VNIVERSIDAD NACIONAL
AVFNOMA DE
MEXICO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

"COMPARACIÓN ENTRE ESQUEMAS DE SEGURIDAD: PROGRAMA PREP Y PROPUESTA DE RECOPILACIÓN DE DATOS ELECTORALES DE URNA ELECTRÓNICA DEL IEDF"

T E S I S

QUE PARA OBTENER EL GRADO DE:

MAESTRO EN INGEIERÍA (COMPUTACIÓN)

P R E S E N T A:

JESÚS HERNÁNDEZ CABRERA

DIRECTOR DE TESIS: DR. ENRIQUE DALTABUIT GODAS

México, D.F. 2005.

Dedicatoria

A mis padres...

por ser el sol del amanecer

y mi luna entre las estrellas

Agradecimientos

Doy gracias a dios por permitirme llegar a este momento... dar otro paso más en mi vida.

A mis padres gracias y de nuevo esta tesis es un logro de ustedes.

A mis hermanos, hermanas, cuñados y sobrinos que me dan aliento para seguir superándome.

Especialmente al Doctor Enrique Daltabuit Godas por el tiempo y dedicación que amablemente tubo hacia mi persona.

A mi amigo, M. en C. Marcelo Pérez Medel por apoyarme y guiarme desde que era mi profesor.

A mis amigos, que gracias a dios son muchos y sobre todo a aquellos que han estado cerca de mi en los momentos más difíciles.

A la Universidad Nacional Autónoma de México y profesores de la Facultad de Estudios Superiores Aragón.

A todos, muchas gracias.

Índice

Índice de Figuras

Capítulo 1

Capítulo 2

Capítulo 3

Introducción

En el mes de junio de 2004, el Instituto Electoral del Distrito Federal (IEDF), realizó una invitación a diferentes instituciones educativas a colaborar en el diseño y construcción de una urna electrónica para agilizar las actividades de una jornada electoral.
Dicho proyecto consta de diferentes etapas, dentro de las cuales estuvieron:

1. El diseño y construcción de un prototipo funcional.
2. La construcción de 60 urnas para pruebas piloto.

El Laboratorio de Cómputo del Centro Tecnológico Aragón, perteneciente a la Escuela Nacional de Estudios Profesionales Aragón de la UNAM, aceptó a participar activamente con un grupo de trabajo, en particular en la etapa de "Diseño y construcción del prototipo funcional", grupo en el cual fungí como líder de proyecto.

Las características técnicas a satisfacer fueron establecidas por el instituto electoral, éstas estaban centradas en: la seguridad, la transparencia y la agilización de las actividades relacionadas con una elección electoral. Las características fueron cubiertas satisfactoriamente por parte del Laboratorio de Cómputo, haciendo uso de las tecnologías existentes, dando como resultado una buena propuesta de urna electrónica que, posteriormente, serviría como base para determinar las características más relevantes e integrarlas al diseño final.
Dentro de las características más relevantes en la solución propuesta por el grupo esta la utilización al 100% de software libre: en el programa de urna electrónica para la etapa

de votación [8], en la implementación del sistema operativo Linux como base para el funcionamiento del programa de votación, así como la programación con bibliotecas graficas GTK+[1] y el uso de lenguaje C estándar, además de la implementación de GnuPG[2] para establecer un esquema de seguridad de los datos electorales.

La importancia de la seguridad en el envió de los resultados electorales nos hace que exista una especial atención en salvaguardar la integridad, confiabilidad y confidencialidad de los mismos, lo cual nos conlleva a analizar proyectos relacionados con el acopio de información electoral: El más importante de estos proyectos es el Programa de Resultados Electorales Preliminares (PREP) que es el resultado de varios comicios electorales a nivel nacional, la experiencia acumulada desde las elecciones federales de 1994 (Año de su primera implementación), hasta las elecciones federales de 2003, han demostrado su mejoría, tanto en tiempos como en confiabilidad.

Objetivos

Los objetivos de esta tesis son:

- exponer y analizar las características en cuanto a la confidencialidad e integridad de la información, así como los aspectos relacionados a los esquemas de recopilación de datos del PREP y el prototipo de Urna Electrónica para posteriormente, hacer un análisis comparativo entre los dos esquemas.

- Determinar mejoras en cada uno de los proyectos, principalmente, en el proyecto de Urna Electrónica.

- Analizar la viabilidad del proyecto de Urna Electrónica comparándolo con el proyecto PREP, haciendo énfasis en la diferencia de escenarios de implementación.

[1] Proyecto Gimp Tool Kit, bibliotecas graficas para desarrollo de aplicaciones con interfaces gráficas en el sistema operativo Linux. http://www.gtk.org/

[2] Implementación libre de PGP (Pretty God Privacy) programa para intercambio seguro de información que utiliza criptografía asimétrica http://www.gnu.org

Organización de la tesis

En el primer capítulo se establece el escenario y se definen los datos electorales relacionados con ambos proyectos, así como un análisis de datos sociodemográficos que adquieren relevancia en el esquema de acopio de información planteada por cada uno de estos proyectos.

En el segundo capítulo se hace un análisis de la implementación de seguridad en el PREP para el acopio de información, tanto en seguridad lógica y física.

En el capítulo tres realizamos una descripción más detallada del proyecto de urna electrónica y la implementación de la seguridad en el mismo.

En el capítulo cuatro hacemos el análisis comparativo de ambas soluciones para determinar los puntos fuertes y débiles en ambos esquemas de seguridad; de este análisis se busca complementar ambos proyectos, si es el caso.

Finalmente se exponen los resultados del análisis comparativo, las conclusiones y el trabajo futuro del presente proyecto.

Capítulo 1

Características de los datos electorales y análisis de la problemática de acopio de datos electorales electrónicos.

La seguridad informática en los procesos electorales en México, se ha convertido en una necesidad ineludible para garantizar la confianza en los comicios. Se tiene como experiencia lo ocurrido el 6 de Julio de 1988, cuando a unas horas de haberse iniciado el sistema de información que hacia público los resultados parciales, sin ninguna explicación oficial el sistema encargado dejó de funcionar, sólo se mencionaba que el sistema de acopio de los resultados "se había caído". Este incidente generó gran desconfianza en la ciudadanía, ya que se proclamó un triunfo sin tener el conteo final de las urnas electorales.

Esta experiencia, dio como resultado una reforma a la Constitución Política de los Estados Unidos Mexicanos que en agosto del siguiente año se reflejo en la creación del Instituto Federal Electoral cuyos principales objetivos han sido: erradicar la ilegitimidad, la duda ciudadana, desconfianza y sospecha que rodeaba los procesos electorales.

Ya en 1991, se iniciaron proyectos para dar certeza y confiabilidad a los procesos electorales. Algunos de los puntos a atacar por el IFE, fueron: las proclamaciones de triunfo adelantadas sin tener información oficial y objetiva de los resultados. Para ello se creó un primer sistema de información denominado: Sistema de Información de los Resultados Preliminares Electorales (SIRE). Este sistema tenía como actividades

principales: el acopio de información electoral en los consejos Distritales correspondientes, su transmisión segura al IFE, integración y procesamiento de dicha información y, finalmente, la emisión pública de los resultados. Fue utilizado el 18 de agosto de 1991 en las elecciones de la Cámara de Diputados, la mitad de la cámara de senadores y la Asamblea de Representantes del Distrito Federal. Aunque al principio el sistema funcionó bien, al cierre de las votaciones y entrega de los paquetes electorales para su procesamiento, la información fluyó lentamente, tanto que a las 4:25 horas del 19 de agosto, sólo se tenía procesada el 2.8% de la votación y no es si no hasta el martes 20 a la 20:30 horas, cuando se dá por terminado el acopio de los datos electorales; la difusión oportuna de los resultados electorales no se dio. Dada esta primera experiencia, el IFE tomó la decisión de mejorar este sistema y surgió el Programa de Resultados Electorales Preliminares (PREP) cuyo análisis para su construcción comenzó en 1994.

Los objetivos principales de este nuevo sistema son: captar, transmitir y difundir electrónicamente los resultados electorales, conforme estos datos llegaban a las sedes de los distritos electorales y lograr la captura del mayor porcentaje posible en un tiempo razonable. El funcionamiento del PREP se expone en el capítulo 2, el cual tiene como base los datos de la primera copia del acta de escrutinio elaborada por los funcionarios de casilla; para entender los datos relacionados con estos proyectos es necesario hacer un resumen del sistema de votación en México, en el cual el sistema PREP es ya una parte fundamental en elecciones federales.

1.1 Sistema de votación en México

1.1.1 Logística y metodología

A grandes rasgos se listan a continuación antecedentes específicos relacionados con los dos sistemas a analizar en esta tesis, datos relacionados con el PREP y Urna Electrónica:

Tipos de casilla

Según la Constitución Electoral se deben dividir las casillas en básica y contiguas, tomando los siguientes criterios.

- *Sección electoral*: Es la fracción territorial de los distritos electorales para la inscripción de los ciudadanos en el Padrón Electoral y en las listas nominales de electores. Por cada sección debe haber un número de 50 electores como mínimo y 1500 como máximo.
- *Casilla básica*: Es aquella que se instala para sufragar en cada sección electoral, en el caso de que la sección electoral sea mayor a 750 electores la casilla básica contendrá la lista nominal de los 750 primeros votantes.

- *Casilla contigua*: Si el número de electores es mayor a 750 se divide la lista nominal entre este número y existirán tantas casillas contiguas como resulten de la división incluida la básica.

- *Casilla extraordinaria*: Se instala una casilla extraordinaria cuando las condiciones geográficas de una sección dificultan que todos los electores de ésta puedan trasladarse a un mismo sitio, se podrá acordar la instalación de este tipo de casillas en lugares de fácil acceso para los electores.

- *Casilla especial*: Se instalan para recibir los votos de los electores que temporalmente se encuentran fuera de la sección que corresponde a su domicilio.

Contar con la lógica de división de casillas electorales es importante en los sistemas informáticos utilizados para agilizar los procesos electorales, debido a que estos datos son muy útiles al hacer validaciones, se crea un catálogo en la base de datos correspondiente y controla el avance de acopio de resultados electorales.

Funcionarios de casilla

Cada una de las casillas deberá estar conformada por siete ciudadanos que fungirán

como: Presidente, secretario, escrutador y segundo escrutador, y tres suplentes en caso de que alguno de los propietarios no pueda ejercer su puesto por alguna circunstancia. Sus funciones son:

Antes del día de la votación: Capacitarse para desempeñar correctamente sus responsabilidades, en el caso de la urna electrónica, la capacitación será con detalles más técnicos y requerirá que los presidentes de casilla cuenten con cierto conocimiento en el manejo de computadoras a nivel básico, aunque un experto sería mejor.

El día de la votación: Instalar y clausurar la casilla, en el caso de la urna electrónica deberá conocer el procedimiento de armado de la urna electrónica y encendido de la misma, el diseño propuesto está pensado para que esta tarea sea sencilla y además automatiza el llenado de actas de apertura porque automáticamente imprime dichas actas.

Permanecer en la casilla: Desde su instalación hasta su clausura, la apertura de la casilla es idealmente a las 8:00 am y el cierre es a las 6:00 pm, en caso de que se requiera se puede prorrogar el cierre; la descicion es tomada por el presidente de casilla, consultando a los funcionarios de casilla.

Recibir la votación: el presidente debe recibir y cotejar la identificación de los ciudadanos para permitirle el sufragio, en caso de cumplir con los requisitos que manda la Constitución.

Efectuar el escrutinio y cómputo: De manera manual y a la vista de los observadores, los funcionarios de casilla deberán hacer las siguientes tareas de escrutinio y cómputo:

- Efectuar el conteo de electores que votaron en dicha casilla.
- Efectuar el conteo de las boletas sobrantes de cada elección.
- Efectuar el conteo del sentido del voto para cada uno de los partidos políticos o candidatos de todas las elecciones.

[3] Las credenciales actuales cuentan con un código de barras bidimensional, las credenciales anteriores unidimensional, pero por medio de programación es posible obtener el código unidimensional.a partir del bidimensional

- Detectar los votos que se consideran como nulos y contarlos para registrarlos en las actas de escrutinio y cómputo.

En el método tradicional utilizado por el PREP se utiliza la primera acta de escrutinio que se muestra en la figura 1.1; como podemos ver esta acta es llenada a mano por el secretario de la casilla, lo que puede llevar a cometer errores en el llenado; o simplemente no ser legible para los capturistas en el caso del sistema PREP. Este inconveniente puede llevar a inconsistencias que se detectaron y se les dieron un tratamiento especial en el sistema PREP: dado que no podían ser desechados se capturaron y se marcaron como datos inconsistentes, posteriormente, podrían rescatarse las inconsistencias yéndose al respaldo físico de los resultados electorales. Dentro de estas inconsistencias detectadas están:

- La sección especificada en el acta no corresponde con la registrada en la base de datos o no existe.
- El estado precisado en el acta no existe en la base de datos.

El tipo de casilla especificado en la acta no existe en el catálogo de tipos de casilla.

- No concuerdan el número de boletas extraídas y el número de votos precisados en el acta.
- El número de boletas extraídas supera en número a las que aparecen en la lista nominal.

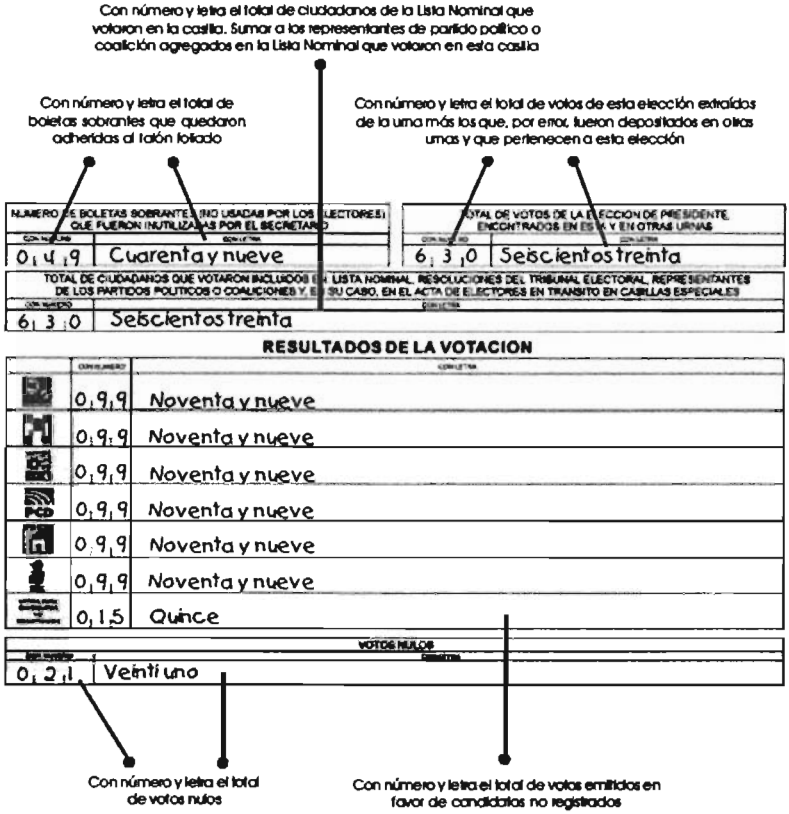

Figura 1.1. Acta de escrutinio y cómputo.

- Diferencia en la suma de los votos por partido o candidatos y el número de ciudadanos que votaron o diferentes al número de boleas extraídas de la urna.
- En los casos en que las letras no eran legibles, simplemente, se permitía ingresar los datos y se sustituía por un signo de "#", ya que no se puede poner un número al azar, pero tampoco se puede dejar de capturar dicha casilla.

La figura 1.2 nos muestra el avance de casillas capturadas a lo largo de las 20 horas que se tomaron para la elección de 1997 y el historial en registro de estas inconsistencias. En la grafica se observa, en el eje horizontal las horas desde las 18:00 del día de la elección, hasta las 16:00 horas del día 7 de julio; en el eje vertical se presenta el porcentaje total de casillas capturadas. Se muestran dos curvas: una curva

representa el porcentaje de avance de casillas capturadas sin problemas de inconsistencia y la segunda manifiesta la suma del porcentaje de casillas capturadas de la primera curva más las inconsistencias; las cuales representaron un 9.88 % de las actas totales que se recibieron.

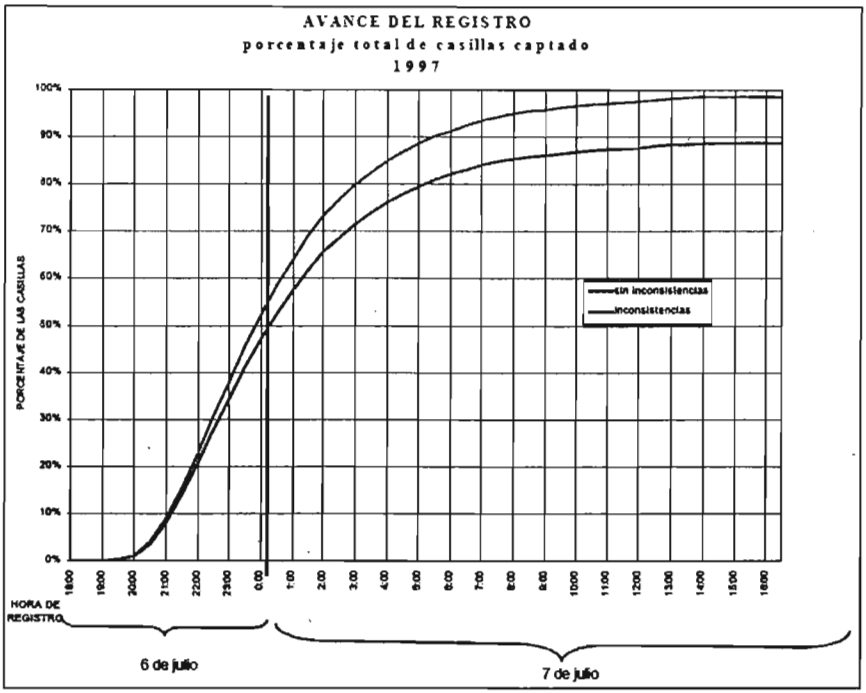

Figura 1.2 Gráfica de avances de acopio de resultados y porcentaje de inconsistencias [1]
(Original a color)

En la propuesta de urna electrónica, además de agilizar el tiempo de acopio de resultados electorales, se busca disminuir errores humanos al automatizar el proceso electoral lo más posible. Como ejemplo, tomemos los datos anteriores, el proceso de escrutinio y cómputo de datos electorales se hará de manera automática, tomando en cuenta medidas de seguridad necesarias (se exponen en el capítulo 3) y con la facilidad de auditar la votación, para que no exista ninguna duda en los resultados electorales.

1.1.2 Método tradicional de conteo de resultados electorales.

Es importante analizar los métodos de escrutinio y cómputo de los votos, debido a que ello nos da una idea clara de cómo se pueden llegar a cometer errores involuntarios por parte de los funcionarios de casilla.

El procedimiento tradicional para contabilizar los votos es el siguiente, nótese la cantidad de tareas a realizar para llenar las respectivas actas:

1. El primer escrutador contará de la lista nominal el número de ciudadanos que votaron.
2. El secretario deberá inutilizar las boletas sobrantes con dos rayas diagonales.
3. Se vacía la urna y el segundo escrutador contará las boletas extraídas.
4. Los escrutadores separan y cuentan los votos válidos, apartan los votos nulos y los votos a candidatos no registrados.
5. Se separan las boletas agrupadas por votos a partidos políticos, nulos y candidatos no registrados.
6. El secretario llena el acta de escrutinio y cómputo.

Se repiten estos pasos tantas veces como tipo de elecciones hubo.

Envío de información.

Una vez que los funcionarios de casilla llenen las actas correspondientes, se procede a armar el paquete electoral que se va a entregar en la junta distrital correspondiente. El punto más importante para el envío de la información en el sistema PREP, es la integración del sobre PREP, que consta de un sobre translúcido con la primera de las tres copias de las actas de escrutinio y cómputo (figura 1.1), sólo se debe tener cuidado de introducirlo, de tal manera, que los datos sean legibles sin necesidad de extraer la acta del sobre.

Al introducir la primera copia de las actas de escrutinio y cómputo se debe sellar y se llenará la ceja del sobre que tiene un formulario como se muestra en la figura 1.3,

la cual sirve para identificar la casilla correspondiente.

Estos sobres deberán ser llevados a la junta distrital correspondiente, los cuales serán puestos en el buzón de recepción y el funcionario obtendrá como comprobante la ceja desprendible de datos del mismo sobre, una vez que el personal del Instituto la haya llenado.

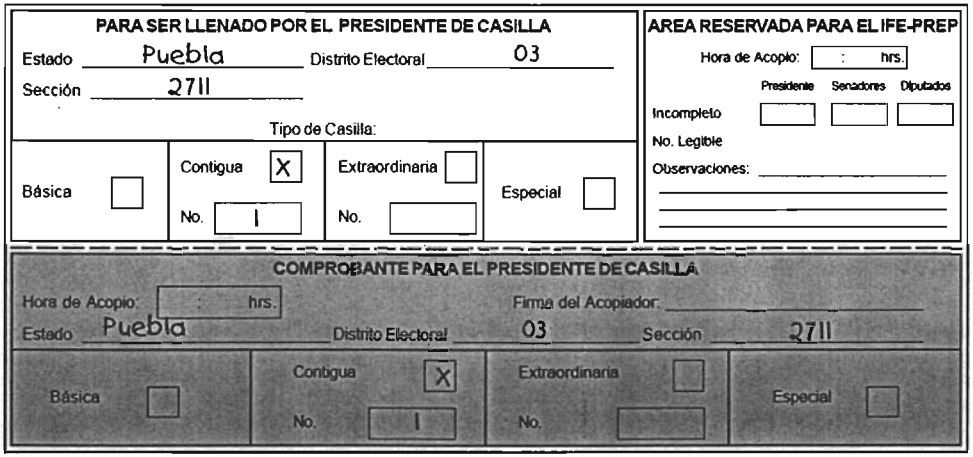

Figura 1.3 ceja de datos del sobre PREP.

El envío de la información se realizará a partir de la captura de los datos del sobre. El procedimiento de captura y procesamiento de esta información se trata con mayor detalle en el capítulo 2.

1.2 Análisis demográfico.

Es necesario hacer un análisis de las características demográficas en donde se desempeñan los dos sistemas que analizaremos en la presente tesis.

Los tres aspectos importantes son: servicios de electricidad, telecomunicaciones y comunicaciones terrestres.

En México, según estadísticas del INEGI hasta Marzo de 2003, el 95.4 % de los hogares cuentan con electricidad, este dato nos da una idea de que no en todas las localidades es posible conectar una urna electrónica, por ejemplo, en Chiapas el

número de hogares sin electricidad es un 11.6 %. Se debe considerar este aspecto para el funcionamiento a nivel nacional. El proyecto de urna electrónica está enmarcado en el Distrito Federal, que aunque cuenta con un 98.3 % de hogares con electricidad, existen localidades en su periferia sin este servicio, por tal motivo fue necesario diseñar la urna electrónica para que fuera autónoma en cuanto a energía, el requerimiento mínimo de respaldo autónomo de energía es de 12 horas de duración de las pilas internas del prototipo, además de contar con circuitos de fuente conmutada para la carga de las pilas. Estas consideraciones se reflejan en el incremento de complejidad en el diseño de los proyectos de este tipo, lo que puede causar fallas o contingencias inesperadas.

Las telecomunicaciones son un aspecto crucial para el funcionamiento efectivo de ambos proyectos; nuevamente, la infraestructura en el estado de Chiapas no es la adecuada para las transmisiones. Tenemos que por cada 100 habitantes en Chiapas existen 4.7 líneas telefónicas. A nivel nacional se cuenta con 15.7 líneas. En el caso del Distrito Federal la densidad de este tipo de servicio es mejor, 39.5%, aunque no nos garantiza que en todas las localidades de la entidad, en donde se va a instalar una Urna Electrónica, va a existir un teléfono para lograr comunicaciones. En general, el porcentaje de hogares con teléfono es de 47.9 por ciento.

El trasporte de paquetes electorales en una comunidad rural o de datos electrónicos de la Urna Electrónica en una comunidad rural es una variable a tomar en cuenta para el análisis de ambos proyectos. Las diferencias son considerables entre las características sociodemográficas de los dos entornos en donde se lleva a cabo la aplicación, representan un impacto en la logística de ambos sistemas. En el caso de PREP aumenta el tiempo para tener un porcentaje de captura cercano al 100%, como lo podemos observar en la figura 1.2 en el cual las 7 primeras horas tienen avances significativos el acopio, después de esas primeras horas el avance disminuye,

principalmente, por este factor de acceso a los consejos Distritales. En el caso de la uma Electrónica del DF, es una entidad con buena infraestructura de comunicaciones, pero no está exenta de este tipo de contrariedades.

1.3 Características de los principales parámetros de seguridad.

Es importante proteger los resultados electorales debido a que al utilizar tecnología informática existe la posibilidad (si no se implementa un esquema de seguridad) de que los datos sean alterados y/o sustituidos.

Los parámetros de seguridad que deben cumplirse para contribuir a la confianza en las elecciones se listan a continuación:

- Establecer canales de comunicación seguras sin posibilidades de suplantación o que permitan su detección oportuna.
- La seguridad en el transporte de los datos desde el servidor de base de datos central a los diferentes centros o servidores de difusión.
- Verificar la integridad de la información antes de procesarla.
- La calidad del software es primordial en este tipo de sistemas.
- Hacer uso de algoritmos de cifrado probados.
- Autenticar las comunicaciones y registrar quién está transmitiendo y desde dónde.
- Autenticar las entidades que transmiten los archivos hacia el equipo integrador.
- Contar con una base de datos para controlar el avance de las transmisiones
- Contar con un catálogo de datos electorales e implementar mecanismos de detección de datos duplicados.
- Establecer políticas de seguridad y control de acceso a lugares sensibles a un sabotaje.
- Mantener disponibles los datos en todo momento y evitar ataques de denegación de servicios en la publicación de resultados.

Controlar el uso de Terminales de captura, o en su caso, al equipo integrador de datos y a dispositivos portátiles de almacenamiento.

Capítulo 2

Análisis de la solución dada por el Programa de Resultados Electorales Preliminares.

La seguridad en los procesos electorales en México se ha convertido en un elemento crucial para el éxito de las elecciones. En la presente tesis se analizará la seguridad del Programa de Resultados preliminares (PREP) que busca agilizar el acopio de resultados y el proyecto de Urna Electrónica que busca automatizar los procesos de las elecciones y acopio de información, ambos proyectos sin descuidar la seguridad de los datos electorales.

En este capítulo analizaremos el PREP de 2003 y sus elementos de seguridad implementados para su éxito, este programa ha probado su alta efectividad como a continuación se explica.

La infraestructura creada para este programa esta conformada por 300 Centros Distritales de Acopio y Transmisión de Datos (CEDAT), dos Centros Nacionales de Recepción de los Resultados Electorales Preliminares (CENARREP), uno en el IFE de Tlalpan y otro en el World Trade Center, con el fin de descentralizar información por cuestiones de seguridad.

La logística del funcionamiento del PREP consiste en la entrega por parte de cada uno de los funcionarios de casilla del sobre traslúcido, en el cual contiene una copia de las actas de escrutinio y cómputo de la jornada electoral. El CEDAT procesa los paquetes electorales llevando a cabo las siguientes actividades:

1. Recepción del sobre PREP por parte de los funcionarios del CEDAT y entrega de un recibo al funcionario de casilla.
2. Cada uno de los capturistas del CEDAT cuenta con una caja de entrada y una de salida; se reparten los sobres PREP uno por uno a la caja de entrada de los capturistas para ser procesadas.
3. Los datos de la casilla y de los votos por cada partido se capturan dos veces para corroborar la información. Terminada la captura se transmitía la información al CENARREP. Cabe mencionar que este procedimiento se repite dependiendo del número de elecciones, por cada elección habrá un sobre PREP.
4. En una terminal de impresión de cada CEDAT un elemento del personal, conocido como verificador, se encarga de acopiar los acuses de recibo de cada sobre. El orden de los acuses de recibo debía corresponder con el orden de las actas transmitidas, esta correspondencia será cotejada por el verificador.
5. Una vez cotejados los recibos. Se engrapan y si no había diferencias se apartaban para que un acopiador los llevara al archivo del CEDAT; en el caso de que hubiera discrepancias, se le anexaba una hoja de corrección con señalizaciones de los errores; posteriormente, se entregaba a un supervisor para que dé su autorización de baja de los datos correspondientes y se realizará la capturara nuevamente.
6. En cada distrito existía una computadora personal, con la cual los consejeros y representantes de partido podían cotejar que los datos transmitidos correspondían al resultado de cada casilla. De haber un error se notificaba al coordinador del CEDAT para su corrección.
7. Una vez que se concluye el proceso de captura, transmisión y verificación se le recoge a cada capturista su Terminal de Captura Remota (TCR) y se guarda en una caja identificada por el número de orden del capturista que la utilizó. Las TCR ya cerradas y firmadas se entregan por parte del coordinador del CEDAT al vocal ejecutivo del distrito en cuestión.

Debido a que el esquema antes mencionado, se basa en la transmisión de datos se debe, contar con la confianza que estos estén bien protegidos; para ello el esquema de seguridad se le atribuyó una gran importancia, debido a que su función primordial era brindar total protección al sistema contra cualquier boicot o posibles agresiones, así como prevenir algún tipo de contingencia que pudiera ocurrir [1]. Debían considerarse muchos aspectos, existía un temor generalizado por la posibilidad de atentados.

Los elementos que definieron la estrategia en la protección del PREP fueron:

1. Seguridad. Resistir ataques externos.
2. Confiabilidad. Capacidad para que el sistema cumpliera sus metas.
3. Credibilidad. Convencer de que el Programa se ejecutaba correctamente.
4. Transparencia. Claridad de todos los métodos y procedimientos.

La seguridad no estaría basada totalmente en el secreto; se tenía presente que habían demasiadas personas involucradas en la operación del Programa y mantener ocultos aspectos cruciales del sistema, obstaculizaría el buen desempeño e iría en contra del principio de transparencia. En la actualidad, no necesariamente las nuevas tecnologías garantizan la seguridad de manera absoluta, existen algunas que ya han sido probadas y que han resistido numerosos ataques sin fallar que podrían resultar más seguras. Es por esto que la tecnología de protección del PREP 2003 se sustentó, en gran medida, en los sistemas de cifrado conocidos ampliamente, así como en técnicas de detección de alteraciones en documentos electrónicos (algoritmos de resumen y firmas digitales) y principios de teoría de la probabilidad.

Con el fin de tener la mayor transparencia posible en este proceso electoral, los sistemas a través de los cuales operó el PREP 2003, fueron diseñados utilizando tecnología de cifrado y autenticación. Así, para generar la huella dactilar digital de cada acta se optó por basarse en algoritmos MD5 para autenticación y DES para cifrado, que son los más conocidos internacionalmente en lo que se refiere a la seguridad en el manejo de la información.

La integridad de los datos debía protegerse desde el momento en que entraran al sistema hasta que se difundieran. La amenaza principal era la alteración de los datos en el tránsito y almacenamiento; para cubrir este punto se usó la criptografía, tecnología muy bien conocida, es decir, el cifrado de los datos con algoritmos estándar y usando firmas digitales.

El método de cifrado más conocido y aceptado es el DES (Data Encryption Standar), desarrollado hace más de dos décadas. La manera en la que se usó el DES fue un triple cifrado, el mensaje se cifraba usando tres llaves. Cada una de las llaves usadas en el DES eran de 56 bits de longitud, generaba una longitud total de 168 bits, un nivel suficiente que garantizaba la seguridad requerida para interpretar los mensajes cifrados, con este método se requería probar todas las llaves posibles. Si la longitud de las llaves era lo suficientemente grande, el tiempo necesario para probarlas todas sería aún mayor, por lo tanto, para cuando se lograran descifrar ya habría pasado un lapso considerable.

2.1 Seguridad Física

No es posible una seguridad completa si no se cuenta con la seguridad física, es decir, resguardar además de controlar el acceso en áreas y computadoras sensibles a un ataque. La seguridad en el programa PREP de 2003, se guiaron con la siguiente misión y objetivos.

2.1.1 Misión y objetivos.

Proteger el sitio donde se llevó a cabo la programación de los diversos dispositivos de cómputo que lo integran para evitar la introducción de algún código malicioso por terceras partes.

Resguardar las claves criptográficas y de autenticación que se emplearon, desde el momento de su creación hasta y el momento de su distribución a los centros de acopio, para garantizar el dispositivo de autenticación de los dispositivos de cómputo.

custodiar el sitio donde se guarden los dispositivos de cómputo durante su preparación hasta su envió para evitar la introducción de código malicioso en los mismos.
Resguardar los dispositivos de cómputo y las claves que se usaron en los centros de acopio durante su envío o distribución y durante su permanencia en los centros de acopio para evitar la introducción de algún código malicioso en los mismos.
Garantizar la continuidad del servicio de la infraestructura en el centro de programación y en los centros de cómputo mientras se realiza la jornada electoral.

2.1.2 Políticas de seguridad.

Las políticas que se implementaron para el éxito del sistema son:

- Participo un oficial de seguridad quien fue el responsable de la implantación de los mecanismos que permitieron desarrollar las políticas.

- Se contó con dos repositorios fiables distintos para resguardar información protegida. Los repositorios tenían acceso en forma mancomunada el oficial de seguridad y el Coordinador General del PREP o la persona a quien este último designó por escrito.

- En la entrada de cada recinto existió un mecanismo de control de acceso que se fundamentó en dos autenticadores, uno biométrico y otro basado en algún conocimiento del individuo.

- Para acceder a las instalaciones del "CENARREP", el personal de seguridad de dichas instalaciones contó, por parte del PREP, con un oficio de autorización que indicaba el nombre de la persona, la fecha y hora en que se presentaba.

- Las identificaciones contaron con fotografía y un mecanismo que autorizaba el nivel de acceso que le correspondía al portador de la misma.

- Se llevaron bitácoras escritas y se almacenaron en sistemas de cómputo en forma removible. Estas bitácoras se resguardaron en repositorios fiables.

- Todos los sitios fueron revisados por el oficial de seguridad, con el apoyo de otros especialistas que se requirieron para identificar los posibles puntos de acceso aparentes o encubiertos, sellándose los que no disponían de sistemas de autenticación. El inventario de los posibles puntos de acceso y el acta que se levanté ante testigos fiables de la revisión y el sellado se resguardó en un repositorio.

- Todos los sistemas de verificación de identidad tenían habilitado un mecanismo de vigilancia de ingresos y egresos, impidiendo la entrada de alguien cuyo regreso no estuviese anotado e impediría la salida de las personas cuyo ingreso no estuviese anotado.

- Se mantuvo un inventario de dispositivos de cómputo y sus periféricos, así como de los usuarios autorizados a ingresar a cualquiera de los sitios. En este inventario se indicaba a qué recintos correspondía cada dispositivo y cada usuario. También contenía un autenticador para cada elemento del inventario. El inventario solo lo podía manipular el oficial de seguridad y debería hacerlo en forma segura. Este inventario se resguardaba en un repositorio.

- Las personas (visitantes, proveedores, etc.) que no fueron parte del personal del PREP, pero que debían acceder a sus instalaciones, fueron fotografiadas y su imagen junto con otros datos que se juzgaron pertinentes, se anotaron en una bitácora de visitantes. Se les expidió una credencial con temporalidad de tres horas que deberían portar en forma visible, y no podían recorrer las instalaciones sin estar acompañados por algún miembro del personal del PREP.

- Los visitantes usaron identificaciones diferentes en diseño y apariencia de aquellas designadas para el personal del PREP.

- Cualquier violación al sistema de control de acceso, fue reportada telefónicamente en el momento en que se detectó a las autoridades policiales e inmediatamente después se les entregó un reporte por escrito.

- Existió un procedimiento escrito donde se indicó cómo reaccionar ante una brecha del sistema de control de acceso

- El translado de dispositivos a los centros de acopio (CEDAT) se realizó por una vía distinta a la que se empleó para el envío de las claves criptográficas necesarias, las cuales se enviaron en el último instante posible. Los envíos se hicieron mediante empresas o sistemas fiables. Se construyó un inventario (lista de envío) de cada uno de los envíos y se guardaron en un repositorio

- Se levantó un acta ante testigos fiables de los envíos que se hicieron, y se recibieron en cada caso.

- El coordinador de centro de acopio (CEDAT) fue el responsable de la seguridad física de los dispositivos que recibieron, así como de las claves criptográficas que les llegaron y tomó las medidas que fueron posibles para resguardarlos.

- Estuvo estrictamente prohibido la introducción de mochilas, bolsas, cajas y/o portafolios a las instalaciones designadas como críticas o de alta sensibilidad.

- No se introdujeron ni se sustrajeron computadoras, medios de almacenamiento ópticos, magnéticos o combinación de estos de las instalaciones del "CENARREP", sin la autorización correspondiente.

- Todos los paquetes provenientes de servicios de mensajería estuvieron perfectamente sellados e indicaban los datos del remitente como el destinatario, fueron canalizados a través del Enlace Administrativo del PREP.

- El contenido de paquetes, bolsas, portafolios, cajas y mochilas fueron revisados al ingresar y abandonar las instalaciones a fin de evitar la sustracción o introducción no autorizada de bienes.

- Las identificaciones, llaves y tarjetas de acceso quedaron bajo la supervisión y responsabilidad del designatario, así como el uso de las mismas, el cual fue el encargado de evitar las copias de dichos elementos. Se entregaron exclusivamente al designatario, quien firmó de recibido, aceptando la responsabilidad y condiciones de reposición.

- El acceso a cada oficina, sala de cómputo y área de trabajo que contenían información secreta o reservada para el PREP se restringió físicamente; y fue responsabilidad del usuario su resguardo.

2.2 Control de acceso

Se tomaron diversas medidas técnicas y administrativas para evitar el acceso de personal no autorizado. En ambos centros se instalaron retenes de control por parte de la Coordinación de Seguridad del IFE, que mantuvo guardias las 24 horas del día. Dos días antes y la noche previa a la jornada electoral se realizó una inspección con perros adiestrados para detectar explosivos.

En el CENARREP I se tomaron medidas tecnológicas adicionales: se instaló un sistema de apertura de puertas mediante código de identificación personal y tarjetas inteligentes; así como un sistema cerrado de televisión con un total de ocho cámaras, ubicadas en diferentes áreas del PREP 2003; un centro de control consistente en un multiplexor de 16 canales, un monitor de 12" y otro de 14" con dos videograbadoras para grabar en videocinta todo lo sucedido en áreas clave.

Se instalaron dos nuevos sistemas de detección: uno de movimiento y otro de humo para una protección perimetral del área del PREP 2003; el primero con un total de 13 detectores ubicados en las oficinas generales y en el interior del centro de cómputo; y el segundo con un total de 20 detectores de tecnología fotoeléctrica, 13 en el entorno de las oficinas, cinco en el centro de cómputo y dos en la sala de control anexa al mismo.

En el CENARREP II también se tomaron las medidas de control de acceso, mediante la instalación de un sistema de apertura de puertas, utilizando un código de identificación personal y tarjetas inteligentes.

De acuerdo al nivel de seguridad, cada credencial incluyó los siguientes datos: área de adscripción, nombre completo, cargo o función y, en esta ocasión, no se utilizaron colores distintivos debido al efectivo control de acceso. Para accesar a determinadas áreas fueron programadas las tarjetas con nivel 1 y nivel 2. Se entregaron personalmente y los portadores firmaron una responsiva, además de que se les informó sobre las restricciones, reglamentos y uso de la credencial.

La tarjeta de seguridad con nivel 1 permitía el acceso a el área de las oficinas generales y el CENARREP.
La tarjeta de seguridad con nivel 2 sólo permitía el acceso a las oficinas generales del PREP 2003.

Otra acción para la seguridad fue la elaboración de listas con fotografía acordes a la base de datos de las credenciales, el propósito era mantener el registro de las entradas y salidas de todo el personal. Estas listas fueron entregadas a la Coordinación de Seguridad del IFE, la cual mantuvo guardias para el resguardo de las oficinas generales del PREP 2003, de los CENARREP y del sótano, espacio en el que se almacenaba todo el equipo y materiales que utilizarían los 300 CEDAT del país.

Por otro lado, la Dirección de Comunicación Social del IFE otorgó acreditaciones al personal (gafete con fotografía) para su acceso a las salas de prensa durante la jornada electoral.

2.3 Esquema de generación de claves criptográficas

Para aplicar el cifrado y la generación de firmas electrónicas se debían producir un número de llaves suficientes; se realizo el cálculo de las que se requerían para el DES, el cual trabaja con llaves de 8 bytes. Pero cada una de las llaves utilizadas eran de 56 bits, debido a la forma en que funciona su algoritmo utilizado en las aplicaciones, éstas requerían que las llaves fueran de una longitud de 64 bits, por esta razón los 56 bytes se acomodaron en 8 bytes, usando los 7 bits más significativos de cada byte.

El proceso de captura remota de resultados es susceptible a que algunas personas pretendan alterar los resultados, para evitar eso se implementó una serie de medidas de seguridad que, consiste en la autenticación rigurosa basada en un sistema de "Llaves" garantizando, así que la alta, baja, captura y transmisión fueran una operación valida y reconocida por el sistema.

La generación de los códigos de seguridad para cada una de las llaves se llevó a cabo utilizando un dispositivo generador de "Ruido Blanco", este aparato aprovecha el comportamiento de ciertos fenómenos físicos para la generación de números aleatorios, fue diseñado por personal perteneciente al Instituto de física de la Universidad Nacional Autónoma de México (UNAM), el dispositivo es externo al computador y fue conectado a uno de los puertos, arrojó como resultado la serie de llaves. Cabe mencionar, que se contó con la participación de la Universidad Anahuac del Norte, pues contaban con la experiencia en la creación del generador de llaves para el PREP de 1997.

Este proceso de generación de "Ruido Blanco" nos garantiza que cada una de las llaves es independiente de todas las demás, es decir, que ninguna llave pueda ser generada a partir de ninguna otra, utilizando algún conjunto de ellas.

Las llaves fueron sometidas a "Pruebas de Aleatoriedad" que consistieron en "pruebas estadísticas para considerar números aleatorios independientes con distribución uniforme", obteniendo como resultado la absoluta aprobación de la aleatoriedad de las llaves.

Esos códigos fueron impresos en la cinta magnética de cada tarjeta mediante un proceso de impresión utilizando dispositivos "Card Printer Ultragrafixs", este proceso plasmó, a su vez, en la misma tarjeta, el rol de que se trataba, entiéndase: Coordinador, Supervisor o Capturista.

Así mismo, el Requerimiento de llaves para las tarjetas, se consideraron: 300 llaves de coordinador, 300 de supervisor y 2,347 para capturistas, multiplicado por dos debido a que se generaron llaves para pruebas nacionales y para el día de la jornada electoral. Esto es: (300X2) + (300X2) + (2347X2) = 5,894

2.4 Manejo de claves criptográficas

- Se usan tarjetas de clave de capturista, supervisor y computadora controladora de entrenamiento y pruebas, éstas se desechan antes de la elección. Es importante marcar externamente las tarjetas donde estará indicado que no se deben de usar en la elección y ponerles algún identificador interno, donde se asiente que son de entrenamiento y prueba para que sean rechazadas en el momento de la elección. Esta identificación puede hacerse a través del número de serie

- Cada computadora de captura, controladora y tarjeta de supervisor, de capturista o de controladora tendrá un número de serie que provea una identificación única.

Se cargan las tarjetas de supervisión, captura y computadora controladora en un cuarto seguro, conectando el grabador de tarjetas a una computadora personal, se ejecuta un

programa que lea la clave correspondiente de la secuencia fundamental de bits aleatorios.

- Se colocan las tarjetas en sobres cerrados y firmados.
- Se almacenan las tarjetas en un cuarto seguro (o caja fuerte) hasta que sean enviadas a los centros de acopio para su uso electoral.
- Se creará una base de datos en las computadoras de conteo que contenga las ternas de claves que corresponden a cada computadora de captura, a su capturista y al supervisor correspondiente. Las ternas se arman en el momento de inicializar los equipos en los CEDAT y se avisa al CENAREP qué terna le toca a cada quién.

2.4.1 Distribución de claves criptográficas

- Las claves se hacen llegar a las computadoras de los centros de acopio de resultados electorales, deben estar disponibles en las computadoras de conteo para que sea posible autenticar la información que se transmita a través de líneas inseguras. Es conveniente que las computadoras de conteo contengan una tabla con el archivo de claves.

- Para propósitos de control, cada clave quedara en su salida identificada por el número del renglón que tenga en el archivo, considerando que todas las claves son de una longitud de 56 bits. Esta identificación se traducirá a un número de serie de cada clave.

Características

Estadísticas de las llaves fueron, las siguientes:

a) Su aleatoriedad debía ser uniforme, es decir, que todos los rangos de llaves tuvieran la misma probabilidad de ocurrir.

b) Que no existiera correlación serial entre las llaves, en el sentido de que dada una cadena de llaves sucesivas, la siguiente llave en la serie tiene la misma probabilidad de ocurrir, independientemente de cuál sea la cadena que le precede y aunque se tuviera un historial de llaves antecesoras, una predicción es esencialmente equivalente a adivinar la siguiente llave, es decir, que el conocimiento de las antecesoras no mejora la predicción.

c) Deberían ser llaves únicas, era una obligación no debía ni una sola, por lo que se manejaron probabilidades muy reducidas para garantizarlo.

d) Las claves generadas debían ser de forma tal que no pudieran ser descifradas por persona alguna, independientemente de su experiencia y conocimiento en el área de la informática, ni por equipo alguno, ejecutando algún programa sofisticado tendente a la ruptura de estas claves, por lo menos no en el momento en el que la información tuviera valor. Sabemos que se pueden romper claves pero se requeriría de cierto tiempo para hacerlo.

Al respecto, se suelen emplear programas de computadora orientados a la generación de códigos pseudo aleatorios para desarrollar estas claves, pero el resultado no es del todo perfecto porque eso implica cierto nivel de predictibilidad y la llave resultante puede ser violada si se dispone de ciertos parámetros.

En el proceso de generación de llaves se emplearon caracteres aleatorios en un ambiente controlado mediante el ruido intrínseco producido por dispositivos electrónicos.

El "generador de llaves", creado desde el PREP 2000, es un dispositivo consistente en un circuito que contiene un diodo Zener, una etapa de amplificación y un decodificador que digitaliza el ruido del diodo obteniéndose los bits, los cuales se envían a una computadora a través de uno de sus puertos de comunicaciones llamado puerto

paralelo, la computadora los recibe y los combina formando con ellos un archivo. Los bits generados se combinan mediante una operación a nivel de bits o booleana (XOR), con una secuencia pseudo aleatoria. El fin es lograr una secuencia de bits con la misma probabilidad de que cada bit consecutivo sea un cero o un uno (50%).

Este dispositivo se basa en el fenómeno físico relativo al ruido eléctrico natural existente en todos los dispositivos electrónicos, las secuencias resultantes son de naturaleza más puramente aleatorias y, por consiguiente, más difíciles de predecir en comparación con aquellas desarrolladas mediante programas especiales para computadora.

2.4.2 Esquema de seguridad en el proceso de captura.

El proceso de captura podía ser susceptible a que alguna persona o grupos tuvieran interés en modificar la información electoral o introducir votos no legítimos al sistema, por lo que se necesitaba reconocer e identificar a cada uno de los puntos desde los cuales se capturaría, se solucionó con un proceso de autenticación muy riguroso basado en la implementación de las llaves para garantizar que el alta, baja, captura y transmisión desde algún equipo de cómputo fuera una operación válida y reconocida por el sistema. Aunque se diera el caso de que alguien contara con el mismo equipo de cómputo, con la tecnología y las herramientas del programa no podría engañar al sistema, pues las terminales permiten entrar en la aplicación solo por medio de contraseñas.

Participaron en el proceso de captura de datos: el coordinador, el supervisor y el capturista. Los dos primeros fueron los encargados de inicializar las controladoras (por razones de seguridad y responsabilidad), el supervisor y el capturista se encargaron de abrir la sesión en una terminal de captura. Una TCR no podía enviar los datos si la controladora no había sido inicializada. Por lo tanto, se generaron tres tipos de tarjeta magnética que almacenaría llaves distintas: una para el coordinador, otra para el supervisor y una para cada capturista, de acuerdo al número de TCR en cada CEDAT.

Se generaron dos juegos de tarjetas, uno para usarse durante las pruebas nacionales y otro para usarse durante la jornada electoral.

Debido a que la TCR no tenía llave y no podía ser grabada en una tarjeta magnética, la controladora almacenó sus llaves. Cada controladora guardó en un dispositivo, conocido como memoria de acceso aleatorio perdurable (Random Access Memory), una secuencia de bytes suficientemente grande para generar las llaves que se requerían para las TCR de captura. Esta secuencia midió 160 bytes (8x20), de la cual se podían generar hasta 20 llaves para TCR.

La carga de llaves para las TCR's se realizaría únicamente en las controladoras. Sin embargo, el centro de cómputo guardaría una relación de las que correspondían a cada tipo de usuario, así como el número de serie de cada una de las llaves, y en el caso de las tarjetas magnéticas identificaría también si la llave correspondía a una prueba nacional o al día de las elecciones.

Al encender la terminal controladora, ésta pedía leer la tarjeta magnética del supervisor y del coordinador, de la cual obtenía la llave y el número de serie (número de tarjeta). Se preparaba un paquete de información llamado criptograma que pedía la autorización al CENARREP, identificando el equipo que quería comenzar a operar. Si el CENARREP lo conocía y podía descifrar el criptograma con las claves acerca de ese equipo le respondía y permitía el acceso. Una vez aceptado en el centro de cómputo, la controladora procedía a generar una llave para cada terminal de captura, la enviaba y esperaba el código de respuesta.
Todo este esquema de llaves se utilizaría para la autenticación y también para proteger la información que debería viajar sin cifrado, pero con normas de seguridad que garantizaran su consistencia y confiabilidad.

Cuando todo estaba listo para realizar la captura, se debía garantizar que no existieran errores en ésta, la información contenida en cada acta era exactamente la misma que se introdujera al sistema, por queso parte el sistema interno de cada terminal de captura

remota pedía el registro dos veces los datos para su validación, si estos coincidían la operación procedía, de lo contrario se repetía el procedimiento hasta que no existieran errores.

- Se requiere la presencia de 3 personas para iniciar el servicio de captura en la TCR.
- Se captura dos veces cada acta para verificar los datos.
- Se imprime un recibo para cotejo de la información.
- Se cuenta con 30% de personal adicional en cada CEDAT.
- El coordinador y el supervisor están capacitados para sustituir, en caso de emergencia, alguna otra función en el CEDAT.

2.5 Seguridad en la transmisión

Un punto sensible en la seguridad fueron las líneas telefónicas de comunicación que se utilizaron para recibir los datos de captura, aunque eran privadas corrían el riesgo de ser intervenidas, sin embargo, no tenía sentido proteger la captura aplicando métodos de autenticación, si cuando esta información se transmitiera podría ser vulnerable a cualquier ataque.

Se cuidaron, esencialmente, las comunicaciones y se trabajó en conjunto con la empresa encargada de dar este servicio para procurar líneas libres de ruido y seguras desde los CEDAT hasta el CENARREP.

La información contenida en las actas de escrutinio no era confidencial, sino al contrario, fue pública. Al término de la jornada electoral, en cada una de las casillas se publicaron inmediatamente los resultados para que los ciudadanos los conocieran; la información a enviarse desde los CEDAT no podía estar cifrada, pues esto iba en contra del principio de transparencia en la transmisión de los datos.

Acciones implantadas

- Se utilizaron "pasaportes informáticos" llamados firmas digitales criptográficas, son claves cifradas para la identificación del origen de la información.

- Se generaron tres tipos de llaves distintas: una para la TCR de captura, una para el coordinador del CEDAT y la última para el supervisor y otra para el capturista.

- Se utilizaron líneas de transmisión de datos conectadas desde antes del inicio de la captura y en forma continua durante la noche.

- Cada transmisión se verificó para asegurar que su transacción era válida y autorizada.

- Se utilizaron líneas y equipos dobles para una transmisión ininterrumpida de la información.

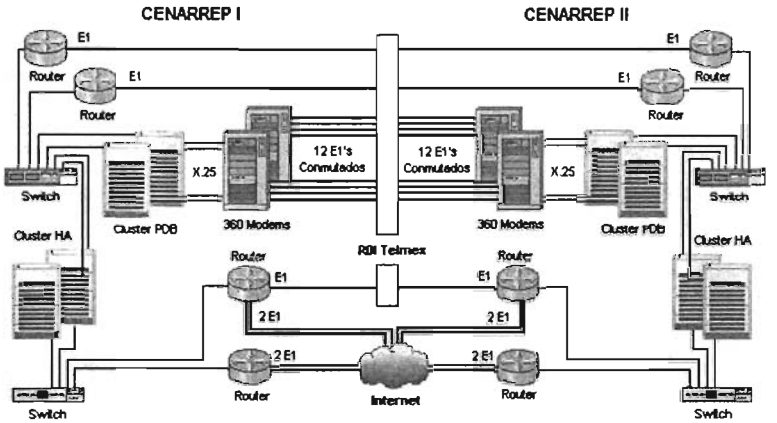

Figura 2.1: Diagrama general de la red del Sistema PREP

Autenticación de las transmisiones

Si los datos de las actas no iban a transmitirse cifrados, se debía asegurar que nadie alterara la información desde su captura hasta su llegada al centro de cómputo y se difundieran los resultados de la misma, por lo que era necesario firmar digitalmente cada paquete de datos. Se eligió el método de cifrado para la firma digital que llevaría cada acta.

Mediante la firma digital criptográfica, se aseguraba que solamente la persona que tuviera la llave podía generar esa firma. Si se mantenían esas llaves bien cuidadas, se sabía que no se alteraría la información de captura. Con tan sólo un bit que fuera alterado haría la firma totalmente diferente.

Además de establecer que un mensaje no había sido alterado, se verificaba que cada transmisión provenía de su emisor. La información fue almacenada en una bitácora donde se registraban los eventos que los centros de cómputo llevaban a cabo.

El equipo de comunicaciones que recibiera las llamadas de las terminales punto de venta, estaba integrado para evitar los inconvenientes de utilizar modems independientes, tarjetas descanalizadoras y de comunicación con el equipo de procesamiento central, además, considerando que debía soportar toda la carga y que cada CEDAT tendría al menos una línea telefónica privada para marcar al centro, el número de modem no debería ser menor a 360 por centro.

Capítulo 3

Análisis de la propuesta del Laboratorio de Cómputo del Centro Tecnológico Aragón en cuanto a la seguridad de urnas electrónicas.

El laboratorio de cómputo del Centro Tecnológico Aragón, de la Escuela Nacional de Estudios Profesionales Aragón, como resultado del convenio firmado con el IEDF para presentar un prototipo de Urna Electrónica para comicios electorales, realizo la siguiente propuesta de seguridad.

El proyecto de Urna Electrónica , consistió en su primera fase, en proponer como institución de educación superior un prototipo de Urna Electrónica para comicios electorales con las características dictadas por el Instituto Electoral del Distrito Federal:

- Garantizar el carácter universal, libre, secreto, directo, personal e intransferible del voto, su autenticidad y efectividad, a fin de evitar cualquier alteración de la información y de los resultados;
- Garantizar la seguridad del ejercicio del voto durante la jornada electoral;
- Permitir al elector la emisión del voto en forma rápida y sencilla;
- Utilizar un mecanismo para la identificación del elector, a fin de evitar intentos de falsificación del voto;
- Ser de fácil instalación y mantenimiento;
- Dar seguridad de que la jornada electoral se realice de forma continua;
- Permitir que el ciudadano emita sucesivamente su voto, en las diferentes elecciones previstas en el Código;
- Impedir que el ciudadano intente votar por segunda ocasión;
- Permitir que el ciudadano, al marcar su opción, visualice los elementos de identificación de su preferencia;
- Permitir al votante corregir su preferencia antes de confirmar el sentido de su voto;

- Permitir la emisión de comprobantes de instalación y apertura de la casilla, del cierre de la votación, de los resultados del cómputo y de la clausura de la casilla;
- Contribuir a evitar los errores humanos en el escrutinio y cómputo de una elección, para dar certeza y confianza a los partidos políticos y a los ciudadanos sobre los resultados electorales;
- Contar con los mecanismos necesarios para recuperar los datos de la votación íntegramente, en caso de falla o avería del equipo;
- Permitir la comparación de los resultados impresos con los guardados en los dispositivos de la urna;
- Garantizar que todos los mecanismos de seguridad sean auditables para que puedan ser analizados en caso de controversia;
- Incluir mecanismos para facilitar el ejercicio del voto a las personas con discapacidad.
- Garantizar la difusión oportuna y confiable de los resultados del cómputo; y
- Reducir los costos en el procedimiento para la emisión y cómputo del sufragio.

En la figura 3.1 se puede observar el resultado (físico) de la propuesta de urna electrónica por parte del Centro Tecnológico Aragón, el cual cumple con normas de ergonomía y otros aspectos de usabilidad que no están al alcance de este proyecto de tesis. La Urna Electronica está diseñada para que la pantalla sea abatible quedando un portafolio portátil y, al mismo tiempo, oculta las salidas de los dispositivos internos que únicamente puede manipular el presidente de casilla.

Las características principales de este diseño son:

1. La Urna está diseñada para que todos los dispositivos pantalla "touch screen", impresora, tarjetas de control, iconografías, suministro eléctrico y caja de impresiones, estén herméticamente sellados y no exista manera alguna de que el usuario interfiera con ellos o con los votos emitidos, evitándose con esto cualquier alteración de la información y de los resultados.

2. Por su diseño ergonómico, fabricación y por los dispositivos que contiene, la Urna es muy sencilla y de fácil manejo, tanto para el jefe de casilla, ya que éste puede rápidamente instalarla por los mecanismos de apertura, control y cierre, así como para el ciudadano que emitirá su voto libre, secreto y directo, ISO 7250 Basic human body measurements for technological design. W1 00 122 085 Anthropometric database (ISO/NP 15535).

3. Para su almacenamiento la Urna Electrónica se puede apilar tanto horizontalmente como verticalmente, lo que permite el ahorro de espacio en bodega y una excelente maniobrabilidad para su traslado.

4. Todos los dispositivos y elementos que constituyen la Urna están contenidos en un sólo encapsulado, que tiene forma de paralepípedo de 32 X 48 X 9 cm.

5. La Urna Electrónica está diseñada ergonómicamente para que se puedan manipular la pantalla "touch screen" y los comandos colocados en la parte inferior, ISO 8995. "Principles of visual ergonomics, ISO 7250 Basic human body measurements for technological design. W1 00 122 085 Anthropometric database (ISO/NP 15535)".

6. La pantalla "touch screen" cuenta con 5 posiciones de 3º cada uno, iniciando por Normatividad desde 30º hasta 45º como máximo, para que el rango de la población nacional pueda tener el mejor ángulo de enfoque en sus votaciones, ISO 9241-2. Ergonomic requirements for office work with visual display terminals.

7. Para la protección de la pantalla "touch screen", se adaptó a la Urna una pequeña lámina de acero inoxidable calibre 20, que se desplaza horizontalmente mediante un sistema de broches, para que en la bodega de almacenamiento o en el traslado se reduzcan los daños por impactos.

8. Con base en la iconografía, esto es la descripción común de imágenes, en la parte inferior de la pantalla "touch screen", se colocaron los comandos (botones) necesarios para que el usuario pueda efectuar su votación. Utilizando la Normatividad de Colores, en las unidades de aceptar, cancelar y direcciones (flechas), así como la inclusión del Alfabeto Braile respondiendo con ello a las necesidades especiales de la población. Dichos comandos serán fabricados en Elastómero Termoplástico (Santoprene), ya que este material tiene una gran durabilidad por ser resistente a la fatiga, al ozono, a los rayos ultravioleta, ácidos, álcalis, petróleos, lubricantes, lo que sin duda retribuirá en un excelente desempeño y un largo ciclo de vida, ISO 11429. Ergonomics – System of signals.

9. Para garantizar la autenticidad y efectividad de la participación electoral, en la parte superior de la urna, se colocará una mirilla de Estireno Acrilonitrilo (SAN), un copolímero de gran rigidez y resistencia a la abrasión, que además de ser estable térmicamente es resistente a grasas, aceites y substancias aromáticas, para que el ciudadano observe la impresión de su voto inmediatamente que efectúa la elección de sus candidatos.

10. La Urna está habilitada con una caja interna no transparente, con las mismas características técnicas descritas en el párrafo anterior, con la que se logra un doble efecto visual, ya que por un lado se puede observar que existe la recepción de los votos efectuados por los ciudadanos, pero por otro, que no se puede saber por quién se vota. Asimismo, esta caja almacena toda la información recabada, teniendo un sistema de seguridad (cerradura), que únicamente se puede retirar para fines de auditoria por autoridades electorales.

11. La Urna cuenta con una Manija Retráctil, que tiene un doble objetivo, facilitar su transportación y ser, al mismo tiempo, un mecanismo de protección, ya que al

abatirse, oculta las salidas de los dispositivos internos, que únicamente puede manipular el jefe de casilla.

12. La Urna sin dispositivos tiene un peso aproximado de 940 gramos.

13. La Urna electrónica utiliza una pila que brinda una autonomía en el suministro eléctrico hasta por doce horas continuas.

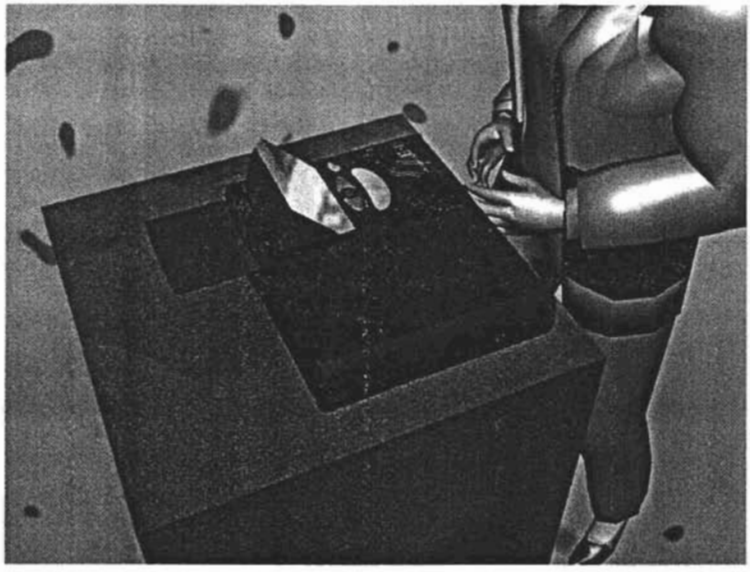

Figura 3.1 Prototipo de Urna Electrónica propuesta por el Centro Tecnológico Aragón

La propuesta de software para la urna electrónica dio como resultado las siguientes etapas de funcionamiento: previa a la votación, etapa de votación y posterior a la votación.

Cada una de estas etapas están conformadas por un número de funcionalidades que se pueden observar en el diagrama de estados de la figura 3.2; donde los estados que están encerrados en el recuadro, es la etapa de votación y corresponde a todos las funcionalidades contenidas en la urna electrónica. El estado de generación de archivos binarios y carga del sistema operativo forman parte de la etapa de pre-votación; los estados de envío y recepción de la información son parte de la etapa posterior de la

votación. Cada de una de estas etapas se describen a continuación y se explican las consideraciones de diseño que se tomaron para cumplir con los objetivos.

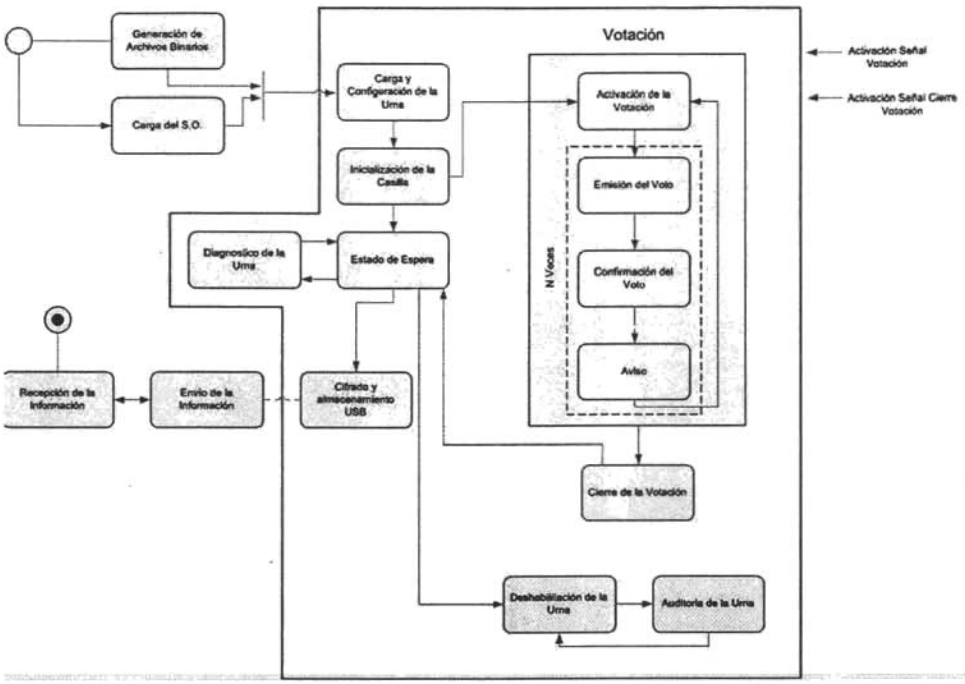

Figura 3.2: Diagrama de estados del proyecto de Urna Electrónica

3.1 Etapa de funcionamiento: Previa a la votación.

Se diseñó un sistema integrador de información, cuya sede son las oficinas del IEDF, dentro del cual se podrían hacer las siguientes tareas:

- Configurar el número de elecciones a llevarse a cabo el día de la elección y las elecciones en si: Jefe de gobierno, Jefe delegacional, etc.
- Registrar los datos relacionados con los partidos políticos participantes, incluidos logotipos y sonido.
- Dar de alta a los candidatos a participar y relacionarlo con un partido político y un tipo de elección.

- Emitir reportes registro.
- Generar archivos binarios a utilizar por la urna electrónica y almacenarlos en un dispositivo portátil (Flash memory). Estos archivos binarios son generados a partir de la base de datos de este sistema integrador y lo almacena en archivos planos en formato binario y con una estructura predefinida para mantener las referencias de los datos. Estos archivos son utilizados en la etapa de votación para la configuración y apertura de las urnas (se explica más adelante).
- Firmar digitalmente dichos archivos, almacenando las firmas junto con los archivos binarios para verificar la autenticidad de los mismos.
- Copiar el "pubring.gpg" con la llave del distrito y del equipo integrador; Copiar el "secring.gpg" con la llave privada del distrito.
- Este sistema integrador también fue diseñado para tener la capacidad de recibir los datos de los resultados electorales de la jornada (estados de la Post-Votación).

3.2 Etapa de funcionamiento: Votación

Para esta etapa se utilizó una sistema embebido PC-104, específicamente el Kit de desarrollo VIPER (figura 3.3), Arcom Embedded Linux [12], el cual cuenta con sistema operativo LInux con un KERNEL 2.4.además de contar con herramientas de desarrollo para programar aplicaciones en Java, C estándar y aplicaciones graficas con GTK+; también trae integrada una pantalla LCD y una membrana Touch-Screen de 5.5 pulgadas con la opción 6.4 pulgadas y 10 pulgadas.

Analizando las diferentes posibilidades para desarrollar la aplicación se escogió el lenguaje C y las librerías graficas GTK+ en base a las siguientes consideraciones:

- Se tomó la decisión de utilizar software libre para, de esta forma, no tener dificultades por si algún interesado en revisar la existencia o no de un código malicioso, lo pudiera hacer sin restricciones de licencias y derechos de autor; la licencia GNU de Linux si lo permite.

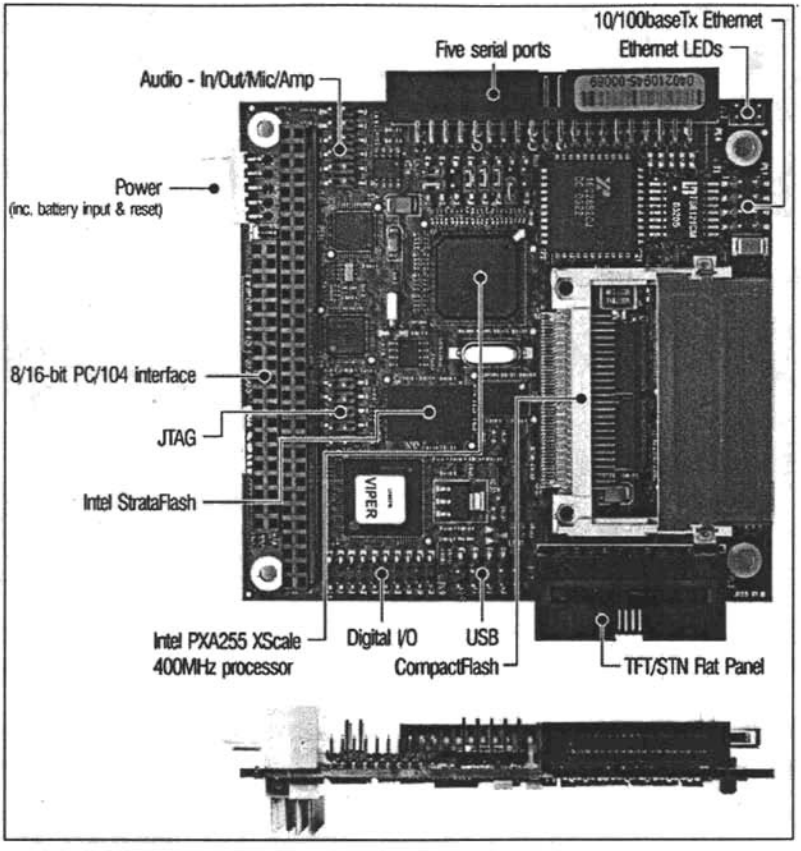

Figura 3.3 Kit de desarrollo Viper

- Se decidió desarrollar en lenguaje C porque, tiene una relación muy estrecha con el sistema operativo Linux, debido a que es el lenguaje con el cual se sigue desarrollando dicho sistema operativo.
- La interfaz de usuario se desarrolló con librerías gráficas GTK+, que están escritas en C y en el paradigma orientado a objetos y hacen fácil la programación.

En esta etapa se encuentran las funcionalidades del sistema del siguiente diagrama de casos de uso.

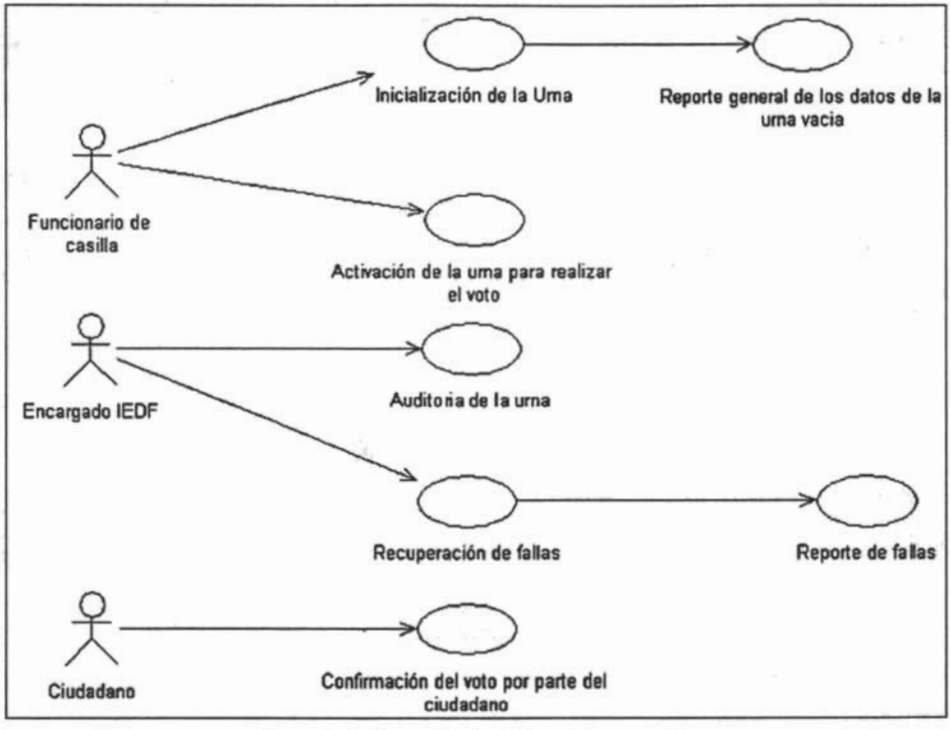

Figura 3.2: Caso de uso: Etapa de votación.

El caso de uso de inicialización de la Urna, el funcionario de casilla realiza las siguientes acciones para llevar a cabo esta tarea:

- Enciende la urna electrónica e introduce el dispositivo USB, el cual contiene los archivos binarios generados en la etapa Previa a la votación.
- Hace un diagnóstico de dispositivos de la urna electrónica, si los dispositivos funcionan bien, se procede a solicitarle la contraseña al funcionario de casilla. Una vez autenticado el sistema solicita la introducción de los datos relacionados a la casilla a abrir: Sección y tipo de casilla.
- Una vez introducidos estos datos, el sistema lee desde el dispositivo USB los archivos binarios construidos en la etapa anterior (Pre-votación, en el equipo integrador) y sus respectivas firmas digitales. Verifica su autenticidad y si son correctas las firmas, el sistema obtiene los datos para la votación

relacionados con dicha casilla y los almacena en la unidad de almacenamiento persistente (Flash Memory).

- El sistema emitirá las siguientes impresiones:
  - Reporte de diagnóstico
  - Acta de apertura
  - Y actas de urna vacía para cada una de las elecciones.

Figura 3.4: Muestra de una boleta creada dinámicamente en base a los datos leídos de los archivos binarios

- Dicha información servirá de base a la aplicación para generar las planillas correspondientes.

El caso de uso Activación de la Urna para realizar el voto, es un mecanismo diseñado con el fin de enviar una señal desde la mesa de funcionarios de casilla, por medio de un dispositivo electrónico conectado a la Urna Electrónica que está compuesto por dos botones y un semáforo, el cual tiene la siguiente funcionalidad:

- Una vez identificado el votante de la manera tradicional (Credencial de Elector) el presidente de casilla procede a presionar el botón de activación de la urna, ya que por seguridad, la Urna está desactivada y sólo con el botón se puede habilitar. Una vez que se presiona el botón, el semáforo, en el dispositivo (a la vista de todos)cambia a verde y, de esta manera, el ciudadano puede pasar a la casilla a emitir su voto.

- Los representantes de partidos y funcionarios de casilla, deben verificar que una persona se encuentre sola, mientras el semáforo está en verde.
- El ciudadano emite su voto, con su respectiva confirmación (figura 3.5); en la Urna Electrónica se imprime un ticket indicando la orientación del voto, para que el ciudadano lo verifique. A este ticket no tendrá acceso el ciudadano, sólo podrá verlo, pero no podrá extraerlo de la Urna.

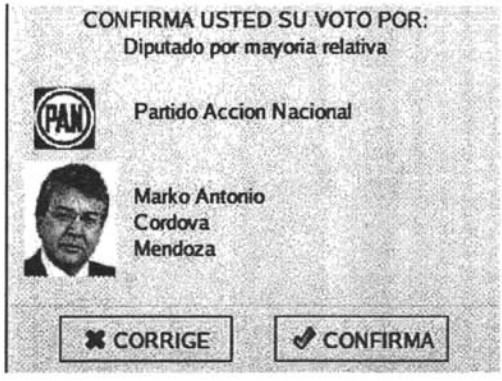

Figura 3.5: Pantalla de confirmación

- En la Urna se emiten el número de votos dependiendo de la cantidad de elecciones, al finalizar éstas, se deshabilita la Urna y el sistema envía una señal al dispositivo activador para que cambie el semáforo de verde a rojo, indicando que la casilla se debe desocupar.
- Este proceso se lleva a cabo desde la apertura de la casilla, hasta que se cierra la casilla.

El caso de uso Cierre de votación, se encarga de realizar el escrutinio y cómputo de los votos, llevando a cabo la siguiente metodología:

- Si a la hora de cierre no hay un ciudadano emitiendo su voto (semáforo en verde), la Urna Electrónica presenta la pantalla de cierre de votación, solicitando la clave del presidente de casilla. Si se desea mantener la casilla abierta, se cancela la autenticación, y la Urna solicitará la clave hasta dentro de 30 minutos posteriores a la cancelación.

- En el caso de autenticarse correctamente la Urna, se procede al cómputo de votos.
- Se construye el acta de escrutinio y cómputo en un archivo y su respectiva firma digital.
- Se pregunta el número de impresiones que se desean (figura 3.6) y se emiten ese número de actas de escrutinio y cómputo.

Figura 3.6: Pantalla de introducción del número de impresiones del acta de escrutinio.

- Se pide insertar el dispositivo USB para que el sistema almacene los siguientes archivos cifrados con sus respectivas firmas digitales:
  - Archivo de votos
  - Bitácoras de aplicación

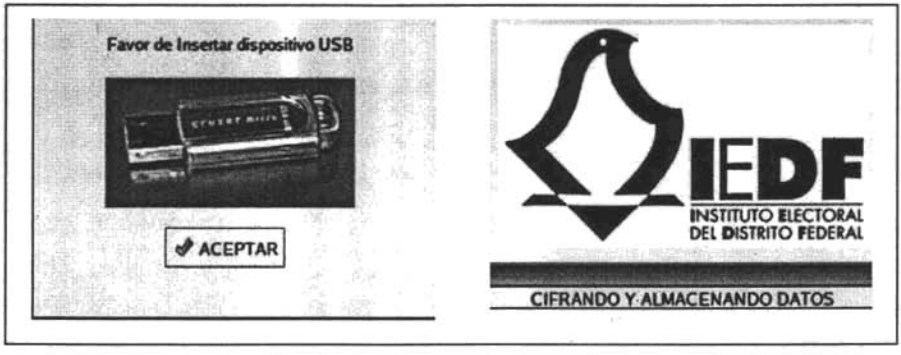

Figura 3.7: Cifrado y almacenamiento de datos.

Estos archivos cifrados y originales se conservan en la unidad de almacenamiento persistente para posibles tareas de auditoria.

- Una vez terminado el proceso de cierre de votación, la urna se deshabilita, se apaga para ser desensamblada y pueda se pueda transportar a el distrito correspondiente.

3.3 Etapa de funcionamiento: Posterior a la votación

En esta etapa se transmiten los datos de la elección que están almacenadas en el dispositivo USB hacia las oficinas centrales, es análogo al procedimiento del capítulo 2, en el cual el presidente de casilla lleva las actas de escrutinio y cómputo (sobre membreteado con papelería) a las oficinas centrales. En el caso de que se tratara de archivos digitales cifrados y firmados, el procedimiento para llevar a cabo esta actividad sería el siguiente:

1. El presidente de casilla se traslada con la Urna Electrónica (maletín) hacia las oficinas distritales correspondiente a la casilla, junto con el dispositivo USB, que servirá para hacer la transmisión de datos hacia las oficinas centrales del Instituto Electoral de Distrito Federal.

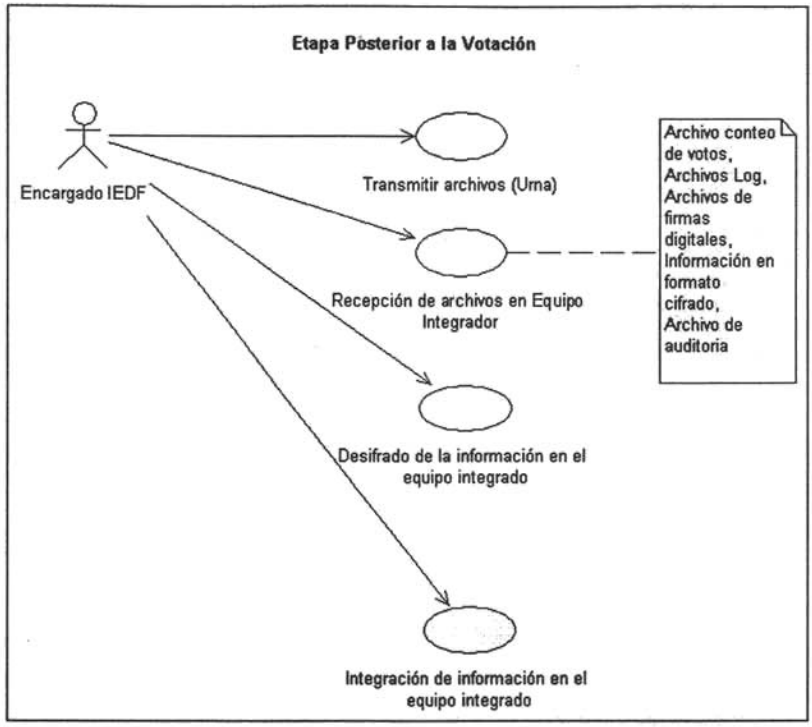

Figura 3.8: Diagrama de casos de uso de la etapa de post-votación.

2. Se recibe y en un buzón de entrada los dispositivos, se procede a integrar en un equipo portátil conectado en red con una computadora del distrito electoral que funge como integrador distrital de resultados. La integración de los resultados se hacen siguiendo los siguientes pasos:
    a. Introducir la memoria usb al puerto de entrada de la terminal y se da clic en el botón de integración y automáticamente realizan las siguientes tareas:

        Verifica las firmas digitales de los archivos:

        votos.bin.gpg

        AppLog.gpg

b. Si las firmas son correctas, se descifra el archivo votos.bin, se almacena temporalmente en memoria para su lectura y, posteriormente, se integra en la base de datos del integrador distrital.
c. Se almacenan en el disco duro del integrador distrital los archivos cifrados, con sus respectivas llaves, para ello se crea una carpeta con el nombre de la casilla, por ejemplo, la carpeta "1002b", que correspondería a la casilla 1002 básica.
d. Posteriormente, un programa residente en el equipo integrador distrital se encarga de transmitir y administrar los paquetes electorales electrónicos. Los archivos son transmitidos cifrados hacia el servidor central del Instituto Electoral del Distrito Federal, el esquema a detalle de dicho envío se analiza más adelante en este capítulo.

3. El servidor central se encarga de integrar la información y determinar el grado de avance del acopio.

3.4 Seguridad Física de la Urna Electrónica.

El motivo por el cual se analiza la seguridad física de la Urna Electrónica, es la consistencia de los datos y su confiabilidad. Se debe tener la certeza de que los datos estarán resguardados en todo el proceso y sólo personas autorizadas tienen acceso a por métodos seguros.

Un aspecto es proveer mecanismos de seguridad en la operación física de las Urnas Electrónicas, esta área tiene que ver con el diseño físico de los gabinetes.

El otro aspecto es establecer las políticas de seguridad para el manejo de la información, principalmente, en las etapas de Pre-votación y Post-votación.

3.4.1 Mecanismos de seguridad física del gabinete de urna electrónica

En cuanto a seguridad física se cuentan con dos aspectos, el primero de ellos es el relacionado al resguardo del gabinete de seguridad en la mampara de votación. El segundo aspecto es establecer mecanismos para permitir acceder a elementos internos

de la urna electrónica de personal autorizado, por ejemplo mecanismo para abrir la urna y extraer los votos impresos.
La Urna Electrónica no puede ser abierta en ningún momento por gente ajena a la autoridad electoral. El presidente de casilla, responsable de instalarla, encenderla y configurarla para su funcionamiento solo tiene acceso a unos cuantos componentes de la urna pero desde el exterior, el principal es el acceso al conector de usb que servirá para cargar los datos específicos para la elección y la sección configurada.

El gabinete está diseñado para cerrar herméticamente en dos únicas piezas y con un mecanismo de apertura especial, lo que dificulta su apertura a personas ajenas.
El gabinete con los componentes contenidos, pesa 9.04 kg (tabla 1), por lo cual es necesario protegerlo de posibles caídas y/o sabotajes. La solución fue diseñar broches para asegurar la urna a la mesa de las mamparas.

Elemento	Peso aproximado kg.
Pila	6.5
Impresora	0.4
Unidad de respaldo	0.5
Hardware computadora	0.7
Gabinete	0.94
TOTAL Aproximado	**9.04**

3.5 Esquema de seguridad

La seguridad informática es otro punto vital en este proyecto, fue importante utilizar algoritmos confiables, lo cual nos llevo a usar GnuPG que es un software para el cifrado de información con algoritmos matemáticamente confiables y ampliamente usados en Internet para el intercambio de información de manera confidencial, en lo que se refiere a la autenticación de remitentes, así como para detectar integridad de archivos digitales de información.

También se buscó que el sistema fuera 100% auditable, por eso se tomo la decisión de utilizar software GNU[4], para tener acceso a todo el código fuente sin contar con restricciones legales, entre otras muchas ventajas.

Para el respaldo de energía se propuso un sub-sistema con la característica de actuar como no-break. El diseño ha sido implementado y probado satisfactoriamente, auque en su etapa de prototipo el circuito está separado, lo cual lo hace ocupar espacio, este circuito se puede integrar en una tarjeta, lo cual reduciría su tamaño drásticamente.

3.5.1 Esquema de generación de claves.

El prototipo de Urna Electrónica se ha orientado a la utilización de software GNU, por lo tanto, se analizaron herramientas criptográficas disponibles para realizar el cifrado y descifrado de información, así como la creación de firmas digitales. El resultado fue la elección de GnuPG[5] el cual cuenta con las siguientes características:

- Reemplazo completo de PGP de licencia propietaria.
- No utiliza algoritmos patentados.
- Con licencia GPL, escrito desde cero.
- Funcionalidad mejorada con respecto a PGP y mejoras de seguridad con respecto a PGP 2.
- Descifra y verifica mensajes de PGP 5, 6 y 7.
- Soporta ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 y TIGER.
- Facilidad de implementación de nuevos algoritmos utilizando módulos.
- Fuerza que el identificador de usuario (User ID) esté en un formato estándar.
- Soporta fechas de caducidad de claves y firmas.

[4] Mayor información del proyecto GNU disponible en: http://www.gnu.org/philosophy/philosophy.es.html
[5] Proyecto GNU Privacy Guard. http://www.gnupg.org

- Soporta inglés, danés, holandés, esperanto, estonio, francés, alemán, japonés, italiano, polaco, portugués (brasileño), portugués (de Portugal), ruso, español, sueco y turco.
- Sistema de ayuda en línea.

Creación de las llaves

Se propuso la creación de 41 par de llaves, 40 para las urnas de los diferentes distritos electorales y 1 para el equipo integrador con cede en el IEDF. La creación se llevará a cabo en el equipo integrador en la etapa de pre-votación, incluyéndolas en el dispositivo USB para su posterior instalación (automática) en la urna electrónica. Es importante mencionar que se integran las "huellas dactilares" de cada llave para verificar su integridad.

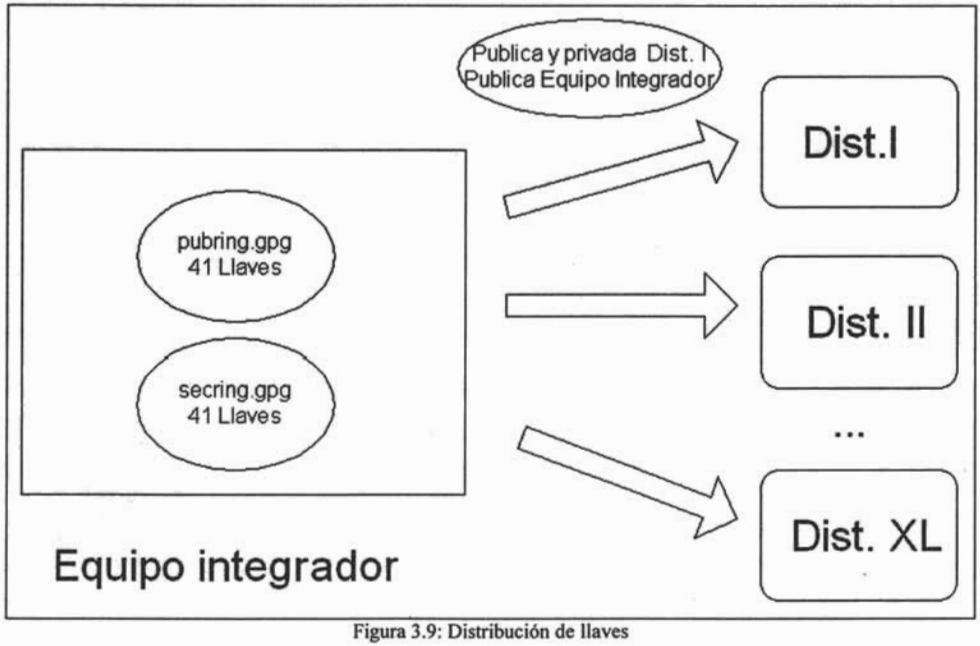

Figura 3.9: Distribución de llaves

El siguiente procedimiento de creación de llaves se llevó a cabo para cada una de éstas.

Por favor seleccione tipo de clave deseado:

(1) DSA y ElGamal (por defecto)

(2) DSA (sólo firmar)

(4) RSA (sólo firmar)

Su elección:

Se selecciona la opción 1.

Después se muestra en pantalla:

El par de claves DSA tendrá 1024 bits.

Listo para generar un nuevo par de claves ELG-E. el tamaño mínimo es 768 bits

el tamaño por defecto es 1024 bits

el tamaño máximo recomendado es 2048 bits

¿De qué tamaño quiere la clave (1024)?

Se teclea el número 2048

Se utilizó este tamaño para determinar tiempos de cifrado y descifrado en la arquitectura ARM, se logró un descifrado en menos de 30 segundos de toda la información necesaria; En cuanto al descifrado, fue sólo necesario en el equipo integrador, el cual por sus características tiene mayor poder de cómputo.

A continuación muestra:

Por favor, especifique el período de validez de la clave.

0 = la clave nunca caduca

<n> = la clave caduca en n días

<n>w = la clave caduca en n semanas

<n>m = la clave caduca en n meses
<n>y = la clave caduca en n años

¿Validez de la clave (0)?

Se elige la opción 0.

A la pregunta ¿Es correcto (s/n)?

Se responde s.

En la consola se muestra:

Necesita un identificador de usuario para identificar su clave. El programa construye el identificador a partir del Nombre Real, Comentario y Dirección de Correo Electrónico de esta forma:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos:

Se teclea ie_df en Nombre y apellidos, el nombre y apellido debe de constar de al menos 5 caracteres.

Dirección de correo electrónico:

Se teclea la dirección de correo electrónico que se desea.

Comentario:
Se teclea algún comentario para la llave.
¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir?
Se teclea V

Necesita una frase contraseña para proteger su clave secreta.

Introduzca frase contraseña:

Se teclea la contraseña que se desee y se confirma.

A continuación se pide al usuario que mueva el ratón para generar números pseudo aleatorios que formarán las llaves.

Integridad de las llaves.

Para comprobar la integridad de las llaves, se realiza lo siguiente. Ya elaboradas éstas, se deben crear los archivos FPrivadaDE, FPublicaDE y FPublicaIN de la siguiente manera:

1.gpg --fingerprint --list-key de_df | head -n 2 | tail -n 1 | cut -b 23- > FPrivadaDE
2.gpg --fingerprint –list-key de_df | head -n 2 | tail -n 1 | cut -b 23- > FPublicaDE
3.gpg --fingerprint –list-key integrador | head -n 2 | tail -n 1 | cut -b 23- > FPublicaIN

Donde: **de_df**:Es el nombre de usuario para un distrito electoral.
integrador: Es el nombre de usuario para las llaves del equipo integrador.

Se crean archivos para verificar la autenticidad con MD5 de los archivos que contienen las huellas dactilares: md5fpPrivadaIE, md5fpPublicaIE y md5fpPublicaIN como sigue:

1.md5sum FPrivadaIE > md5fpPrivadaIE
2.md5sum FPublicaIE > md5fpPublicaIE
3.md5sum FPublicaIN > md5fpPublicaIN

Durante la ejecución de la Urna Electrónica (etapa de pre-votación), se importan las llaves, se instalan y con GPG se verifican sus huellas dactilares, se comparan con los archivos que se encuentran en el dispositivo USB. Si estos son iguales, se continúa con la aplicación, de otra manera la Urna Electrónica se deshabilita, enviando antes un mensaje al usuario de que la integridad de las llaves no es correcta.

3.6 Manejo de claves criptográficas

Las llaves, creadas con el procedimiento antes explicado, se deben integrar a un anillo de confianza para tener la certeza de que estamos haciendo uso de las llaves seguras. GnuPG trabaja con anillos de confianza y utiliza el mismo para validar las claves de otras personas, dado que nosotros no firmaremos las claves de todo el mundo, sólo la de nuestro grupo de confianza, en este caso las llaves del IEDF y las de los 40 distritos electorales. Por lo tanto, iremos armado este anillo de confianza que será local y propia de cada subsistema (Urna Electrónica, integrador) que trabaje con GPG, porque la confianza es algo subjetivo de cada persona y los valores permanecerán en una base de datos propia trustdb.gpg que es la base de datos de las llaves de confianza de GnuPG.

Le asignaremos un nivel de confianza al poseedor de esa clave, es decir, nosotros consideramos que esa persona firma las claves de otros y así poder extender el uso; para GPG cualquier clave que firmemos personalmente será considerada en principio válida.

Existe un indicador de GPG que asocia nuestro nivel de confianza en el propietario de la clave a cada clave pública de nuestro anillo de claves.

La instalación de la base de datos de llaves de confianza, se hará junto con el sistema operativo y las aplicaciones relacionadas con la Urna Electrónica. El esquema de carga se hace por medio de imágenes de sistema operativo y sistemas de archivos. Es decir, una vez que se tiene un sistema operativo optimizado y revisado de posibles debilidades de seguridad, se crea una imagen de este sistema que será instalada a todas las urnas con la simple copia de la imagen. Aquí se pueden incluir (en el sistema de archivos) los archivos binarios (ejecutables) de GnuPG y los archivos de base de datos de las llaves GnuPG a utilizar.

3.7 Esquema de seguridad del proceso de votación

El proceso esquema de identificación del presidente de casilla, quien es el encargado de instalar la casilla, es por medio de una contraseña GPG cuyo esquema de generación ya ha sido discutida.

En la etapa de votación, se utilizan las llaves y los mecanismos de cifrado en la apertura de la casilla para verificar las firmas digitales de las llaves.

La Urna Electrónica comienza con un "splash" de presentación del IEDF que dura un instante (figura 3.10).

Figura 3.10: Splash de inicio de Urna Electrónica.

A continuación se pide que se inserte el dispositivo USB (figura 3.10) para comprobar la integridad las llaves, se inserta y se da aceptar, en caso contrario aparecerá una venta de error, si la venta de error se muestra tres veces el sistema se apagará.

Figura 3.11: Petición de inmersión del dispositivo USB (Flash memory).

Si la revisión de la integridad de las llaves es correcta, se procede a pedir la clave del presidente de casilla (figura 3.12), que corresponde a la llave distribuida para el distrito electoral correspondiente.

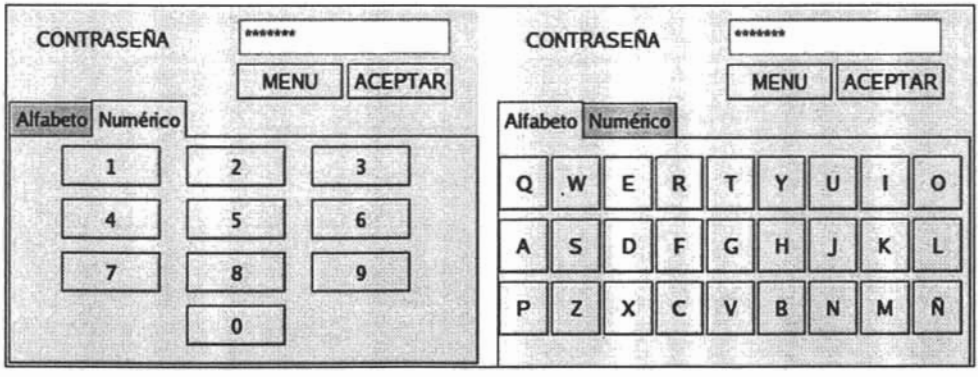

Figura 3.12: Panel Touch Screen para la introducción de contraseña alfanumérica.

Se utiliza esta contraseña para descifrar y verificar las firmas de los archivos que se van a cargar en la Urna Electrónica, estas firmas se encuentran incluidas en el dispositivo USB como se explicó en la etapa previa a la votación.

A continuación analizan los dispositivos de la Urna Electrónica, que finalizan con la impresión del diagnóstico (figura 3.13), apareciendo la fecha y hora de impresión.

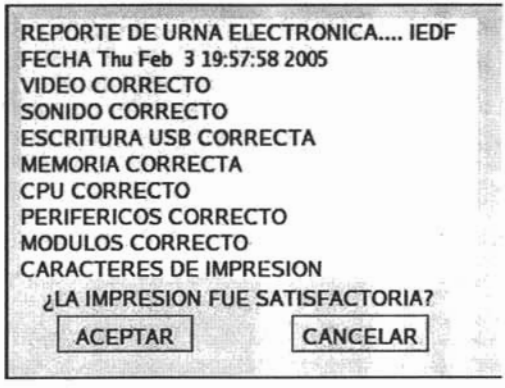

Figura 3.13: Reporte de diagnóstico de dispositivos.

En el caso de que algún dispositivo no funcione correctamente (se permiten 3 intentos) la Urna Electrónica se deshabilita enviando el mensaje correspondiente y se procede a sustituirla con una Urna Electrónica de contingencia.

Una vez que se pasó este punto, se procede a configurar la urna electrónica con los datos correspondientes a la sección y el tipo de casilla correspondiente. Para ello, se tienen que introducir estos datos por medio de dos pantallas (figura 3.14).

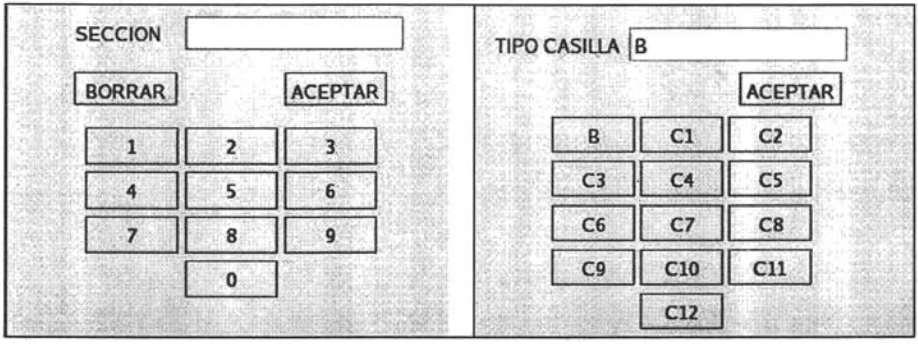

Figura 3.14: Captura de sección y tipo de casilla

Se introducen estos datos, el programa de Urna Electrónica procede a "filtrar" los datos específicos para esta sección, a partir de los archivos binarios que se encuentran en el dispositivo USB; resultado de la etapa de pre-votación.

Antes de hacer este proceso la aplicación de Urna Electrónica verifica la firma de los archivos binarios con la instrucción "gpg –verify archivo_binario". De igual manera, si no se cumple con la integridad de estos archivos, se deshabilita la Urna Electrónica. Los archivos filtrados se guardan en la unidad de almacenamiento físico interno de la Urna y la aplicación de Urna Electrónica pasa a un estado de espera en donde se habilitará el procedimiento de votación.

Activación de la urna para emisión del voto

Una de las problemáticas a solucionar en el proyecto, fue diseñar un mecanismo seguro de habilitación de la Urna Electrónica y permitir al ciudadano emitir su voto. Para llevar a cabo esta tarea se construyó un dispositivo activador con un PIC con conexión a la

Urna Electrónica al puerto serial, en lo que respecta a su diseño se tomaron las siguientes consideraciones:

1. Se debe permitir que el ciudadano emita un solo voto.
2. La urna electrónica estará deshabilitada para emitir el voto en todo momento en que no haya un ciudadano en la mampara.
3. La habilitación se hará desde la mesa de funcionarios por el presidente de casilla, previa identificación del elector.
4. Debe existir un indicador a vista de todos (funcionarios, representantes y observadores) del estado de la urna por medio de un semáforo de tres colores rojo, verde y amarillo(deshabilitada, habilitada para votar y tiempo de votación excedido).
5. En el caso de que se emita la señal de votación y el ciudadano se tarde más del tiempo preestablecido para emitir su sufragio se inhabilitará (no perderá las votaciones emitidas) y se emitirá un indicador amarillo. El presidente tomará la decisión, dependiendo si el ciudadano aún está presente, de darle otros noventa segundos para continuar con su votación. Si el ciudadano abandona la casilla y la luz está en amarilla, se activará por medio de una señal un proceso de limpia de sufragio y el mismo no será contado.

3.8 Esquema de seguridad en el envío del resultado de la votación

3.8.1 Seguridad en la transmisión

En cuanto a la Seguridad en la transmisión utilizada para el envió de los resultados de cada Distrito hacia el Centro de Operaciones de el Instituto Electoral del Distrito Federal estará basada en una Virtual Private Network (VPN).

Una VPN es una red privada construida sobre la infraestructura de una red pública (recurso público, sin control sobre el acceso de los datos), que normalmente es Internet.

Es decir, en vez de utilizarse enlaces dedicados (como el X.25 y Frame Relay) para conectar redes remotas, se aprovecha la infraestructura de Internet.

La principal motivación para la implantación de las VPN, es la financiera: los enlaces dedicados son demasiados caros, principalmente, cuando las distancias son largas. Por otro lado, existe Internet, que por ser una red de alcance internacional, cuenta con puntos de presencia diseminados por todo el mundo. Las conexiones con Internet tienen un costo más bajo que los enlaces dedicados, principalmente cuando las distancias son largas.

Internet es una red pública, donde los datos en tránsito pueden ser "leídos por cualquier equipo". La seguridad en la comunicación entre las redes privadas es imprescindible, se hace necesaria una forma de cambiar los datos codificados, de forma que si fuesen capturados durante la transmisión, no puedan ser descifrados. Los datos transitan codificados por Internet en "Túneles Virtuales" creados por dispositivos VPN que utilizan criptografía; y esos dispositivos que son capaces de "entender" los datos codificados forman una "red virtual" sobre la red pública.

Los dispositivos responsables para la formación y administración de la red virtual, para propiciar una comunicación con seguridad, deben ser capaces de garantizar:

1. La seguridad de los datos, en el caso que fuesen interceptados durante la transmisión, no pueden ser decodificados.
2. Integridad de los datos, además de no ser decodificados (seguridad), los datos no pueden ser modificados durante la transmisión.
3. La autenticación, garantiza de que los datos están siendo trasmitidos o recibidos del dispositivo remoto autorizado y no de un equipamiento cualquiera. Se tiene la certeza de que el con el cual fue establecido el túnel, es el dispositivo remoto autorizado y no otro equipamiento haciendose pasar por él.

3.8.2 Esquema de transmisión de datos

Una vez terminada la Jornada Electoral, los datos recavados en cada Urna Electrónica son recopilados por el distrito electoral encargado de recolectar dicha información de sus correspondientes Casillas.

Estos archivos serán enviados al IEDF por medio de un programa de transmisión que ocupara la VPN para comunicarse con el Instituto Electoral del Distrito Federal, en donde los recibirán para verificar la validez de los datos.

Para lograr el esquema de la información se necesitó de diferentes herramientas y tecnologías, para generar un correcto y seguro envió de la información, entre las cosas que contamos para la transmisión, está lo siguiente:

- Una Aplicación, la cual será la indicada para enviar los datos cifrados instalada en cada uno de los distritos electorales que, además, podrá almacenar localmente los resultados parciales.
- Una Virtual Private Network, una red privada que se extiende mediante un proceso de encapsulación y en su caso de cifrado de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.
- Una Base de Datos, capaz de almacenar todos y cada uno de los datos de los archivos cifrados enviados a través de la VPN.
- Una Aplicación, que recibirá esta información de forma segura para su almacenamiento en la Base de Datos.

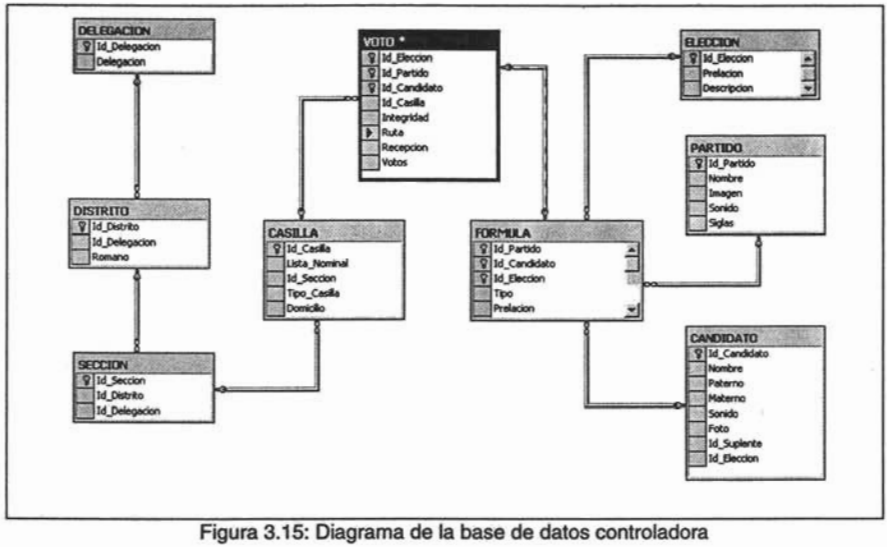

Figura 3.15: Diagrama de la base de datos controladora

Entre la aplicación distrital y el equipo integrador existirán mecanismos de software para verificar automáticamente la firma digital, haciendo uso de las llaves públicas de cada uno de los distritos electorales.

3.8.3 Autenticación de las transmisiones

La autenticación de las transmisiones se realizará usando de las llaves asimétricas de cada uno de los distritos electorales. Se comprobará la procedencia de cada archivo, verificado la respectiva llave del distrito que esta transmitiendo en ese momento y se encuentra en la base de datos de confianza de GnuPG, instalado en el equipo integrador.

Cada vez que se verifique la integridad de los archivos de las Casillas, se cambiará el valor de 0 a 1 del campo integridad en la tabla con nombre "VOTO"

Figura 3.16 Campo para registrar la integridad en la transmisión de los archivos.

De acuerdo a lo anterior, conoceremos los archivos de las casillas que han sido verificados en su integridad. Posteriormente, descifraremos todos y cada uno de los archivos de las Casillas para registrar los votos en la Base de Datos.

Gracias a todo este proceso, tendremos datos sobre los cuales es posible aplicar un conjunto de técnicas para obtener un resultado significativo del avance de los resultados en un lapso de tiempo bastante corto.

Capítulo 4

Comparativa entre esquemas de seguridad: programa PREP y propuesta de recopilación de datos electorales de una urna electrónica

El objetivo de este capítulo es determinar las diferencias y la efectividad de los esquemas de seguridad. Así como analizar las herramientas de seguridad utilizadas y arquitecturas de implementación. El esquema de transmisión segura que se plantea en ambas soluciones se analizará a detalle con el fin de determinar el grado de confianza en los datos finales, objetivo principal de ambos sistemas.
Además las diferencias demográficas y otras variables relacionadas con respecto a su impacto en el funcionamiento óptimo de ambos proyectos.

4.1 Análisis comparativo entre los dos esquemas de seguridad física.

Es importante hacer notar que el control de acceso a los sitios de programación de los diferentes módulos del PREP, adquiere una vital importancia porque se debe garantizar que el código ejecutable que estará instalado en todos los dispositivos TCR es seguro y no contiene código malicioso.

En el proyecto de Urna Electrónica, adquiere aún más relevancia debido a que el código involucrado interviene en más etapas de la votación. El éxito en la Urna Electrónica depende de los módulos programados en las tres etapas, la responsabilidad de salvaguardar la integridad de los datos y de los archivos ejecutables se triplica, dificulta el control de dicho sistema, lo que puede llegar a generar desconfianza en los ciudadanos, partidos políticos y candidatos. Si esto se llega a dar, se podría decir que el proyecto fracasó, porque una de los principales objetivos era mantener la confianza y transparencia en los procesos electorales. La solución resulta sencilla y requiere de cierto grado de participación, consiste en la realización de tres acciones:

- **Transparencia**: Debido a que todo el código reutilizado para este proyecto esta basado en la licencia GNU, es posible colocar a la vista de todos el código fuente y la documentación de las aplicaciones. Esto no quiere decir que se va tener acceso a los lugares físicos donde se codifican dichas aplicaciones. Una vez que está desarrollado el software y probado, se pone a la vista de todos el código fuente de las aplicaciones a implementar en las diferentes etapas de la votación.

- **Auditoría del código fuente**: Una vez terminado el desarrollo del software se procede a distribuir estos archivos fuente a todos aquellos interesados (principalmente partidos políticos) en revisar su funcionamiento, los cuales comprobarán que la finalidad del código sea aquél que está establecido en las características técnicas del proyecto y revisarán la inexistencia de algún código malicioso. En caso de haberlo se procede depurar dicho código y a repetir la auditoria. Una vez realizada la revisión de todos los interesados y que todos estén conformes con el resultado, se procede a compilar, a partir de este código fuente las aplicaciones finales. Ahora puede surgir la siguiente pregunta por parte de los auditores de éste código:¿Cómo sé que el código que me entregaste para que revisara, es el mismo que se va a compilar finalmente para su utilización en las Urnas Electrónicas?. La respuesta es sencilla, al mismo tiempo que se distribuyan los archivos fuente, se proporcionará junto con cada uno de ellos su

respectiva firma digital. En el momento de la compilación los auditores de código podrán realizar, si lo desean, el cálculo de las firmas digitales y compararlas con las firmas distribuidas para la revisión.

- **Auditablididad de datos:** Un esquema similar se debe seguir en la distribución de datos electorales para la auto-configuración de las Urnas Electrónicas:
  - Llevar a cabo el registro y captura de datos de partidos y candidatos. Cerrar dicho registro según marque la ley electoral (Tiempos y Requisitos).
  - Distribuir los archivos binarios para su revisión por parte de los interesados con sus respectivas firmas digitales.
  - Crear las copias en los dispositivos USB para su distribución a la vista de todos los interesados (auditores) y permitirles verificar las firmas digitales de los archivos binarios.

Además, estos datos se pueden revisar en el momento que se desee, junto con la operación de la Urna Electrónica examinando sus bitácoras de aplicación, las actas de apertura, y actas de escrutinio y cómputo.

Por otro lado, para la publicación de resultados en la parte exterior de la casilla, la realizarán los funcionarios de casilla a partir de las actas de escrutinio y cómputo que se imprimen en la etapa de votación, al cierre de la casilla. Lo anterior a la vista de los representantes y funcionarios de casilla, quienes verificarán que el cartelón fue llenado con los datos arrojados en dicha impresión del acta.

4.2 Análisis comparativo entre los dos esquemas de cifrado.

En este apartado se comparan los algoritmos y métodos criptográficos para el resguardo de su información y, además, el esquema empleado.

La capacidad de cómputo en los dispositivos de cada propuesta son muy diferentes el uno del otro. Las TCR's utilizadas para la captura de las actas del sobre PREP tienen un procesador de la familia Z80, el cual lo hace un dispositivo barato, pero con bajo

poder de cómputo. La capacidad de cómputo no es un factor importante en lo que se refiere a la captura de los datos electorales, simplemente, lo que hace es obtener la información para e integrarla en la base de datos. La terminal no requiere procesar una gran cantidad de datos, cada una de las actas se almacenan en 50 bytes, aproximadamente, de los cuales se debe generar un resumen con el algoritmo MD5, determinando que en cuanto a la capacidad de cómputo resultó ser suficiente para este tipo de algoritmo para verificar la integridad. El método de llave simétrica de la autenticación y cifrado en el PREP, la capacidad y velocidad del procesador resultó ser lo suficientemente capaz en la implementación de los algoritmos de cifrado sobre los archivos necesarios para autenticar la terminal, por otro lado es ésta sencillez de la arquitectura de las TCR's que las hacen baratas, confiables y fáciles de auditar. En otras palabras ¿Para qué tener más de lo que se va a utilizar realmente?, si los algoritmos de triple DES y MD5 comprobaron ser lo suficientemente confiables y con buen desempeño en las TCR's.

En el caso de la Uma Electrónica, se contaba con una mejor arquitectura de hardware para implementar el prototipo; en un principio, se analizó la posibilidad de llevarlo a cabo en una arquitectura Celaron; posteriormente, en dispositivos PALM y; finalmente, en un dispositivo PC104, que es un arquitectura de dispositivos embebidos para el área de control de procesos. Pero han llegado a evolucionar, tanto este tipo de computadoras que los conjuntos de circuitos (Chip set), se encuentran más desarrollados, incluso, cuentan con la misma cantidad de unidades funcionales que una PC de escritorio, a diferencia de tener frecuencias de procesamiento inferiores, regularmente entre 100 a 650 MHz.

El prototipo de Uma Electrónica se utilizó, específicamente, un procesador PXA255 con arquitectura ARM fabricado por INTEL y con una frecuencia 133 MHz, equivalente a un procesador 486, ésto permitió la implementación de algoritmos de cifrado computacionalmente más demandantes e, incluso, podemos decir que con bastante holgura en el procesamiento de datos. Por eso, se tomó la decisión de implementar claves asimétricas en este proyecto, teniendo como resultado buenos tiempos en el cifrado de la información, un factor de compresión, debido a la naturaleza de los

algoritmos. La facilidad de recompilar bibliotecas para arquitectura ARM permitió la ejecución de GnuPG (como ya se platicó en el capítulo 3), y con él, la capacidad de utilizar diferentes algoritmos de cifrado.
También se analizó la posibilidad de recompilar el Kernel 2.6 recién liberado, el cual cuenta con características de ahorro de energía, librerías de seguridad ya incluidas en el núcleo del sistema operativo.
Estas diferencias en el Hardware justifican las respectivas implementaciones de algoritmos de cifrado.

4.2.1 Esquema de generación de llaves criptográficas.

El proceso de generación de llaves criptográficas debe hacerse mediante mecanismos seguros. A continuación se mencionan las diferencias importantes en cuanto al proceso de generación de estas llaves en los dos proyectos.

En el caso del PREP se buscó simplificar este proceso, debido a que se utilizaron tarjetas inteligentes para almacenar estas llaves, el resguardo se realizaba de manera física y su distribución era cuestión de logística. En cambio en la Uma Electrónica la distribución de llaves fue de forma electrónica y la autenticación de éstas llaves se garantizan por medio de la creación de un círculo de confianza.

Otro punto importante a destacar es el método de creación de las claves criptográficas en el proyecto PREP, durante un evento llevado a cabo en las instalaciones de IFE y a vista de todos con fines de transparencia. Consistió en la creación de las llaves, utilizando una computadora sin disco duro y arrancando el sistema operativo desde un disco flexible con MS-DOS, se ejecutaron lo programas generadores de las claves digitales necesarias y se almacenaron en sólo un disco (flexible). Lo anterior da como resultado total confiabilidad, se tiene certeza de que no existe una copia al alcance de personas maliciosas.

Como vimos en el capítulo 3, existe una llave privada muy importante por resguardar, esta es la llave privada del equipo integrador. Para protegerla se recurre a la "frase contraseña" que requiere GnuPG. Se propuso que ésta estuviera en poder de tres personas diferentes y que cada una conociera sólo parte de la frase. Debido a que GnuPG permite introducir una "frase contraseña" de 15 caracteres alfanuméricos (incluso, más grande) se estipuló que al momento de crear la llave y, al solicitar dicha frase, tres personas diferentes introdujeran 5 caracteres cada uno de ellos. De la misma manera, se acordó para iniciar el equipo integrador, la introducción de dicha contraseña por parte de los tres y de esa manera mantener la llave en memoria para las respectivas tareas de descifrado de información y no fuera necesario guárdala en disco duro.

4.3 Análisis comparativo entre los dos esquemas de envío de información.

En este apartado analizaremos la metodología empleada en ambos sistemas para la comunicación entre los consejos Distritales y oficinas centrales, así como la verificación de la integridad y autenticación.

Ambos sistemas tienen una tarea en común, que es una de las más importantes de la jornada electoral: transmitir de manera segura los resultados electorales a las oficinas centrales del correspondiente Instituto Electoral del Distrito Federal.

Una diferencia importante está descrita en los dos esquemas de comunicación, mientras que en un escenario nacional, como es el caso del PREP, lo más adecuado para la transmisión entre los CEDAT's y el CENARREP era por medio de Modems. En lo que se refiere a la Urna Electrónica se hace por medio de una VPN, por cuestiones de costo. Este punto de ser posible, se debe invertir en la implementación de líneas dedicadas desde los distritos electorales hacia las oficinas centrales, de tal forma que se elimine la carga extra en la implementación de túneles de comunicación seguros, porque con el esquema de seguridad implementado es más que suficiente.

La segunda fase del proyecto de Urna Electrónica, consta de la construcción de 60 urnas semi-industriales con la finalidad de hacer pruebas piloto y determinar la

efectividad en el diseño de las diferentes etapas del proyecto. Las comunicaciones entre dispositivos van a jugar un papel importante en dichas pruebas, depende de éstas que la efectividad en el acopio de los datos sea la esperada.

4.3.1 Seguridad en la transmisión

Aunque la estructura de los datos es prácticamente el mismo, la forma en que se obtienen digitalmente es distinta como ya lo hemos visto. En el PREP con las TCR's y en la Urna Electrónica, automáticamente con una rutina de la aplicación que nos deja los resultados en una memoria flash. La autenticación del usuario en el PREP se llevó a cabo por medio de una programación intema de las terminales con una llave simétrica, además de la verificación de las claves del capturista y supervisor del CEDAT

En la Urna Electrónica se permite el envió de la información desde las oficinas Distritales sólo desde las computadoras que tienen su respectivo canal de comunicación en la VPN, tambien es posible verificar los archivos enviados con las firmas digitales adjuntas con GnuPG.

En ambos proyectos se tomaron en cuenta métodos de identificación física de los dispositivos empleados para la captura y envío de la información. En la Urna Electrónica es posible hacer esto verificando el número de serie de la memoria flash con un catálogo almacenado en la base de datos del equipo integrador.

4.4 Comparación en aspectos demográficos

La importancia de las diferencias demográficas en ambos sistemas es importante, debido a que el buen desempeño depende de la disponibilidad de servicios de comunicación.

Estas características demográficas que se mencionan en el primer capítulo, concluyen en que la Urna Electrónica encontrará dificultades en un escenario nacional, debido a la cantidad de variables que aportan las deficiencias en comunicaciones y, por otro lado, es posible implementar este proyecto en una entidad con una mejor infraestructura como lo es el Distrito Federal, escenario para el desarrollo de este proyecto. Aún con

estas dificultades, este proyecto puede madurar en entidades aisladas del país e ir expandiéndose, de tal forma, que se logre controlar las variables imprevistas, actualmente es un buen avance al buscar alternativas en la agilización de los comicios. En el caso del PREP, el transporte de los datos electorales se hace por medio de una línea telefónica y un Modem, sólo se debe tener especial cuidado en la calidad de la línea. El impacto de las dificultades demográficas en los diferentes esquemas son diferentes por razones muy visibles. En primer lugar, el aspecto de la recompilación de sobres prep. Comparándolo con la recompilación de los dispositivos USB, en cuanto a la Uma Electrónica. Aquí entran dos variables importantes a tomar en cuenta, la primera de ellas es el tiempo de vida útil de una memoria USB, es de 5 años de garantía[6] con un uso intensivo, lo cual nos obliga a verificar el estado de las memorias antes de cada elección y, eventualmente, sustituirlas por nuevas. Esto mismo les ocurre a las TCR's de el sistema PREP, cada vez que se va a llevar a cabo una elección se procede a probar y rehabilitar las terminales para adecuarla a la elección en turno.

Costos

Los costos en el desarrollo de los dos proyectos difieren, principalmente, por las características de hardware que se desprenden de las necesidades de cada uno de los proyectos. Como ya lo mencionamos, las TCR's tienen una arquitectura muy sencilla. Y por lo tanto, en el precio se ve reflejado una TCR nueva, específicamente, la utilizada en el PREP de 2003 marca Verifone, modelo Ovni 395, la cual fue resultado de una licitación. Tiene un costo aproximado de 267.5 dólares, con la ventaja de ser un dispositivo que es ampliamente usado en puntos de venta, bancos y negocios para el cobro. Esto permite que el respaldo y soporte técnico sea más fácil de adquirir. El desarrollo de Umas Electrónicas está planteado para ser desarrollada por un sistema embebido y, los costos de éste se incrementan por la cantidad de elementos necesarios (impresora, controladora de USB, tarjeta de audio, puerto serial, etc...) para el funcionamiento de la Urna.

Estos costos se pueden ver reflejados de la misma manera en la distribución de los distritos y su correlación con la cantidad de dispositivos necesarios. Por ejemplo, para

[6] http://www.intel.com/design/flash/leftnav/documentation.htm

cada distrito, en el último ejercicio del PREP, fueron necesarias 12 terminales de captura La Urna Electrónica establece el uso de una urna por cada sección electoral o, más de una, si dicha sección sobrepasa de 750 votantes. Estamos hablando de una diferencia de 12 terminales de captura contra 208 Urnas Electrónicas en promedio por cada distrito electoral. En el caso específico de una elección en el Distrito Federal, haciendo cuentas estimativas tenemos que la inversión para sólo un distrito de TCR's, nos daria 35,310 pesos y la inversión para Urnas Electrónicas sería aproximadamente de $1,040,000[7] pesos, tomando en cuenta que para tales cantidades, la construcción de dichas urnas deben ser de manera industrial, esto reduciría su costo dramáticamente.

[7] Esta cifra es aproximada y dependiendo de los dispositivos a implementar que aun pueden cambiar.

Conclusiones.

Ya analizadas las diferencias entre ambos sistemas podemos complementar una con otra; En primera instancia, una diferencia importante en los dos sistemas es la manipulación de datos. En el PREP se necesita hacer una captura manual de las actas electorales, la cantidad de gente involucrada es mayor, los mecanismos y herramientas de seguridad a implementar deben ser más meticulosos. Por su lado, la Urna Electrónica busca disminuir, lo más posible, el contacto humano directo con los datos electorales resultantes, automatizando los procesos que se llevan a cabo en la jornada electoral. Lo anterior, nos llevó a una nueva discusión: ¿Quién o cómo aseguramos que estos métodos de automatización son correctos y qué no se esta haciendo trampa?. Le respuesta a esta pregunta se encuentra en la inclusión de nuevas características en el funcionamiento de la Urna, descritas en el capítulo 3 y 4, cuyos resultados se resumen a continuación.

Mejoras al esquema de seguridad

Ampliación de los alcances de seguridad en etapas de construcción de Urnas Electrónicas.

Se determinaron las deficiencias en cuanto alcances de seguridad, es importante completarlos en caso de ser necesario.

Como parte de este análisis se discutió la posibilidad de modificación de los datos entre el proceso de escrutinio y cómputo e integración de los datos ¿Cómo aseguramos que el acta de escrutinio y cómputo contenido en la memoria USB es el mismo que se está entregando en las oficinas Distritales, o cómo verifico esa concordancia por medio de

algún mecanismo? La respuesta a esta necesidad, es la inclusión de la firma digital de el archivo del acta de escrutinio y cómputo al final de la impresión de cada acta. Recordemos que a cada acta se le calcula su firma digital y, una vez realizado el escrutinio, la Uma Electrónica pregunta cuántas copias impresas de esta acta se necesitan (uno por representante de partido y funcionarios de casilla).

Por otro lado, de los partidos políticos tienen la capacidad de corroborar los datos electorales comparando las firmas digitales de la boleta impresa en su poder y la firma Electrónica calculada por el programa de recepción de resultados electorales.

Este mismo mecanismo se puede implementar en otra etapas en donde se firman digitalmente archivos, lo que permite dar mayor confiabilidad del proyecto de Uma Electrónica. Por ejemplo, en el caso de entrega de los archivos binarios en el dispositivo USB al presidente de casilla, una vez que se proceda a iniciar la Uma Electrónica, a partir de los datos contenidos en la USB, se calcula la firma digital y se muestra en pantalla, para que sea verificada con la firma digital impresa.

Establecer un mecanismo de creación de llaves criptográficas de manera segura.

En el caso de Uma Electrónica, cómo se encuentra en etapa de prototipo aún, no se establece el procedimiento para crear las claves Electrónicas de manera segura. En el PREP se hace tomando consideraciones, por ejemplo generarlas en un equipo sin disco duro, se generan las llaves y solamente se almacenan en un solo dispositivo de almacenamiento para construir las tarjetas controladoras. Se establece un mecanismo para la generación de las llaves criptográficas para la Uma Electrónica, proponemos que la creación de las claves se realice a la vista de todos y contraseña GnuPG que protege las llaves deb estar distribuida en que solo tres personas,cada uno de estos individuos conocerá una parte de la contraseña (frase secreta en el caso de GnuPG, que protege a las llaves asimétricas), de tal forma que solamente cuando estas tres personas ingresen su parte de la contraseña en el sistema se podrá descifrar la información. Si no se pueden descifrar los archivos recibidos, los datos no se pierden,

solamente no es posible leerlos para su integración en la base de datos.

Establecimiento de una infraestructura de llaves públicas (PKI) en el proyecto de Urna Electrónica.

Recurriendo a la utilización de CAs (entidades certificadoras), es posible instalar un sistema de claves públicas, que permita efectuar la autenticación efectiva (a través de certificados digitales), cifrar y autenticar información mediante la firma digital creada utilizando las claves construidas en la etapa de pre-votación.

Estos sistemas disponen de mecanismos para generar y recuperar claves, revisten gran importancia, una vez que se pierde una clave. El efecto para el usuario puede ser de un nivel de gravedad importante, dado que el resultado predecible es la pérdida del acceso a la información cifrada y, por tanto, es necesario implementar una infraestructura de este tipo. Como en el caso de la Urna Electrónica en el Distrito Federal, se contara con una clave en el equipo integrador y un par de llaves para cada una de las 40 Juntas Distritales, como están conectadas en una red privada (WAN) es posible implementar la entidad certificadora en las oficinas centrales del IEDF y solamente se utilizará esta infraestructura para la transmisión de datos.

Seguridad física de los sitios de programación.

Aunque el código del software final a implementar en las Urnas Electrónicas debe estar a la vista de todos, por motivos de transparencia, se debe resguardar el código original y físicamente los lugares en donde se construye. Los mecanismos para autenticar los archivos ejecutables de dicho código ya está implementado, pero no podemos dejar a un lado el resguardo físico, porque si no se hace esto, una tercera persona podría modificar el código a su conveniencia, generando los archivos de autenticación que serían tomados por el sistema como correctos. Es por eso que se implementará en la siguiente etapa de la Urna Electrónica, el control de acceso a sitios donde se esté programando las aplicaciones para las tres etapas de la Urna Electrónica. Esta segunda etapa consta de la construcción de 60 Urnas semi-industriales con el fin de realizar una prueba piloto que servirá, en un principio, para verificar las características del proyecto.

Desde el punto de vista de seguridad se buscarán posibles debilidades y se popondrán y/o proponer soluciones en caso de que sea necesario.
En una tercera etapa, cuyo objetivo será la construcción de un número mayor de Urnas Electrónicas industriales (por medio de una licitación), se trabajará un mecanismo de prueba del hardware, equivalente a la verificación del software que en la presente tesis se planteó.

presenten el análisis de ambos sistemas, del presente trrabajo se ha detectado la diferencia en el número de variables a controlar, desde un punto de vista general y de seguridad. La logística de la distribución de aproximadamente 11,123 Urnas Electrónicas no es trivial, a diferencia de la distribución, en promedio, de 12 terminales de captura que servirán para acopiar datos de más de 17 secciones por terminal. En el esquema de autenticación del PREP, estamos hablando de la generación de 1020 llaves simétricas y no de los 41 par de llaves asimétricas del proyecto de Urna Electrónica, lo cual permite que su administración y distribución sea más sencillo desde el punto de vista informático.

El tiempo promedio en el que un votante debe efectuar su sufragio es de 60 segundos(tiempo ideal) sin importar que se cuente con una afluencia constante durante todo el día. Desgraciadamente, en la práctica la afluencia es intermitente, habrá momentos en que se conglomerará la Urna para emitir el voto. En primera instancia, porque el proceso de votar con una Urna Electrónica es conceptualmente más fácil, pero el promedio de gente que no a utilizado una computadora, aumentará el promedio real de tiempo de emisión del voto.

El objetivo de la segunda etapa del proyecto de Urna Electrónica es determinar esas variables y buscarle soluciones efectivas, principalmente, para la agilización en la emisión del voto, además de concientizar a las personas de la importancia de tener presentes estos aspectos y tomar acciones necesarias para que el proyecto no fracase.

La confianza en los procesos electrónicos de acopio de información debe ser total, en ambos casos existirá la capacidad de que los ciudadanos sigan, momento a momento, el avance de los resultados acopiados. Pero quién le asegura a los ciudadanos que esos datos son íntegros y que no han sido modificados a conveniencia por alguien en el transcurso de la jornada electoral. En primera instancia el ciudadano debe tener una "confianza ciega", pero esto no es suficiente. Por lo tanto, se establecieron mecanismos para quien desee revisar el código y la seguridad del proceso, lo pueda hacer con toda libertad y, de tal manera, que no quede duda de la autenticidad de:

- Los datos de los partidos y los candidatos distribuidos son los originales y no han sufrido cambio alguno, se utilizó la firma digital para verificar la información.
- El programa realiza lo que conceptualmente debe hacer, es decir, verifica que no haya modificaciones en el código que puedan beneficiar a algún partido o candidato. La solución es la apertura del código fuente para la revisión, implementando de igual manera el uso de firmas digitales.
- Los resultados extraídos de la Urna Electrónica, de la jornada electoral, se logra con el uso de cifrado con llave asimétrica y firma digital, actualmente ,implementado con GnuPG.
- Los datos publicados en el exterior de la casilla, una vez finalizada la jornada electoral, son los mismos que se extrajeron de la Urna Electrónica; además ser congruentes con los publicados hacia el público en general (sitios web). Esta actividad se logra imprimiendo la firma digital en el acta de escrutinio y cómputo, para futura verificación de las casillas.
- Los resultados que están en la base de datos central son congruentes con los publicados en los sitios de difusión.

Por lo anterior podemos observar que el programa PREP tiene una historia que contar, ha madurado bastante y los resultados son cada vez más rápidos. Esta experiencia puede ser utilizada en la etapa de acopio de resultados del proyecto de Urna Electrónica, que es un proyecto joven, se necesita trabajar más y concientizar poco a poco el uso de dichos dispositivos.

En resumen, tenemos las siguientes conclusiones:

Es posible lograr la confianza de la ciudadanía en este tipo de proyectos si las cosas se hacen de manera correcta y a la vista de todos. Un punto fuerte de estos proyectos es la inclusión de entidades educativas para asegurar el buen funcionamiento de los mismos.

La utilización de software libre permite la inspección a fondo del código, de tal forma que no es necesario pagar derechos de autor para buscar algún código malicioso en él. Además, permite la adecuación del sistema operativo al proyecto (Urna Electrónica) al contar con el código fuente de Linux.

Los esquemas planteados para la recopilación de datos son los adecuados a cada proyecto, en el caso de PREP se demostró que la utilización de las TCR's era lo más conviene porque se trata de un sistema para un entorno federal y los recursos demandados en el cifrado de información eran los suficientes. Para la Urna Electrónica, el esquema de integración de datos por medio de dispositivos de almacenamiento portátil permite que estos no sean manipulados, se asegura su integridad utilizando firmas digitales y cifrado asimétrico.

La seguridad de procesos electorales con Urnas Electrónicas inicia desde la construcción de las mismas, hasta la publicación de los resultados. Para ello, se deben especificar políticas y, posiblemente, un estándar mexicano para la revisión de seguridad informática en Urnas Electrónicas. En diferentes entidades del país cuentan con propuestas propias de Urna Electrónica.

Es posible incluir características de seguridad del proyecto PREP al proyecto de Uma Electrónica, el más importante fue la inclusión de seguridad física en lugares de programación y construcción de componentes.

No nos queda la menor duda que en un futuro el uso de Urnas Electrónicas será tan natural para un ciudadano, no habrá inconvenientes en su implementación, sólo que depende de la integración de otros estados en la participación de este proyecto para lograrlo, obviamente, no será en un periodo corto de tiempo. Otros países ya están

haciendo ejercicios reales, con los cuales se ha aprendido que es posible llevar a cabo una jornada electoral mediante Urnas Electrónicas de manera segura.

En general, la viabilidad del proyecto de Urna Electrónica es a mediano plazo y se recomienda introducir su utilización de modo paulatino, realizando ejercicios y analizando la tarea del usuario.

Trabajo Futuro

Como lo comentamos en los primeros capítulos, el proyecto de Urna Electrónica forma parte de un convenio de participación entre dependencias educativas como el Instituto Politécnico Nacional (IPN), la Universidad Autónoma Metropolitana (UAM) y la Universidad Nacional Autónoma de México (UNAM), con el Instituto Electoral del Distrito Federal (IEDF); dividida en fases, la primera (tema de esta tesis) con término en diciembre del año pasado. La segunda, que está iniciando al momento de escribir estas líneas, tiene como objetivo la creación de 60 Urnas semi-industriales para pruebas piloto; A diferencia de la primera fase, estas Urnas serán construidas en colaboración por parte de las 4 instituciones arriba mencionadas.

Las características de estas 60 Urnas son el resultado de la revisión de las diferentes soluciones propuestas en cada entidad educativa, les realizaron pruebas a los prototipos entregados por parte de la Unidad Informática del IEDF; Para organizar esta colaboración, entre grupos de trabajo, se determinaron las mejores propuestas de las instituciones y se le asigno a cada una su responsabilidad de la siguiente forma:
El IPN desarrollará la parte de hardware de la Urna, incluyendo el habilitador de la Urna e integrará todos los componentes dentro de la carcasa.
La UNAM desarrollará la carcasa y revisará la seguridad informática de la Urna Electrónica, incluyendo la revisión de estándares y el software base.
La UAM se encargará del aseguramiento de calidad del software y del desarrollo de los procedimientos técnicos.

La Unidad de Informática del IEDF, como responsable de la integración de todo el proyecto, desarrollará el software de la Urna y se encargará del dispositivo de identificación de votantes.

Bibliografía

[1] GUERRA Ortiz Victor, Dr. Alberto Alonso y Coria, Lic. Jorge Carreto sangines. "Programa de resultados Preliminares". Instituto Federal Electoral – Universidad Nacional Autónoma de México., Mexico 1999.

[2] FISH, Eric A., White Gregory B., "Secure computer and networks, analysis and design implementation", CRC Press. USA 2000.

[3] NASH Andrew, William Duane, Celia Joseph, Derek Brink. "PKI: Infraestructura de Claves Públicas", Osborne McGraw Hill. 2003.

[4] HARLOW Erick,"Desarrollo de Aplicaciones Linux Con Gtk y Gdk+", Prentice Hall 1999. ISBN: 8483221969

[5] GOERZEN John,"Linux programming bible", IDG Books Foster City, USA 2000

[6] FUJIOKA, A, Okamoto, T., and Ohta, K. A practical secret voting scheme for large scale elections. In *Advances in Cryptology - AUSCRYPT '92*, Springer-Verlag, Berlin. 1993

[7] Lorrie Faith Cranor, Electronic Voting,Crossroads ACM - Computer Security, 1997

[8] Eric A. Fischer,Election Reform and Electronic Voting Systems DREs):Analysis of Security Issues,ACM Noviembre 2003.

Referencias de internet

ARCOM empresa de dispositivos PC-104
http://www.arcom.com/devkit-linux-viper.htm

Manual de funcionario de casilla 2002 – 2003 IFE

http://www.ife.org.mx/InternetCDA/BibliotecaVirtual/

Historia del Instituto Federal Electoral

http://www.ife.org.mx/InternetCDA/MenuSuperior

Datos demográficos 2003, INEGI

http://www.e-mexico.gob.mx/wb2/eMex/eMex_INEGI__Estadisticas_sociodemograficas