que proporciones los enlaces necesarios entre LAN para hacer posible lo que han nombrado autopista de la información. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios (host). Estas LAN acceden a la subred de la WAN por medio de un router.

Las WAN interconectan LAN, que proporcionan acceso a las computadoras o servidores de ficheros en otros lugares, como las WAN conectan redes de usuario sobre un área geográfica

grande, hace posible que las empresas puedan comunicarse a grandes distancias. Mediante el uso de WAN es posible que computadoras sean compartidos con lugares diferentes.

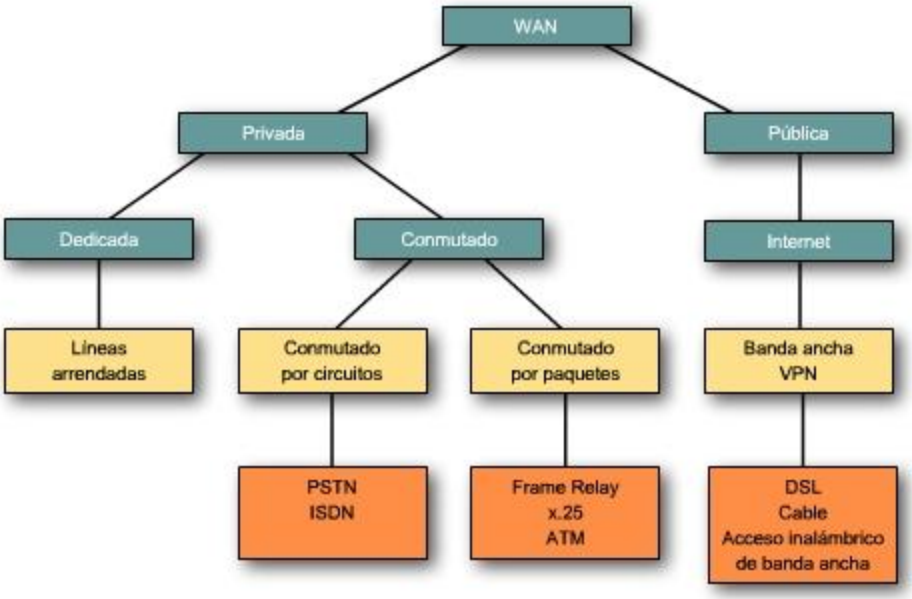
Las WAN proporcionan comunicaciones instantáneas a través de grandes áreas geográficas.

La posibilidad de enviar a alguien un mensaje instantáneo en cualquier lugar del mundo ofrece las mismas capacidades de comunicación que solo eran posibles si las personas estaban en la misma oficina física.

El software de colaboración ofrece acceso a los recursos y a la información real permitiendo reuniones remotas en lugar de personas. Las redes de área amplia también han creado un clase de trabajadores denominadas tele trabajadores personas que no tienen que abandonar su casa para ir a trabajar. Las WAN están diseñadas para hacer lo siguientes:

- Operar sobre grandes áreas geográficamente separadas.
- Permitir que los usuarios mantengan comunicación en tiempo real con otros usuarios.
- Proporcionar recursos remotos a tiempo completo conectados a los servicios locales.
- Ofrecer servicios de correo electrónico, transferencias de ficheros y comercio electrónico.

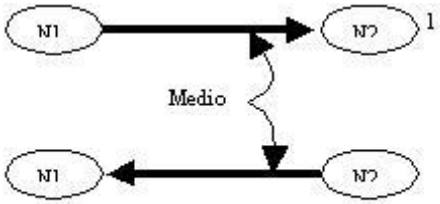
Opciones de conexión de enlace WAN



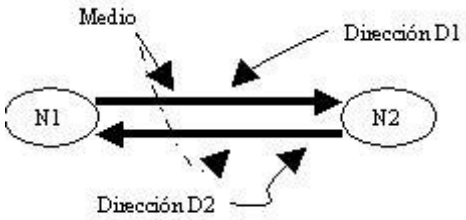
Dado que se trabajará sobre el Internet, abordaremos algunos aspectos: La finalidad del Internet es conectar muchas redes LAN, a través de una conexión troncal backbone, y puede hacer uso de distintos tipos de comunicación como de protocolos:

11. Tipos de comunicación:

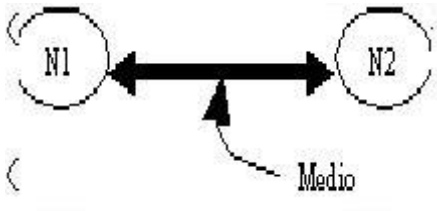
Comunicación Simplex o Bidireccional:



Comunicación Half - Duplex:



Comunicación Full-Dúplex:



Los protocolos sobre los que trabajan son establecidos por las organizaciones internacionales, como la ISO, IEEE, y ANSI. Cabe mencionar que estos estándares deben proporcionar alta fiabilidad, alta seguridad, inmunidad al ruido.

Se entiende por alta fiabilidad: Al porcentaje de la tasa de error mientras se encuentra en operación, es decir a la cantidad de bits erróneos que se transmiten, en el caso de la fibra óptica este porcentaje es menor.

Alta Seguridad: La fibra óptica ofrece un medio seguro de transmisión, está solo se puede interrumpir solamente si se corta.

Inmunidad al ruido: Se refiere a la interferencia electromagnética que retardarían la transmisión de la información.

12. Arquitectura de Redes

La arquitectura de red es el medio más efectivo en cuanto a costos para desarrollar e implementar un conjunto coordinado de productos que se puedan interconectar. La arquitectura es el plan con el que se conectan los protocolos y otros programas de software. Esto es benéfico tanto para los usuarios de la red como para los proveedores de hardware y software.

12.1. Características de la Arquitectura

- **Separación de funciones:** Dado que las redes separa los usuarios y los productos que se venden evolucionan con el tipo, debe haber una forma de hacer que las funciones mejoradas se adapten a la ultima. Mediante la arquitectura de red el sistema se diseña con alto grado de modularidad, de manera que los cambios se puedan hacer por pasos con un mínimo de perturbaciones.

- **Amplia conectividad:** El objetivo de la mayoría de las redes es proveer conexión óptima entre cualquier cantidad de nodos, teniendo en consideración los niveles de seguridad que se puedan requerir.

- **Recursos compartidos:** Mediante las arquitecturas de red se pueden compartir recursos tales como impresoras y bases de datos, y con esto a su vez se consigue que la operación de la red sea más eficiente y económica.

- **Administración de la red:** Dentro de la arquitectura se debe permitir que el usuario defina, opere, cambie, proteja y de mantenimiento a la de.
- **Facilidad de uso:** Mediante la arquitectura de red los diseñadores pueden centra su atención en las interfaces primarias de la red y por tanto hacerlas amigables para el usuario.

- **Normalización:** Con la arquitectura de red se alimenta a quienes desarrollan y venden software a utilizar hardware y software normalizados. Mientras mayor es la normalización, mayor es la colectividad y menor el costo.

- **Administración de datos:** En las arquitecturas de red se toma en cuenta la administración de los datos y la necesidad de interconectar los diferentes sistemas de administración de bases de datos.

- **Interfaces:** En las arquitecturas también se definen las interfaces como de persona a red, de persona y de programa a programa. De esta manera, la arquitectura combina los protocolos apropiados (los cuales se escriben como programas de computadora) y otros paquetes apropiados de software para producir una red funcional.

- **Aplicaciones:** En las arquitecturas de red se separan las funciones que se requieren para operar una red a partir de las aplicaciones comerciales de la organización. Se obtiene más eficiencia cuando los programadores del negocio no necesitan considerar la operación.

12.2. Funciones de la Arquitectura Ethernet

12.2.1. Encapsulación de datos

- Formación de la trama estableciendo la delimitación correspondiente.
- Direccionamiento del nodo fuente y destino.
- Detección de errores en el canal de transmisión.

12.2.2. Manejo de Enlace

- Asignación de canal.
- Resolución de contención, manejando colisiones.

12.2.3. Codificación de los Datos

- Generación y extracción del preámbulo para fines de sincronización.
- Codificación y decodificación de bits.

12.2.4. Acceso al Canal

- Transmisión / Recepción de los bits codificados.
- Sensibilidad de portadora, indicando tráfico sobre el canal.
- Detección de colisiones, indicando contención sobre el canal.

12.2.5. Formato de Trama

- En una red Ethernet cada elemento del sistema tiene una dirección única de 48 bits, y la información es transmitida serialmente en grupos de bits denominados tramas. Las tramas incluyen los datos a ser enviados, la dirección de la estación que debe recibirlos y la dirección de la estación que los transmite

- Cada interface Ethernet monitorea el medio de transmisión antes de una transmisión para asegurar que no esté en uso y durante la transmisión para detectar cualquier interferencia.

- En caso de alguna interferencia durante la transmisión, las tramas son enviadas nuevamente cuando el medio esté disponible. Para recibir los datos, cada estación reconoce su propia dirección y acepta las tramas con esa dirección mientras ignora las demás.

- El tamaño de trama permitido sin incluir el preámbulo puede ser desde 64 a 1518 octetos. Las tramas fuera de este rango son consideradas inválidas.

12.2.5.1. Campos que Componen la Trama

12.2.5.1.1. El preámbulo: Inicia o encabeza la trama con ocho octetos formando un patrón de 1010, que termina en 10101011. Este campo provee sincronización y marca el límite de trama.

12.2.5.1.2. Dirección destino: Sigue al preámbulo o identifica la estación destino que debe recibir la trama, mediante seis octetos que pueden definir una dirección de nivel físico o múltiples direcciones, lo cual es determinado mediante el bit de menos significación del primer byte de este campo. Para una dirección de nivel físico este es puesto en 0 lógico, y la misma es única a través de toda la red Ethernet. Una dirección múltiple puede ser dirigida a un grupo de estaciones o a todas las estaciones y tiene el bit de menos significación en 1 lógico. Para direccionar todas las estaciones de la red, todos los bits del campo de dirección destino se ponen en 1, lo cual ofrece la combinación FFFFFFFFFFFFH.

12.2.5.1.3. Dirección fuente: Este campo sigue al anterior. Compuesto también por seis octetos, que identifican la estación que origina la trama.

Los campos de dirección son además subdivididos: Los primeros tres octetos son asignados a un fabricante, y los tres octetos siguientes son asignados por el fabricante. La tarjeta de red podría venir defectuosa, pero la dirección del nodo debe permanecer consistente. El chip de memoria ROM que contiene la dirección original puede ser removido de una tarjeta vieja para ser insertado en una nueva tarjeta, o la dirección puede ser puesta en un registro mediante el disco de diagnostico de la tarjeta de interfaces de red (NIC). Cualquiera que sea el método utilizado se deber ser cuidadoso para evitar alteración alguna en la administración de la red.

12.2.5.1.4. Tipo: Este es un campo de dos octetos que siguen al campo de dirección fuente, y especifican el protocolo de alto nivel utilizado en el campo de datos. Algunos tipos serian 0800H para TCP/IP, y 0600H para XNS.

12.2.5.1.5. Campo de dato: Contiene los datos de información y es el único que tiene una longitud de bytes variable que puede oscilar de un mínimo de 46 bytes a un máximo de 1500.

El contenido de ese campo es completamente arbitrario y es determinado por el protocolo de alto nivel usado.

12.2.5.1.6 Frame Check Secuence: Este viene a ser el último campo de la trama, compuesto por 32 bits que son usados por la verificación de errores en la transmisión mediante el método CRC, considerando los campos de dirección tipo y de dato

12.3. Protocolo

Cada protocolo define dos interfaces diferentes:

- Interfaz del servicio (service interface).
- Interfaz sus iguales (peer interface).

12.3.1. Interfaz del servicio: Define la interfaz con otros objetos en el mismo computador que deseen utilizar sus servicios de comunicación. Por ejemplo, solicitud de envío y recepción de mensajes.

12.3.2 Interfaz con sus iguales: Define la forma y el significado de los mensajes que son intercambiados entre instancias locales y remotas del protocolo.

13. Modelo OSI

La International Standard Organization (ISO) fue una de las primeras organizaciones en definir formalmente la forma de conectar computadores. Esta organización creó el estándar Open System Interconection (OSI).

Esta arquitectura estándar define un particionamiento de las funcionalidades de las redes en siete capas donde uno o más protocolos implementan cada capa.

Esta arquitectura la podemos dividir en capas inferiores y capas superiores.

Las capas inferiores lidian con las señales eléctricas, trozos de datos binarios y encaminamiento de paquetes a través de las redes.

Las capas superiores se encargan de la gestión de las solicitudes del los clientes, respuestas de los servidores, representación de los datos y los protocolos de redes desde el punto de vista del usuario.

Funciones que deben ser cumplidas en una red

- Control de Errores: hacer más confiable el canal.
- Control de Flujo: evitar que un nodo lento sea inundado con PDU´s.
- Segmentación y Ensamblaje: El emisor corta en pedazos más pequeños un mensaje y el receptor restituye el mensaje original.
- Multiplexación: compartir el canal.[6]

Interfaz del servicio:

Define la interfaz con otros objetos en el mismo computador que deseen utilizar sus servicios de comunicación. Por ejemplo, solicitud de envío y recepción de mensajes.

14. Seguridad y manejo de redes.

Queda pendiente la seguridad de la información sobre la autopista informática para ello se hace uso de encriptación o denominado Data EncryptionSystem (DES) el cual permite codificar y decodificar la información para evitar la intervención de terceros en la manipulación

[6]Redes de computadoras – Introducción – Arquitectura de Redes, Gilberto Díaz

y recepción de información. Internet hace uso de protocolos para solventar la seguridad de los datos, se mencionan:

- ✓ **TCP/IP:** Protocolo de comunicación que permite la interconectividad entre varios ordenadores, ya sean de diferencia lógica (software) o física (hardware).
- ✓ **ICMP (Protocolo de mensajes para el control Interred):** Regula la transmisión de mensajes de error y control entre los sistemas principales y las puertas.
- ✓ **ARP (Protocolo de resolución de direcciones):** Asigna direcciones Internet a direcciones físicas.
- ✓ **RARP (Protocolo de resolución de direcciones inversa):** Asigna direcciones físicas a direcciones Internet.
- ✓ **UDP (Protocolo de datagrama de usuario):** Permite establecer servicios de envío de paquetes fiables y sin conexión entre los clientes.
- ✓ **FTP (Protocolo de Transferencia de archivos):** Proporciona servicios de nivel de aplicación para la transferencia de archivos.
- ✓ **RIP (Protocolo de encaminamiento de información):** Determina el mejor método de encaminamiento.
- ✓ **OSPF (Open Shortest Path First):** Protocolo alternativo de encaminamiento.
- ✓ **DNS (Sistema de nombre de dominio):** Determina la dirección numérica a partir del nombre de la máquina.
- ✓ **BOOTP (Boot Protocol):** Inicia una máquina de red simplemente leyendo la información de arranque que se encuentra disponible en un servidor.
- ✓ **TFTP (Protocolo de traslado de archivo trivial):** Es un método simple de transferencia de ficheros que utiliza como transporte el protocolo UDP.

Para abordar la prueba del segundo elemento como es el software o la implementación habilitada se realizaran mediciones con la finalidad de ofrecer un sistema robusto, confiable y eficaz como resultado de su construcción. En esta etapa se debe incorporar la planificación de una base de datos la cual debe estar normalizada-. Construir un software <<robusto>> va a depender de muchos factores como la integridad de la base de datos, del tipo de TIC´s utilizada, la seguridad y capacidad de probarse a sí mismo. Del mismo modo el resultado desarrollará un enfoque de mejora continua al proceso de prueba.

El diseño de base de datos relacionales tiene como objetivo la definición de una <<buena>> colección de esquemas. Un mal diseño pueden originar: Repetición de la información, Imposibilidad de representar cierta información (Anomalías en la inserción, modificación y borrado). En cambio un buen diseño tiene que conseguir: Eliminar la redundancia de los datos, asegurar que todas las relaciones entre los atributos estén representadas y facilitar el control de las modificaciones para evitar violaciones de las restricciones de integridad.

El activo más importante en las organizaciones públicas, privadas y de cualquier índole, es la información que tienen. Entre más grande es la organización más grande es el interés de mantener la seguridad en la red, por lo tanto, es de suma importancia el asegurar la seguridad de la información.

La seguridad no es solamente el implementar usuarios y contraseñas, es el implementar políticas que garanticen la seguridad tanto física como lógica de la información. Dentro del entorno de la red se debe asegurar la privacidad de la información y de proteger las operaciones de daños no intencionados como deliberados.

Dentro de las redes inalámbricas el sentido de seguridad es más sentido debido a la naturaleza de las mismas. En sus inicios la seguridad en este tipo de redes era muy deficiente y algunas personas de daban a la tarea de encontrar redes inalámbricas para acceder a ellas desde las calles.

14.1. Planificación de la Seguridad en Redes

La planificación de la seguridad en el diseño de la red es de suma importancia pues de esto depende el buen desempeño de la red y nos evita trabajo posterior y pérdida de datos y posibles daños a la red.

En ocasiones se considera el tema de seguridad fuera de tiempo lo cual trae consecuencias de retrabado, gastos excesivos y posibles pérdidas de información.

Algunos puntos que debemos tomar en cuenta son:

- Accesos no autorizados.

- Daño intencionado y no intencionado.
- Uso indebido de información (robo de información).

14.2. Permisos de acceso

La seguridad basada en autentificación de usuario es la más usada, nos permite administrar y asignar derechos a los usuarios de la red. Permitiendo o denegando los accesos a los recursos a través de una base de datos en el servidor.

El trabajo del administrador deberá incluir la administración de usuarios. Otra manera de administrar usuarios es mediante el uso de grupos de usuarios, el cual nos da la facilidad de aplicar las políticas de seguridad a grupos específicos los cuales heredaran estas a los miembros de dicho grupo.

14.3. Medidas Adicionales

Se debe tomar en cuenta el uso de cortafuegos que permita administrar el acceso de usuarios de otras redes así como el monitorear las actividades de los usuarios de la red, permitiendo el tener una bitácora de sucesos de red.

Las bitácoras son de gran utilidad para aplicar auditorias a la red. La revisión de los registros de eventos dentro de la red permite ver las actividades de los usuarios dentro de la red, esto permite al administrador darse cuenta de los accesos no autorizados por parte de los usuarios y tomar las medidas que faciliten incrementar la seguridad.

La auditoria permite monitorear algunas de las siguientes actividades o funciones:

- Intentos de acceso.
- Conexiones y desconexiones de los recursos designados.
- Terminación de la conexión.
- Desactivación de cuentas.
- Apertura y cierre de archivos.
- Modificaciones realizadas en los archivos.
- Creación o borrado de directorios.

- Modificación de directorios.
- Eventos y modificaciones del servidor.
- Modificaciones de las contraseñas.
- Modificaciones de los parámetros de entrada.

Estas medidas se podrán implementar más o menos fáciles dependiendo de nuestro sistema operativo de red, ya que algunos sistemas operativos tienen la facilidad de administrar las auditorias que el administrador determine en forma sencilla. Se puede implementar algoritmos de encriptación de datos para la información relevante. Hay algunos organismos que certifican este tipo de software y garantizan la confidencialidad de los datos a través de la red, en especial en Internet, donde la seguridad de nuestra información es delicada. El funcionamiento de estos sistemas de encriptación funcionan de la siguiente manera: el emisor aplica el algoritmo de encriptación a los datos, estos viajaran a través de la red de tal forma que si algún intruso quiera verla no le será posible. Al llegar al destino se aplicara un algoritmo inverso que permita traducir los datos a su forma original.

También se pueden implementar medidas de identificación biométrica como lectores de huella digital, escaneo de palma de mano, entre otros, esta tecnología es más segura que la simple identificación de nombre de usuario y contraseña ya que el usuario no tendrá que recordar contraseñas que en algunos casos son complejas y difíciles de recordar además que a diferencia de las contraseñas la huella digital no se puede transferir a otros usuarios y no puede ser robada.

14.4. Protocolos

En informática, un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red por medio de intercambio de mensajes. Éste es una regla o estándar que controla o permite la comunicación en su forma más simple, puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos. A su más bajo nivel, éste define el comportamiento de una conexión de hardware.[7]

[7] Protocolos, http://es.kioskea.net/contents/internet/protocol.php3

Un protocolo es un método estándar que permite la comunicación entre procesos (que potencialmente se ejecutan en diferentes equipos), es decir, es un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red. Existen diversos protocolos de acuerdo a cómo se espera que sea la comunicación. Algunos protocolos, por ejemplo, se especializarán en el intercambio de archivos (FTP); otros pueden utilizarse simplemente para administrar el estado de la transmisión y los errores (como es el caso de ICMP).

En Internet, los protocolos utilizados pertenecen a una sucesión de protocolos o a un conjunto de protocolos relacionados entre sí. Este conjunto de protocolos se denomina TCP/IP.

Entre otros, contiene los siguientes protocolos:

- **HTTP**
- **FTP**
- **ARP**
- **ICM P**
- **IP**
- **TCP**
- **UDP**
- **SMTP**
- **Telnet**
- **NNTP**

14.4.1. Propiedades típicas

Si bien los protocolos pueden variar mucho en propósito y sofisticación, la mayoría especifica una o más de las siguientes propiedades:

- Detección de la conexión física subyacente (con cable o inalámbrica), o la existencia de otro punto final o nodo.
- Handshaking.
- Negociación de varias características de la conexión.

- Cómo iniciar y finalizar un mensaje.
- Procedimientos en el formateo de un mensaje.
- Qué hacer con mensajes corruptos o formateados incorrectamente (corrección de errores).
- Cómo detectar una pérdida inesperada de la conexión, y qué hacer entonces.
- Terminación de la sesión y/o conexión.

14.4.2. Protocolo orientado a conexión y protocolo no orientado a conexión

14.4.2.1. Protocolos orientados a conexión: Estos protocolos controlan la transmisión de datos durante una comunicación establecida entre dos máquinas. En tal esquema, el equipo receptor envía acuses de recepción durante la comunicación, por lo cual el equipo remitente es responsable de la validez de los datos que está enviando. Los datos se envían entonces como flujo de datos. TCP es un protocolo orientado a conexión.

14.4.2.2. Protocolos no orientados a conexión: Este es un método de comunicación en el cual el equipo remitente envía datos sin avisarle al equipo receptor, y éste recibe los datos sin enviar una notificación de recepción al remitente. Los datos se envían entonces como bloques (datagramas). UDP es un protocolo no orientado a conexión.

14.4.3. Protocolo e implementación

Un protocolo define únicamente cómo deben comunicar los equipos, es decir, el formato y la secuencia de datos que van a intercambiar. Por el contrario, un protocolo no define cómo se programa el software para que sea compatible con el protocolo. Esto se denomina implementación o la conversión de un protocolo a un lenguaje de programación.

Los protocolos de comunicación permiten el flujo información entre equipos que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas hablen el mismo idioma. El protocolo TCP/IP fue creado para las comunicaciones en Internet.

Para que cualquier computador se conecte a Internet es necesario que tenga instalado este protocolo de comunicación.[8]

14.4.4. Niveles de abstracción

En el campo de las redes informáticas, los protocolos se pueden dividir en varias categorías. Una de las clasificaciones más estudiadas es la OSI.

Según la clasificación OSI, la comunicación de varios dispositivos ETD se puede estudiar dividiéndola en 7 niveles, que son expuestos desde su nivel más alto hasta el más bajo:

Nivel	Nombre	Categoría
Capa 7	Nivel de aplicación	**Aplicación**
Capa6	Nivel de presentación	
Capa 5	Nivel de sesión	
Capa 4	Nivel de transporte	
Capa 3	Nivel de red	**Transporte de Datos**
Capa2	Nivel de enlace de datos	
Capa 1	Nivel físico	

A su vez, esos 7 niveles se pueden subdividir en dos categorías, las capas superiores y las capas inferiores. Las 4 capas superiores trabajan con problemas particulares a las aplicaciones, y las 3 capas inferiores se encargan de los problemas pertinentes al transporte de los datos.

Los protocolos de cada capa tienen una interfaz bien definida. Una capa generalmente se comunica con la capa inmediata inferior, la inmediata superior, y la capa del mismo nivel en otros computadores de la red. Esta división de los protocolos ofrece abstracción en la comunicación.

[8] Protocolo informática, http://es.wikipedia.org/w/index.php?title=Protocolo_(informática)&oldid=60754847

Una aplicación (capa nivel 7) por ejemplo, solo necesita conocer cómo comunicarse con la capa 6 que le sigue, y con otra aplicación en otro computador (capa 7). No necesita conocer nada entre las capas de la 1 a la 5. Así, un navegador web (HTTP, capa 7) puede utilizar una conexión Ethernet o PPP (capa 2) para acceder a la Internet, sin que sea necesario cualquier tratamiento para los protocolos de este nivel más bajo. De la misma forma, un router sólo necesita de las informaciones del nivel de red para enrutar paquetes, sin que importe si los datos en tránsito pertenecen a una imagen para un navegador web, un archivo transferido vía FTP o un mensaje de correo electrónico.

Ejemplos de protocolos de RED

- **Capa 1: Nivel físico**
  - ✓ Cable coaxial o UTP categoría 5, categoría 5e, categoría 6, categoría 6a Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232.

- **Capa 2: Nivel de enlace de datos**
  - ✓ ARP, RARP, Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC, CDP

- **Capa 3: Nivel de red**
  - ✓ IP (IPv4, IPv6), X.25, ICM P, IGMP, NetBEUI, IPX, Appletalk.

- **Capa 4: Nivel de transporte**
  - ✓ TCP, UDP, SPX.

- **Capa 5: Nivel de sesión**
  - ✓ NetBIOS, RPC, SSL.

- **Capa 6: Nivel de presentación**
  - ✓ ASN.1.

- **Capa 7: Nivel de aplicación**
  - ✓ SNMP, SMTP, NNTP, FTP, SSH, HTTP, CIFS (también llamado SMB), NFS, Telnet, IRC, POP3, IM AP, LDAP, Internet Mail 2000, y en cierto sentido, WAIS y el desaparecido GOPHER.

14.5. Fases de desarrollo de una web

Para elegir las herramientas a utilizar, antes debemos identificar las fases del proceso que forman el ciclo de vida de un desarrollo web.

- **Diseño:** El diseño consiste en crear esbozos de la web final mediante una herramienta gráfica.

- **Maquetación HTML:** La maquetación consiste en convertir los esbozos creados en la fase anterior en plantillas HTML, su respectiva hoja de estilos, y las imágenes usadas.

- **Programación cliente**: La programación cliente consiste básicamente en Javascript. Una web puede no tener necesidad de hacer programación cliente, como puede ser una pequeña web corporativa con poca información estática, o puede que requiera enormes esfuerzos en esta fase, como ocurre con los proyectos Web 2.0.

- **Programación servidor:** En esta fase, que se desarrolla junto con la anterior, crearemos la aplicación web en un lenguaje de servidor, como la que usaremos PHP.

- **Depuración:** Esta fase enlaza la anterior con la siguiente, y es donde haremos las pruebas unitarias, aserciones, trazas.

- **Pruebas en local**: En nuestro servidor local haremos todas las pruebas posibles.

14.6. Navegadores

Un navegador o explorador web, conocido en inglés como web browser es un programa o software , por lo general gratuito, que nos permite visualizar páginas web a través de Internet además de acceder a otros recursos de información alojados también en servidores web, como pueden ser videos, imágenes, audio y archivos XML.

Pero un navegador también nos permite almacenar información o acceder a diferentes tipos de documentos en el disco duro, acceder a redes privadas, y crear marcadores (bookmarks). El acceso a otras páginas web a través de los hiperenlaces (hipervínculos o enlaces) se llama navegación, término del que deriva el nombre de navegador, aunque una minoría prefieren llamarlo ojeador que sería la traducción literal de la palabra browser.[9]

Algunos navegadores vienen incorporados a su sistema operativo como es el caso de Internet Explorer en Windows Microsoft, Safari en Mac OS X, o Firefox, Opera o Flock en Linux.

- Un Explorador Web o Navegador es un programa que permite visualizar páginas web en la red además de acceder a otros recursos, documentos almacenados y guardar información.
- El Navegador se comunica con el servidor a través del protocolo HTTP y le pide el archivo solicitado en código HTML, después lo interpreta y muestra en pantalla para el usuario.
- Los más populares son Internet Explorer, Mozilla Firefox, Safari, Opera y Google Chrome. Algunos Navegadores vienen integrados en el SO como Internet Explorer en Windows.

14.6.1. Cómo funciona el navegador

Los navegadores se comunican con los servidores web por medio del protocolo de transferencia de hipertexto (HTTP) para acceder a las direcciones de Internet (URLs) a través de los motores de búsqueda.

[9] Que es un navegador, explorador o buscador, http://www.masadelante.com/faqs/que-es-un-navegador

La mayoría de los exploradores web admiten otros protocolos de red como HTTPS (la versión segura de HTTP), Gopher, y FTP, así como los lenguajes de marcado o estándares HTML y XHTML de los documentos web. Los navegadores además interactúan con complementos o aplicaciones (Plug-ins) para admitir archivos Flash y programas en Java (Java applets).

14.6.2. Características de los navegadores

Todos los navegadores incluyen la mayoría de las siguientes características: navegación por pestañas, bloqueadora de ventanas emergentes, soporte para motores de búsqueda, gestora de descargas, marcadores, corrector ortográfico, y atajos del teclado. Para mantener la privacidad casi todos los navegadores ofrecen maneras sencillas de borrar cookies, cachés web y el historial.

Las suites de Internet son aquellos exploradores web que incluyen programas integrados capaces de leer noticias de Usenet, correos electrónicos, e IRC, que son chats de texto en tiempo real a través de los protocolos IMAP, NNTP y POP.

Suelen utilizar el protocolo de seguridad HTTPS a través de los protocolos criptográficos SSL/TLS para proteger los datos de intercambio con los servidores web. También suelen contar con protección antiphishing y antimalware.

14.7. HTTP

HTTP es el protocolo mediante el cual se transfiere la información en Internet, es el encargado de descargar la información de una página web a la computadora. El significado de http es Protocolo de Transferencia de Hipertexto (*hypertext transfer protocol* en ingles).

Las páginas web están creadas con un lenguaje de programación llamado HTML (HyperText Markup Language) las cuales a su vez están alojadas en servidores para poder visualizarlas cada vez que se requiera utilizando la dirección (URL) asignada a estas, y es aquí cuando el http entra en acción.

Cuando algún cliente solicita la información que hay en un servidor web tecleando la dirección (URL), el Protocolo de Transferencia de Hipertexto http descarga la información solicitada para que el cliente pueda visualizarla.[10]

El proceso más detallado sería el siguiente:

- **Se realiza una conexión:** El cliente trata de hacer una conexión con el servidor de la dirección web que fue tecleada.
- **Se envía una solicitud:** Una vez establecida la conexión el cliente (navegador) envía una petición al servidor web para tratar de descargar la información contenida en este.
- **Respuesta:** El servidor web envía una respuesta, en este caso sería la descarga de la información solicitada por el cliente.
- **Desconexión:** Una vez recibida la respuesta se procede a realizar la desconexión. Esta puede venir tanto del cliente como del servidor web.

14.8. Apache

Apache es el servidor web hecho por excelencia, su configurabilidad, robustez y estabilidad hacen que cada vez millones de servidores reiteren su confianza en este programa. La historia de Apache se remonta a febrero de 1995, donde empieza el proyecto del grupo Apache, el cual está basado en el servidor Apache httpd de la aplicación original de NCSA. El desarrollo de esta aplicación original se estancó por algún tiempo por lo que varios web máster siguieron creando sus parches para sus servidores web hasta que se contactaron vía email para seguir en conjunto el mantenimiento del servidor web, fue ahí cuando formaron el grupo Apache.

Fue así como fue creciendo el grupo Apache, hasta lo que es hoy. Aquella primera versión y sus sucesivas evoluciones y mejoras alcanzaron una gran implantación como software de servidor inicialmente solo para sistemas operativos UNIX y fruto de esa evolución es la versión para Windows.

[10] www.wevxs.com

Apache es una muestra, al igual que el sistema operativo Linux (un Unix desarrollado inicialmente para PC), de que el trabajo voluntario y cooperativo dentro de Internet es capaz de producir aplicaciones de calidad profesional difíciles de igualar.

La licencia Apache es una descendiente de la licencias BSD, no es GPL. Esta licencia permite hacer lo que quieras con el código fuente siempre que les reconozcas su trabajo.[11]

Razones del porqué la popularidad de este software libre grandemente reconocido en muchos ámbitos empresariales y tecnológicos:

- Corre en una multitud de Sistemas Operativos, lo que lo hace prácticamente universal.
- Apache es una tecnología gratuita de código fuente abierto. El hecho de ser gratuita es importante pero no tanto como que se trate de código fuente abierto. Esto le da una transparencia a este software de manera que si queremos ver que es lo que estamos instalando como servidor, lo podemos saber, sin ningún secreto, sin ninguna puerta trasera.
- Apache es un servidor altamente configurable de diseño modular. Es muy sencillo ampliar las capacidades del servidor Web Apache. Actualmente existen muchos módulos para Apache que son adaptables a este, y están ahí para que los instalemos cuando los necesitemos. Otra cosa importante es que cualquiera que posea una experiencia decente en la programación de C o Perl puede escribir un modulo para realizar una función determinada.
- Apache trabaja con gran cantidad de Perl, PHP y otros lenguajes de script. Perl destaca en el mundo del script y Apache utiliza su parte del pastel de Perl tanto con soporte CGI como con soporte mod perl. También trabaja con Java y páginas jsp. Teniendo todo el soporte que se necesita para tener páginas dinámicas.
- Apache te permite personalizar la respuesta ante los posibles errores que se puedan dar en el servidor. Es posible configurar Apache para que ejecute un determinado script cuando ocurra un error en concreto.

[11] Apache, http://www.digitallearning.es/blog/apache-servidor-web-configuracion-apache2-conf/

- Tiene un alto grado de confiabilidad en la creación y gestión de logs. Apache permite la creación de ficheros de log a medida del administrador, de este modo puedes tener un mayor control sobre lo que sucede en tu servidor.

14.9. Wamp

Un servidor WAMP es un PC con Windows que dispone de un servidor Apache, un gestor de bases de datos MySQL y el lenguaje de programación PHP. Las siglas WAMP son un acrónimo de Windows + Apache + MySQL + PHP.

Instalar y configurar un servidor Apache, un servidor MySQL y el lenguaje PHP, así como configurarlo para que interrelacionen entre ellos y el servidor funcione perfectamente, es una tarea compleja que solo pueden acometer informáticos profesionales. Para simplificar la tarea de instalar Apache + PHP + MySQL en Windows y acercar al gran público la posibilidad de disfrutar de estos servicios, existen los llamados paquetes WAMP que instalan y configuran automáticamente dichas aplicaciones para Windows y que proporcionan:[12]

- Servidor Web Apache
- Base de datos MySQL
- Lenguaje de programación PHP
- Accesos para el arranque y la parada de los servicios
- Facilidades para la configuración de los servicios

Un Servidor WAMP ofrece Apache + PHP + MySQL en un sistema Windows

Disponer de un Servidor WAMP, nos permitirá instalar aplicaciones web accesibles desde nuestra red local, y si abrimos el puerto 80 de nuestro router, también serán accesibles desde

[12] Wamp, http://recursostic.educacion.es/observatorio/web/es/software/servidores/800-monografico-servidores-wamp

Internet. La gran mayoría de las aplicaciones web libres existentes, requieren de Apache + MySQL + PHP para funcionar. Podemos instalar estas aplicaciones por separado y después configurarlas, pero instalando un paquete WAMP se instalan y configuran automáticamente dichas aplicaciones para Windows. Apache + MySQL + PHP son la base para poder instalar infinidad de aplicaciones web libres, entre las que destacamos:

- **Gestores de Contenidos orientados a sitios web:** Joomla, Drupal
- **Gestores de Contenidos orientados a educación:** Claroline, Moodle, Dokeos, MediaWiki
- **Blogs:** WordPress, Serendipity
- **Wikis:** Mediawiki, Tikiwiki, Dokuwiki
- **Foros:** phpBB, myBB
- **Galerías de imágenes:** Gallery, Coppermine

14.10. HTML

HTML es u n lenguaje de programación que se utiliza para el desarrollo de páginas de Internet. Se trata de la sigla que corresponde a Hyper Text Markup Language, es decir , Lenguaje de Marcas de Hipertexto, que podría ser t r aducido como Lenguaje de Formato de Documentos para Hiper texto.

EL HTML se encarga de desarrollar una descr ipción sobr e los contenidos qu e aparecen como textos y sobre su estruct ura , complement ando dich o text o con diversos objet os com fotografías, animaciones.

Es u n lenguaje muy simple y general qu e sirv e para definir otros leng uajes que tienen que ver con el formato de los document os. El t ex t o en él se crea a part ir de etiqu etas, también llamada stags, que permiten interconectar diversos conceptos y formatos.[13]

Si quieres crear sitios web, no hay otra solución que aprender HTML. Incluso si usas un programa como Dreamweaver, para la creación de sitios web, poseer unos conocimientos

[13] Que es HTML, http://definicion.de/html/

básicos de HTML hacen la vida mucho más fácil y tus sitios w eb mucho mejores. La buena noticia es que HTML es fácil de aprender y de usar. [14]

Pruebas en hosting

Realizaremos las últimas pruebas en el servidor del hosting para comprobar que el cambio de servidor no ha afectado a nada. Para evitar problemas, nuestro servidor local debe tener exactamente la misma configuración que el servidor del hosting.

14.11. PHP

Acrónimo de PHP Hypertext Preprocessor, es un lenguaje Open Source interpretado de alto nivel, especialmente pensado para desarrollos web y el cual puede ser embebido en páginas HTML. La mayoría de su sintaxis es similar a C, Java y Perl y es fácil de aprender. La meta de este lenguaje es permitir escribir a los creadores de páginas web, páginas dinámicas de una manera rápida y fácil, aunque se pueda hacer mucho más con PHP.

PHP no es lo mismo que un script escrito en otro lenguaje de programación como Perl o C, En vez de escribir un programa con muchos comandos para crear una salida en HTML, escribimos el código HTML con cierto código PHP embebido (introducido) en el mismo, que producirá cierta salida. El código PHP se incluye entre etiquetas especiales de comienzo y final que nos permitirán entrar y salir del modo PHP.

Lo que distingue a PHP de la tecnología Javascript, la cual se ejecuta en la máquina cliente, es que el código PHP es ejecutado en el servidor. El servidor web puede ser incluso configurado para que procese todos los ficheros HTML con PHP.

Lo mejor de usar PHP es que es extremadamente simple para el principiante, pero a su vez, ofrece muchas características avanzadas para los programadores profesionales.

[14] http://es.html.net/tutorials/html/lesson2.php

Aunque el desarrollo de PHP está concentrado en la programación de scripts en la parte del servidor, se puede utilizar para muchas otras cosas.

PHP puede hacer cualquier cosa que se pueda hacer con un script CGI, como procesar la información de formularios, generar páginas con contenidos dinámicos, o mandar y recibir cookies. Y esto no es todo, se puede hacer mucho más.

14.11.1. Características de PHP

- Orientado al desarrollo de aplicaciones web dinámicas con acceso a información almacenada en una base de datos.
- Es considerado un lenguaje fácil de aprender, ya que en su desarrollo se simplificaron distintas especificaciones, como es el caso de la definición de las variables primitivas, ejemplo que se hace evidente en el uso de php arrays.
- El código fuente escrito en PHP es invisible al navegador web y al cliente ya que es el servidor el que se encarga de ejecutar el código y enviar su resultado HTML al navegador. Esto hace que la programación en PHP sea segura y confiable.
- Capacidad de conexión con la mayoría de los motores de base de datos que se utilizan en la actualidad, destaca su conectividad con MySQL y PostgreSQL.
- Capacidad de expandir su potencial utilizando módulos (llamados *ext's* o extensiones).
- Posee una amplia documentación en su sitio web oficial, entre la cual se destaca que todas las funciones del sistema están explicadas y ejemplificadas en un único archivo de ayuda.
- Es libre, por lo que se presenta como una alternativa de fácil acceso para todos.
- Permite aplicar técnicas de programación orientada a objetos. Incluso aplicaciones como Zend framework, empresa que desarrolla PHP, están totalmente desarrolladas mediante esta metodología.
- No requiere definición de tipos de variables aunque sus variables se pueden evaluar también por el tipo que estén manejando en tiempo de ejecución.
- Tiene manejo de excepciones (desde PHP5).
- Si bien PHP no obliga a quien lo usa a seguir una determinada metodología a la hora de programar, aun haciéndolo, el programador puede aplicar en su trabajo cualquier técnica de programación o de desarrollo que le permita escribir código ordenado, estructurado y manejable. Un ejemplo de esto son los desarrollos que en PHP se han

hecho del patrón de diseño Modelo Vista Controlador (M VC), que permiten separar el tratamiento y acceso a los datos, la lógica de control y la interfaz de usuario en tres componentes independientes.

14.11.2. Inconvenientes

- Como es un lenguaje que se interpreta en ejecución, para ciertos usos puede resultar un inconveniente que el código fuente no pueda ser ocultado. La ofuscación es una técnica que puede dificultar la lectura del código pero no necesariamente impide que el código sea examinado.
- Debido a que es un lenguaje interpretado, un script en PHP suele funcionar considerablemente más lento que su equivalente en un lenguaje de bajo nivel, sin embargo este inconveniente se puede minimizar con técnicas de cache tanto en archivos como en memoria.

Las variables al no ser tipadas dificulta a los diferentes IDEs para ofrecer asistencias para el tipeado del código, aunque esto no es realmente un inconveniente del lenguaje en sí. Esto es solventado por Zend Studio añadiendo un comentario con el tipo a la declaración de la variable.[15]

Existen tres campos en los que scripts escritos en PHP son usados.

14.11.2.1. Scripts en la parte del servidor: Este es el campo más tradicional y el principal campo de trabajo. Se necesitan tres cosas para que esto funcione. El parseador PHP (CGI ó módulo), un servidor web y un navegador. Se necesita correr el servidor web con PHP instalado. El resultado del programa PHP se puede obtener a través del navegador, conectando con el servidor web. Consultar la sección Instrucciones de instalación para más información.

14.11.2.2. Scripts en línea de comandos: Se puedes crear un script PHP y correrlo sin ningún servidor web ó navegador. Solamente se necesita el parseador PHP para usarlo de esta manera. Este tipo de uso es ideal para scripts ejecutados regularmente desde cron (en

[15] PHP, http://es.wikipedia.org/wiki/PHP

Unix ó Linux) ó el Planificador de tareas (en Windows). Estos scripts también pueden ser usados para tareas simples de procesado de texto.

14.11.2.3. Escribir aplicaciones gráficas clientes: PHP no es probablemente el mejor lenguaje para escribir aplicaciones gráficas, pero si se maneja bien PHP, y se deseara utilizar algunas características avanzadas en programas clientes, se puede utilizar PHP-GTK para escribir dichos programas. Es también posible escribir aplicaciones independientes de una plataforma. PHP-GTK es una extensión de PHP, no disponible en la distribución principal.

PHP puede ser utilizado en cualquiera de los principales sistemas operativos del mercado, incluyendo Linux, muchas variantes Unix (incluido HP - UX, Solaris y OpenBSD), Microsoft Windows, Mac OS X, RISC OS y probablemente alguno más. PHP soporta la mayoría de servidores web de hoy en día, incluyendo Apache, Microsoft Internet Information Server, Personal Web Server, Netscape y iPlanet, Oreilly Website Pro server, Caudium, Xitami, OmniHTTPd y muchos otros. PHP tiene módulos disponibles para la mayoría de los servidores, para aquellos otros que soporten el estándar CGI, PHP puede usarse como procesador CGI.

Con PHP no se está limitado a resultados en HTML. Entre las habilidades de PHP se incluyen, creación de imágenes, ficheros PDF y películas Flash sobre la marcha. También se pueden presentar otros resultados, como XHTM y ficheros XML. PHP puede autogenerar estos ficheros y grabarlos en el sistema de ficheros en vez de presentarlos en la pantalla.

Quizás la característica más potente y destacable de PHP es su soporte para una gran cantidad de bases de datos. Escribir un interfaz vía web para una base de datos es una tarea simple con PHP.

PHP también tiene soporte para comunicarse con otros servicios usando protocolos tales como LDAP, IMAP, SNMP, NNTP, POP3, HTTP, COM (en Windows) y muchos otros. También se pueden crear raw sockets. PHP soporta WDDX para intercambio de datos entre lenguajes de programación en web. Y hablando de interconexión, PHP puede utilizar objetos Java de forma transparente como objetos PHP Y la extensión de CORBA puede ser utilizada para acceder a objetos remotos.

PHP tiene unas características muy útiles para el proceso de texto, desde expresiones regulares POSIX Extended ó Perl hasta parseador de documentos XML. Para parsear y acceder documentos XML, soportamos los estándares SAX y DOM. Se puede utilizar la extensión XSLT para transformar documentos XML.

14.12. MYSQL

Es un sistema para la administración de bases de datos relacionales (RDBMS) rápido y sólido. Las bases de datos permiten almacenar, buscar, ordenar y recuperar datos de forma eficiente. El servidor de MySQL controla el acceso a los datos para garantizar el uso simultáneo de varios usuarios, para proporcionar acceso a dichos datos y para asegurarse de que solo obtienen acceso a ellos los usuarios con autorización. Por lo tanto, MySQL es un servidor multiusuario y de proceso múltiple.

Se pueden apreciar importantes cambios como compatibilidad con subconsultas, tipos GIS para almacenar datos geográficos, compatibilidad mejorada con internacionalización, procedimientos almacenados, la caché de consultas de MySQL, que mejora considerablemente la velocidad de las consultas repetitivas que suelen ejecutar las aplicaciones Web.

MySQL es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones. MySQL desde enero de 2008 una subsidiaria de Sun Microsystems y ésta a su vez de Oracle Corporation desde abril de 2009— desarrolla MySQL como software libre en un esquema de licenciamiento dual.

Al contrario de proyectos como Apache, donde el software es desarrollado por una comunidad pública y los derechos de autor del código están en poder del autor individual, MySQL es patrocinado por una empresa privada, que posee el copyright de la mayor parte del código.

MySQL funciona sobre múltiples plataformas, incluyendo:

- AIX
- BSD
- FreeBSD

- HP-UX
- Kurisu OS
- GNU/Linux
- Mac OS X
- NetBSD
- OpenBSD
- OS/2 Warp
- QNX
- SGI IRIX
- Solaris
- SunOS
- SCO OpenServer
- SCO UnixWare
- Tru64
- eBD
- Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8 y Windows Server (2000, 2003 y 2008).
- OpenVMS9

14.12.1. Caracteristicas

Inicialmente, MySQL carecía de elementos considerados esenciales en las bases de datos relacionales, tales como integridad referencial y transacciones. A pesar de ello, atrajo a los desarrolladores de páginas web con contenido dinámico, justamente por su simplicidad.

Poco a poco los elementos de los que carecía MySQL están siendo incorporados tanto por desarrollos internos, como por desarrolladores de software libre. Entre las características disponibles en las últimas versiones se puede destacar:

- Amplio subconjunto del lenguaje SQL. Algunas extensiones son incluidas igualmente.
- Disponibilidad en gran cantidad de plataformas y sistemas.

- Posibilidad de selección de mecanismos de almacenamiento que ofrecen diferente velocidad de operación, soporte físico, capacidad, distribución geográfica, transacciones.
- Transacciones y claves foráneas.
- Conectividad segura.
- Replicación.
- Búsqueda e indexación de campos de texto.

MySQL es un sistema de administración de bases de datos. Una base de datos es una colección estructurada de tablas que contienen datos. Esta puede ser desde una simple lista de compras a una galería de pinturas o el vasto volumen de información en una red corporativa. Para agregar, acceder a y procesar datos guardados en un computador, usted necesita un administrador como MySQL Server. Dado que los computadores son muy buenos manejando grandes cantidades de información, los administradores de bases de datos juegan un papel central en computación, como aplicaciones independientes o como parte de otras aplicaciones.

MySQL es un sistema de administración relacional de bases de datos. Una base de datos relacional archiva datos en tablas separadas en vez de colocar todos los datos en un gran archivo. Esto permite velocidad y flexibilidad. Las tablas están conectadas por relaciones definidas que hacen posible combinar datos de diferentes tablas sobre pedido.

MySQL es software de fuente abierta. Fuente abierta significa que es posible para cualquier persona usarlo y modificarlo. Cualquier persona puede bajar el código fuente de MySQL y usarlo sin pagar. Cualquier interesado puede estudiar el código fuente y ajustarlo a sus necesidades. MySQL usa el GPL (GNU General Public License) para definir qué puede hacer y qué no puede hacer con el software en diferentes situaciones. Si usted no se ajusta al GPL o requiere introducir código MySQL en aplicaciones comerciales, usted puede comprar una versión comercial licenciada.[16]

[16] MySQL, http://es.wikipedia.org/wiki/MySQL

14.13. MySQLi

MySQLi es una extensión de PHP que permite acceder a ciertas funciones disponibles a partir de MySQL 4.1 que no se pueden emplear con la extensión tradicional, proporciona:

- Mayor velocidad y seguridad.
- Interfaz procedimental u orientado a objetos.
- Soporte de transacciones.
- Nuevo protocolo binario de MySQL 4.1 que permite ciertas funciones como la ejecución de sentencias preparadas.[17]

La Extensión MySQL, es el conjunto de funciones que usamos con frecuencia como, mysql_connect, mysql_select_db. Que está pensada para ser usada de una manera procedural y con versiones de MySQL anteriores a la 4.1.3, pero que también puede ser usada con las nuevas versiones.

Para comenzar a usar mysqli es necesario instanciar la clase mysqli pasándole como parámetros el nombre del servidor, el usuario de la base de datos MySQL, la contraseña y el nombre de la base de datos MySQL.[18]

```
$mysqli = new mysqli('servidor', 'usuario', 'contraseña', 'base_de_datos');
```

14.14. Razones para utilizar PHP y MySQL.

Al desarrollar un sitio de esta índole, se pueden utilizar una gran cantidad de productos diferentes:

- ✓ Hardware para el servidor web
- ✓ Un sistema operativo
- ✓ Software de servidor web
- ✓ Un sistema de administración de base de datos
- ✓ Un lenguaje de secuencia de comandos o de programación como SQL.

[17] MySQLi, http://rua.ua.es/dspace/bitstream/10045/13363/12/12c-mysqli.pdf
[18] http://angelfqc.host22.com/blog/2010/12/25/introduccion-a-mysqli/

Por separado estos programas son potentes, a continuación mencionaremos ventajas de su uso en nuestra aplicación:

Brindan flexibilidad para ejecutar los programas en local, en nuestra red local o en la nube**,** dependiendo de las necesidades.

Solo se cargan las bibliotecas, pues PHP ya contiene funciones integradas las cuales se pueden ir llamando de acuerdo a las necesidades requeridas para que no vuelva lento el motor de PHP, es decir se puede modular tanto el sistema de votación como su programación.

La ventaja de usar mysql es el uso de trigger que no son más que procedimientos almacenados que se asocian a eventos, esto permite emitir vistas con agilidad y restringir el acceso a terceros.

Podemos decir también que es estos software son gratuitos, modulares (como se mencionaba antes), multi - plataforma, y extensibles. Cabe recalcar que son portables, facilitan el aprendizaje, tienen acceso a código abierto.

MySQL es un motor rápido, tiene capacidad de conectarse a muchos sistemas de bases de datos, en cuanto a conexión y seguridad pueden conectarse a internet desde cualquier lugar.

Ventajas del uso de estándares web

- Independencia de dispositivo.
- Simplificar el código y reducir el tamaño de los archivos.
- Proporcionar sitios web que sean accesibles a más gente.
- Mayor tiempo de vida.
- Reducción en el tiempo de desarrollo y mantenimiento.
- Compatibilidad con futuros navegadores web.
- Facilidad de adaptación.

Para desarrollar el sistema en línea se realizo encuestas para confirmar la necesidad y confianza que generaría su implementación generando los siguientes resultados. De una muestra de diversa de la población entre estudiantes, amas de casas, técnicos y comerciantes se deduce que un 70% son mujeres y un 29% son hombres todos tienen cedula y un 1% no tiene cedula nacional.

Se adjunta al final documento utilizado como plantilla de encuesta (encuesta no.1). Dentro de algunas de las preguntas que se hicieron están:

- ¿Edad hábil de votación?
- ¿Poseen cédula?
- ¿Han votado? ¿Opinión del sistema actual de votación, lento, presentación de resultados rápidos?

Como es un sistema que se colocará en línea se pregunta si hacen uso de internet, con qué frecuencia, si tienen familia en el extranjero. Estas se hacen pues la finalidad es que ellos participen en actividades electoral presidencial de nuestro país sin importar donde se encuentren. Se adjuntara archivo de encuesta en anexos.

Nuestro sistema constara de cuatros aplicaciones, y cinco tablas; las cuales mencionaremos y describiremos sus funciones a continuación:

14.15. Navicat

Navicat es una de las herramientas más fiables y rápidas para la administración de bases de datos, que te permitirán simplificar la gestión de las bases de datos y reducir los costos de administración. Diseñado para satisfacer las necesidades de los administradores de bases de datos, desarrolladores y pequeñas y medianas empresas.

Navicat dispone de una interfaz gráfica muy intuitiva, que le permitirá crear, organizar, acceder y compartir información de forma fácil y segura.

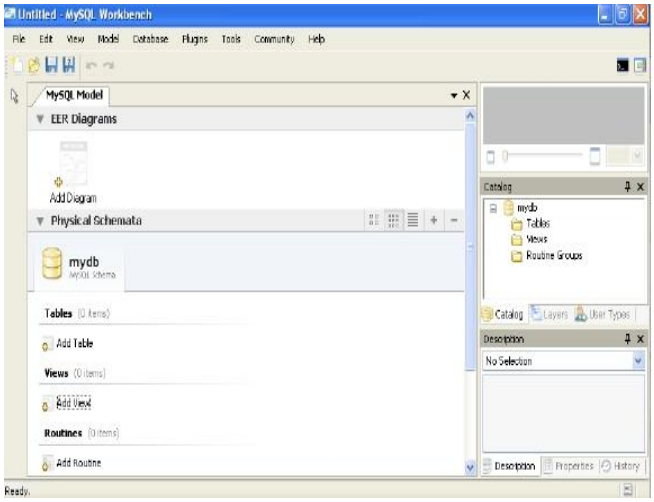
Navicat es muy conocido, de confianza, y se usan a diario en todo el mundo por las empresas globales, organismos gubernamentales e instituciones educativas. Desde comienzos de 2001, Navicat ha sido descargado más de 2.000.000 de veces en todo el mundo y tiene una base de clientes de más de 50.000 usuarios. Además está ahora disponible en 7 idiomas.

Está disponible para MySQL, Oracle y PostgreSQL, para administración/desarrollo local y remoto.[19]

El software es un programa de mantenimiento y consulta de bases de datos, es compatible con sistemas libres como mySQL u otros como Oracle, que tiene como bandera su simplicidad de uso respecto a un programa de mantenimiento pesado y complejo.

De forma que si queremos consultar de forma rápida una tabla o de crear alguna gestión sobre la misma lo podemos hacer sin perder mucho tiempo. Lógicamente las personas que no nos dedicamos a esto profesional agradeceremos esta simpleza a la hora de gestionar sistemas de BD.[20]

14.16. WorkBench



MySQL Workbench es una herramienta visual de diseño de bases de datos que integra desarrollo de software, Administración de bases de datos, diseño de bases de datos, creación y mantenimiento para el sistema de base de datos MySQL. Es el sucesor de DBDesigner 4 de fabFORCE.net, y reemplaza el anterior conjunto de software, MySQL GUI Tools Bundle.[21]

[19] Navicat, http://www.blueorb.es/tag/navicat/
[20] http://www.applesfera.com/general/navicat-gestiona-de-forma-comoda-sistemas-de-bases-de-datos
[21] WorkBench, http://www.monografias.com/trabajos88/mysql-worckbench/mysql-worckbench.shtml

14.17. CSS

CSS es un lenguaje de hojas de estilos creado para controlar el aspecto o presentación de los documentos electrónicos definidos con HTML y XHTML. CSS es la mejor forma de separar los contenidos y su presentación, y es imprescindible para crear páginas web complejas.

Separar la definición de los contenidos y la definición de su aspecto presenta numerosas ventajas ya que obliga a crear documentos HTML/XHTML, bien definidos y con significado completo. Además mejora la accesibilidad del documento, reduce la complejidad de su mantenimiento y permite visualizar el mismo documento en infinidad de dispositivos diferentes.

Al crear una página WEB, se utiliza en primer lugar el lenguaje HTML/XHTML para marcar los contenidos, es decir para designar la función de cada elemento dentro de la página: párrafo, titular, texto destacado, tabla, lista de elementos.

Una vez creados los contenidos, se utiliza el lenguaje CSS para definir el aspecto de cada elemento: color, tamaña y tipo de letra del texto, separación horizontal y vertical entre elementos, posición de cada elemento dentro de la pagina.[22]

CSS es Hojas de Estilo en Cascada (Cascading Style Sheets), es un mecanismo simple que describe cómo se va a mostrar un documento en la pantalla, o cómo se va a imprimir, o incluso cómo va a ser pronunciada la información presente en ese documento a través de un dispositivo de lectura. Esta forma de descripción de estilos ofrece a los desarrolladores el control total sobre estilo y formato de sus documentos.[23]

14.18. Fancy Box

Es un script con el que podemos abrir imágenes, páginas web, videos. De forma muy elegante, en ventanas tipo Popup, con jQuery.
Lo primero que debemos hacer es incluir la función dentro de nuestro sitio.

[22] CSS, http://www.librosweb.es/css/pdf/introduccion_css.pdf
[23] http://www.w3c.es/Divulgacion/GuiasBreves/HojasEstilo

```
view plain  copy to clipboard  print  ?
01. <script type="text/javascript" src="../js/jquery-1.7.1.min.js"></script>
02. <script type="text/javascript" src="../js/jquery.fancybox.pack.js"></script>
03. <link rel="stylesheet" type="text/css" href="../js/jquery.fancybox.css" />
```

Incluimos los Javascript de jQuery y fancyBox y el CSS de fancyBox.

Para hacerlo funcionar solo tenemos que especificarle un "id" o "class" a nuestros enlaces para después ejecutar fancyBox sobre ese "id" o "class".
En este caso hemos utilizado el enlace con clase (class="ejemplo_1") sobre una imagen que vamos a ampliar. Mostramos la imagen en pequeño (foto1p.jpg) y obviamente vamos a ampliar la imagen (foto1.jpg) que fancyBox coge automáticamente del "href" del enlace:[24]

```
view plain  copy to clipboard  print  ?
01. <a class="ejemplo_1" href="../img/foto1.jpg" title="Imagen simple"><img src="..
/img/foto1p.jpg" width="200" height="150" /></a>
```

Ahora vamos a ejecutar la función fancyBox sobre el enlace con este sencillo código:

```
view plain  copy to clipboard  print  ?
01. <script type="text/javascript">
02. $(document).ready(function(){
03.     $(".ejemplo_1").fancybox({ });
04. });
05. </script>
```

14.18.1. Fancy Box Permite

- Mostrar imágenes, elementos HTML, películas en formato SWF, IFrames y peticiones AJAX.
- Cambiar el aspecto de la interfaz gráfica mediante código CSS.
- Agrupar elementos relacionados, además de añadir elementos de navegación.
- Si se añade el plugin para movimientos del ratón, permite responder al scrolling del ratón.
- Crear transiciones profesionales entre elementos añadiendo el "easing plugin".
- Añadir efectos de sombreado bajo el elemento resaltado.[25]

[24] Fancy Box, http://www.actualidadjquery.es/2012/01/06/fancybox-abrir-imagenes-paginas-web-y-videos-en-ventanas-tipo-popup-con-jquery/
[25] Fancy Box, http://www.usosweb.com/content/tutorial-fancybox

14.19. JQuery

JQuery es un framework Javascript, es un producto que sirve como base para la programación avanzada de aplicaciones, que aporta una serie de funciones o códigos para realizar tareas habituales. Por decirlo de otra manera, framework son unas librerías de código que contienen procesos o rutinas ya lis tos para usar. L os programadores utilizan los frameworks para no tener que des arrollar ellos mismos las tareas más básicas , puesto que en el propio framework ya hay implementaciones que están probadas , funcionan y no se necesitan volver a programar.[26]

jQuery es una biblioteca de JavaScript, que permite simplificar la manera de interactuar con los documentos HTML, manipular el árbol DOM, manejar eventos, desarrollar animaciones y agregar interacción con la técnica AJAX a páginas web.

JQuery es software libre y de código abierto, posee un doble licenciamiento bajo la Licencia MIT y la Licencia Pública General de GNU v2, permitiendo su uso en proyectos libres y privativos. JQuery, al igual que otras bibliotecas, ofrece una serie de funcionalidades basadas en Java Script que de otra manera requerirían de mucho más código, es decir, con las funciones propias de esta biblioteca se logran grandes resultados en menos tiempo y espacio.

14.19.1. Características

- Selección de elementos DOM.
- Interactividad y modificaciones del árbol DOM, incluyendo soporte para CSS 1-3 y un plugin básico de XPath.
- Eventos.
- Manipulación de la hoja de estilos CSS.
- Efectos y animaciones.
- Animaciones personalizadas.
- AJAX.
- Soporta extensiones.

[26] JQuery, http://www.desarrolloweb.com/articulos/introduccion-jquery.html

- Utilidades varias como obtener información del navegador, operar con objetos y vectores, funciones para rutinas comunes.
- Compatible con los navegadores Mozilla Firefox 2.0+, Internet Explorer 6+, Safari 3+, Opera 10.6+ y Google Chrome 8+.

14.20. MaxMInd

Max Mind, servicio de geolocalización global que contiene la procedencia geográfica de la mayoría de las direcciones IP mundiales, actualizado de manera permanente, le per mite la exacta identificación de la ubicación en tiempo real de su audiencia Inter net por país, región, hasta el detalle de la respectiva ciudad.

La exactitud de identificación de usuarios a nivel mundial es del 99.8%.

Las bases de datos de direcciones IP se actualizan continuamente, más de 2.000 clientes utilizan el ser vicio GeoIP de Max Mind en todo el mundo.[27]

14.21. Zebra Pagination

Es una paginación genérica librería PHP que genera automáticamente los enlaces de navegación (HTML siguiente, página anterior y específica), teniendo en cuenta el número total de registros y el número de registros procedentes de cualquier fuente (arrays, base de datos) que se mostrarán por página.

[27] MaxMind, http://teledifusion.es/index.php?option=com_content&view=article&id=15&Itemid=33&lang=es

Capitulo 3

1. Resultados

Como resultados de la Investigación se tienen las siguientes tablas que representan el proceso de normalización en cada etapa.

1.1. Análisis

1era forma Normal

Fig. 3.1

2da Forma Normal

Aún se tienen datos redundantes por lo tanto se procede a normalizar

Fig. 3.2

Aún con datos redundantes se procede a la tercera forma norma

3era Forma Normal

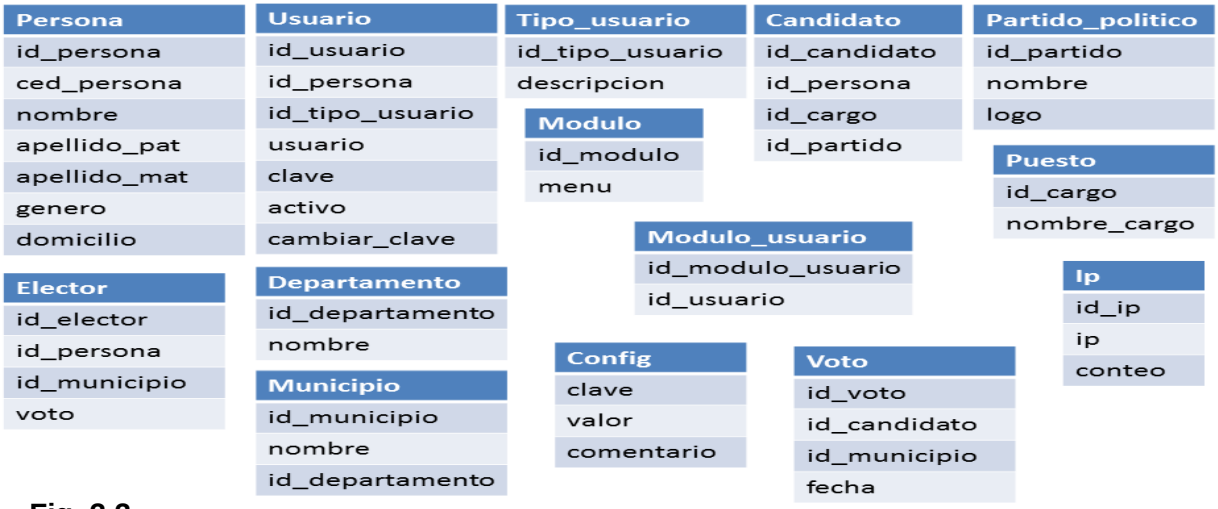
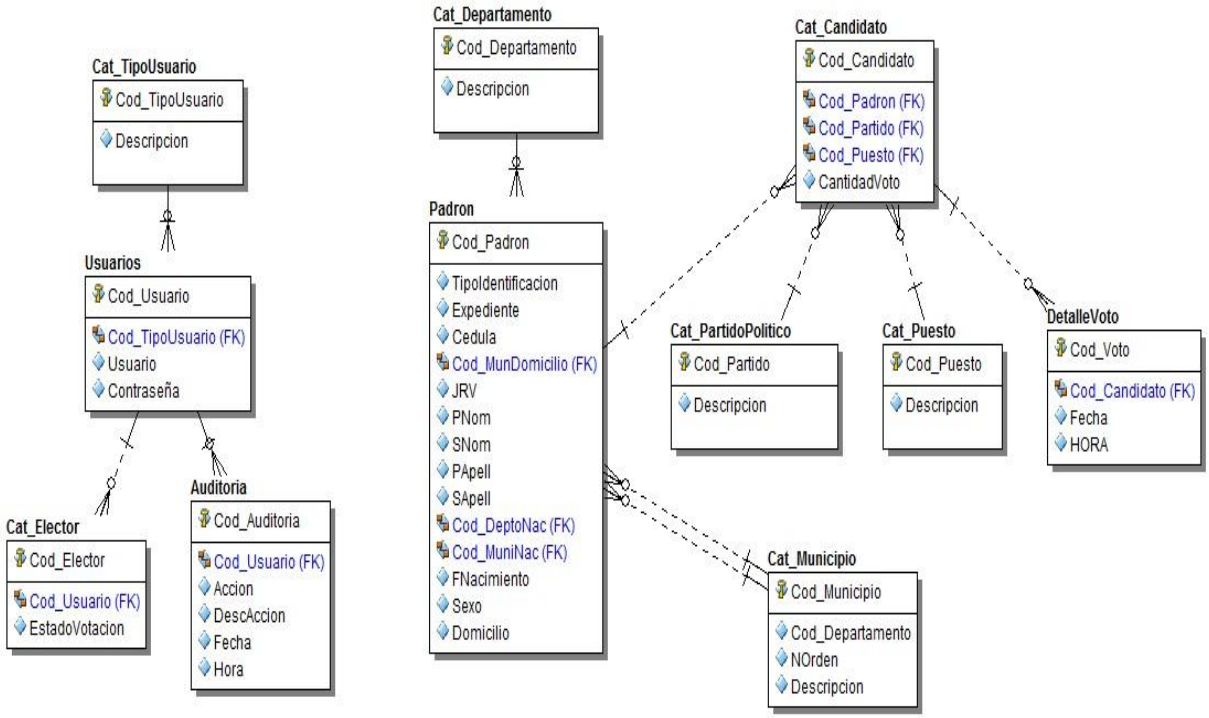


Fig. 3.3



1.2. Diseño

Para el diseño de la Aplicación Web se tienen las siguientes pantallas:

Pantalla de Inicio del Sistema

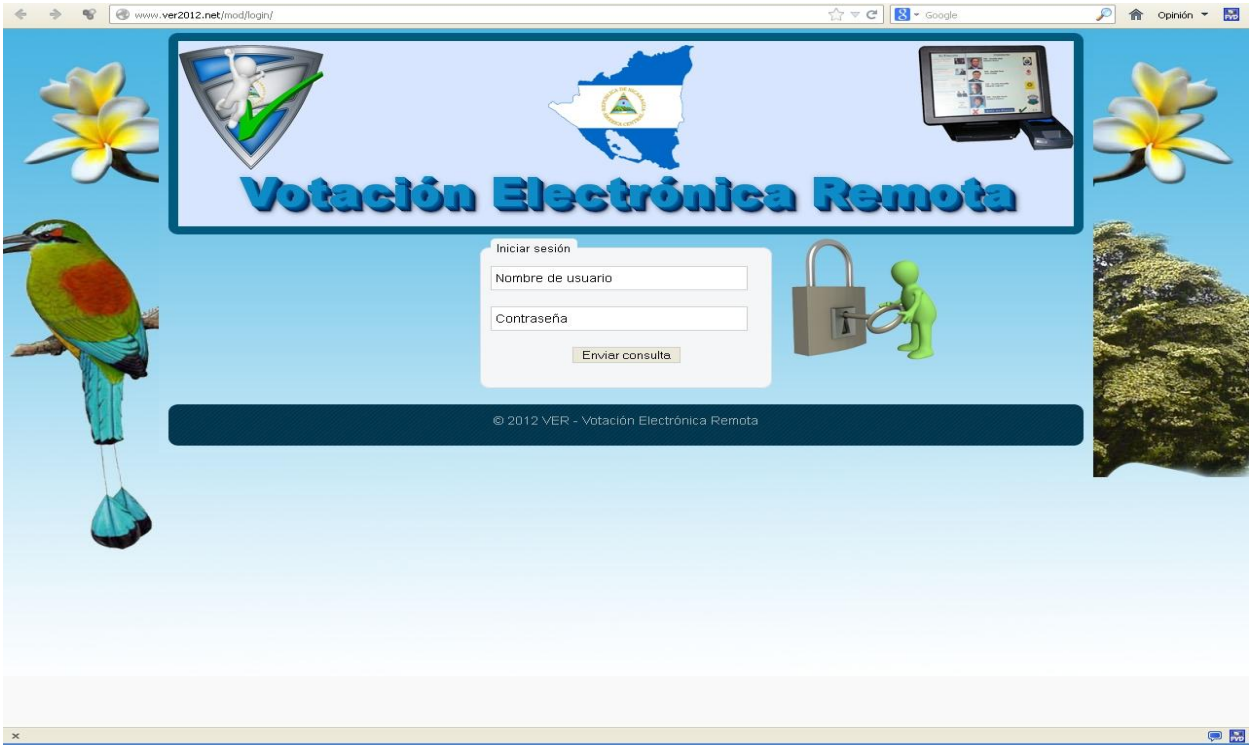


Fig. 3.4

Pantalla de cambio de contraseña

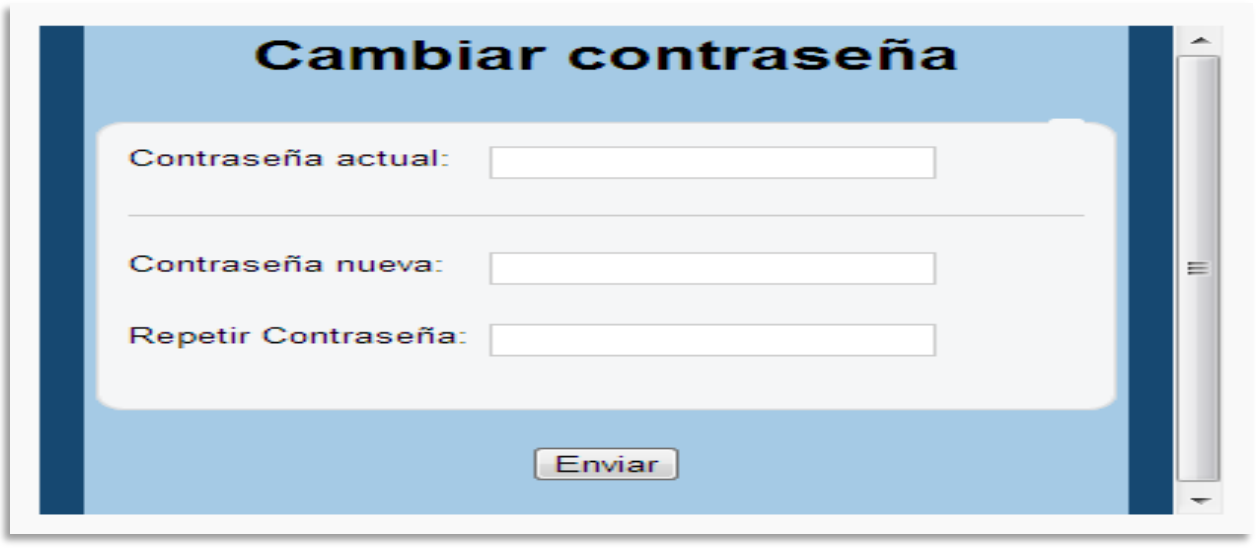


Fig. 3.5

Pantalla de Votación

Figura 3.6

Pantalla de Resultados, una vez que los comicios electorales hayan culminado.

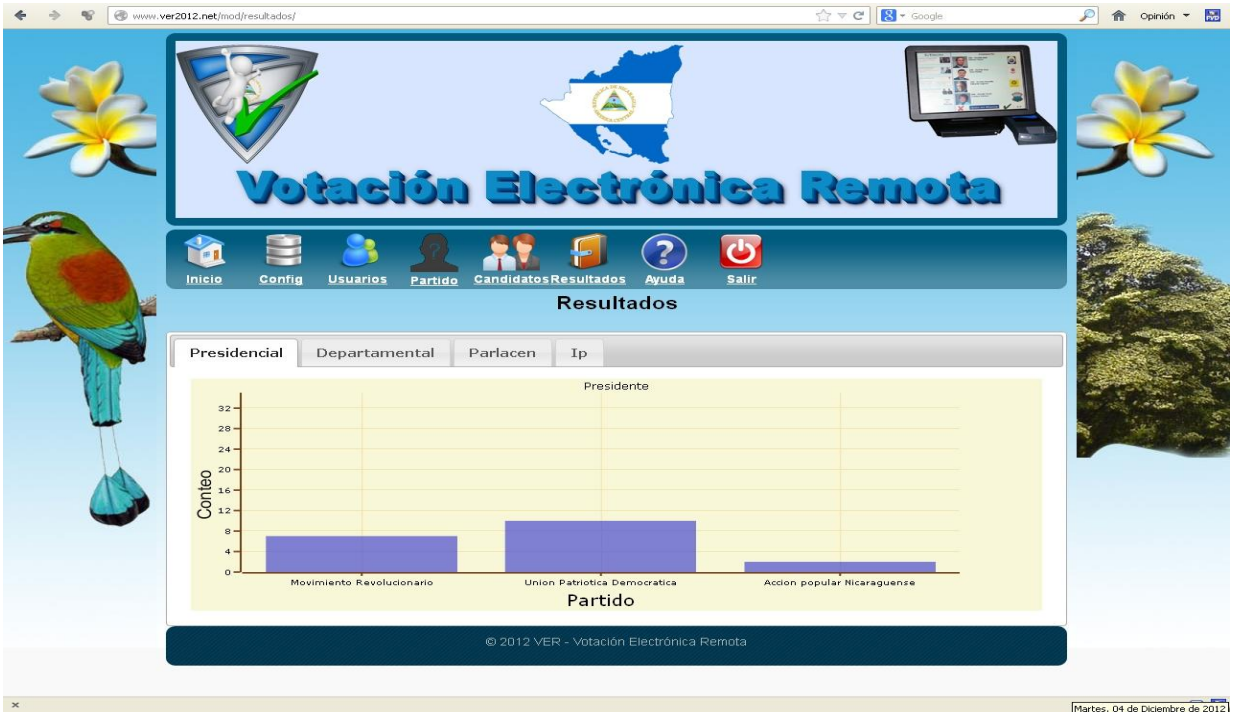


Figura 3.7

Pantallas del Administrador

Pantalla de Inicio

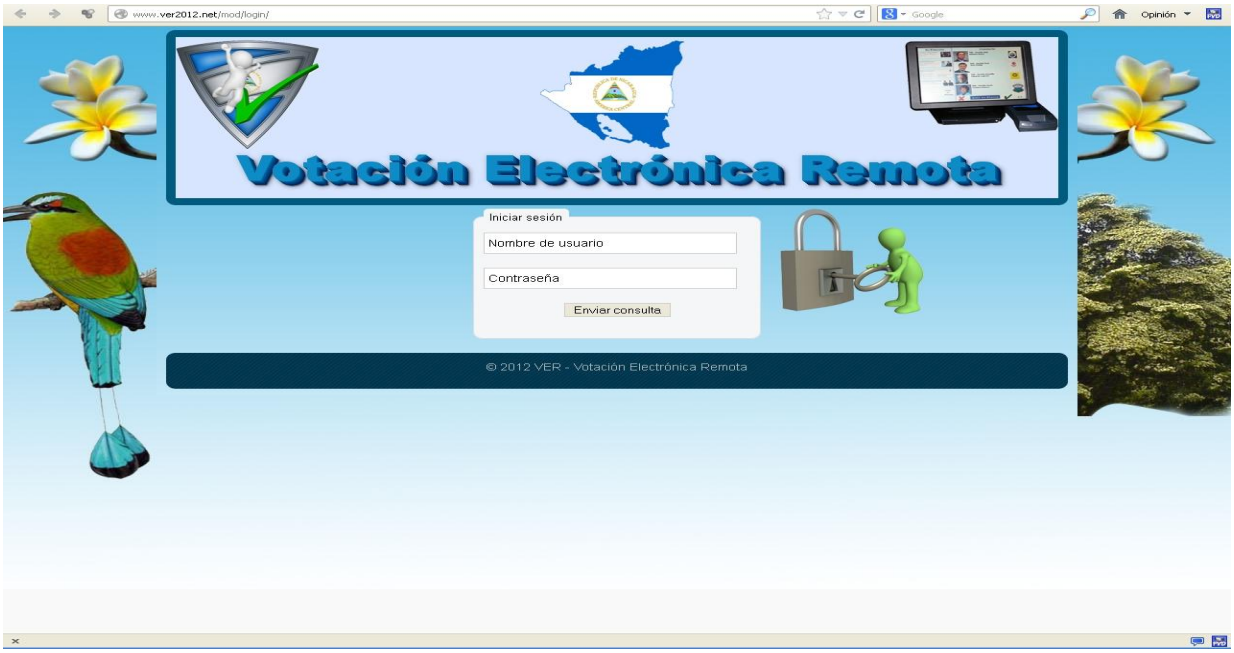


Fig. 3.8

Pantalla de Bienvenida al Administrador

Fig. 3.9

Pantalla de Configuración

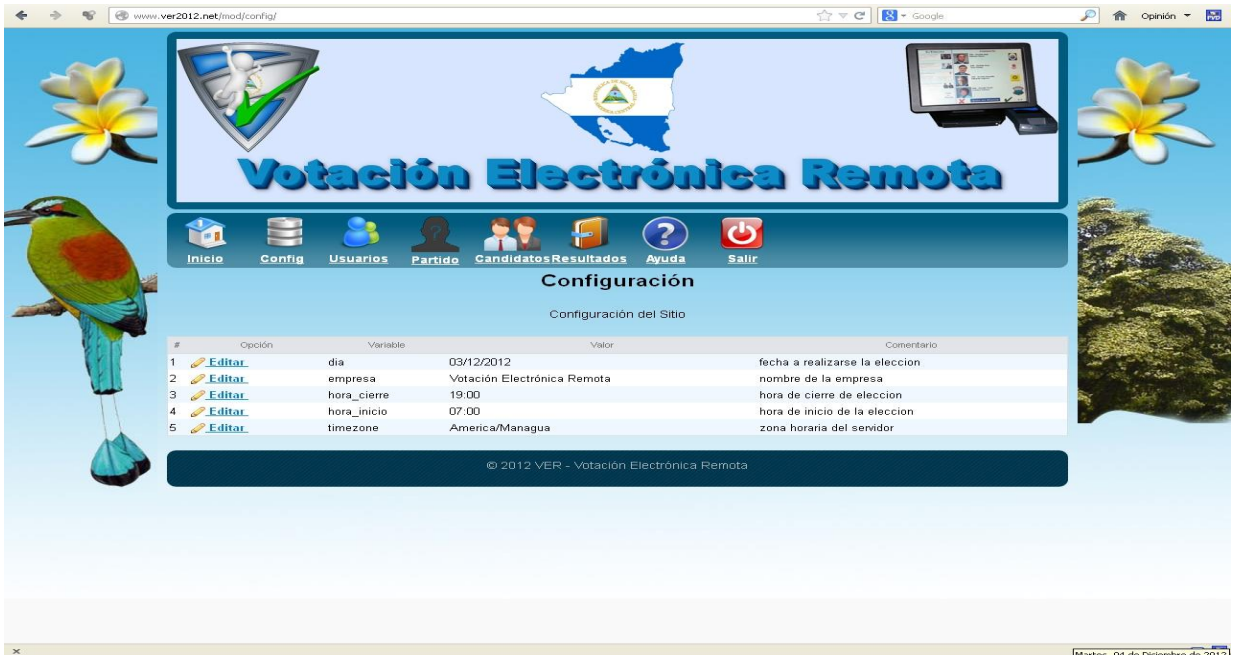


Fig. 3.10

Pantalla de Partidos

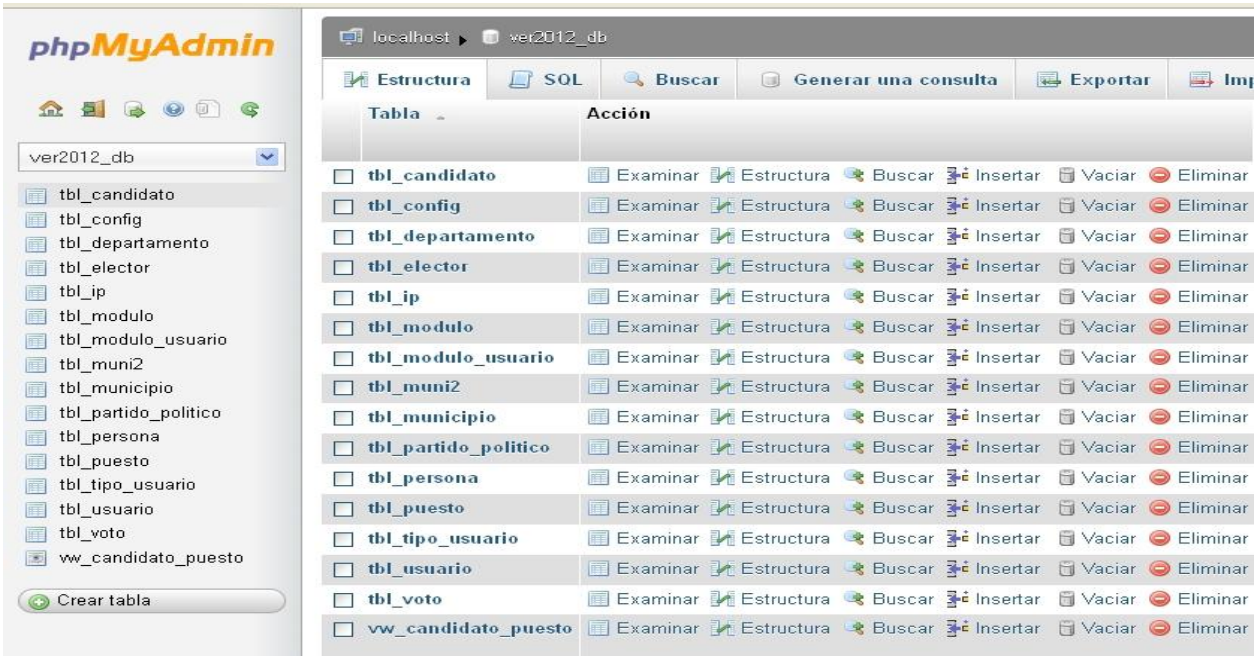
Fig. 3.11

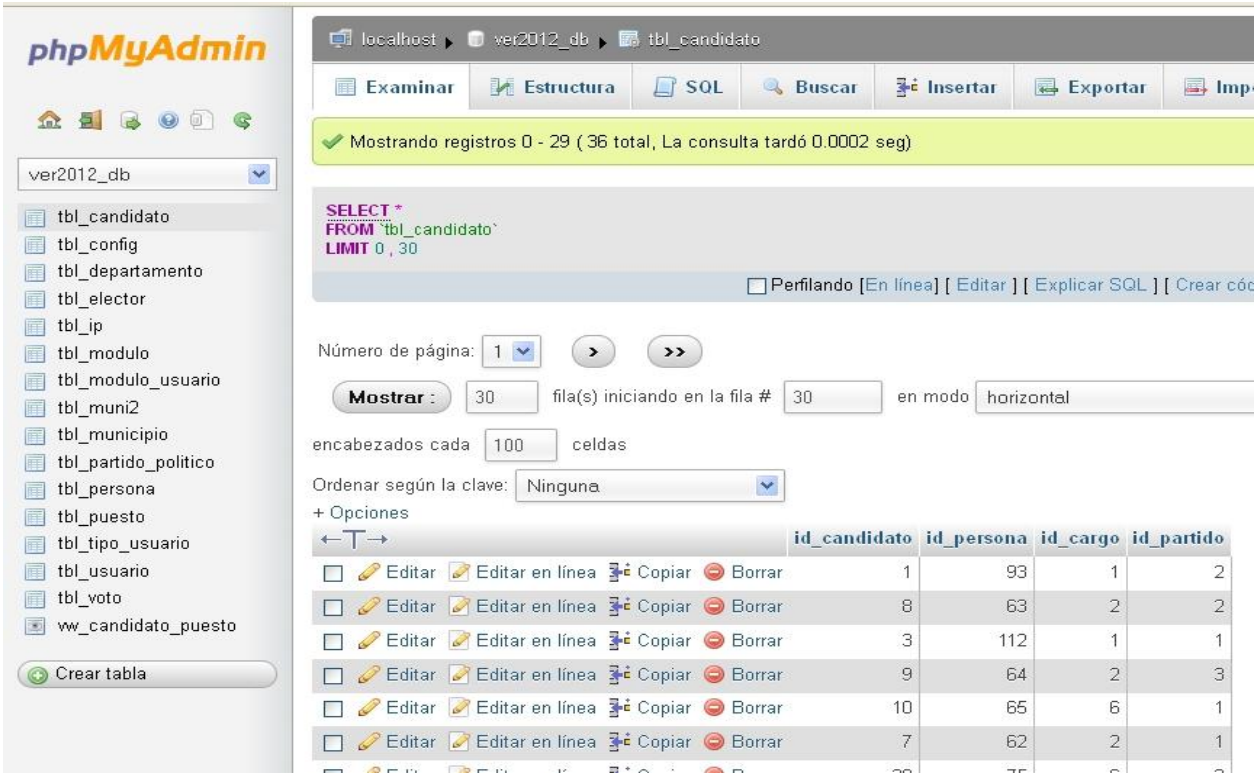
Pantalla de Resultados

Fig. 3.12

1.3. Implantación

Código Fuente





Capítulo 4

1. Diseño Metodológico

1.1. Tipo de Investigación: El tipo de investigación seleccionada es Descriptiva y Propositiva.

El objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables. Los investigadores no son meros espectadores, sino que recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

Y es propositiva porque se diseñará una propuesta estratégica que permita recoger el voto de los nicaragüenses en el extranjero.

1.2. Herramientas adecuadas para el diseño y desarrollo de un sitio web

Para el desarrollo de la Aplicación web se hizo instaló un servidor web Apache en la máquina donde se desarrolló la aplicación, con el fin de hacer pruebas rápidamente, así de esta manera, se editó un fichero PHP. En cada prueba se actualiza el navegador para ver los cambios, así de esta misma forma se hace el procedimiento para la configuración establecida de un servidor local con Appserver.

En el diseño se consideraron los siguientes puntos:

- El diseño sea amigable
- Fácil de acceder
- Comprensible

Con el propósito de que la aplicación sea útil y que el ciudadano se apropie de ella.

Para esta investigación la ingeniería web es utilizada para aplicar de forma sistemática, disciplinada y cuantificable la calidad de la aplicación web.

En cuanto a los atributos de calidad en la web, se trató de cumplir con los requisitos de calidad para aplicaciones web tales como:

Como las aplicaciones web tienen sus particularidades requieren de un proceso que sea iterativo e incremental.

Para este estudio se usaron las siguientes fases:

1. Planteamiento y formulación: En esta etapa se identificaron los objetivos de la aplicación.
2. Planificación: Ya una vez planteado el problema, se pudo estimar los costos, riesgos y esfuerzo durante el desarrollo.
3. Análisis: En esta etapa se establecieron los requerimientos técnicos, gráficos y de contenido.
4. Ingeniería: aquí se trabajaron en paralelo dos cosas el diseño del contenido y el diseño de la producción, en cuanto a gráficos, contenido de texto, etc…
5. Generación de páginas y pruebas: Aquí se probó que el contenido dinámico se genere correctamente, que las validaciones aplicadas estén en buen funcionamiento, en cuanto a los gráficos de la aplicación que lleven los datos correspondientes según las votaciones que se generen.

Durante el desarrollo se aplicó encuesta, para validar la necesidad de introducir una herramienta que ayude a capturar el voto de los ciudadanos nicaragüenses en el extranjero. Al final del documento se adjunta la plantilla de la encuesta aplicada a los sujetos de estudio.

Dentro de algunas de las preguntas que se hicieron están:

- ¿Posee cédula?
- ¿Ha votado? ¿Opinión del sistema actual de votación, lento, presentación de resultados rápidos?
- ¿Qué opina usted de implementar un sistema de votación electrónica para familiares radicados en el extranjero?

Dado que este sistema funciona en línea se pregunta si hacen uso de internet, con qué frecuencia y si tienen familia en el extranjero. Éstas interrogantes, se realizaron con la finalidad de que nuestros familiares residentes en otros países participen en las elecciones presidenciales sin importar donde se encuentren.

De aquí se capturó la información a utilizar para desarrollar una base de datos con calidad, tomando en cuenta varios factores adicionales como:

- ✓ El ancho de banda,
- ✓ Capacidad de almacenamiento del servidor en donde se alojará el sitio como medidas correlativas de seguridad para ofrecer a los ciudadanos nacionales y extranjeros de nacionalidad nicaragüense un sistema eficiente.

En consecuencia con la información recopilada y los requerimientos a satisfacer en el sistema se clasificaron objetos necesarios para la construcción de la base de datos. Así pues una vez que se cumple con la edad idónea se convierten en **Electores,** y conforme a requisitos preestablecidos en la Constitución Política y en la ley de rango constitucional o Ley Electoral se clasifican a los **Candidatos**, los cuales deben circunscribirse en una afiliación política para pertenecer a un **Partido Político** y entrar en el **Proceso Electoral**, éstas representaciones entran en el juego de elecciones cada cierto período y representan por medio de **Votos** a nuestros gobernantes, es así como surge la idea de mejorar y modernizar el actual sistema electoral con que cuenta nuestro país.

Las entidades a definir contienen atributos generales tales como:

Nombres, apellido paterno, apellido materno, edad, fecha nacimiento, dirección, nacionalidad, DNI o cedula de identificación. Para la entidad de candidato verificamos que cumpla con los requisitos mencionados previamente, y subsecuentemente éste se afilie a un partido para entrar en contienda electoral; la entidad de votos contendrá atributos como identificador de candidato, un identificador de municipio, y la fecha y hora en que se realizó el voto. ¿Cuál es la finalidad de estos atributos en la entidad de Voto? Pues, evitar en lo posible el fraude. Una persona o Elector solo podrá votar una única vez, se determinará por su identificación complementándose ésta con un usuario y contraseña asignados inicialmente por el CSE* (Consejo Supremo Electoral) el cual se deberá modificar para poder realizar su derecho al ejercicio de votar

Por otra parte se crearon tablas con módulos que contienen secciones indexada de cada una de las funciones que se presentarán en el sistema, como módulo de Configuración del sistema en general, módulo de votaciones, módulo de candidatos, módulo de partidos, módulo de usuarios (personas previamente registradas en el sistema por funcionarios encargados de gestionar el padrón electoral) y el módulo de resultados. A estos módulos solo se tienen acceso mediante una asignación previa la que determina la jerarquía y amplitud de uso del mismo (sistema), privilegios asignados por el administrador

Estos datos están generalizados, a continuación se revisan las formas normales para depuración y construcción de un sistema robusto.

1ra Forma Normal: Se definen las entidades por orden y clasificación según el sistema de votación. **Fig. 3.1**
Como se tienen datos redundantes en una misma tabla, se debe realizar una segunda normalización (**2da Forma Normal**). **Fig. 3.2**

Todavía queda depurar aún más las tablas pues hay datos redundantes en tablas donde no corresponde, aplicaremos la **3ra Forma Normal, Fig. 3.3** se aclara que aquí aparecen otras tablas debido a la necesidad de manipular eficientemente la base de datos. En todas las elecciones las personas naturales con edad para ejercer voto, se convierte en Elector.

Finalmente, teniendo ya las tablas definidas se debe abordar lo que es la seguridad. Asimismo, estas reglas de seguridad que se aplican al sistema protegerán contra la intervención de terceros mal intencionado, los bien llamados hacker o sniffer; se debe recordar que se usarán datos sensibles que demandan integridad y confidencialidad máxima.

2. Explicación del sistema

En la pantalla de inicio **Fig. 3.4**, aquí el elector podrá escribir su usuario y contraseña, que efectivamente ya obtuvo en una verificación.

Una vez que el elector ha digitado su usuario y contraseña el sistema inmediatamente le pide que cambie la contraseña actual y digite una nueva contraseña**,** de manera que el elector sea únicamente quien esté a cargo de su nueva contraseña y solo sea el únicamente quien la administre. El botón enviar permite que este sea registrado y guardado en la base de datos. **Fig. 3.5**

Luego el sistema le pide que digite su usuario y la contraseña nueva. Cuando el elector realiza esto, entonces le aparece la pantalla de votación. **Fig. 3.6**

Esta pantalla ofrece al elector tres opciones:

- ✓ Inicio
- ✓ Votar
- ✓ Salir

La opción inicio es donde se encuentra la bienvenida al sistema, la opción votar es la pantalla de elección presidencial, donde se pueden apreciar las imágenes que simulan una boleta, en ella aparecen los candidatos que corren como presidentes en las elecciones. Cada boleta tiene el nombre del partido, su bandera y la foto de los candidatos. Dentro de esto se encuentran los botones de votar, donde al hacer clíck éste envía un cuadro de diálogo que permite al elector asegurar su voto, si el elector hace clíck en el botón **SÍ** del cuadro de diálogo este hace el envío del voto al servidor de alojamiento en donde se almacenan los votos. Si el elector hace clíck en el botón **NO** del cuadro de diálogo, entonces el elector puede decidir con seguridad por quién votar.

Una vez que se efectúa el voto, el sistema le muestra al elector otra pantalla para las votaciones de Diputados Departamentales, esta pantalla tiene el mismo procedimiento que la pantalla de votación para presidente, una vez dado el clíck sobre el botón votar del candidato y partido de preferencia se confirma el voto. Inmediatamente efectuado el voto para diputados departamentales, el sistema muestra otra pantalla para elegir a los diputados al parlacén, esta pantalla tiene el mismo procedimiento que las pantallas anteriores.

En cada paso donde el elector efectúa su voto, aparece un cuadro de diálogo que le confirma que su voto ha sido depositado satisfactoriamente.

Si el elector quiere volver a votar, el sistema no le permitirá hacer dicha acción porque este ya ejerció su derecho, una vez que el elector realiza su voto, el sistema pasa a ese elector de estado activo a estado inactivo, quedando registrado de esa forma, con el fin de evitar doble voto con un mismo usuario.

Cuando los comicios culminen, los votantes podrán entrar al sitio web donde podrán ver los resultados de las elecciones. **Fig. 3.7**

Como se puede observar, hay tres pestañas:

- ✓ En la pestaña Presidencial aparece un gráfico de barra en donde se muestran los partidos que estuvieron corriendo en los comicios, y conforme a las votaciones varia el tamaño de las barras. Cuando el puntero se coloca sobre las barras se puede apreciar la cantidad de votos que obtuvo cada partido. Esto mismo sucede para las pestaña Departamental y Parlacén.
- ✓ En la pestaña IP se puede apreciar el lugar (país), de donde fue emitido el voto. Llevando de esta manera, un registro de esta información.

Para las pantallas del administrador:

Se inicia siempre con la pantalla de inicio. Como se puede observar esta es la misma pantalla de inicio para el elector. **Fig. 3.8**

El administrador digita su usuario y contraseña debidamente correcto, sino lo hace así, aparece un cuadro de diálogo que le indica que su usuario y/o contraseña es incorrecto y que por favor vuelva a digitar su respectiva contraseña.

Esta es la pantalla de inicio en donde se da la bienvenida al administrador. **Fig. 3.9** Como se puede observar, existe un menú conformado por:

- ✓ Inicio
- ✓ Config
- ✓ Usuarios
- ✓ Partido
- ✓ Candidatos
- ✓ Resultados
- ✓ Ayuda
- ✓ Salir

En la pantalla Configuración **Fig. 3.10** se tienen las opciones de editar. Aquí el administrador edita el día y la hora en que se realizaran los comicios, una vez cumplido el tiempo el sistema no permite a ninguna persona realizar votos.

En la pantalla de Partidos **Fig. 3.11** están inscritos los partidos que están participando en los comicios aquí el administrador digita los partidos con sus candidatos a presidente y vicepresidente, así como los nombres de los candidatos que van a diputados por partido.

En la pantalla de Resultados **Fig. 3.12** el administrador puede ir viendo como se mueven los resultados. Este gráfico refleja los votos para cada partido ya sea de presidente, diputados departamentales y de parlacén, así como el lugar de donde proceden los votos a través del IP.

3. Estudio de Factibilidad – Técnica, Económica y Operativa

Epistemológicamente: Desde el punto de vista de la investigación se encuentra ubicado en el paradigma tecnológico, porque busca resolver problemas de tipo práctico y su objetivo es promover tecnologías o esquemas de acción derivados de conocimientos teóricos.

Social: Se pretende cambiar el método manual de votaciones de nuestra sociedad para alcanzar una mayor credibilidad, eficiencia y economía del sistema democrático participativo a nivel interno o externo (nacionales residentes en extranjero). Nuestro aporte es la construcción de un sistema web que simule las elecciones sean estas presidenciales, municipales u otras.

Efectos directos o indirectos: Existen motivos que nos permiten advertir la clara necesidad de una reforma electoral debido a las serias falencias que caracterizan al sistema actual. Una acción de ésta índole incidirá de manera positiva en el afianzamiento de la democracia al país y restaurará la confianza en el Poder Electoral. Brindará seguridad a la ciudadanía del respeto de su voluntad, confianza a la comunidad internacional, inversores y donantes.

Factibilidad ambiental: Factor muy importante, pues con la ejecución de ésta aplicación se reduciría aproximadamente un ochenta por ciento el uso del papel, promoviendo así la preservación de los árboles, menor uso de productos químicos, contaminación por quema de hidrocarburos, ya que se reduciría la necesidad de transporte de materiales. Y promoverá transferencias tecnológicas al país.

Económica: La oportunidad de Costo de oportunidad – efectividad, determina el menor costo para alcanzar los resultados esperados. La aplicación de esta propuesta representará una disminución a mediano plazo del costo de las elecciones que se realizan en el país. Considerando que en Nicaragua se realizan las elecciones más costosas de Centroamérica.

Técnica: La aplicación de este sistema significaría el ingreso de Nicaragua a la tecnología de punta. La consolidación de la inversión en infraestructura de telecomunicación y la capacitación de recursos humanos especializados.

Jurídico - Institucional: Citamos textualmente “En Nicaragua, la Coordinadora Civil para la Emergencia y la Reconstrucción (CCER) presentó, en abril de 2003, ante representantes de medios de comunicación, su propuesta de reforma a la Ley Electoral que incluye la posibilidad de escoger a los candidatos a cargos públicos a través del voto electrónico, reduciendo así los costos electorales. El tema sigue en discusión”.

Factibilidad se refiere a la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas. Generalmente la factibilidad se determina sobre un proyecto.

El estudio de factibilidad, es una de las primeras etapas del desarrollo de un sistema informático. El estudio incluye los objetivos, alcances y restricciones sobre el sistema, además de un modelo lógico de alto nivel del sistema actual, en el caso de este proyecto no existe. A partir de esto, se crean soluciones alternativas para el nuevo sistema, analizando para cada una de éstas, diferentes tipos de factibilidades.

Los tipos de factibilidades básicamente son:

- Factibilidad técnica: si existe o está al alcance la tecnología necesaria para el sistema.
- Factibilidad económica: relación beneficio costo.
- Factibilidad operacional u organizacional: si el sistema puede funcionar en la organización.

Para cada solución factible, se presenta una planificación preliminar de su implementación.

Estos resultados se entregan a la gerencia, quienes son los que aprueban la realización del sistema informático.

3.1. Factibilidad Técnica

Adquirir la tecnología necesaria para realizar el sistema de votación electrónica remota y de si estos poseen la capacidad técnica para soportar los daros requeridos por el sistema, la idea es que el sistema propuesto (**VER2012**) ofrecerá respuestas adecuadas a las peticiones sin importar el numero y ubicación de los usuarios.

La capacidad técnica de los equipos ofrece garantías de exactitud, confiabilidad, facilidad de acceso y seguridad de los datos.

De acuerdo a la tecnología necesaria para la implantación del Sistema de Votación Electrónica para las elecciones presidenciales en Nicaragua, se evaluó bajo dos enfoques: Hardware y Software.

3.1.1. Hardware

En cuanto a Hardware, específicamente el servidor donde debe estar instalado el sistema propuesto, este debe cubrir con los siguientes requerimientos mínimos:

- ✓ HP ProLiant ML350 G6 Torre Xeon E5504 2.8 HGZ Torre 5U.
- ✓ RAM 4GB DDR3 SDRAM.
- ✓ Memoria Cache L3.
- ✓ Disco Duro 2 x 500 GB 15000 RPM SCSI.
- ✓ Almacenamiento DVD-RW SATA.
- ✓ Video ATI RN50 64 MB.
- ✓ Tarjeta de Red 2x Gigabit Ethernet.
- ✓ OS Certificado Suse Linux.
- ✓ Monitor HP TFT L1710.
- ✓ Teclado HP USB.
- ✓ Mouse HP USB
- ✓ UPS APC SUA2200I de 2200 VA

A continuación se describe especificaciones técnicas necesarias para la implantación del sistema VER2012.

Servidor	HP Proliant ML350 G6 Xeon E5504 2.8 GHZ, OS Certificado Suse Linux.	Equipo para la recepción de datos
Servidor	HP Proliant ML350 G6 Xeon E5504 2.8 GHZ, OS Certificado Suse Linux.	Equipo espejo, para el backup de los datos.
Equipo de Escritorio	HP Pavilion P6 2307 Intel Core i7 3.4 GHZ, RAM DDR3 8 GB	Equipo para uso interno, tareas varias.
Cable UTP	Cable de Red cat. 5e, 4 pares de cable par trenzado, Gigabit Ethernet 155 Mbps. Caja de 100 mts.	Se usara para las conexiones internas
Jack	6 Cajas Roseta, Tapa Ciega, Marco de Conector, Marco de Caja, Conector Hembra Jack RJ - 45, instaladas de forma externa en la pared	Se usara para las conexiones internas.
Canaletas	12 Canaletas Plásticas Lisas 3mts.	Se usara para las conexiones internas.
Conectores	12 Conectores RJ – 45 Nexxt	Se usara para armar cada punto de red.
Canaletas	12 Canaletas Salva cables 3mts.	Se usara para las conexiones internas.
Crimpadora	1 Crimpadora de RED RJ - 45	Se usara para el armado del cable.
Etiquetas	Etiquetas de Cable de RED	Se usara para el etiquetado de cada cable de red.
Capuchones	24 Capuchones para proteger cable de RED RJ45	Para proteger cable de red.
Probador	Probador – Tester de RED	Se usara para verificar el armado correcto de cada cable de RED.
Switch	1 Switch CISCO de acceso catalyst serie 4500, 8 puertos	Aportara un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.
Switch	1 Switch CISCO de distribución catalyst serie 2960, 8 puertos	Para proteger la información importante, mantenga a los usuarios no autorizados alejados de la red y consiga un funcionamiento

		ininterrumpido. Dispositivos que presentan disponibilidad y redundancia altas para asegurar la fiabilidad
Switch	1 Switch CISCO de núcleo WS – C3560G, 8 puertos	Esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante, también puede conectarse a los recursos de Internet. Para el reenvió grandes cantidades de datos.
Router	1 Router CISCO 2851, administrable	Ofrece agilidad, rendimiento e inteligencia, además de ofrecer comunicaciones seguras entre la LAN local y la nube (ISP).
ISP – Fibra Óptica	Enlace dedicado de servicio de internet 1:1 de fibra óptica de 3.5 Mbps.	Servicio de internet para las conexiones locales.
Disco Duro Externo	Disco Duro externo Iomega de 3 TB	Disco duro que funcionara como backup entre el servidor espejo a través de VMWare, Maquina virtual.
Multifuncional	1 HP Laser Jet MI522NF (Impresora, Scanner, Copiadora y Fax). Memoria 64MB. Velocidad del Procesador 450 MHZ. Conectividad Redes Ethernet, USB	Para la impresión de resultados de votación
Tonner	3 Tonner para Multifuncional HP	Necesario para las impresiones
Gabinete	1 Gabinete de RED Great Lakes de 24U Enhanced series server rack	Equipo donde serán instalados transceiver IPS, router, switch´s, server, UPS.
Escritorio	1 Escritorio para computadora color café.	Para ser usado para el multifuncional.

Taladro	1 Taladro Bosch con sus brocas.	Utilizada para realizar el cableado interno.
Desarmadores	1 Juego de Desarmadores de 4 piezas marca stanley	Utilizada para realizar el cableado interno.
Escalera	1 Escalera Metálica de 2.5 mts.	Utilizada para realizar el cableado interno.
UPS	1 Estabilizador con batería integrado TrippLite Internet Office de 750 W	Para la conexión de equipos internos.
UPS	2 UPS TrippLite SU2200 RTXL2UA de doble conversión, smart online, 2U en rack/torre 110/120 V	Para la conexión de los dos servidores y equipos de comunicación.
VoIP	1 Sistema Innomedia MTA 6328XT	Equipo de voz a través de IP para la comunicación segura ya sea interna o externa.
Antivirus	1 Licencia de Kaspersky Antivirus para Linux File Server	Instalado en los 2 equipos servidores.
Antivirus	1 Licencia de Kaspersky Internet Security para Windows 7	Instalado en equipo de oficina.
Windows	1 Licencia de Windows 7	Sistema Operativo para instalarse en equipo de escritorio
MsOffice	1 Licencia de MsOffice 2007	MsOffice 2007 para instalarse en equipo de escritorio.
Dominio y Hosting	1 Dominio y Hosting con proveedor local	Dominio y Hosting para sitio www.ver2012.net

3.1.2. Software

En cuanto al software tenemos:

OS Certificado Suse Linux.

Windows 7

MsOffice 2007

Kaspersky Antivirus para Linux File Server.

Kaspersky Internet Security para Windows 7

3.2. Factibilidad Económica

Los estudios de factibilidad económica incluyen análisis de costos y beneficios asociados con cada alternativa del proyecto. Con análisis de costos/beneficio, todos los costos y beneficios de adquirir y operar cada sistema alternativo se identifican y se hace una comparación de ellos.

Presupuesto para la instalación del sistema de votación electrónica para las elecciones presidenciales de Nicaragua www.ver2012.net

3.3. Factibilidad Operativa

Esta factibilidad comprende una determinación de la probabilidad de que un nuevo sistema se use como se supone.

Un nuevo sistema puede ser demasiado complejo para los usuarios de la organización o los operadores del sistema. Si lo es, los usuarios pueden ignorar el sistema o bien usarlo en tal forma que cause errores o fallas en el sistema.

En el caso del sistema VER2012, es un proceso a largo plazo con el fin de obtener mejores resultados en lo referente a la credibilidad de nuestro sistema electoral.

La Factibilidad Operativa permite predecir, si se pondrá en marcha el sistema propuesto (VER2012), aprovechando los beneficios que ofrece, a todos los usuarios - electores involucrados con el mismo. Por otra parte, el correcto funcionamiento del sistema en cuestión, siempre estará supeditado a la capacidad de los empleados encargados de dicha tarea.

La necesidad y deseo de un cambio en el sistema electoral actual, llevó al desarrollo de un sistema de votación electrónica en línea, que de una manera más sencilla y amigable, cubra todos los requerimientos, expectativas y que proporcione la información en forma oportuna y confiable.

4. Seguridad

La seguridad es un elemento de primer nivel que debe considerarse desde la concepción inicial del sistema y participa desde el principio en las decisiones del diseño. Su objetivo primordial en la información es mantener la integridad, disponibilidad y confidencialidad de los datos del sistema eliminando o reduciendo la vulnerabilidad del mismo. Abarca tres partes: el hardware, el software y los datos.

Con **integridad** de datos nos referimos a la completitud y corrección de los mismos haciendo que la única forma de modificarlos, sea de una manera controlada y por elementos autorizados.

La **confidencialidad** es la propiedad que asegura que la información existente en un sistema de computación o aquella que es transmitida, sea leída o entendida únicamente por personas o entidades autorizadas.

Garantizar la **disponibilidad** indica que los datos u objetos estarán accesibles por entidades autorizadas cuando éstas las requieran, confiando en la autenticidad que dichos objetos son los que dicen ser.

La seguridad está delimitada por áreas o zonas consideradas de la siguiente manera:

- **Área de influencia:** Es la zona más externa del sistema, donde es factible realizar acciones contra la integridad de ésta área.

- **Área de exclusión:** Es el espacio concéntrico exterior al área protegida, de utilización restringida o acceso limitado.

- **Área protegida:** Es la zona delimitada por barreras físicas en el que se ejerce un cierto control de movimientos y permanencia.

4.1. Mecanismos de seguridad

Las políticas de seguridad deben estar sostenidas sobre tres principios fundamentales, éstas van desde ser preventivas, de corrección o detección, y de repuesta.

a. **Prevención:** En ésta parte se utilizan métodos de autentificación, identificación, control de acceso, transmisión segura en plataformas heterogéneas.
b. **Detección:** Se realizan chequeos de integridad, también se provee y presenta información al instante sobre el estado actual del sistema (aquí tanto proveedor como el administrador comparten responsabilidad del correcto funcionamiento).
c. **Respuestas:** Se implementan métodos de backups (respaldo) y auditoría inclusive si un intruso ha vulnerado el sistema, y que área explotó

Entre las medidas de seguridad de carácter técnico se encuentran:

- ✓ **Identificación y autentificación de usuarios**
- ✓ **Control de Accesos.**
- ✓ **Confidencialidad e Integridad.**
- ✓ **Cifrado de datos/Encriptación.**
- ✓ **Cortafuegos.**
- ✓ **Valorar la seguridad que brindará el servidor.**

4.1.1. Identificación y autentificación de usuarios: El proceso de solicitud, manejo y cierre de las cuentas de usuarios debe provenir de un superior, en este caso del director de informática (en su defecto el administrador) y de acuerdo a los requerimientos o posiciones, se crea el perfil de acceso en el sistema.

4.1.2. Control de accesos: La amplitud del rango de accesos se determina mediante privilegios y separación de los mismos según tipos de usuarios; los cuales se han dividido en cuatro clases Administrador, Verificador, Candidato y Elector. Además se desarrollan políticas de seguridad en práctica como encriptación de datos (usuario y su respectiva password o contraseña) haciendo uso de MD5, y defensas antes amenazas de Sql inyección, por ejemplo.

4.1.3. Confidencialidad e Integridad: Nos referimos a que la información únicamente sea conocida por personas autorizadas, **integridad** hace que su contenido permanezca inalterado solo podría ser modificado por autoridades correspondientes.

4.1.4. Cifrado de datos: Todas las medidas de seguridad que implementemos son importantes, ejemplo; si guardamos las contraseñas encriptadas en la base de datos, lograremos que cualquiera que intente tenga acceso a la misma no pueda saber cuál es la contraseña que decidió utilizar y esto se refleja en la privacidad. Para ello haremos uso de MD5.

¿Qué es **MD5**? MD5 es un algoritmo informático criptográfico que habitualmente representa una cadena de 32 caracteres ampliamente usado para proporcionar seguridad a un archivo de internet. Este ofrece protección al usuario contra los caballos de Troya, y virus que algún otro usuario pudiera incluir en el sistema. Lo usaremos para cifrar los accesos de los electores al sistema.

4.1.5. Cortafuegos: Son conjuntos de aplicaciones o equipos ubicados entre dos redes que establecen políticas de acceso entre las partes. Mediante un firewall, se pueden establecer reglas para hacer cumplir ciertas restricciones como tráfico de conexiones de salida.

Ejemplos de amenazas

¿Qué es **Sql Inyección**? Es un método de infiltración que se vale de la vulnerabilidad informática presente en un sistema en el nivel de validación de entradas para realizar consultas a una base de datos; ésta puede ocurrir en cualquier lenguaje de programación.

5. Desarrollo.

En tanto se ha definido la duración de los procesos para cada etapa de desarrollo del sistema (ver cronograma en anexos), comenzamos a diseñar cada módulo que compone el proceso de votación en línea a través de código, pruebas haciendo uso de las herramientas web.

Una vez instalado el sistema en línea realizaremos pruebas meritorias de seguridad para brindar a usuarios (personas o electores) un medio fiable y seguro de realizar su voto de forma secreta como lo establece la ley constitucional. Además tomamos en cuenta las políticas de respaldo de la información que permita superar efectos de fallas. Del mismo modo tiene parte de responsabilidad el prestador del servicio o quien en este caso nos brinde el alojamiento. Éste debe garantizar que el servicio sea cien por ciento seguro, y este activo el sitio de forma permanente, y en especial ese día.

Acá exponemos unas pantallas para el acceso a nuestro sistema conforme los pasos a seguir para lograr depositar nuestro voto en lo que denominaríamos sin importar la ubicación “Urna electrónica” (Anexos. ver fig. a. pantalla de inicio.)

Cabe mencionar que los datos de acceso se proporcionaran a la ciudadanía utilizando el método actual de verificación un mes antes del día “D” las elecciones a celebrarse. Posteriormente al usuario o elector se le sugerirá que tiene un periodo determinado para cambiar sus accesos (Anexos. ver fig. b. Cambio de accesos).

Hecha la observación anterior se nos mostrará una pantalla donde podemos elegir a nuestro candidato o partido de preferencia, mediante “Votación” (Anexos. ver fig. c. Pantalla de votación).

Para dar continuidad, seleccionamos el botón de **“Votar**”, la cual ilustrará boletas con las opciones de los candidatos en disputas electorales, sean éstas presidenciales, municipales, departamentales; según el período (Anexos ver fig. d Pantalla de Boletas).

El administrador, es el encargado de vigilar que exista seguridad durante el periodo de elecciones. También éste tiene derechos de dar de alta o de baja a los usuarios, y proporcionarle la amplitud de privilegios. Esto es válido igualmente para la sección de

candidatos y partidos. La sección de Resultados se limitará a una hora prevista según la hora definida de cierre de “urnas de votación electrónica”.

5.1. Resultados de votaciones

En conclusión, para los reportes de votaciones en las elecciones presidenciales celebradas a través de la participación de nicaragüenses residentes en el extranjero; hacemos referencia a una función que detecta la ubicación geográfica por IP.

Dicha función se llama GeoIP, esta clase sirve para obtener de qué país es un nicaragüense que ejerce su voto fuera de la nación, por su IP. Se utiliza una base de datos de la cual extraeremos un fragmento para explicar cómo funciona.

Su estructura

Id	**Sólo índice**	**El resultado de la búsqueda es el índice buscado, o 0 si es desconocido.**
Country	Sólo índice	El resultado de la búsqueda es un índice de país, o 0 si es desconocido.
Región	Sólo índice	El resultado de la búsqueda es un país y región, empaquetados, o 0 si es desconocido.
City	Índice + datos	El resultado es un apuntador a los datos de la ciudad.
Name	Índice + datos	El resultado de la búsqueda es un apuntador a string terminado en 0x00.

La representación de los datos una vez concluido el cierre de votación (el cual se regirá con hora local) se mostrará vía internet; cabe mencionar que adicionalmente se le facilitará una copia de las actas entregadas en CD como respaldos a los partidos políticos. Podrán si así lo desean los ciudadanos revisar los resultados de las elecciones desde la misma página web una vez concluidos los procesos electorales.

6. Conclusiones

Aún con todas las facilidades tecnológicas y en donde el Internet ha abierto nuevos campos de aplicación para el ejercicio de la democracia, Nicaragua aún realiza su proceso electoral de forma manual.

El mecanismo que se usa en los procesos electorales de Nicaragua en la actualidad, no permite la participación de nicaragüenses con cédula activa que se encuentran fuera del país.

Para Nicaragua, al menos una propuesta estratégica de Aplicación Web para capturar el voto de los nicaragüenses fuera del país es una oportunidad para reflexionar sobre la participación ciudadana de los comicios.

Para agilizar la obtención de los resultados electorales se hace necesario desarrollar un mecanismo electrónico que permita acelerar este proceso sin perder el control de los datos, de manera que los resultados no sean de días sino de horas.

Una aplicación web pudiera motivar a incrementar la participación de nicaragüenses dentro y fuera del país, con el fin de incentivar a la población en el uso de la tecnología actual. Proporcionando así toda la seguridad web.

Esta aplicación vista a largo plazo bajaría los costos que actualmente se gastan en este tipo de procesos, ya que su inversión requeriría solo de mantenimiento una vez implantado.

7. Recomendaciones Básicas

- Se debería contemplar en la ley electoral alguna reforma que permita que los nicaragüenses en el extranjero puedan ejercer su derecho al voto, a través de alguna aplicación web.

- En cuanto a la aplicación web, se debería emplear una serie de procedimientos con el fin de evaluar y monitorear el sistema y su entorno y recopilar información sobre el comportamiento de los diferentes servicios y así poder tomar las medidas necesarias ante una posible falla.

- En la verificación de acceso se recomienda usar un logueo seguro mediante https, y uso de contraseñas largas con combinación de mayúsculas, minúsculas, y en lo posible intercalar algún número. Los certificados https "fue desarrollado por Enterprise Integration Technologies (EIT) permiten tanto el cifrado como la autentificación digital en sitios web.

- Para una mejor seguridad en este tipo de sistema se propone el uso de tecnología biométrica (huella dactilar) lo cual no daría lugar a fraudes o hurto de voto. Esta tecnología ya ha sido probada en la región latinoamericana con excelentes resultados. En Nicaragua, se emplea por el momento en el control de asistencia de empleados en Instituciones públicas y privadas.

- Para el sistema de monitoreo de votaciones se recomienda que el administrador de seguridad debe contar con técnicas de detección de sniffer para que la estabilidad del sistema no se vea comprometida. De la misma manera deben hacerse test de DNS.

- Asegurar que sólo el administrador de la máquina tenga permiso de acceso a estos directorios y archivos.

- Se recomienda que el código fuente sea propiedad de la Autoridad electoral responsable y no de una firma proveedora de materiales.

- El hardware y software, así como el código fuente deberían de estar disponible para inspecciones en todo momento de gente experta en el tema, así como la documentación de respaldo.

.

8. Cronograma de Trabajo

9. Referencias Bibliográficas

9.1. Bibliografía

Romero Flores, R. Téllez Valdez, J. (2010) Voto electrónico, derecho y otras implicaciones. Recuperado el 15 de marzo del 2012, de http://biblio.juridicas.unam.mx/libro.htm?l=2801

Tuesta Soldevilla, F. (2004) El voto electrónico. Recuperado el 22 de abril del 2012, de http://www.web.onpe.gob.pe/modEscaparate/caratulas/tuesta2.pdf

Puiggalí J. Voto electrónico. Recuperado el 25 de abril del 2012, de http://jcel.unizar.es/jcel07/ponencias/JCEL_Voto_Electronico.pdf

(2004) Sondeo de opinión pública. Equipo del Proyecto "Monitoreo e Incidencia sobre el proceso de transición democrática y gobernabilidad en Nicaragua. Recuperado el 27 de abril del 2012, de http://ipade.org.ni/viejo/htdocs/docs/publicaciones/SegSondeo.pdf

9.2. Web grafía

Instituto de investigaciones jurídicas. Recuperado el 7 de marzo del 2012, de http://www.juridicas.unam.mx

Busaniche, B. (2010) Voto Electrónico: Los riesgos de una ilusión. Recuperado el 7 de marzo del 2012, de http://www.vialibre.org.ar/wp-content/uploads/2009/03/evoto.pdf

Panizo, L.A. (2008). Aspectos tecnológicos del voto electrónico. Recuperado el 9 de marzo del 2012, de http://www.onpe.gob.pe

Conteo y consolidación de los votos. Recuperado el 9 de marzo del 2012, de http://www.idea.net/publications/ies/upload/

Morales Rocha, V.M. Seguridad en los procesos de voto electrónico remoto: Registro, votación, consolidación de resultados y auditoria. Recuperado el 9 de marzo del 2012, de http://www.tesisenred.net/bitstream/handle/10803/7043/01VMmr01de01.pdf?secuence=1

Téllez Valdez, J (2010). El voto electrónico. Recuperado el 9 de marzo del 2012, de http://www.te.gob.mx/documentacion/publicaciones/Temas_selectos/14_voto.pdf

Aleuy, M (2011). El voto electrónico: La votación electrónica. Recuperado el 24 de marzo del 2012, de http://ebookbrowse.com/12983199018-voto-electronico-pdf-d118568669

Mendoza, J. (2008). No videntes nicas quieren voto secreto. Recuperado el 27 marzo del 2012, de http://www.elnuevodiario.com.ni/politica/28394

Red de conocimientos electorales. Recuperado el 31 de marzo del 2012, de http://aceproject.org/ace-es/focus/fo_e-voting

Observatorio del voto – e en Latinoamérica. Recuperado el 19 de abril del 2012, de http://www.voto-electronico.org/

Protocolos: Tipos de Protocolos. Recuperado el 13 de julio del 2012, de http://es.kioskea.net/contents/internet/protocol.php3

Protocolo (Informática): Propiedades típicas. Recuperado el 22 de julio del 2012, de http://es.wikipedia.org/w/index.php?title=Protocolo_(informática)&oldid=60754847

Que es un navegador, explorador o buscador. Recuperado el 13 de septiembre del 2012, de http://www.masadelante.com/faqs/que-es-un-navegador

(2012) ¿Qué hace un servidor web como apache?: Configuración. Recuperado el 3 de octubre del 2012, de http://www.digitallearning.es/blog/apache-servidor-web-configuracion-apache2-conf/

Ruiz, A. (2010) Servidores WAMP. Recuperado el 3 de octubre del 2012, de http://recursostic.educacion.es/observatorio/web/es/software/servidores/800-monografico-servidores-wamp

Definición de HTML. Recuperado el 3 de octubre del 2012, de http://definicion.de/html/

PHP. Recuperado el 3 de octubre del 2012, de http://es.wikipedia.org/wiki/PHP

MySQL. Recuperado el 3 de octubre del 2012, de http://es.wikipedia.org/wiki/MySQL

(2008) MySQLi: Programación en Internet. Recuperado el 14 de octubre del 2012, de http://rua.ua.es/dspace/bitstream/10045/13363/12/12c-mysqli.pdf

(2011) Navicat. Recuperado el 14 de octubre del 2012, de http://www.blueorb.es/tag/navicat/

Aranibar, N. (2011) MySQL WorkBench. Recuperado el 14 de octubre del 2012, de http://www.monografias.com/trabajos88/mysql-worckbench/mysql-worckbench.shtml

Introducción al CSS. Recuperado el 28 de octubre del 2012, de http://www.librosweb.es/css/pdf/introduccion_css.pdf

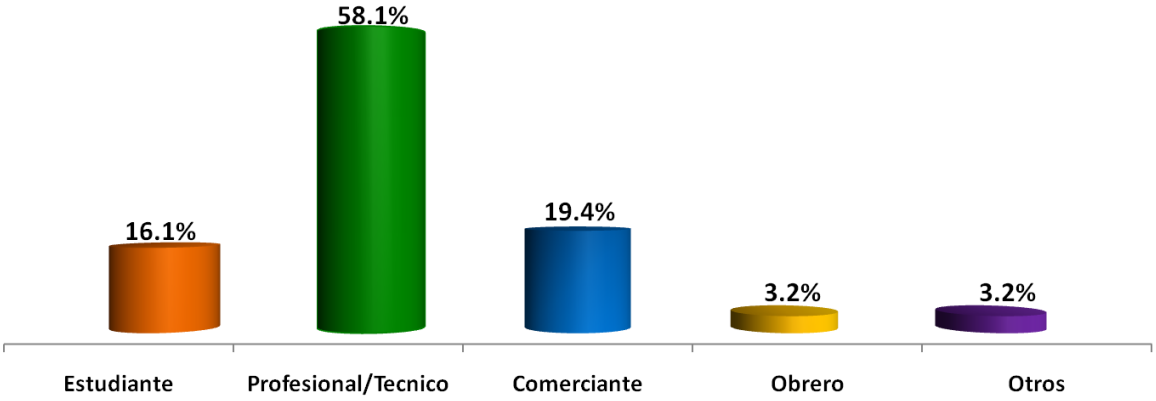
(2012) jQuery. Recuperado 31 de octubre del 2012, de http://www.actualidadjquery.es/2012/01/06/fancybox-abrir-imagenes-paginas-web-y-videos-en-ventanas-tipo-popup-con-jquery/

(2012) Fancybox. Recuperado el 31 de octubre del 2012, de http://www.usosweb.com/content/tutorial-fancybox

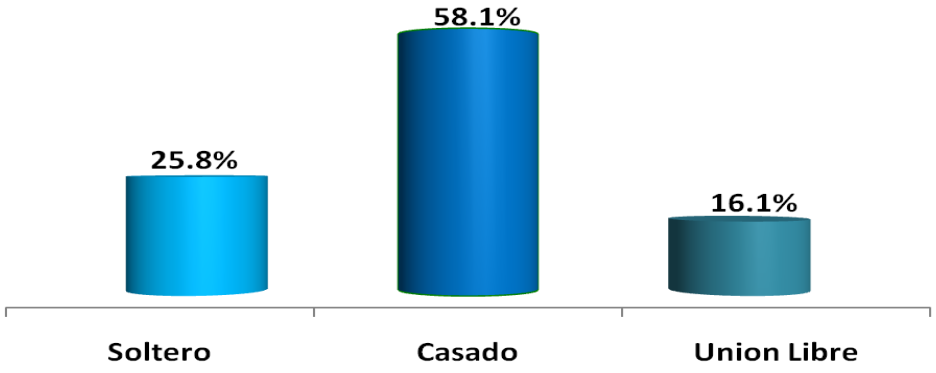
Álvarez, M.A. (2009) jQuery: Introducción a jQuery. Recuperado el 3 de noviembre del 2012, de http://www.desarrolloweb.com/articulos/introduccion-jquery.html

Caracterización de la muestra

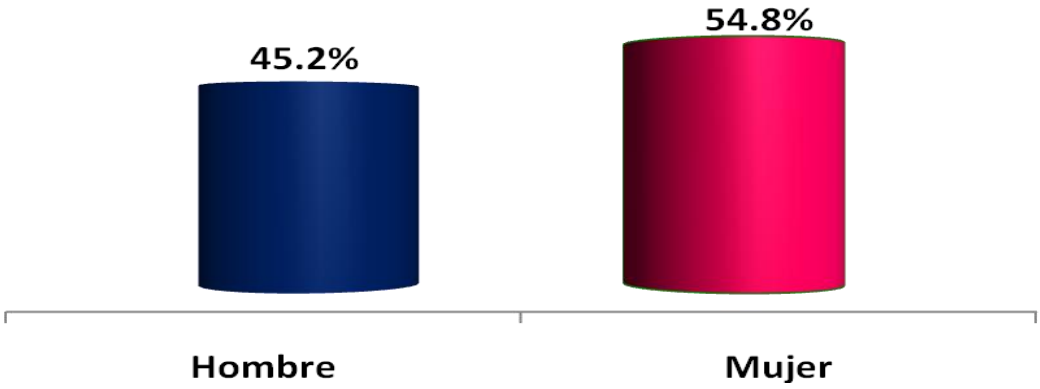
Ocupación entrevistados



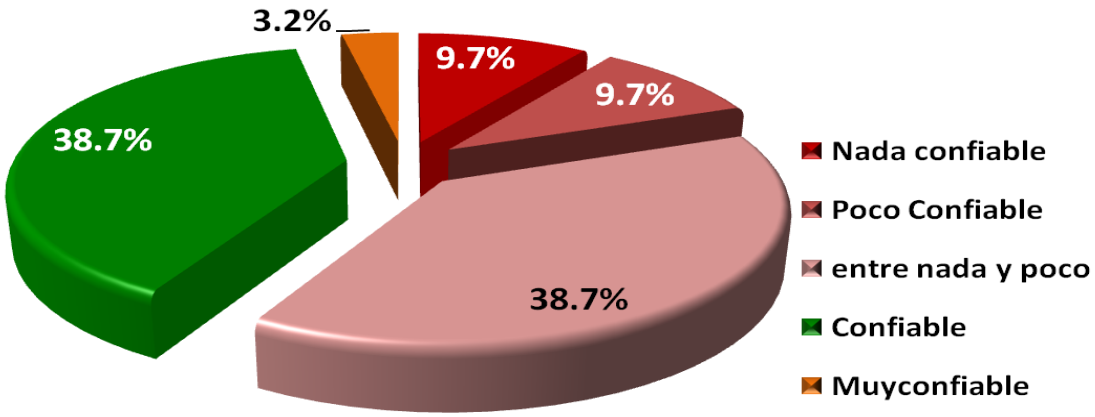
Estado civil



Genero del entrevistado



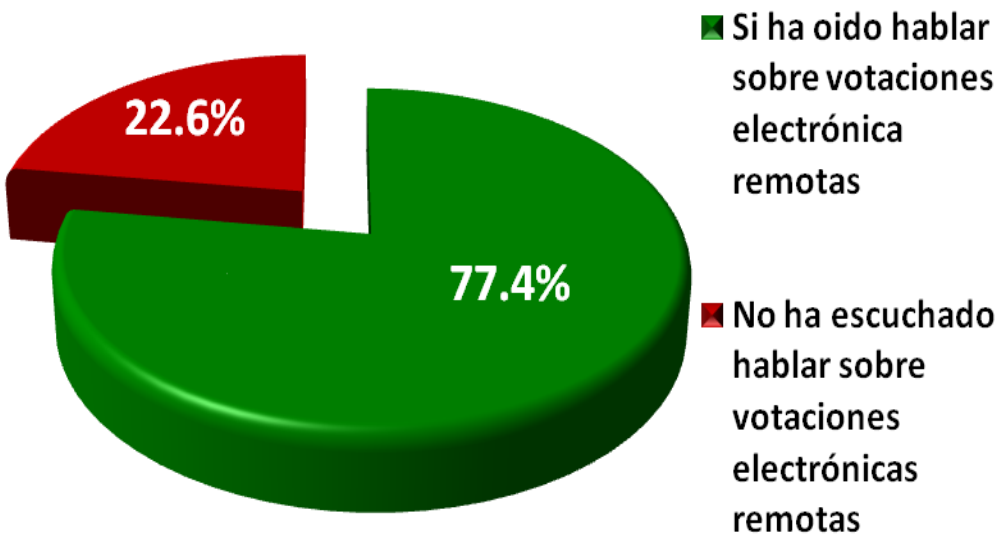
Confiablidad en el proceso de votación electoral en Nicaragua



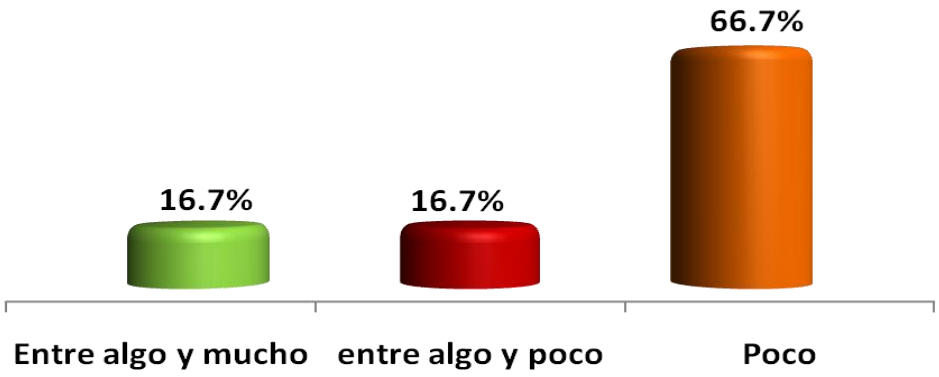
Grado de Acuerdo o desacuerdo en…

	Acuerdo	Desacuerdo	Total
El proceso de votación es lento.	38.7%	61.3%	100%
El proceso de conteo de votos es tardado.	93.5%	6.5%	100%
Para brindar los resultados de las votaciones se llevan muchos días.	96.8%	3.2%	100%
Se invierte demasiado dinero en boletas, tintas, etc.	96.8%	3.2%	100%

Grado de conocimiento sobre votaciones electrónicas remotas

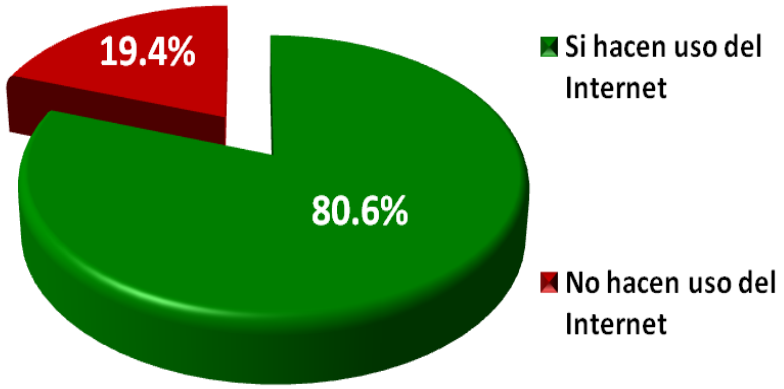


Cuanto sabe sobre el tema de votaciones electrónicas remotas?

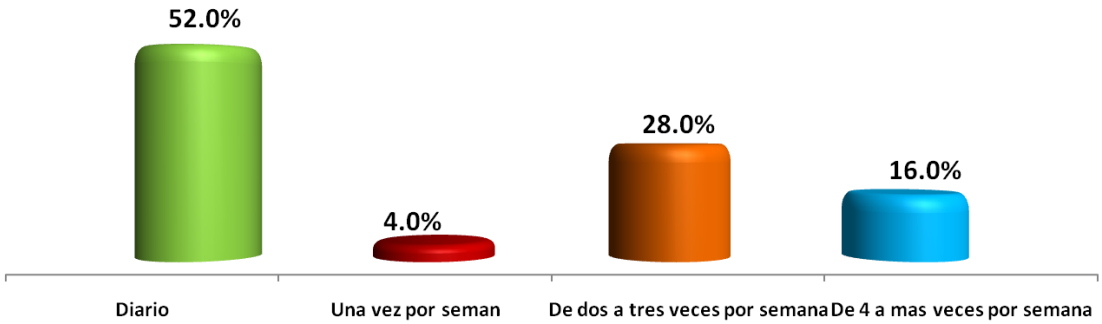


Usuarios de Internet

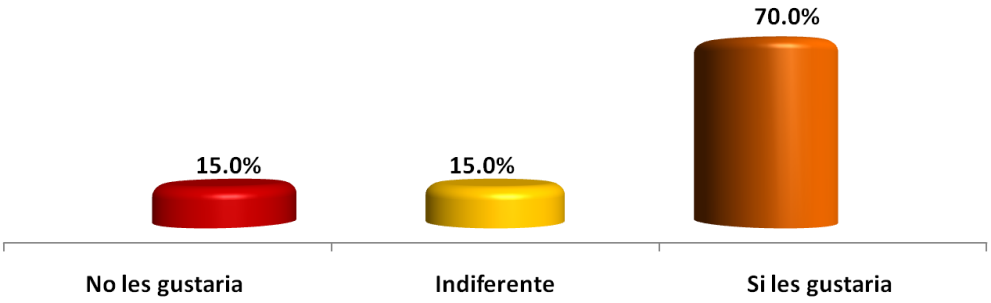
Base =25 (80.6%)



Frecuencia con que hacen uso del Internet



Grado de aceptación a que familiares con nacionalidad nicaragüenses en el extranjero participen desde el lugar donde se encuentran en votaciones electorales de Nicaragua



Herramientas libres para seguridad informáticas y redes

1. **Spyware:**

   - **AD- Aware Se Personal [windows]** Herramientas para remover spyware, el cual mantiene una base de datos de spyware conocidos y tiene a su vez la capacidad de identificar código malicioso.

   - **Windows Defender[Windows]** Servicio proporcionado por Microsoft Protege la computador de spyware y popups

2. **Antivirus**

   - **McAffeAvertStinger:** Herramienta usada para remover un virus o worm específico.

   - **AVG Anti-virus:** Otra suite efectiva de escaneo de virus.

3. **Utilidades Web.**

   - **Firefox** El navegador Open Soucer más popular, de arquitectura segura y altamente adaptable por el uso.

Diccionario de Datos

tbl_candidato

Field	Type	Null	Default	Comments
id_candidato	int(10)	No		
id_persona	int(10)	No		
id_cargo	int(10)	No		
id_partido	int(10)	No		

tbl_config

Field	Type	Null	Default	Comments
clave	varchar(255)	No		
valor	tinytext	No		
comentario	tinytext	No		

tbl_departamento

Field	Type	Null	Default	Comments
id_departamento	int(10)	No		
nombre	varchar(25)	No		

tbl_elector

Field	Type	Null	Default	Comments
id_elector	int(10)	No		
id_persona	int(10)	No		
id_municipio	int(10)	No		
voto	tinyint(1)	No		1 Activo,0 inactivo
tipo	tinyint(1)	No	0	1-pre,2-dep,3-par, 1+2=pre+dep, 1+2+3=pre+dep+par

tbl_ip

Field	Type	Null	Default	Comments
id_ip	int(10)	No		
ip	varchar(16)	No		
conteo	int(10)	No	0	

tbl_muni2

Field	Type	Null	Default	Comments
id_municipio	varchar(4)	No		
id_departamento	int(10)	No		
municipio	varchar(25)	No		

tbl_municipio

Field	Type	Null	Default	Comments
id_municipio	int(10)	No		
id_departamento	int(10)	No		
nombre	varchar(25)	No		

tbl_modulo

Field	Type	Null	Default	Comments
id_modulo	int(10)	No		
menu	varchar(45)	No		

tbl_modulo_usuario

Field	Type	Null	Default	Comments
id_modulo_usuario	int(10)	No		
id_modulo	int(10)	No		
id_usuario	int(10)	No		

tbl_partido_politico

Field	Type	Null	Default	Comments
id_partido	int(10)	No		
nombre	tinytext	No		
logo	text	No		

tbl_persona

Field	Type	Null	Default	Comments
id_persona	int(10)	No		
id_municipio	int(10)	No		
ced_persona	varchar(17)	No		
nombre	varchar(25)	No		
apellido_pat	varchar(15)	No		
apellido_mat	varchar(15)	No		
genero	char(1)	No		
domicilio	tinytext	No		

tbl_puesto

Field	Type	Null	Default	Comments
id_cargo	int(10)	No		
nombre_cargo	varchar(25)	No		

tbl_tipo_usuario

Field	Type	Null	Default	Comments
id_tipo_usuario	int(10)	No		
descripcion	varchar(45)	No		

tbl_voto

Field	Type	Null	Default	Comments
id_voto	int(10)	No		
id_partido	int(10)	No		
id_municipio	int(10)	No		
tipo	tinyint(1)	No	0	1-pre,2-dep,3-par
fecha	timestamp	No	CURRENT_TIMESTAMP	

Pantallas del Sistema

Fig. a. Pantalla de inicio

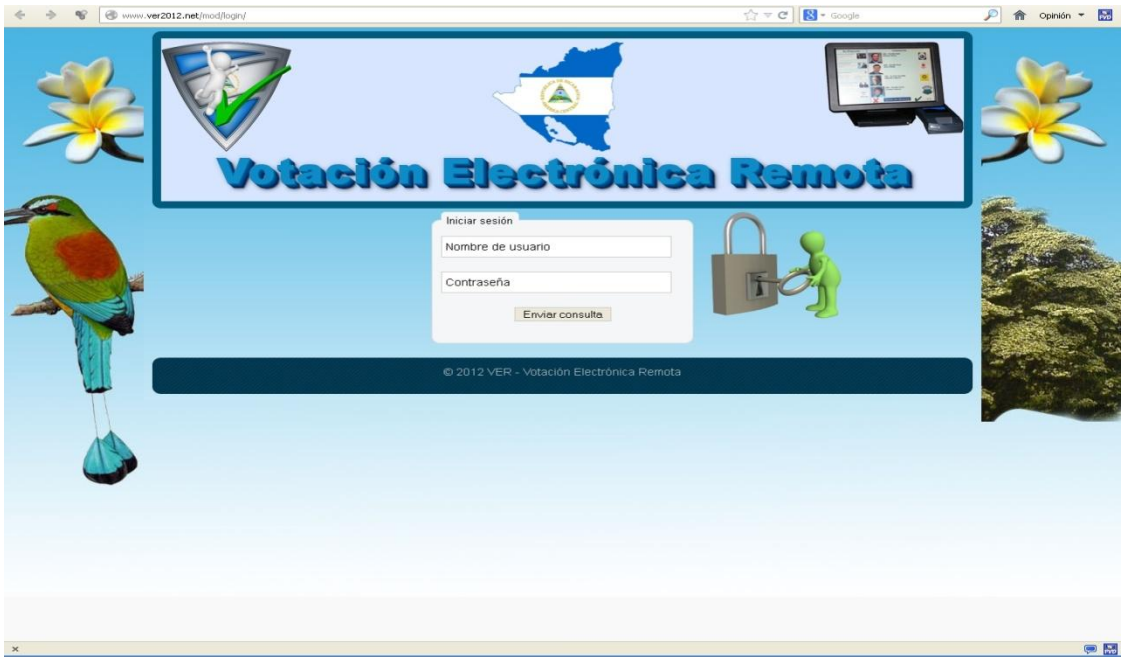


Fig. b. Cambio de accesos

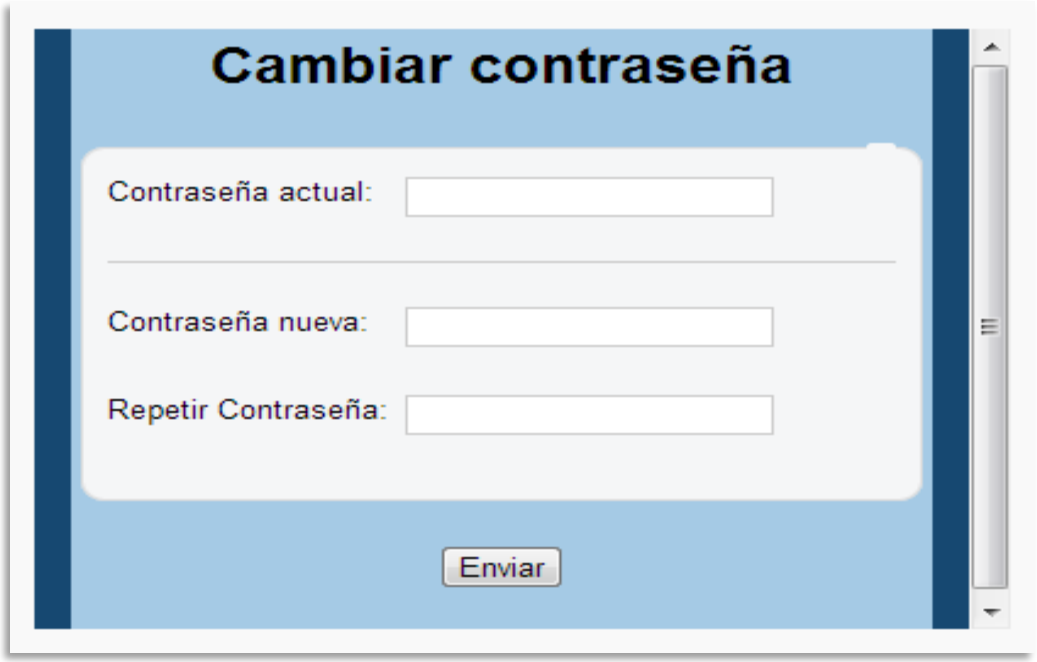


Fig. c. Pantalla de votación Presidencial

Fig. c.1 Pantalla de votación Departamental

Fig. c.2 Pantalla de votación Diputados al PARLACEN

Fig. 1.1 Servidor HP

Fig. 1.2 HP Pavilion P6 2307

Fig. 1.3 Cable de RED UTP CAT 5e

Fig. 1.4 Caja Roseta UTP

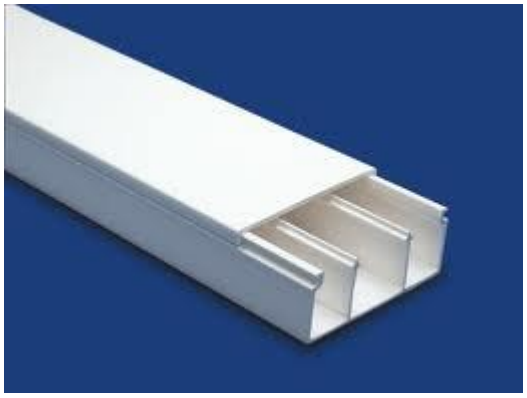


Fig. 1.5 Canaleta Plásticas lisas para RED

Fig. 1.6 Conectores RJ – 45

Fig. 1.7 Canaletas Plásticas Lisas Salva cables

Fig. 1.8 Crimpadora

Fig. 1.9 Etiqueta de RED

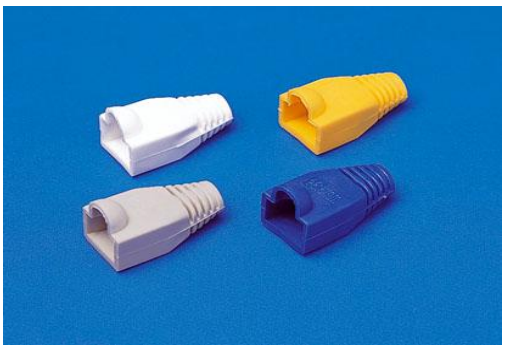


Fig. 1.10 Capucha para cable de RED UTP

Fig. 1.11 Tester de RED

Fig.1.12 Switch CISCO Catalyst 4500

Fig.1.13 Switch CISCO Catalyst 2960

Fig.1.14 Switch CISCO Catalyst C3560G

Fig.1.15 Router CISCO 2851

Fig.1.16 Disco Duro Externo Iomega 3 TB

Fig.1.17 Multifuncional HP LaserJet MFP 1522nf

Fig.1.18 Gabinete de RED Great Lakes de 24U

Fig.1.19 Escritorio para PC

Fig.1.20 Taladro Bosch

Fig.1.21 Desarmadores Stanley

Fig.1.22 Escalera Metálica

Fig.1.23 UPS TrippLite Internet Office 750

Fig.1.24 TrippLite SU2200 RTXL2UA

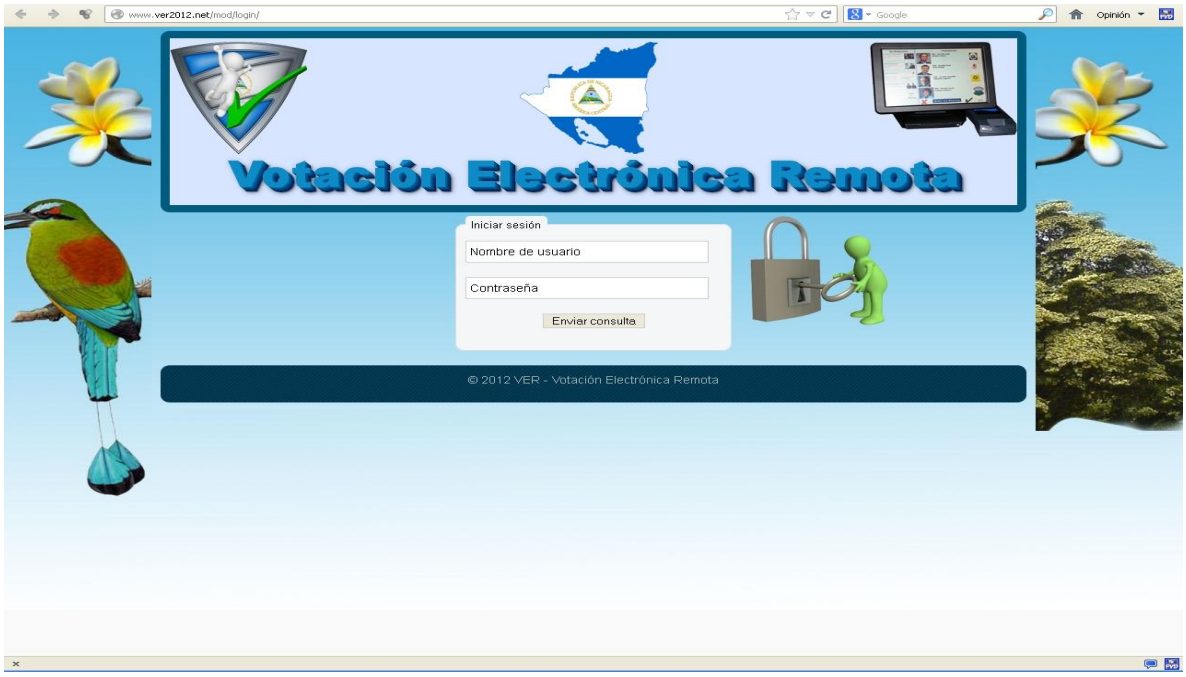
Fig. 1.25 Innomedia MTA 6328 XT VoIP

Manual de Administrador

En el presente manual describiremos como funciona el sistema y los pasos a seguir para acceder a cada una de las funciones que presente VER (sistema de votacion remota). Primeramente explicamos las operaciones que puede realizar el administrador del sitio.

En esta ocasión vamos a contar como es que funciona con usuario de administrador.

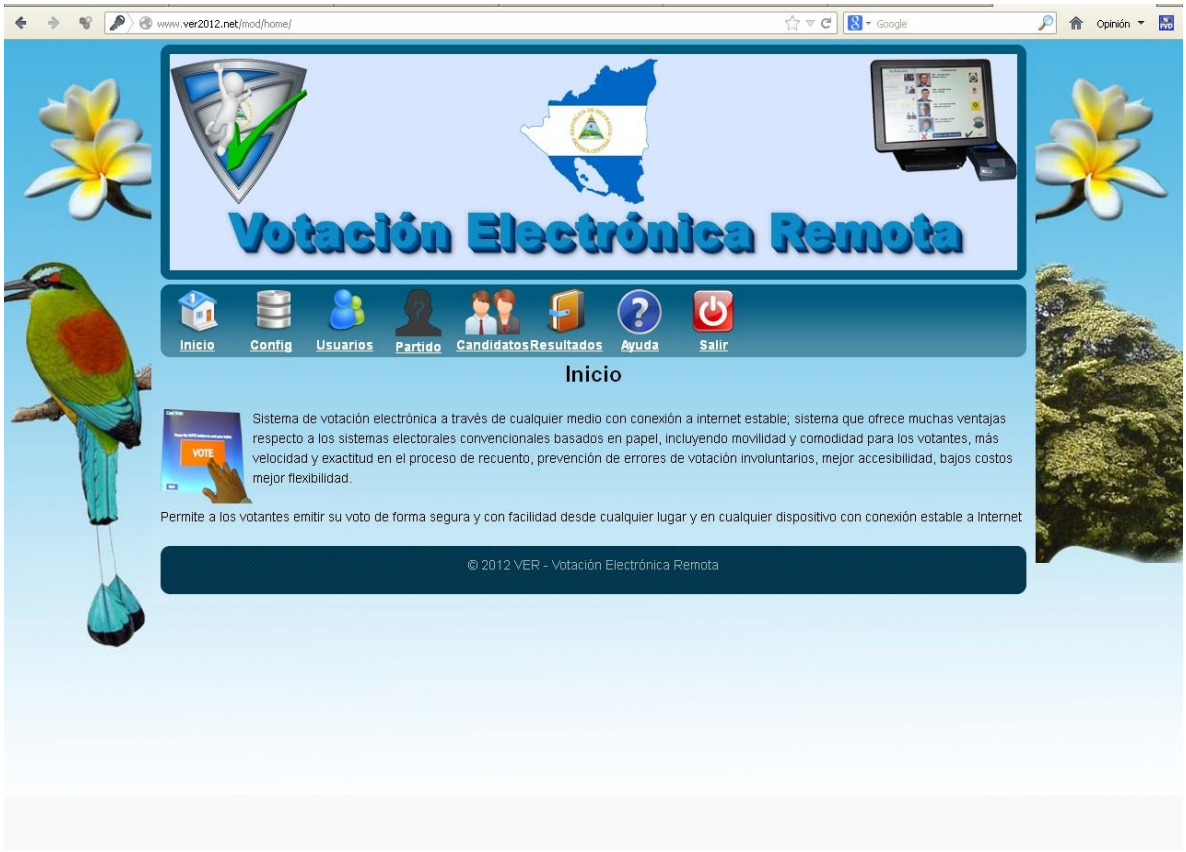
Primeramente, cargamos la pantalla del sitio y nos mostrará la siguiente pantalla:



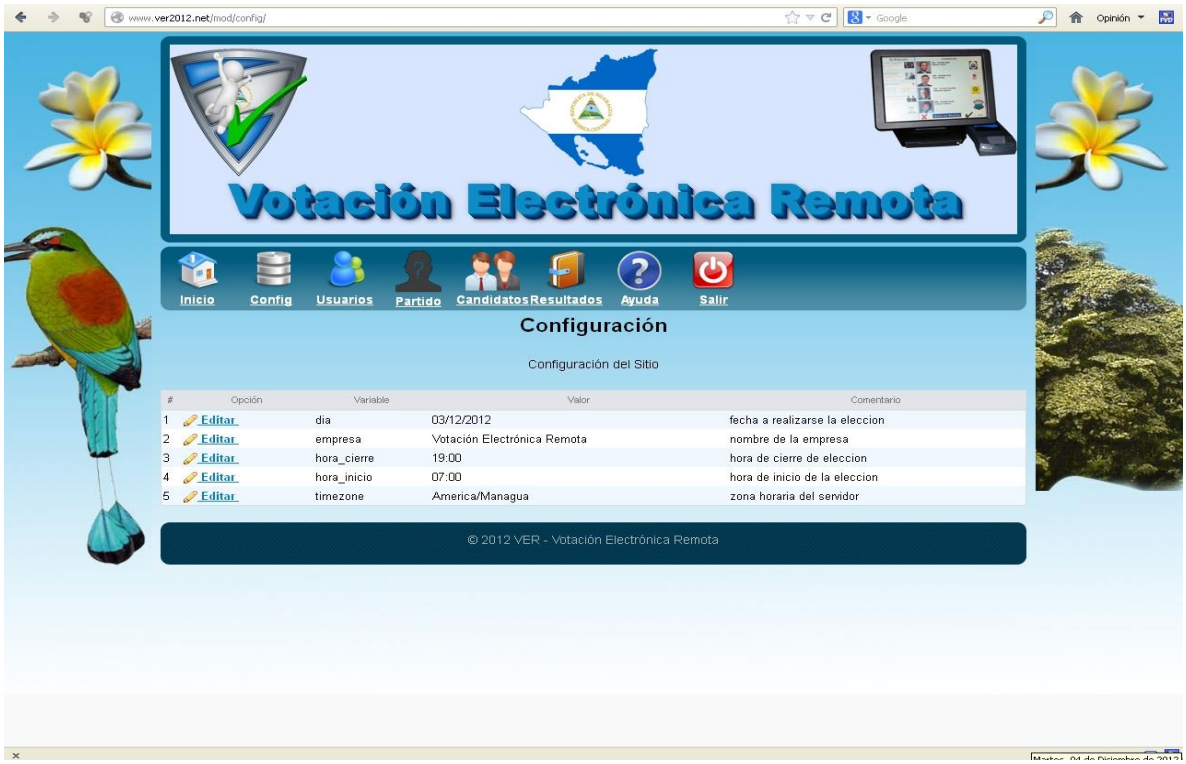
Allí podemos ingresar con los respectivos datos de administrador los cuales se proporcionaran directamente a administrador, una vez que ha ingresado éste puede tener control a los siguientes funciones del menú.

El administrador tiene el mayor rango de privilegios de acceso a Configuración, Usuarios, Partidos, Candidatos, y a Resultados.

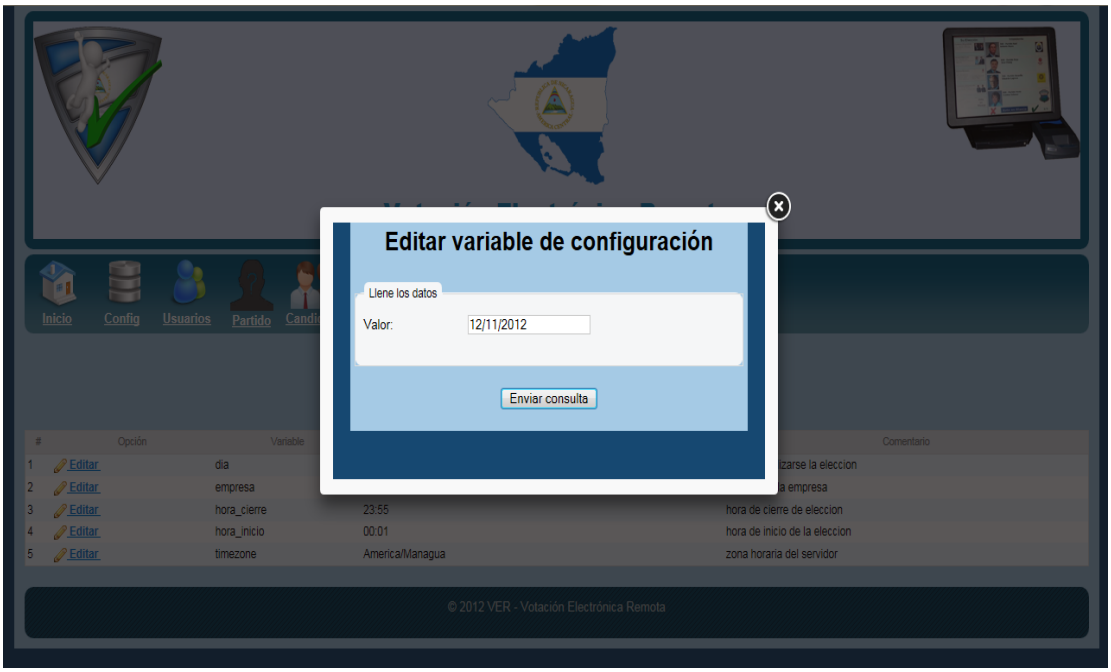
Tiene acceso a la configuración de apertura y cierre de horas para habilitar las votaciones, si no se realiza este cambio él podrá ingresar pero en ningún instante le permitirá visualizar el menú de votación a un elector.



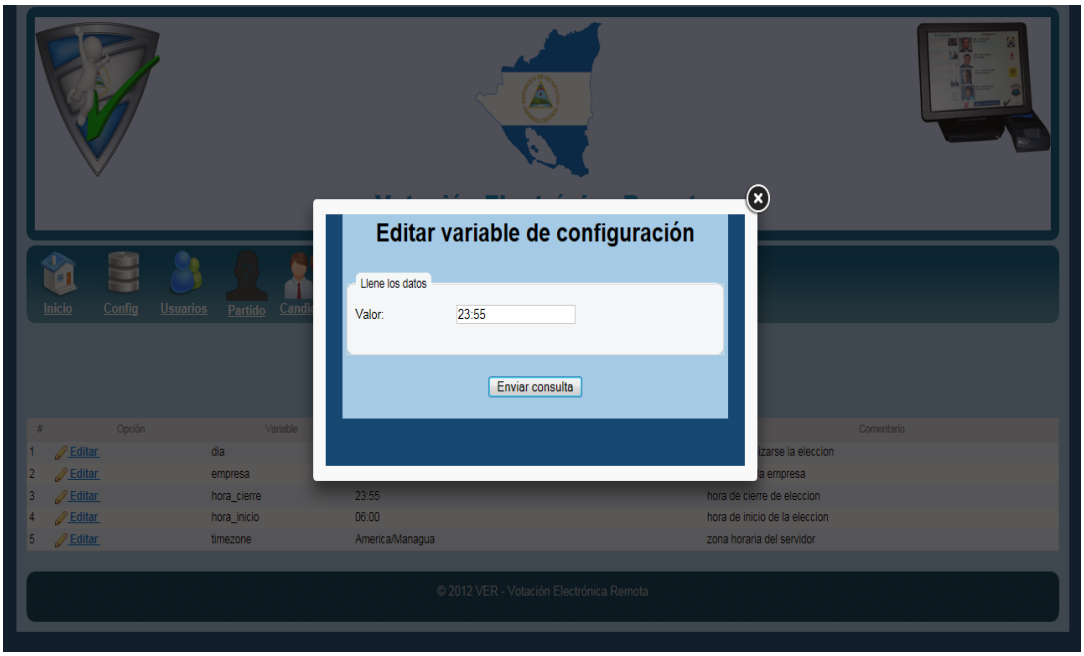
En las siguientes pantallas se presenta una continuidad de cómo puede configurar el sistema. Aquí nos econtramos en el módulo de Configuración, como se puede apreciar hay una opción de “Editar”, donde se puede modificar las principales variables de control de lo que podría decirse “Urna receptora de votos”. Realmente solo es un canal de transmisión por el cual viajarán cada uno de los puntos de votaciones para almacenarse en servidor.



En la siguiente figura se aprecia la edición de la variable fecha de votación



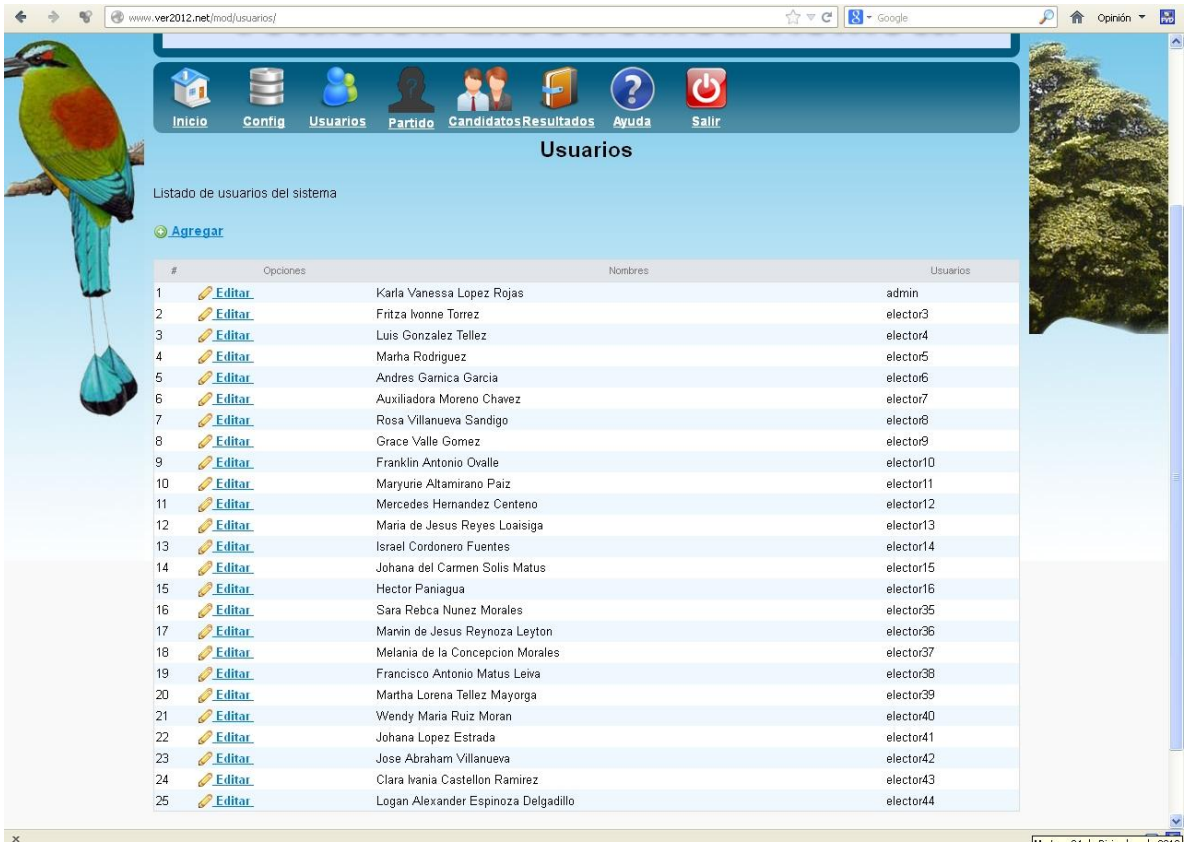
Editando la variable hora de cierre (regidas en formato de 24 horas):



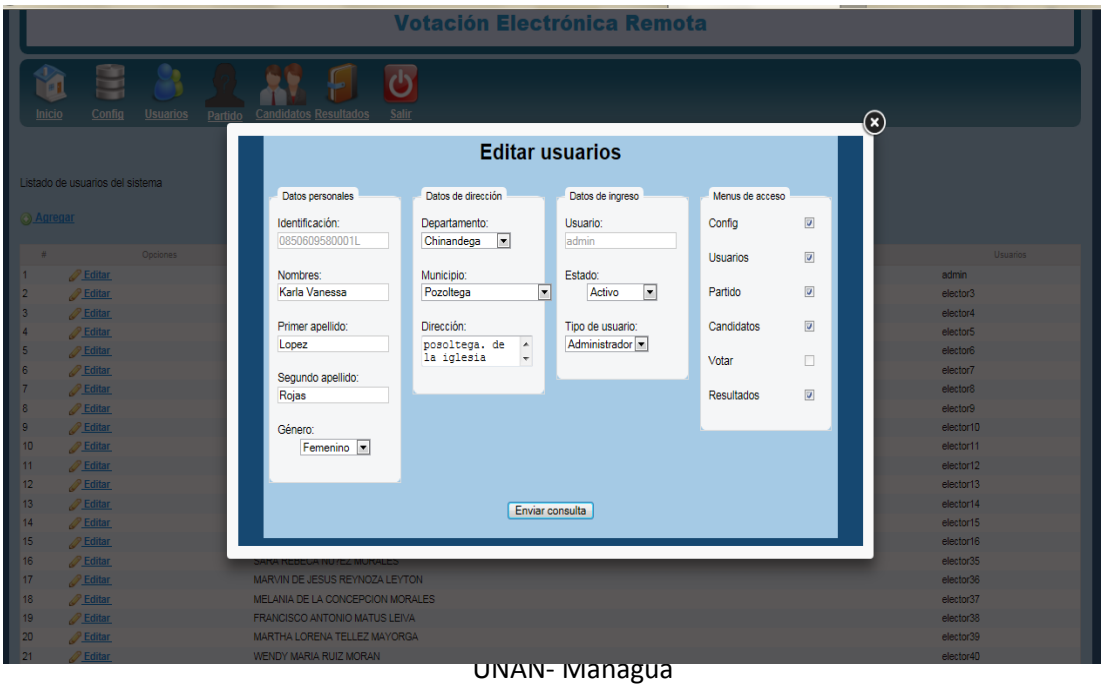
De igual manera se configura la hora de apertura, o el nombre de la empresa.

Ahora podemos acceder a la pestaña de usuarios. Aquí contenemos algunos datos de prueba, y de igual manera se pueden agregar o modificar únicamente el nombre, apellido paterno, apellido materno, cambio de domicilio:

Los datos que se aprecian en la columna de usuarios, serán datos asignado por los funcionarios de CSE (encargados del padrón electoral), de igual manera ellos son encargados de asignar la contraseña.



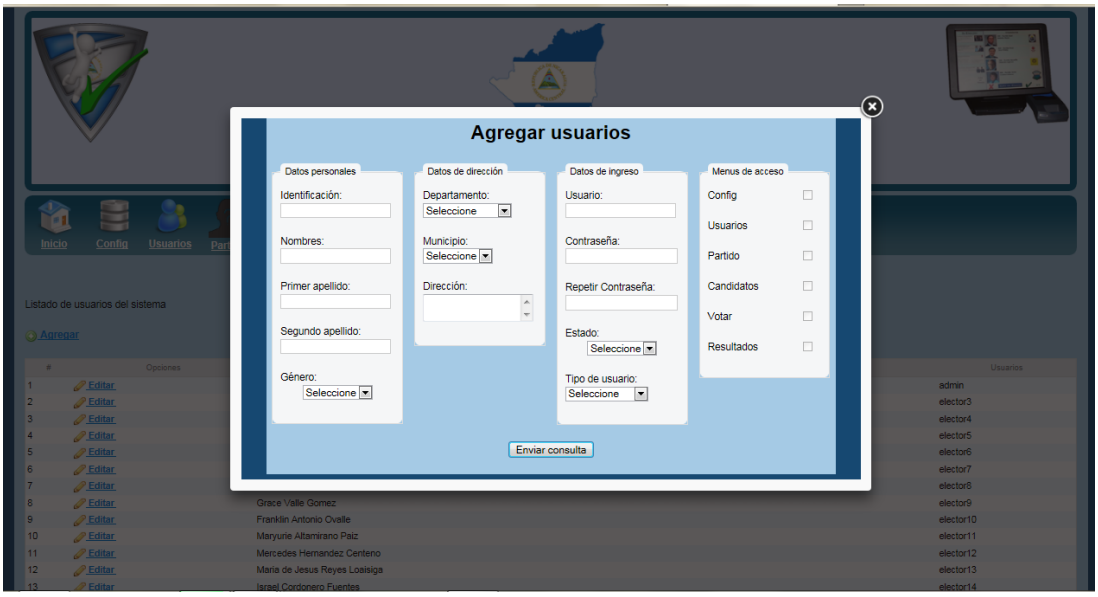
Aquí apreciamos las opciones de menú habilitadas para el administrador exclusivamente:



Claramente la opción de votación está inhabilitada para el administrador del sistema, y el alta del administrador se realiza internamente en la base de datos, así mismo la de los candidatos por partidos políticos.

A continuación mostraremos como editar, y agregar usuarios (o personas con edad hábil de votación). Dejamos en claro que quien administre el sistema debe ser funcionario del Registro civil y que solo se ingresan datos que se asumen por defecto (edad de 16 años por ejemplo) para registrarse, lo que no quiere decir que deje de tener derechos per se.

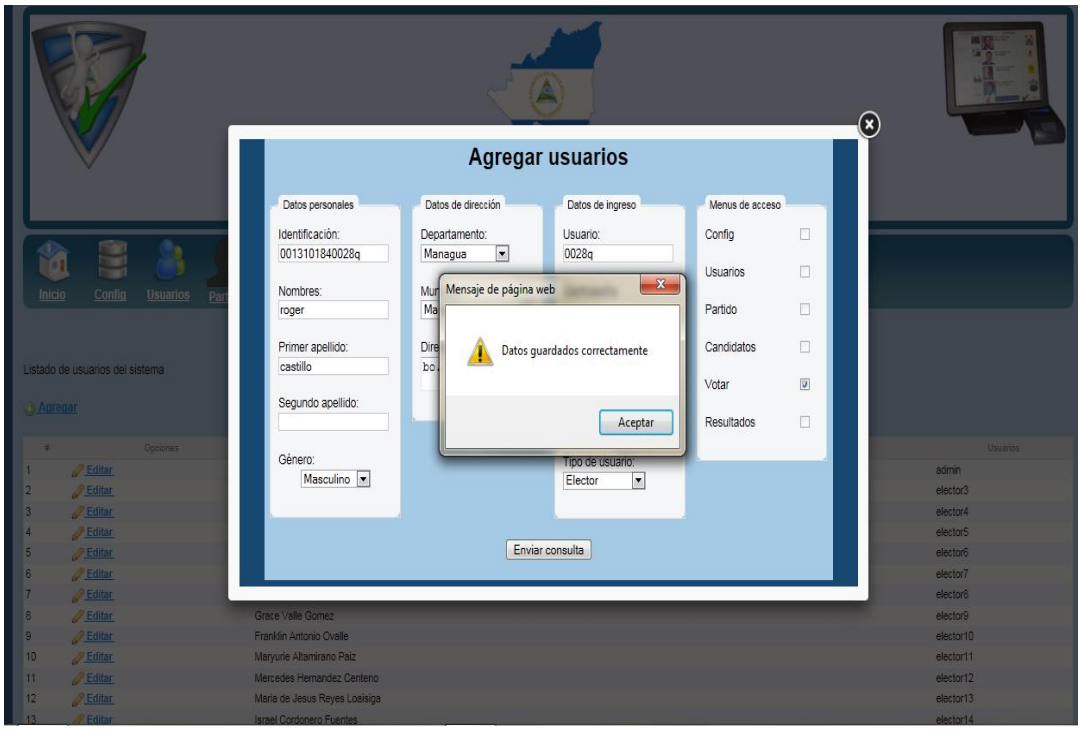
Para agregar a un usuario se presiona o “realiza click“ en la opción “Agregar” del menú usuario, visualizara la siguiente ventana:



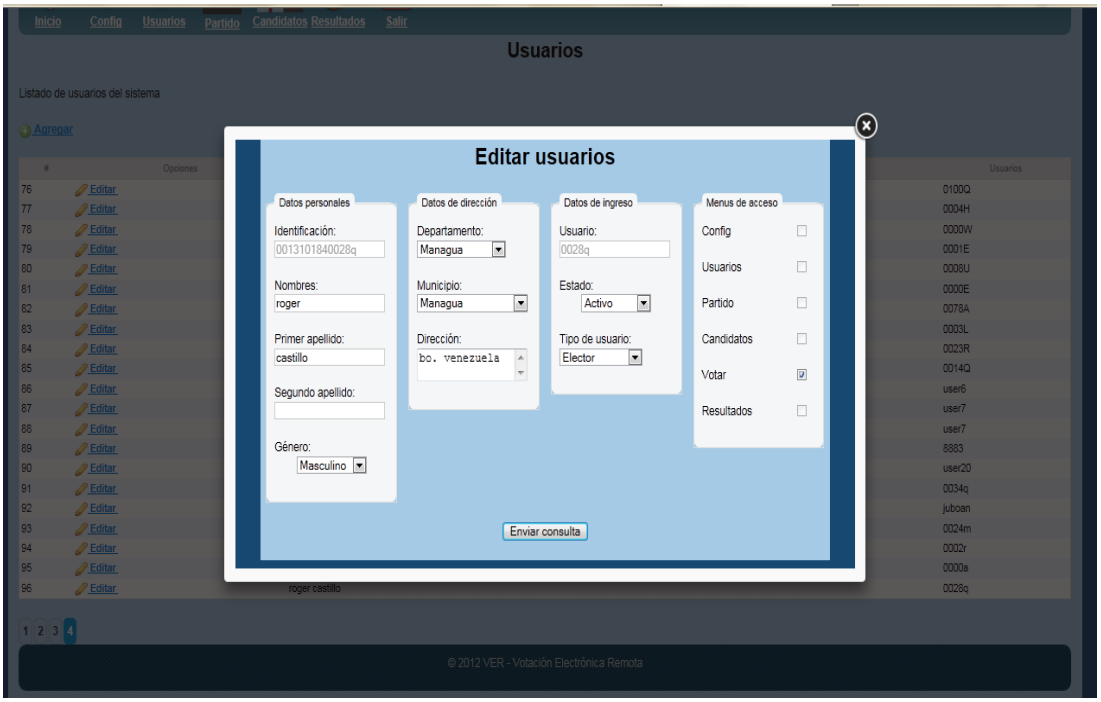
En ella puede agregar DNI, y datos personales, usuario y contraseña, en tipo de usuario debe asignarse las opciones de administrador, elector y candidato, automáticamente se habilita en el caso del elector la opción de “Votar”, ya que es la única función del votante.

En la siguiente estamos ingresando usuario nuevo en el sistema.

Una vez que todos los datos han sido llenados, excepto el segundo apellido pues puede ser que solo contiene un apellido, presionamos en el botón enviar, el cual seguidamente mostrará el siguiente mensaje.



Si clickea en la opción de “editar”, que aparece junto al nombre del usuario, aparecerá una ventana como la siguiente (ya habíamos mencionado que solo se pueden cambiar direccion, nombre en caso de que este incorrectamente escrito.



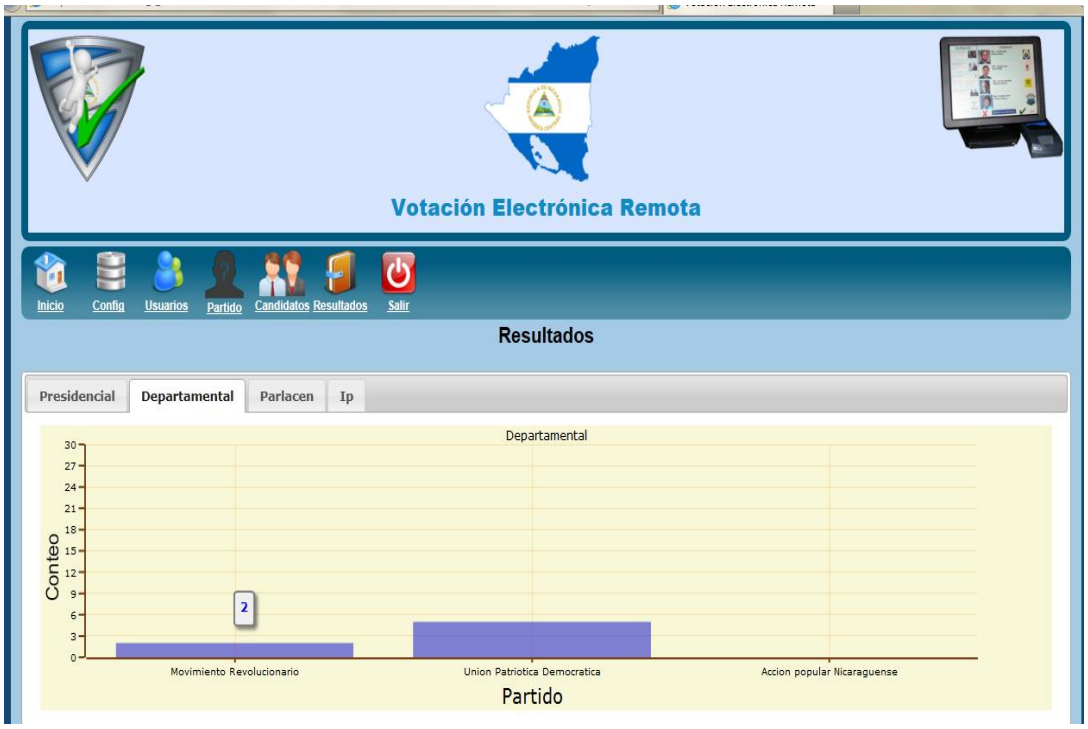
Posteriormente pasamos al módulo de “Partidos”, en ésta pestaña solo podemos visualizar los nombre de los candidatos, y el logo de los partidos políticos, como se mencionó anteriormente son asignaciones internas realizadas por funcionarios de CSE.

En ella visualiza los nombres de los candidatos inscritos en este caso en las elecciones Presidenciales, diputados departamentales, diputados al PARLACEN.

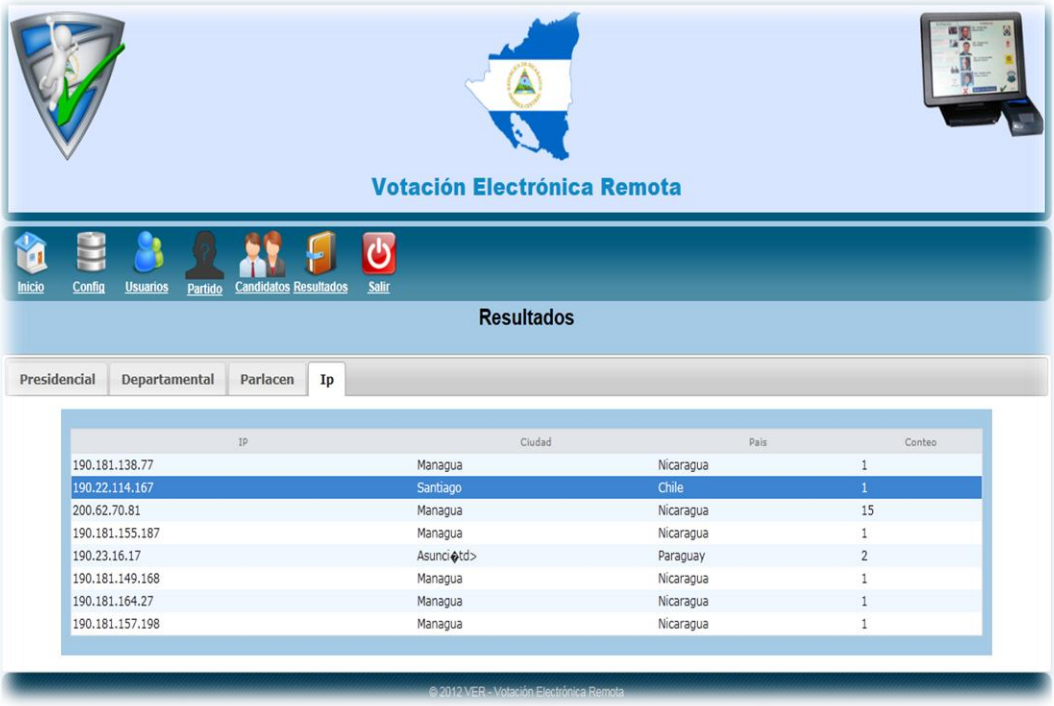
Hablemos de resultados. Tiene acceso a estos el administrador del sitio y los candidatos, esto conduce a mayor transparencia de las elecciones; y se muestran tal como se muestra a continuación, se pueden visualizar por Candidatura Presidencial, Departamental, PARLACEN y aquellos conteos de ciudadanos que realicen su voto desde el exterior.

Aquí se ven los resultados por Presidencial

En la siguiente pantalla se muestra los resultados por Departamentales:



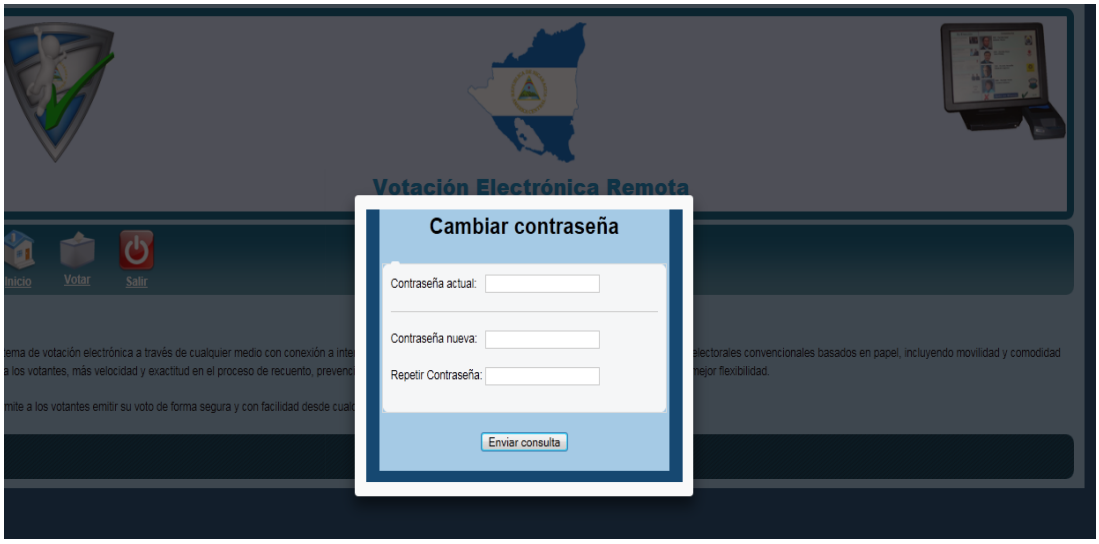
Presentación por votación de ip, en caso de nicaragüense con residencia en el exterior.


Votación Electrónica Remota
Inicio
Config
Usuarios
Partido
Candidatos
Resultados
Salir
Resultados
Presidencial
Departamental
Parlacen
Ip
IP
Ciudad
Pais
Conteo
190.181.138.77 Managua Nicaragua 1
190.22.114.167 Santiago Chile 1
200.62.70.81 Managua Nicaragua 15
190.181.155.187 Managua Nicaragua 1
190.23.16.17 Asunci&#65533;td> Paraguay 2
190.181.149.168 Managua Nicaragua 1
190.181.164.27 Managua Nicaragua 1
190.181.157.198 Managua Nicaragua 1
© 2012 VER - Votación Electrónica Remota

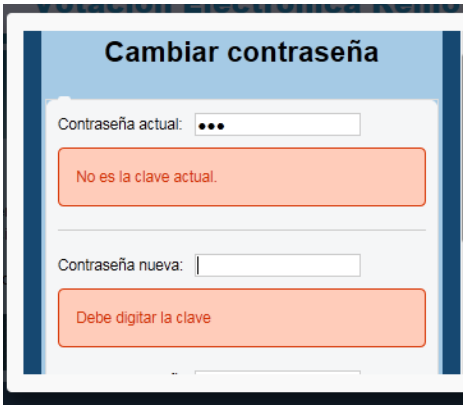
Manual de usuario

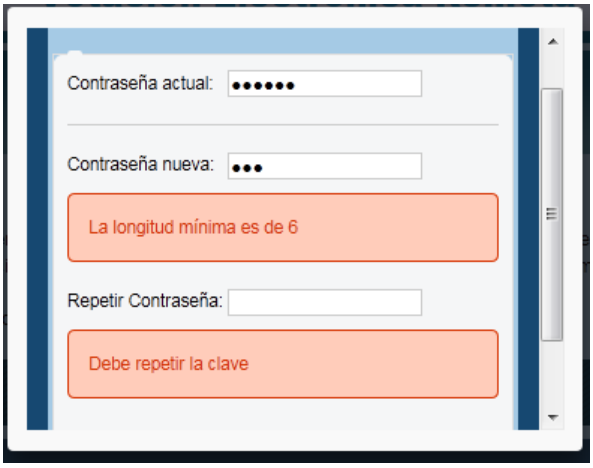
Una vez que el usuario se encuentra dado de alta en el sistema, y obtiene sus accesos mediante CSE en una previa verificación antes de las elección; de la misma manera se les indicará que deberá cambiar sus datos antes de las mismas (elecciones) para evitar que colapse el sitio.

Así cuando ingrese sus datos, continuamente se le presentará una imagen como se aprecia en la siguiente pantalla donde es obligatorio cambiar información para poder ingresar al panel de votación, y ejercer su derecho al sufragio.

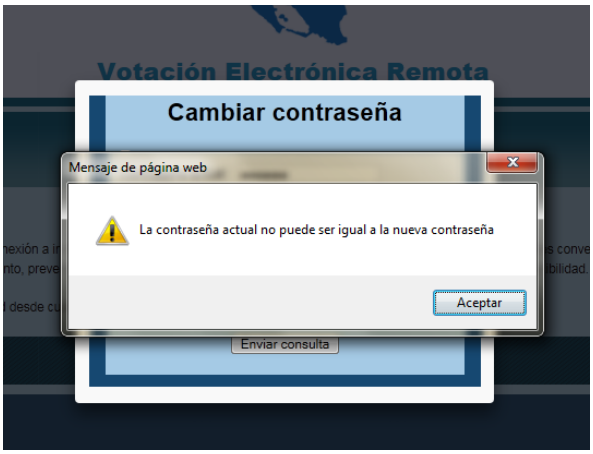


En la siguiente pantalla se valida el cambio de contraseña y que contenga un mínimo de seis caracteres.

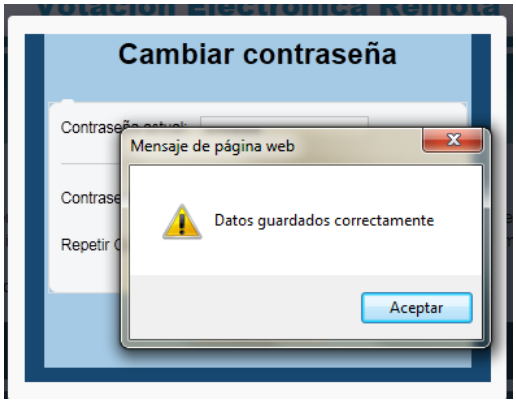




Una vez que ha cambiado sus accesos muestra el siguiente mensaje, si la contraseña es incorrecta.



O bien si ingreso correctamente le dirá:



Y seguidamente tiene acceso al menú de votación, para visualizar las boletas de votaciones debe “clickear” sobre “Votar”, y aparecerán en el orden contenido.

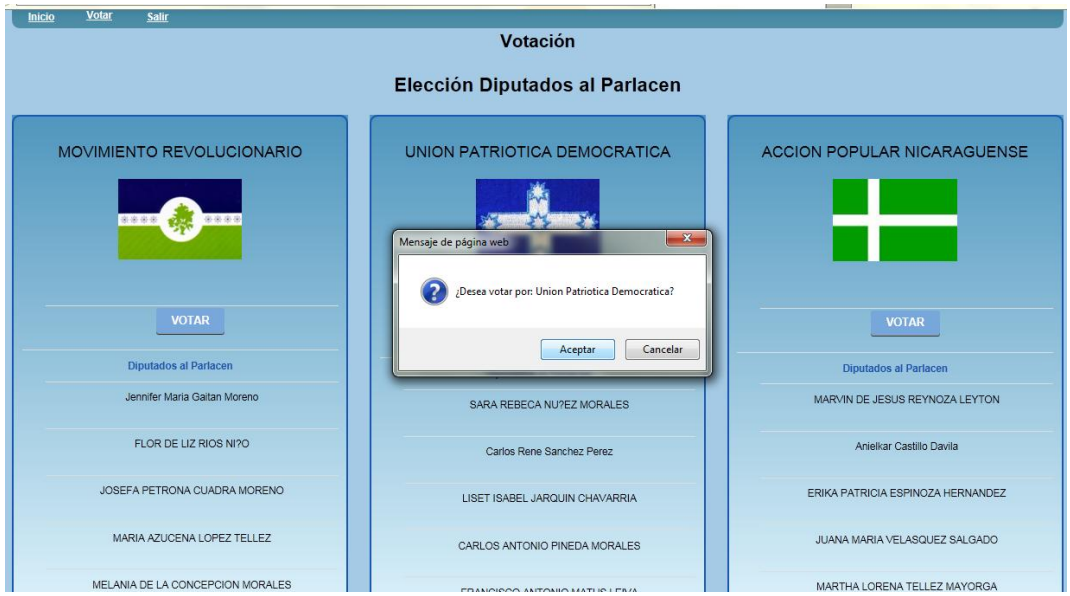
Primero la Elección Presidencial:

Luego que presione “votar” le muestra el siguiente mensaje donde puede cancelar y elegir otro candidato, o bien presionar “Aceptar”, si es así debe visualizar la pantalla de elecciones “departamentales”

Pantalla de elecciones departamentales:

Si presiona aceptar visualizará las elecciones al PARLACEN :

Y si nuevamente “Acepta”



Y finalmente, presenta un mensaje que dice “su voto ha sido agregado”