

MINUTA DE LA SEGUNDA SESIÓN EXTRAORDINARIA DE LA COMISIÓN DE ORGANIZACIÓN Y GEOGRAFÍA ELECTORAL

En la ciudad de México, a las 11 horas 14 minutos del día 25 de febrero del año 2005, en las instalaciones del Instituto Electoral del Distrito Federal, ubicadas en la calle de Huizaches No. 25, Colonia Rancho Los Colorines, delegación Tlalpan, dio inicio la segunda sesión extraordinaria de la Comisión de Organización y Geografía Electoral.

LISTA DE ASISTENTES.

María Elena Homs Tirado	Consejera Electoral, Presidenta de la Comisión de Organización y Geografía Electoral.
Bernardo Fernández del Castillo Sánchez	Consejero Electoral, integrante de la Comisión.
Rubén Lara León	Consejero Electoral, integrante de la Comisión.
Iván Huesca Licona	Director Ejecutivo de Organización y Geografía Electoral.
Rodolfo Torres Velázquez	Titular de la Unidad de Informática.
Delia G. del Toro López	Secretaria de la Comisión.

1.- PRESENTACIÓN Y, EN SU CASO, APROBACIÓN DEL PROYECTO DE ORDEN DEL DÍA.

1.- Presentación y, en su caso, aprobación del Proyecto de Orden del Día.

2.- Presentación de las características técnicas del modelo propuesto de urna electrónica integrado por la Unidad de Informática del Instituto Electoral del Distrito Federal.

3.- Presentación y, en su caso, aprobación del "Proyecto de Informe que presenta la ~~Comisión de Organización y Geografía Electoral al Consejo General del Instituto Electoral del Distrito Federal~~ sobre las acciones realizadas para el diseño de una urna electrónica para el ejercicio del voto de los ciudadanos (ACU-696-03 y ACU-018-04) en el periodo del 31 de octubre de 2003 al 25 de febrero de 2005".

4.- Presentación y, en su caso, aprobación del "Anteproyecto de acuerdo que presenta la Comisión de Organización y Geografía Electoral al Consejo General del Instituto Electoral del Distrito Federal, por el que se aprueban las características técnicas del modelo de urna electrónica integrado por la Unidad de Informática, que servirán de base para la producción semi-industrial de sesenta urnas electrónicas; y se autoriza continuar con las etapas de experimentación y pruebas con estos equipos".

1.- PRESENTACIÓN Y, EN SU CASO, APROBACIÓN DEL PROYECTO DE ORDEN DEL DÍA.

Al no haber intervenciones se tomó, por unanimidad, el siguiente acuerdo:

34-E2-05.- Se aprueba el orden del día.

2.- PRESENTACIÓN DE LAS CARACTERÍSTICAS TÉCNICAS DEL MODELO PROPUESTO DE URNA ELECTRÓNICA INTEGRADO POR LA UNIDAD DE INFORMÁTICA DEL INSTITUTO ELECTORAL DEL DISTRITO FEDERAL.

Para el desahogo de este y los puntos posteriores, con fundamento en el artículo 11 segundo párrafo del Reglamento de Sesiones de las Comisiones del Consejo General del Instituto Electoral del Distrito Federal, se aprobó la participación del Lic. Iván Huesca Licona, Director Ejecutivo de la Dirección Ejecutiva de Organización y Geografía Electoral, y del Dr. Rodolfo Torres Velázquez, titular de la Unidad de Informática.

El Dr. Rodolfo Torres Velázquez, titular de la Unidad de Informática, presentó las características del modelo de urna electrónica (diseño base) integrado con las propuestas de los prototipos desarrollados por las instituciones de educación superior con las que el Instituto Electoral del Distrito Federal firmó convenios específicos de colaboración (Universidad Nacional Autónoma de México, Instituto Politécnico Nacional, Universidad Autónoma Metropolitana e Instituto Tecnológico de Estudios Superiores de Monterrey campus Ciudad de México) y las aportaciones de la Unidad de Informática; asimismo, explicó que las actividades siguientes son la producción de los 60 equipos semi-industriales y su correspondiente verificación en campo.

Posteriormente mostró el funcionamiento del modelo presentado en sus etapas antes, durante y después de la jornada electoral y los modelos de carcasas propuestas por las referidas instituciones de educación superior.

Tomando como base la opinión técnica del Dr. Rodolfo Torres Velázquez, en el sentido que el modelo de urna presentado reúne las características consideradas en los acuerdos del 30 de octubre de 2003 (ACU-696-03) y del 23 de marzo de 2004 (ACU-018-04) del Consejo General del Instituto Electoral del Distrito Federal y observando su funcionamiento en las etapas referidas en el párrafo precedente, los integrantes de la Comisión coincidieron en la importancia de informar al Consejo General sobre el avance en el cumplimiento a los acuerdos de referencia y dar a conocer este diseño base de urna electrónica, con la precisión que dicho diseño no es

definitivo y tampoco el que necesariamente podría ser utilizado en una elección constitucional o de participación ciudadana, porque primero se tendrá que probar y validar en campo su funcionamiento y la logística operativa que le acompañaría.

Asimismo, se concluyó que esta Comisión tiene la atribución de continuar con las acciones que la lleven al diseño definitivo de una urna electrónica para el ejercicio del voto de los ciudadanos.

Por lo anterior, los integrantes de la Comisión convinieron en autorizar a la Unidad de Informática a llevar a cabo los trámites necesarios para la producción semi-industrial de hasta 60 equipos, tomando como referencia las características técnicas del diseño base elaborado por esa área, así como continuar con las etapas de experimentación y pruebas en coordinación con la Dirección Ejecutiva de Organización y Geografía Electoral y las demás áreas del Instituto involucradas. Asimismo, mantener informado al Consejo General del Instituto Electoral del Distrito Federal sobre los avances del proyecto y, en su oportunidad, presentar el informe integral sobre la viabilidad de utilizar urnas electrónicas en procesos electorales y de participación ciudadana en el Distrito Federal.

Al no haber más comentarios se tomaron, por unanimidad, los siguientes acuerdos:

35-E2-05.- La Comisión se da por enterada de las características técnicas del diseño base de urna electrónica institucional, elaboradas por la Unidad de Informática a partir de la integración de las propuestas presentadas por las instituciones de educación superior con las que el Instituto Electoral del Distrito Federal suscribió convenios específicos de apoyo y colaboración: la Universidad Nacional Autónoma de México, el Instituto Politécnico Nacional, la Universidad Autónoma Metropolitana y el Instituto Tecnológico y de Estudios Superiores de Monterrey campus Ciudad de México, conforme al anexo "Características técnicas del modelo propuesto de urna electrónica integrado por la Unidad de Informática del Instituto Electoral del Distrito Federal" que consta de 46 fojas y que forma parte integral de esta minuta.

36-E2-05.- La Comisión, con fundamento en los acuerdos del Consejo General del 30 de octubre de 2003 (ACU-696-03) y 23 de marzo de 2004 (ACU-018-04), autoriza a la Unidad de Informática para que se inicie con la producción de hasta 60 urnas electrónicas con las características del diseño base presentado en esta sesión, conforme al anexo "Características técnicas del modelo propuesto de urna electrónica integrado por la Unidad de Informática del Instituto Electoral del Distrito Federal" que consta de 46 fojas y que forma parte de esta minuta, en el entendido que estos equipos no constituyen necesariamente el prototipo final que sería utilizado en ejercicios vinculantes porque aún necesitan ser probados y afinados los detalles de su operación.

37-E2-05.- La Comisión, con fundamento en los acuerdos del Consejo General del 30 de octubre de 2003 (ACU-696-03) y 23 de marzo de 2004 (ACU-018-04), autoriza a la Unidad de Informática para que, en coordinación con la Dirección Ejecutiva de Organización y Geografía Electoral y demás áreas involucradas en el proyecto de diseño de urna electrónica, continúe con las etapas de experimentación y pruebas, técnicas y logísticas, con los equipos que serán fabricados en términos del acuerdo 36-E2-05 de esta Comisión.

3.- PRESENTACIÓN Y, EN SU CASO, APROBACIÓN DEL "PROYECTO DE INFORME QUE PRESENTA LA COMISIÓN DE ORGANIZACIÓN Y GEOGRAFÍA ELECTORAL AL CONSEJO GENERAL DEL INSTITUTO ELECTORAL DEL DISTRITO FEDERAL SOBRE LAS ACCIONES REALIZADAS PARA EL DISEÑO DE UNA URNA ELECTRÓNICA PARA EL EJERCICIO DEL VOTO DE LOS CIUDADANOS (ACU-696-03 Y ACU-018-04) EN EL PERIODO DEL 31 DE OCTUBRE DE 2003 AL 25 DE FEBRERO DE 2005".

Como consecuencia de lo resuelto en el punto anterior los integrantes de la Comisión decidieron reformular el informe que se presentará al Consejo General sobre los avances en el cumplimiento de los acuerdos ACU-696-03 y ACU-018-04, para su aprobación en su siguiente sesión ordinaria.

Al no haber más intervenciones se tomaron, por unanimidad, los siguientes acuerdos:

38-E2-05.- Se da por recibido el documento "Informe que presenta la Comisión de Organización y Geografía Electoral al Consejo General del Instituto Electoral del Distrito Federal, sobre las acciones realizadas para el diseño de una urna electrónica para el ejercicio del voto de los ciudadanos (ACU-696-05 y ACU-018-05), en el período del 31 de octubre de 2003 al 25 de febrero de 2005", al cual se incorporarán las observaciones presentadas durante la sesión.

39-E2-05.- Se aprueba informar al Consejo General del Instituto Electoral del Distrito Federal del avance en los trabajos desarrollados por la Comisión en el proyecto de diseño de una urna electrónica, señalados en los acuerdos del máximo órgano de dirección del 30 de octubre de 2003 (ACU-696-03) y 23 de marzo de 2004 (ACU-018-04).

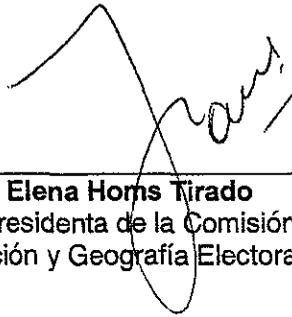
4.- PRESENTACIÓN Y, EN SU CASO, APROBACIÓN DEL "ANTEPROYECTO DE ACUERDO QUE PRESENTA LA COMISIÓN DE ORGANIZACIÓN Y GEOGRAFÍA ELECTORAL AL CONSEJO GENERAL DEL INSTITUTO ELECTORAL DEL DISTRITO FEDERAL, POR EL QUE SE APRUEBAN LAS CARACTERÍSTICAS TÉCNICAS DEL MODELO DE URNA ELECTRÓNICA INTEGRADO POR LA UNIDAD DE INFORMÁTICA, QUE SERVIRÁN DE BASE PARA LA PRODUCCIÓN SEMI-INDUSTRIAL DE SESENTA URNAS ELECTRÓNICAS; Y SE AUTORIZA CONTINUAR CON LAS ETAPAS DE EXPERIMENTACIÓN Y PRUEBAS CON ESTOS EQUIPOS".

Para el desahogo de este asunto y derivado de lo acordado en el punto dos del orden del día, este anteproyecto de informe que había sido solicitado antes de conocer el diseño base, se utilizará como insumo informativo del "Informe de avance en los trabajos desarrollados por la Comisión de Organización y Geografía Electoral en cumplimiento a los acuerdos del Consejo General del 30 de octubre de 2003 (ACU-696-03) y 23 de marzo de 2004 (ACU-018-04)", por lo que se tomó, por unanimidad, el siguiente acuerdo:

40-E2-05.- Para efectos del seguimiento de acuerdos de esta Comisión, se da por recibido el "Anteproyecto de acuerdo que presenta la Comisión de Organización y Geografía Electoral al Consejo General del Instituto Electoral del Distrito Federal, por el que se aprueban las características técnicas del modelo de urna electrónica integrado por la unidad de informática, que servirán de base para la producción semi-industrial de sesenta urnas electrónicas; y se autoriza continuar con las etapas de experimentación y pruebas con estos equipos", elaborado por la Dirección Ejecutiva de Organización y Geografía Electoral

Agotado el orden del día, se determinó levantar la sesión a las 14 horas 5 minutos del 25 de febrero de 2005.

Firmas



María Elena Horns Tirado
Consejera Presidenta de la Comisión de
Organización y Geografía Electoral



Bernardo Fernández del Castillo S.
Consejero integrante de la Comisión de
Organización y Geografía Electoral



Rubén Lara León
Consejero integrante de la Comisión de
Organización y Geografía Electoral

ANEXO

“Características técnicas del modelo propuesto de urna electrónica integrado por la Unidad de Informática del Instituto Electoral del Distrito Federal.”

(Incluye las características que debe cumplir la urna electrónica acorde a los señalado por el acuerdo ACU-696-03 y sus especificaciones técnicas)



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

**CARACTERÍSTICAS TÉCNICAS DEL MODELO PROPUESTO
DE URNA ELECTRÓNICA INTEGRADO POR LA UNIDAD
DE INFORMÁTICA DEL INSTITUTO ELECTORAL DEL
DISTRITO FEDERAL
(ANEXO)**

UNIDAD DE INFORMÁTICA

Febrero 21, 2005



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

México DF, a 21 de Febrero de 2005.

CARACTERÍSTICAS TÉCNICAS DEL MODELO PROPUESTO DE URNA ELECTRÓNICA INTEGRADO POR LA UNIDAD DE INFORMÁTICA DEL INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

2.1 Componentes de Hardware y Sistema Operativo

Tarjeta principal:

- Procesador: Intel PXA255, tecnología RISC, 32 bits, 400MHz.
- Procesador complementario: SA-1111 StrongARM para controlar el USB maestro y dar soporte a PCMCIA y Compact Flash.

Tarjeta secundaria:

- Interface de video: LCD a color XGA (1024x768).
- Conector del backlight: controlado por software con PWM + ON/OFF.
- Interface de touch screen: 4 ó 5 alambres.
- Interface Compact Flash: Conector Tipo II.
- Interface PCMCIA Tipo II
- Regulador integrado.
- Memoria Caché de 32 KB.
- Memoria del sistema: SDRAM de 64 MB 3.3V.
- Memoria Flash: 32 MB.
- Reloj de tiempo real con respaldo de batería.
- Voltaje de alimentación: 5v (1.5W) a 15 V.
- 3 puertos seriales RS232 de 3, 5 y 9 alambres, 3.3V CMOS.



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

- Puerto para panel plano.
- Soporte de teclado externo PS/2.
- 10 puertos configurables de I/O digitales.
- Codec de audio.
- Entrada de micrófono.
- Salida estéreo de 100 mW por canal.
- Boot ROM con imagen de Debian Linux (última versión)
- Dimensiones: 3" x 5" (76.2mm x 127 mm).
- 2 puertos USB Master Hub.

Pantalla:

- Pantalla de LCD de color activo de 6.4" (16 cm)
- Resolución: 640 x 480
- Dot pitch: 0.204 x 0.202 mm (H x V)
- Área activa 130.6 x 97mm (H x V)
- Voltaje de entrada: 5 vcd
- Corriente típica/máxima: 250 / 360 mA
- Tipo de backlight: CCFT
- Tipo de conector DF9MA-31P-1V
- Touch screen resistivo de 6.4"
- Bus de 4 cables
- Inversor CCFT de una y/o dos lámparas (de acuerdo con especificaciones del LCD).
- Voltaje de entrada 9.6-14.4 vdc
- Corriente máxima: 1.2 A



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

- Potencia de salida máxima: 3.9 Watts @ 12 vcd
- Dimensiones: 20mm x 130 mm x 13.5 mm
- Frecuencia típica: 60 kHz
- Cable del LCD. (compatible con salida de tarjeta multipuerto)
- Cable del inversor. (compatible con salida de tarjeta multipuerto)
- Cable del touch screen. (compatible con salida de tarjeta multipuerto)

Impresora y tarjeta controladora.

Impresora:

- Tipo térmica
- Inserción de papel frontal
- Capacidad de corte de papel completo
- Estructura de puntos: 384 puntos/línea
- Dot pitch (horizontal): 0.125 mm (8 puntos/mm) - Dot density
- Dot pitch (vertical): 0.125 mm (8 puntos/mm) – Line feed pitch
- Área efectiva de impresión 48 mm
- Número de columnas: ANK 32 columnas/línea (máximo tamaño de fuente 12 x 24 puntos)
- Velocidad en el puerto serial (bauds): 9600, 19200, 38400, 57600, 115200 (default), 230400, 460800.
- Control de flujo: ninguno, hardware (default), Xon/Xoff.
- Ancho de papel: 58 mm
- Grueso de papel: 60 a 80 μ m
- Velocidad de impresión: 60 mm/seg. (480 puntos línea/seg.) a 8.5v
- Tipo de caracteres: Alfanuméricos, kana: 159 tipos



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

- Caracteres internacionales: 195 tipos
- JIS Kanji: aprox. 6800 tipos
- Dimensiones del carácter:
 - 12 x 24 puntos, 32 columnas
 - 24 x 24 puntos, 16 columnas
 - 8 x 16 puntos, 48 columnas
 - 16 x 16 puntos, 24 columnas
- Interface Conforme a RS232/Centronics
- Voltaje de Alimentación:
 - Para cabezal: 4.2 – 8.5 vdc
 - Para motor: 4.2 – 8.5 vdc
 - Para cortadora: 5 vdc
 - Para tarjeta lógica: 5 vdc
- Dimensiones con cortadora: 83.5 x 43 x 26.4 mm
- Peso: aprox. 120 g

Tarjeta controladora:

- Velocidad de impresión por cable serial, USB e IRDA: 80 mm/seg.
- Compatible con Windows NT, XP, 2000, 98 y Linux
- Voltaje de alimentación: 6 – 8.5 vdc
- Interface para cortadora, sensor de papel atorado y de término de papel.
- Interface IRDA, Serial (9.6 a 921 Kbaud) y USB 1.1
- Compatible para el tipo de impresora térmica
- Cables de interfase serial y alimentación incluidos

Batería

- Tipo: Recargable de Plomo Ácido Sellada (SLA – Sealed Lead Acid).
- Número de celdas = 6 en serie (2V por celda).
- Voltaje nominal (V_{nominal}) = 12V.
- Capacidad nominal (C_{nominal}) = 21AH.
- Peso = 6Kg.
- Resistencia interna = 0.008 Ohms.
- Retención de carga: 97% - 1 mes, 91% - 3 meses, 83% 6 meses.
- Ciclo de carga: 14.4 a 14.7V a 6A.
- Tiempo máximo de almacenamiento: 6 a 9 meses antes de que se sulfate.
- Voltaje de corte = 10.5V

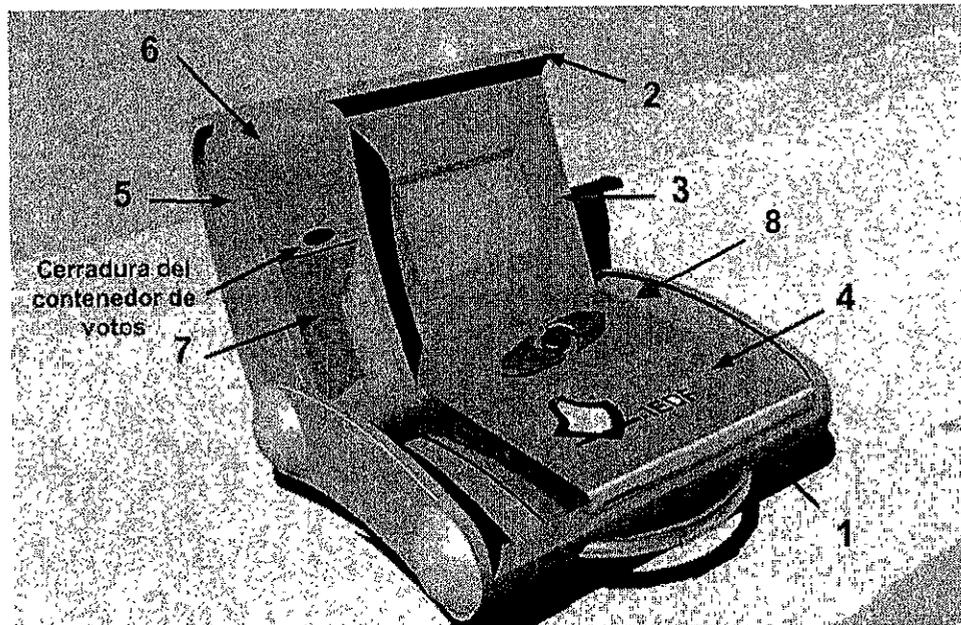
Cubierta exterior

- Diseño ergonómico.
- Sencilla.
- De fácil manejo, para su traslado y almacenamiento.
- Estética.
- Dimensiones apegadas a las requeridas por el IEDF.
- Herméticamente sellada.
- Resistente a los impactos.
- Estabilidad química y térmica.
- Superficie lisa.



- Mantenimiento sencillo.

Las partes del gabinete serán construidas por medio de procesos de inyección de plástico en ocho piezas como se ilustra en la siguiente imagen:



Donde:

1. Base.
2. Cubierta abatible exterior.
3. Cubierta de la pantalla de LCD.
4. Cubierta abatible del hardware y batería.
5. Contenedor de la impresora.
6. Cubierta abatible de acceso a la impresora y rollo de papel.
7. Contenedor de los votos.

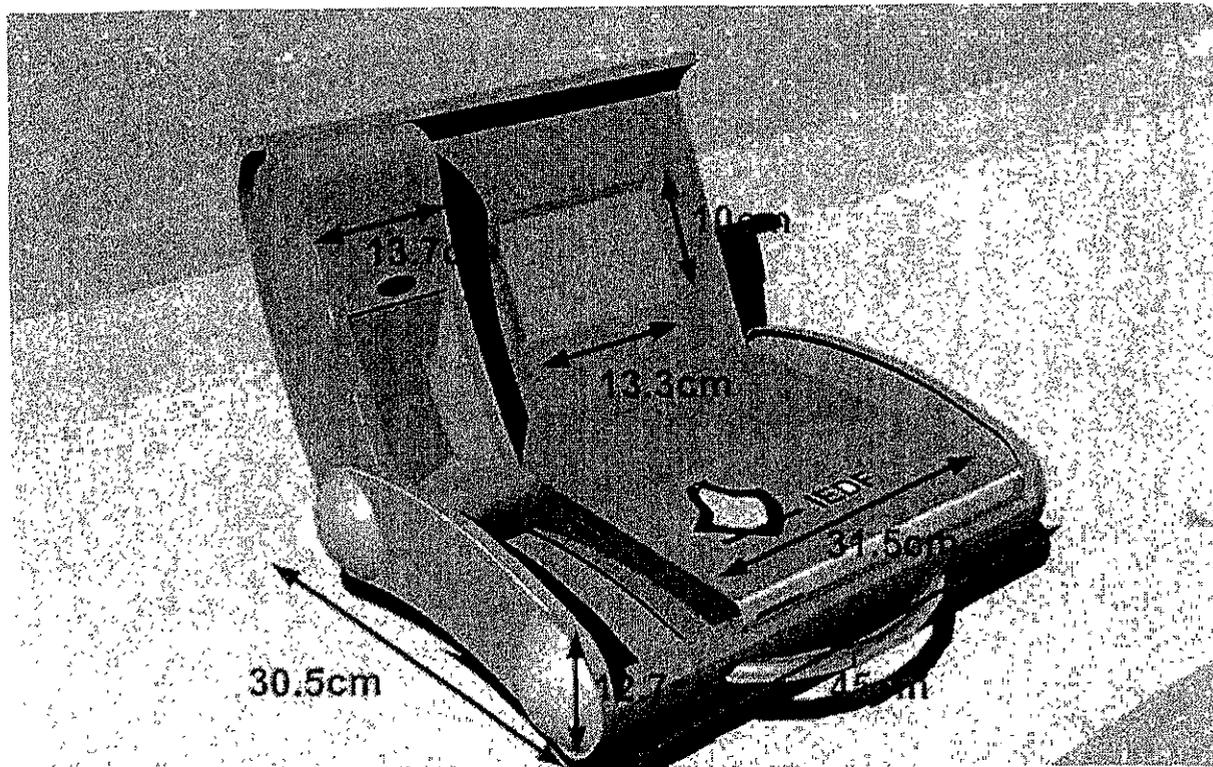


8. Botones con aplicaciones braille

Materiales

- Manija de Acrilonitrilo Butadieno Estireno (ABS)
- Botones de Elastómero Termoplástico (Santoprene)
- Dos Mirillas de Estireno Acrilonitrilo (SAN).
- Urna Electrónica de Acrilonitrilo Butadieno Estireno (ABS).

Medidas:

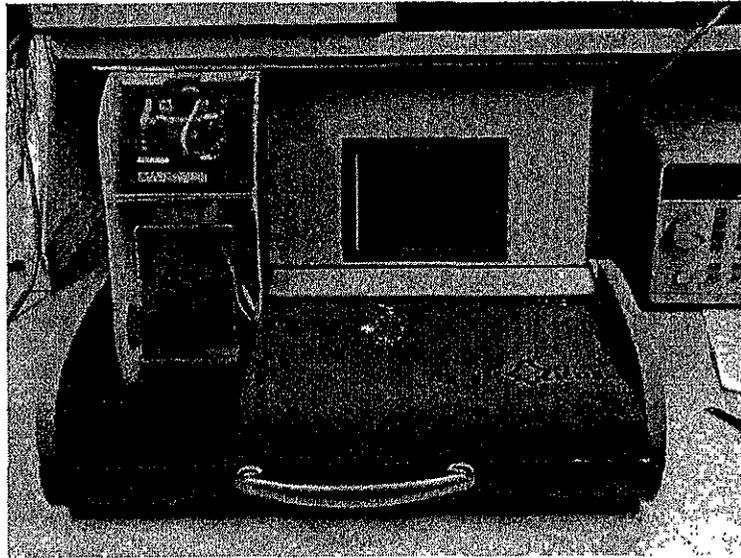


Peso.

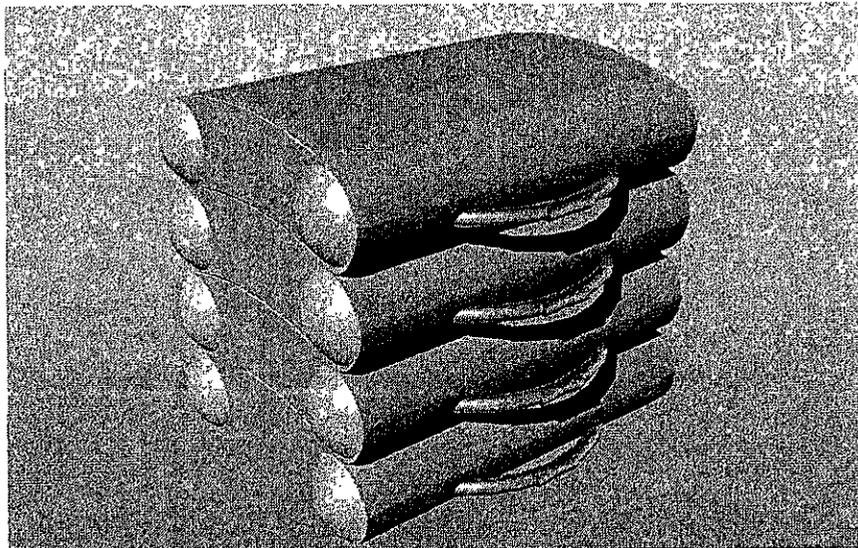
Peso total de la urna 9.5Kg.



La siguiente imagen muestra una maqueta del gabinete de la urna electrónica:



A continuación se muestra el apilamiento de las urnas:



[Handwritten signature]
[Handwritten signature]



2.2. Componentes de Software

El software consiste en tres etapas:

a) Etapa previa a la votación

Esta etapa incluye la siguiente funcionalidad:

- Permitir la carga del sistema operativo desde un medio externo hacia la memoria no volátil de la urna
- Verificar el funcionamiento de los componentes de la urna electrónica e imprimir el resultado de la verificación.
- Monitorear la carga y duración de la batería.
- Generar en una memoria de estado sólido, en un formato específico y con medidas de seguridad suficientes, el o los archivos binarios de la aplicación que serán cargados en la urna electrónica.
- Permitir la carga de las aplicaciones de acuerdo con la elección de que se trate.
- Configurar y realizar la carga de la urna electrónica con los datos específicos de la elección o proceso de participación ciudadana de que se trate.

[Handwritten signatures and initials on the right margin]



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

b) Etapa de votación

Esta etapa incluye la siguiente funcionalidad:

- Permitir a través de un mecanismo de seguridad la inicialización de la urna.
- Generar el reporte de urna vacía.
- Permitir la activación de la urna electrónica para que el ciudadano pueda emitir su voto, mediante un mecanismo de seguridad.
- Desactivar la urna una vez que el ciudadano emitió su voto.
- Permitir que el ciudadano pueda corregir su voto antes de confirmar su elección.
- Registrar la votación en dos memorias de estado sólido y mediante la impresión del voto.
- Notificar cuando un ciudadano no ha emitido su voto en un cierto periodo.
- Llevar el registro completo de auditoría de todos los eventos que ocurren en la urna, incluso de los errores que pudiesen presentarse.
- En caso de alguna contingencia, recuperar la información y generar un reporte de la causa de la falla para proceder al reemplazo de la urna dañada.
- Realizar el cierre de la votación, contabilizando el total de votos e imprimiendo el reporte de escrutinio y cómputo.
- Almacenar los resultados de la votación, el archivo de log, con firma digital en la memoria de estado sólido extraíble.



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

- Deshabilitar la urna electrónica una vez que se ha realizado el cierre de votación y el almacenamiento de la información. Sólo se podrá habilitar nuevamente para fines de auditoría.

c) Etapa posterior a la votación

Esta etapa incluye la siguiente funcionalidad:

- Realizar la transmisión de los archivos contenidos en la memoria de estado sólido hacia un equipo remoto que integra la información.
- Realizar la recepción de los archivos de resultados, log y de firma digital en el equipo integrador y realizar el descifrado de los datos.
- Realizar la integración de la información.

En cada una de las etapas descritas se cuenta con funciones de auditoría y seguridad, que permiten registrar cualquier evento ocurrido durante la operación de la urna, así como del estado de los diferentes dispositivos de hardware y al mismo tiempo garantizar la integridad de la información (aplicación y datos) desde el inicio de operación de la urna hasta la integración de los resultados de la votación.

El software de aplicación para la Urna Electrónica se encuentra desarrollado en la plataforma Linux (Kernel 2.4), específicamente Knoppix y Fedora, el lenguaje de programación utilizado es C++ y su compilador GCC, la utilería de desarrollo para la interfaz gráfica es GTK.

[Handwritten signatures and initials on the right margin]



2.3. Seguridad y Auditoría

2.3.1 Esquema de Seguridad

El esquema de seguridad, basada en criptografía, abarca dos aspectos principales:

- Confidencialidad (cifrado y descifrado).
- Integridad y autenticidad (Firma digital).

La criptografía es una técnica que permite la transformación de textos legibles en secuencias de caracteres no legibles. Estas técnicas utilizan algoritmos y funciones matemáticas que permiten transformar la información en un conjunto de símbolos ilegibles y también permiten el proceso contrario.

La criptografía moderna se basa en dos procesos complementarios: el cifrado y descifrado (también conocidos como encriptación y desencriptación o codificación y decodificación).

El cifrado es el proceso por el que un mensaje de texto legible es transformado en un mensaje ilegible o cifrado mediante una transformación matemática y una clave secreta llamada llave de encriptación.

El descifrado es el proceso inverso al cifrado, a partir de un texto cifrado y una clave secreta se reconstruye el texto original.



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

La firma digital tiene como base un proceso matemático que se aplica a un archivo para garantizar la autenticidad e integridad del mismo.

La seguridad se basará en los esquemas criptográficos conocidos como sistemas de llaves simétricas y sistemas de llaves asimétricas.

2.3.1.1. Sistema de llave Simétrica

Estos algoritmos cifran y descifran usando una sola llave, la llave y los datos son procesados mediante un algoritmo simétrico produciendo datos cifrados. El resultado puede ser enviado mediante un medio inseguro a una parte que contenga la llave original para descifrar los datos. La llave debe permanecer secreta todo el tiempo para que este esquema sea seguro.

Se debe considerar en la seguridad de estos algoritmos el tamaño de la llave. La literatura especializada sugiere que deben evitarse algoritmos que usen llaves de longitud menor a 128 bits. En la práctica 128 bits es suficiente para aplicaciones de propósito general. La longitud mínima propuesta para el esquema de seguridad de la urna electrónica será de 128 bits. Cabe señalar que estos algoritmos son entre 10 y 100 veces más rápidos que los algoritmos utilizados para las llaves asimétricas.



2.3.1.2. Sistema de llaves asimétricas o de llave Pública (Public Key Encryption)

En su forma más conocida los algoritmos de llave pública consisten de dos llaves, una que permanece secreta (llave privada) y otra de libre distribución (llave Pública). Las dos llaves tienen una relación matemática especial y se dice que son inversas criptográficas.

Estos algoritmos son lentos pero tienen la ventaja de que una de las llaves (la pública) puede ser conocida por cualquiera. Generalmente se utilizan para firmar digitalmente los mensajes o archivos.

La llave privada se utilizará para firmar digitalmente los archivos y la llave pública se utilizará para verificar la firma digital del mensaje o archivo.

Al igual que en los algoritmos simétricos la longitud de llave es un factor importante en la seguridad que ofrece el esquema de llave pública; nuevamente la literatura especializada sugiere utilizar llaves de longitud no menor a 1,024-bits que es la que se recomienda como longitud mínima para el esquema de seguridad de la urna electrónica.

2.3.1.3. Firma Digital

La firma digital se utilizará para garantizar la autenticidad de los archivos y aplicaciones que se utilizarán para el funcionamiento de la urna electrónica así como la integridad de dicha información (que no haya sufrido cambio alguno).



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

La firma digital consiste en añadir al archivo un resumen del mensaje original producido por una función matemática y que a la vez es cifrado por la llave privada. Bastaría con que alguien añada, elimine o cambie una sola letra del mensaje para que el resumen del mismo no coincida con el resumen cifrado del mensaje original, detectando de esa manera un mensaje fraudulento.

2.3.2. Esquema Global

A continuación se describe el esquema general de seguridad en el que se llevan acabo los siguientes procesos:

2.3.2.1. Registro de llaves

El esquema de seguridad propuesto inicia con el proceso de generación de las llaves privada y pública mediante las que se firmarán los códigos fuente de las aplicaciones y sistema operativo que se utilizarán en los procesos de pre-votación, votación y post-votación.

Las llaves serán generadas ante las instancias competentes. Una vez realizado dicho proceso se procederá al registro de las mismas ante una autoridad certificadora (que estimamos será el propio IEDF), quien dará fe de la legalidad en el proceso.

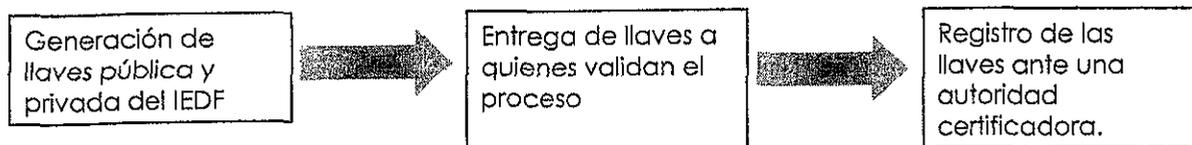


Figura 1. Registro de llaves

2.3.2.2. Etapa de pre-votación

La seguridad informática del proceso de pre-votación se llevará a cabo mediante los siguientes pasos:

- a) Se realizará el firmado digital del código fuente del sistema operativo y de las aplicaciones que se utilizarán durante la Jornada electoral.
- b) Se realizará la generación de llaves pública, privada y las llaves simétricas para la jornada electoral. La llave pública y privada se utilizarán para firmar digitalmente los archivos de configuración, de bitácora, de auditoría, de votos y totalización de votos de la urna electrónica. Las llaves simétricas, 40 en total (una para cada Distrito Electoral), se utilizarán para cifrar los datos que serán transmitidos desde los Distritos Electorales hacia la sede central del Instituto.
- c) Se realizará el proceso de firmado digital de los archivos requeridos para la configuración para cada urna, mediante la llave privada generada por la aplicación para la jornada electoral.
- d) Se realizará la copia de los archivos requeridos para la configuración de cada al dispositivo extraíble.



- e) Se realizará el registro de los números de serie de los dispositivos extraíbles en la base de datos central y se asociarán con cada urna.
- f) Se procederá a la instalación del dispositivo extraíble dentro de la urna y se realizará la configuración de la misma.
- g) Se realizará la verificación del funcionamiento de la Urna tanto de hardware así como de software y se realizará el evento de lacrado de las urnas ante al autoridad electoral.

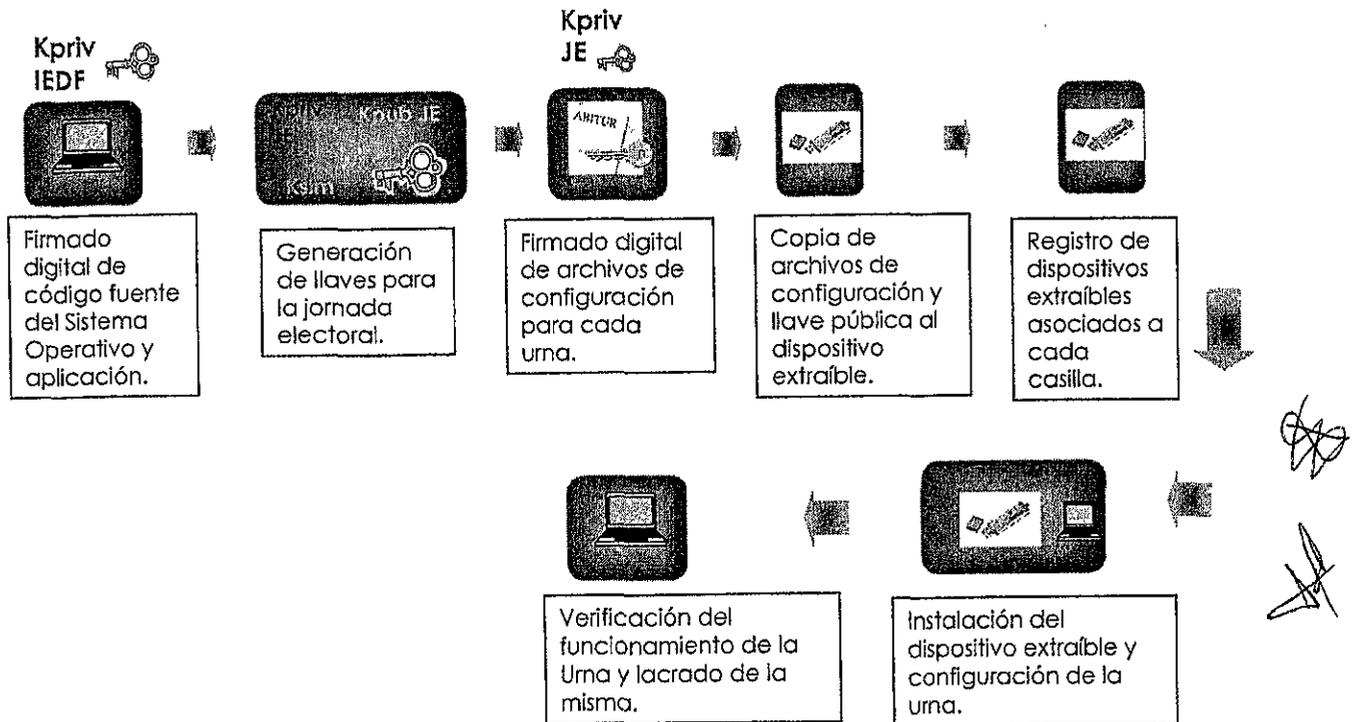


Figura 2. Esquema de seguridad etapa de pre-votación.



2.3.2.3. Etapa de votación

Dentro de la etapa de votación se realizarán los siguientes pasos:

- a) Se verificará el lacrado de la urna para confirmar que ésta no ha sido violentado, ya sea de manera accidental o intencional.
- b) Se verificará el funcionamiento de la urna concretamente lo correspondiente al hardware.
- c) La urna electrónica realizará el proceso de verificación de la firma digital de los archivos de configuración previamente cargados en la urna.
- d) Una vez iniciada la jornada electoral, la urna electrónica realizará el proceso de firmado digital de los archivos de bitácora, de auditoría y de votos cada vez que se emita un sufragio.
- e) Al final de la jornada electoral cuando se proceda a cerrar la urna la propia urna electrónica realizará el proceso de creación de llave pública y privada de la urna, mediante las que se firmarán los archivos que resulten de la votación.
- f) Mediante la llave privada generada en la urna se procederá a realizar el firmado digital de archivos de bitácora, de auditoría y total de votos.
- g) Se realizará el copiado de los archivos previamente firmados al dispositivo extraíble además de la llave pública generada en la urna. Estos archivos también se copiarán en la memoria flash interna de la Urna.

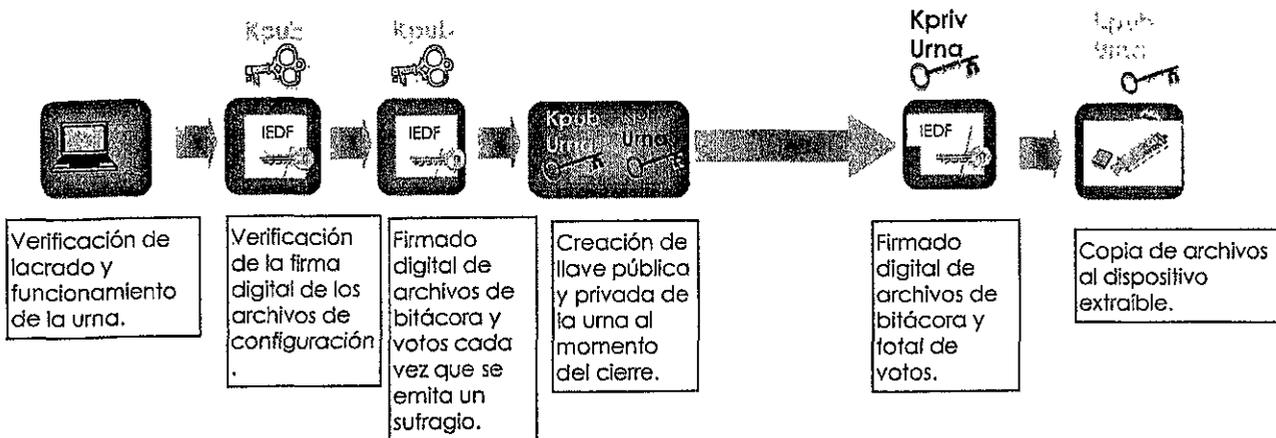
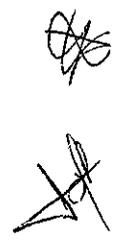


Figura 3. Esquema de seguridad etapa de votación.

2.3.2.4. Etapa de post-votación

Dentro de la etapa posterior a la votación se realizarán los siguientes pasos:

- a) Inicialmente se verificará el número de serie del dispositivo extraíble con el número de serie almacenado en la base de datos central con la finalidad de confirmar que se trate de un dispositivo propiedad del Instituto y que fue previamente registrado para la casilla correspondiente.
- b) Si la verificación del dispositivo extraíble fue satisfactoria, se procede a la verificación de la firma digital de los archivos del dispositivo extraíble, utilizando la llave pública generada en la urna



- c) Si la firma digital corresponde, entonces se procede a copiar los archivos a la base de datos Distrital.
- d) Al final del proceso, se realiza el cifrado de archivos para su envío a la sede central utilizando la llave simétrica correspondiente al Distrito Electoral.
- e) En la sede central se procede a realizar el descifrado de los archivos que se reciben de cada Distrito Electoral utilizando la llave simétrica correspondiente y se realiza el concentrado de los datos en la base de datos central.

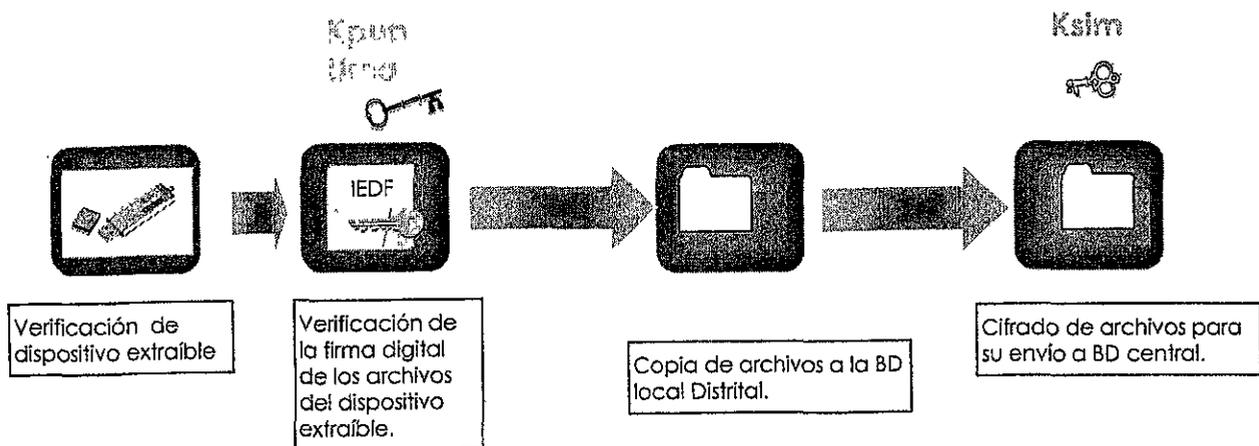


Figura 4. Esquema de seguridad etapa de post-votación.



2.3.3. Auditoria

La auditoria es la actividad consistente en la emisión de una opinión profesional acerca de si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

La integridad de una elección debe estar garantizada por:

- a) Las medidas preventivas como identificación de los votantes, urnas selladas o lacradas durante el proceso de votación.
- b) Medidas de auditoria que detecten errores y fraudes, y permitan la reconstrucción total de una elección.

Los propósitos principales de la auditoria que se realizará a las urnas electrónicas son:

- c) Determinar si la normatividad se ha seguido paso a paso en el proceso.
- d) Proporcionar evidencia de los errores que pudieron haber ocurrido ya sea de manera accidental o de manera deliberada.
- e) Contribuir al aumento de la confianza en el proceso.

El requerimiento central para que los sistemas que se utilicen durante la jornada electoral sean auditables es que contenga información suficiente para permitir la detección y corrección de un error o falsificación.



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

La propuesta del esquema de Auditoria se basa principalmente en la redundancia de la información y la revisión de cada una de las etapas.

Para realizar la auditoria se contará con archivos y comprobantes impresos que permitirán verificar la información de la jornada electoral. La información es generada de forma impresa y magnética. Los archivos electrónicos con los que se contará son los siguientes:

- a) Archivo de totalización de votos.
- b) Archivo de Bitácora que contiene información de los eventos que ocurren durante la jornada electoral.
- c) Archivo de auditoria que contiene información de los resultados que arrojan las auditorias realizadas.

Estos archivos estarán almacenados en la memoria flash y en el dispositivo extraíble de la urna electrónica.

El archivo de Bitácora se generará desde el momento en que es instalado el sistema operativo. Este archivo es tipo texto simple y en él se van agregando todos los eventos que se presentan en la urna, mediante mensajes codificados con anterioridad. (Catálogo de mensajes).

El formato de dicho archivo es el siguiente:

- a) Fecha y hora en que ocurrió el evento
- b) Código de mensaje



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

Las auditorías internas son auditorías simples que realiza cada urna electrónica, cada media hora, y que verifican, entre otros aspectos, que:

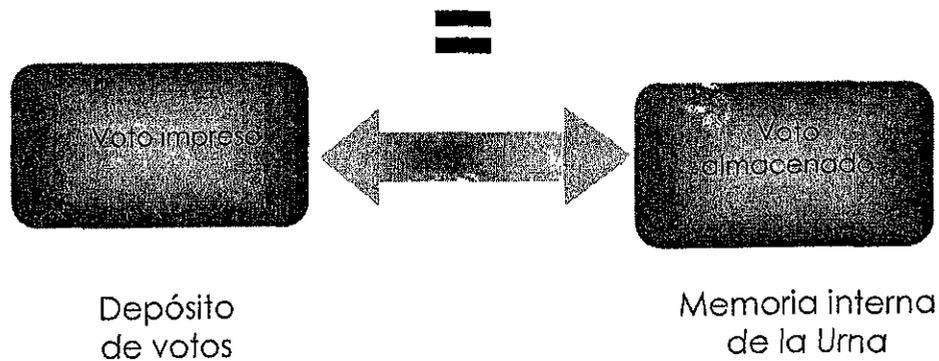
- a) El número de votos de un candidato no haya disminuido respecto al número de votos que tenía en el intervalo anterior de tiempo.
- b) El número total de votos coincida con la suma de votos de cada candidato más el número de votos por ninguno.
- c) El resultado de cada auditoría se graba en el Archivo de Auditoría que a su vez se encuentra en la memoria flash y el dispositivo extraíble de cada urna.

El esquema de seguridad propuesto permite garantizar la integridad y autenticidad de los archivos de bitácora y de Auditoría mediante la firma digital.

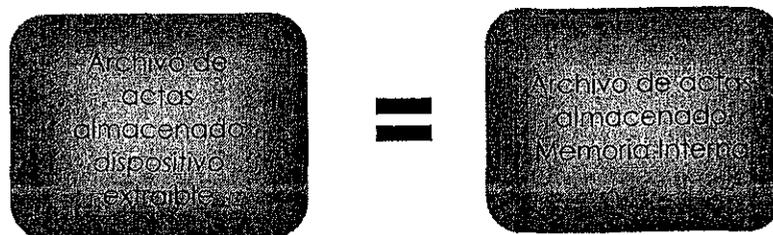
- a) Los archivos de bitácora del sistema se firman digitalmente cada vez que se emite un voto.
- b) Los Archivos de auditoría se firman digitalmente cada vez que se realiza una auditoría.
- c) Ambos archivos se firman digitalmente al final de la votación y son copiados a los dispositivos extraíbles, en conjunto con las actas de totalización de votos de cada urna.

2.3.3.1 Puntos de Auditoría

- a) La auditoría de cada voto generado durante la Jornada Electoral se realiza comparando el voto impreso en papel con el voto grabado en la memoria interna.

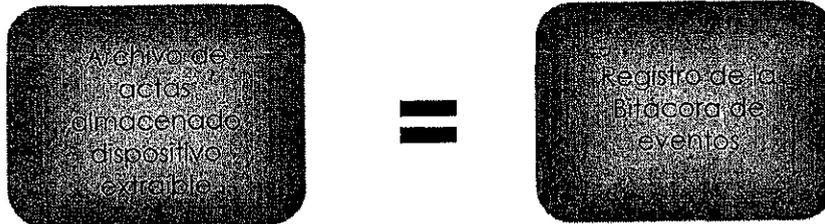


- b) Comparando el voto grabado en la memoria interna y el voto grabado en el dispositivo extraíble.

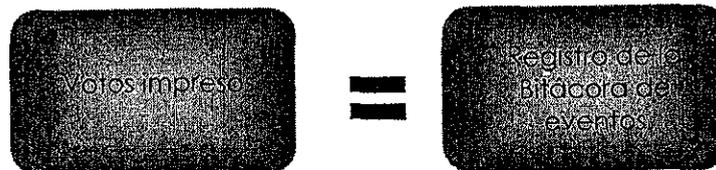


[Handwritten signature]
[Handwritten signature]

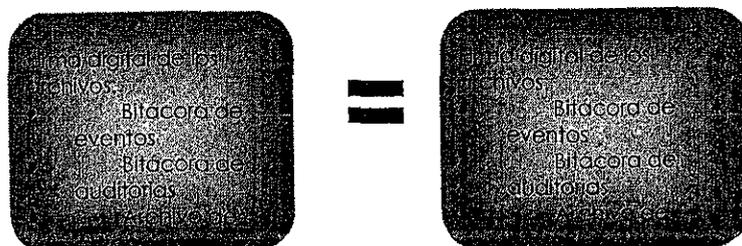
c) Comparando el número de votos totales en el archivo de actas grabado en la memoria interna y los eventos grabados en el archivo de Bitácora.



d) Comparando el número de votos impresos en la urna y los eventos de votación registrados en la bitácora de eventos.

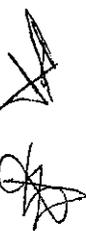


e) Verificación de las firmas digitales de los archivos generados durante el proceso electoral con las llaves registradas ante la autoridad certificadora.



Archivos ubicados en la Urna

Archivos ubicados en el dispositivo extraíble



Handwritten signatures.

- f) Verificación de las firmas digitales de los códigos fuente de la aplicación y sistema operativo con las llaves registradas ante la autoridad certificadora.
- g) Verificación del archivo de Bitácora de auditorías para identificar si se detectaron anomalías en el proceso.

2.4. Procedimientos

Los procedimientos previstos son los siguientes:

- Carga de la batería.
- Carga de la aplicación y de los datos en cada urna electrónica
- Configuración de la urna electrónica
- De operación de la urna electrónica durante la jornada electoral
- De recepción y transmisión de información de la urna electrónica
- De auditoría
- Contingencia de urna electrónica
- Recuperación de datos





INSTITUTO ELECTORAL DEL DISTRITO FEDERAL
SECRETARÍA EJECUTIVA
UNIDAD DE INFORMÁTICA

Características que debe cumplir la urna electrónica que se diseñe, acorde con lo señalado en los acuerdos del 30 de octubre de 2003 (ACU-696-03) y 23 de marzo de 2004 (ACU-018-04) del Consejo General del IEDF.

CARACTERÍSTICA	Aplicación de la característica en la urna electrónica diseñada (integrada por la Unidad de Informática)
a) 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;	La urna electrónica que se ha diseñado incluye un conjunto de procedimientos para todas las etapas del proceso de votación, así como mecanismos de seguridad y auditoría que garantizan la autenticidad y efectividad del voto. Además, los componentes técnicos propuestos para el equipo –hardware- y los programas informáticos –software- permiten el voto universal, libre, secreto, directo, personal e intransferible.
b) Garantizar la seguridad del ejercicio del voto durante la jornada electoral;	Aunado a la característica anterior, el conjunto de mecanismos que contiene la urna diseñada permite asegurar que sólo podrán votar los ciudadanos registrados en la lista nominal de la casilla electoral.
c) Permitir al elector la emisión del voto en forma rápida y sencilla;	La urna electrónica permite una votación ágil y de fácil comprensión para el votante, quien no requiere de conocimientos especializados en computación o informática para manejarla.
d) Utilizar un mecanismo para la identificación del elector, a fin de evitar intentos de falsificación del voto;	El único medio de identificación válida para el elector es su credencial para votar con fotografía, por ello se propone utilizarla en un dispositivo de lectura infrarrojo, independiente de la urna y autónomo en su operación. El dispositivo leerá la credencial para votar con fotografía y desplegará los datos que ésta contiene, tal y como aparece actualmente en los listados nominales de electores que genera el IFE.
e) Ser de fácil instalación y mantenimiento;	La urna electrónica es de fácil instalación ya que sólo requiere de su colocación en una mesa, el despliegue de su cubierta protectora y encender el equipo mediante la llave de activación. Los funcionarios electorales no requieren de conocimientos en cómputo o

[Handwritten signature]

[Handwritten mark]



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

CARACTERÍSTICA	Aplicación de la característica en la urna electrónica diseñada (integrada por la Unidad de Informática)
	informática para la operación de la urna. El diseño propuesto contempla un gabinete que mediante una llave de seguridad permite al personal técnico del IEDF, el acceso fácil a todos los componentes electrónicos para su mantenimiento. El uso de partes móviles se reduce al mínimo. La urna contempla el uso de memorias de estado sólido; no se incluyen discos duros ni unidades de disco flexible que pudiesen dañarse debido a la vibración derivada del traslado y operación de la urna.
f) Dar seguridad de que la jornada electoral se realice de forma continua;	La urna incorpora baterías recargables con una duración de 12 horas continuas. Lo anterior permitirá afrontar exitosamente eventuales fallas en el suministro eléctrico que llegasen a presentarse durante la jornada electoral. En el diseño propuesto se incluyen procedimientos de contingencia, que consideran la utilización de urnas previamente configuradas y a las que se tendría rápido acceso.
g) Permitir que el ciudadano emita sucesivamente su voto, en las diferentes elecciones previstas en el Código;	Los votantes podrán emitir sucesivamente su voto en las diferentes elecciones, pues la urna electrónica despliega en su pantalla, de manera sucesiva, las diferentes boletas electrónicas para la votación, (Jefe de Gobierno, Jefe Delegacional, y Diputados a la Asamblea Legislativa del Distrito Federal), de acuerdo con el distrito, sección y casilla de que se trate.
h) Impedir que el ciudadano intente votar por segunda ocasión;	La urna impide que el ciudadano vote en más de una ocasión para la misma elección. La urna es habilitada por el funcionario de casilla para permitir el voto del ciudadano que ha sido previamente identificado. Una vez que el ciudadano ha terminado de votar para todas las elecciones de que se trate, la urna se deshabilita automáticamente. Será hasta ese momento que la urna será



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

CARACTERÍSTICA	Aplicación de la característica en la urna electrónica diseñada (integrada por la Unidad de Informática)
	habilitada nuevamente por el funcionario de casilla para que vote el siguiente ciudadano de la fila.
i) Permitir que el ciudadano, al marcar su opción, visualice los elementos de identificación de su preferencia;	Al momento en que el ciudadano realiza su voto, en la pantalla de la urna electrónica se despliegan los siguientes elementos: emblema del partido o coalición, fotografías de la fórmula de candidatos, nombre del o los candidatos, todo esto con estricto apego a colores y emblemas de los partidos.
j) Permitir al votante corregir su preferencia antes de confirmar el sentido de su voto;	Para cada una de las elecciones que debe hacer el votante se despliega la opción de confirmar o corregir el sentido del voto. Una vez que el ciudadano confirma su voto, éste se imprime para que el votante corrobore que lo impreso coincide con lo desplegado en la pantalla. El comprobante impreso se deposita automáticamente en un contenedor sellado que eventualmente se abrirá para propósitos de auditoría.
k) 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;	En el diseño se contempla la impresión de todos los comprobantes necesarios para cada una de las etapas de la votación: Reporte de instalación (que incluye la verificación del funcionamiento de todos los componentes de la urna). Reporte de apertura (archivos de votación en ceros, urna vacía). Reporte de cierre de la votación. Reporte de resultados del cómputo. Reporte de clausura de casilla.



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL
SECRETARÍA EJECUTIVA
UNIDAD DE INFORMÁTICA

CARACTERÍSTICA	Aplicación de la característica en la urna electrónica diseñada (integrada por la Unidad de Informática)
l) 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;	Los programas de cómputo –software- utilizados en la urna electrónica, y previo a su utilización, serán verificados exhaustivamente por todos los involucrados. Además, el software se someterá al escrutinio público de manera permanente. Con todo ello se asegura que no existan errores en la contabilidad de los votos.
m) Contar con los mecanismos necesarios para recuperar los datos de la votación íntegramente, en caso de falla o avería del equipo;	En el diseño se incorpora un procedimiento de grabación simultánea de los votos en dos dispositivos de almacenamiento. Con ello se tendrá un respaldo en caso de falla de alguno de esos dos dispositivos. De manera adicional, se tendrán los comprobantes impresos de votación que permitirán reconstruir íntegramente la votación.
n) Permitir la comparación de los resultados impresos con los guardados en los dispositivos de la urna;	En virtud de que se contará con comprobantes impresos de votación se podrán comparar éstos con los registros almacenados en la urna electrónica.
o) Garantizar que todos los mecanismos de seguridad sean auditables para que puedan ser analizados en caso de controversia;	La urna electrónica tiene implementados mecanismos de seguridad, con base en el cifrado de datos y en la firma digital, que son auditables. Existe registro de todos los eventos que ocurren en la urna que puede ser revisado en cualquier momento para propósitos de auditoría. Se contemplan siete puntos de auditoría que permitirán detectar cualquier alteración de los registros de votos.
p) Incluir mecanismos para facilitar el ejercicio del voto a las personas con discapacidad.	La urna electrónica cuenta con tres teclas con aplicaciones braille y con audífonos que facilitarán el ejercicio del voto a personas con discapacidad visual.

[Handwritten signature]

[Handwritten mark]



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

CARACTERÍSTICA	Aplicación de la característica en la urna electrónica diseñada (integrada por la Unidad de Informática)
a) Garantizar la difusión oportuna y confiable de los resultados del cómputo; y	Los cálculos hasta ahora realizados manualmente por los funcionarios de casilla, serán efectuados por los programas de cómputo -software- de la urna. Lo anterior, brindará una mayor rapidez y confiabilidad en el cómputo de resultados y se evitarán los errores humanos de conteo. Se incluye software que facilitará a los Consejos Distritales y al Consejo General la consolidación y difusión de los resultados.
r) Reducir los costos en el procedimiento para la emisión y cómputo del sufragio.	Con la utilización de la urna electrónica se disminuye considerablemente el volumen de material electoral, pues dejarían de utilizarse las boletas impresas, y se reduce el número de funcionarios por casilla, ello redundará, en el mediano plazo, en menores costos de organización de las elecciones.
De manera adicional, la Urna electrónica que se proponga debe contar con autonomía en el suministro eléctrico hasta por doce horas continuas.	La urna electrónica incluye batería y un circuito de alimentación eléctrica, que aseguran la autonomía operativa de la urna hasta por doce horas continuas.

México DF, a 18 de Febrero de 2001

ESPECIFICACIONES TÉCNICAS DE LOS PROTOTIPOS DE URNA ELECTRÓNICA

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
1. Componentes de hardware y sistema operativo	<p>Applied Data Systems, Inc (BitsyX) Procesador: 32 bits, 400 MHz Intel PXA255(RISC) Pantalla: 6.4" active color VGA LCD; Forma LQ64D343, 3M/Dynapro 6.4" resistive touchscreen. Alimentación: 5V I/O: 2 USB (host y esclavo), 3 seriales RAM: SDRAM 64 MB.32 MB Flash S. O.: Linux (Debian), Kernel 2.4.26 Impresora: Fujitsu FTP-628MCL353#01, Interfaz Serial, Tarjeta Controladora PRN 608S(linux), 6-8 V, 0.2 A, 1A pico Batería: Power Sonic PSH 12180 21AH 12 V, 6 kg. de peso. Lector de código de barras: KANESCAN CCD Barcode Scanners. Interfaces: USB, RS232, PS2.</p>	<p>Arcom (Viper) Procesador: 32 bits, 400 MHz Intel PXA255(RISC) Pantalla: NEC 320x240 pantalla a color TFT. Pantalla Táctil Análoga Alimentación: 5V I/O: puertos duales USB, 5 seriales RAM: SDRAM 64 MB.32 MB Flash S. O.: Linux (Red Hat), Kernel 2.4.21 Impresora: Epson M260, matriz de punto, 12V 10%, 2A, 5A pico Batería: Panasonic LCRD1217P, 17 AH, 12 v, 6.5 kg. de peso. Pic</p>	<p>Arcom (Viper) Procesador: 32 bits, 400 MHz Intel PXA255 (RISC) Pantalla: NEC 320x240 pantalla a color TFT. Pantalla Táctil Análoga Alimentación: 5V I/O: puertos duales USB, 5 seriales RAM: SDRAM 64 MB.32 MB Flash S. O.: Linux (Red Hat), Kernel 2.4.21 Impresora: Zebra Cameo 3, 7.2V, 1.6AH Batería: N-Charge Power System Radio Frecuencia</p>	<p>Applied Data Systems, Inc (BitsyX) Procesador: 32 bit, 400 MHz Intel PXA255 (RISC) Pantalla: 6.4" active color VGA LCD; Forma LQ64D343, 3M/Dynapro 6.4" resistive touchscreen. Alimentación: 5V I/O: 2 USB (host y esclavo), 3 seriales RAM: SDRAM 64 MB.32 MB Flash S. O.: Linux (Debian), Kernel 2.4.26 Impresora: Fujitsu FTP-628MCL353#02, Interfaz Serial, Tarjeta Controladora (windows), 6-8 V, 0.2 A, 1A pico Batería: Power Sonic PSH 12180 21AH, 12 V, 6 kg. de peso. GPS: Deluo Gps lite, modelo 90-020. Protocolo de datos NMEA 0183 v2.2. Lector de código de barras: MS9520 VOYAGER.Interfaces: USB, RS232, PS2.Interfaces: USB, RS232, PS2. Bluetooth: Adaptador USB ANYCOM Blue USB-100, 2.4-2.4835GHz Activador</p>	<p>Applied Data Systems, Inc (BitsyX) Procesador: 32 bit, 400 MHz Intel PXA255 RISC) Pantalla: 6.4" active color VGA LCD; Forma LQ64D343, 3M/Dynapro 6.4" resistive touchscreen. Alimentación: 5V I/O: 2 USB (host y esclavo), 3 seriales RAM: SDRAM 64 MB.32 MB Flash S. O.: Linux (Debian), Kernel 2.4.26 Impresora: Fujitsu FTP-628MCL353#01, Interfaz Serial, Tarjeta Controladora PR 608S(linux), 6-8 V, 0.2 A, 1A pico Batería: Power Sonic PSH 12180 21AH 1 V, 6 kg de peso. Se integran estos componentes, debic a su baja potencia de consumo y alimentación de un solo voltaje, aden de que trae integrado el sistema Linux en su versión más estable Debian Kern 2.4.26 Actualmente, se analiza la posibilidad de integrar una pantalla de 10.4".</p>



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
Seguridad y Auditoría	<p>La seguridad esta basada en OPENSLL. En la aplicación del generador de medios se genera una llave para cada una de las urnas y se lleva un control del número de serie del dispositivo USB y de la flash de la urna. Los dispositivos USB que utilizan para configurar cada una de las urnas cuenta con la información cifrada y firmada. También, se cifran y firman los resultados de la votación junto con el archivo de log.</p> <p>El algoritmo utilizado para el cifrado y firmado digital es el AES (Advanced Encryption Standard) para el cifrado simétrico, RSA para las llaves públicas y privadas y SHA1 para la huella electrónica de los archivos.</p> <p>Para la auditoría se utiliza el syslogd de Linux para grabar la actividad de la aplicación de la urna. Se genera un archivo de bitácora general y un archivo de bitácora especial para los eventos de hardware. La estructura del archivo de</p>	<p>La seguridad (cifrado y revisión de firmas digitales para la aplicación y datos empaquetados) estará a cargo de GnuPG recompilado para la arquitectura ARM de la urna electrónica, con un anillo de confianza que incluye el equipo integrador.</p> <p>Se utilizan dos juegos de llaves (pública y privada). Uno para el equipo integrador y uno para la urna electrónica y se intercambian entre ambos sus respectivas llaves públicas.</p> <p>El software utilizado para implementar la seguridad fue GnuPG, y utilizan llaves públicas y privadas.</p> <p>Además se implementaron otros módulos y aplicaciones libres, para el sonido, impresión, manejo de energía y seguridad del sistema operativo.</p> <p>Los algoritmos utilizados para el cifrado y firmado digital son DSA y El gamal. El algoritmo para la huella electrónica es SHA-1 y para verificar la integridad utilizan MD5.</p> <p>Para la auditoría se utiliza el log utilizado por el sistema operativo.</p>	<p>El algoritmo utilizado para el cifrado y firmado digital es Curvas elípticas con campos finitos tipo B163 con la Librería Miracle.</p> <p>Se generan un juego de llaves pública y privada para cifrar cada uno de los votos registrados en la urna electrónica</p> <p>En la parte de auditoría utiliza el log utilizado por el sistema operativo, se genera un archivo de bitácora general en texto plano.</p> <p>La estructura del archivo de bitácora registra la fecha, hora y se concatena con el mensaje de texto de cada una de las actividades realizadas por la aplicación.</p>	<p>Basado en la API de Seguridad de Linux más reconocida OpenSSL. Se utiliza una interfaz genérica que permite intercambiar algoritmos. Esta interfaz genérica o maestra es llamada EVP (enveloped). Se cifra de manera aleatoria.</p> <p>El algoritmo utilizado para el cifrado y firmado digital es AES RSA y DSA.</p> <p>En la parte de auditoría se genera dos archivos de log, uno que guarda todos los eventos de la urna y otro que guarda sólo cuando existe falla en el grabado de los votos. Realizan una auditoría intermedia cada 30 minutos para verificar que el total del número de votos corresponda con la suma de todos los votos para cada partido. Cuentan con una aplicación que muestra los registros por tipo de evento en base al catálogo propuesto.</p>	<p>Se propone utilizar un esquema de seguridad basado el la API OpenSSL porque es la más conveniente debido que es un esquema muy robusto y aplicación esta muy generalizada. Además por ser parte de Linux, no es necesario recompilar el kernel.</p>



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
	bitácora está formado por tres campos: el primero especifica el programa y el PID que escribe en el archivo; el segundo indica la fecha y la hora y finalmente el resto del renglón es el mensaje que se registra. Se escribe en tres partes, en el archivo el syslogd de linux, el archivo de respaldo que se escribe en el dispositivo extraíble y el que se escribe en la memoria interna y que se especifica en el archivo de configuración. El archivo es de tipo texto.	Se genera un archivo de bitácora general en texto plano. Los eventos generados por la aplicación se agregan al archivo de manera secuencial, con el siguiente formato. Descripción del evento, fecha y hora del sistema en el momento que se produjo. Se genera también un archivo separado de bitácora de inicialización de la urna.			
3. Aplicaciones de apoyo pre-votación y post-votación	<p>Aplicación Pre-votación</p> <p>Cuenta con una aplicación denominada "MARU" (Módulo de Acceso Remoto a la Urna, la cual tiene la finalidad de:</p> <ol style="list-style-type: none"> 1. Generar las llaves públicas y privadas. 2. Crear los códigos de barras para el acceso a las urnas, a través del Estándar BARCODE 128 y se utiliza PERL para su impresión. 3. Carga de catálogos de datos utilizando base de 	<p>Aplicación Pre-votación</p> <p>Cuenta con una aplicación denominada "SADE" (Sistema de Administrador de Datos Electorales), que tiene la finalidad de:</p> <ol style="list-style-type: none"> 1. Registrar los datos de los partidos y candidatos, así como sus datos multimedia que servirán para el funcionamiento de la urna. 2. Dar de alta y/o editar el catalogo de elecciones, para la jornada electoral. 	<p>Aplicación Pre-votación</p> <p>Cuenta con una aplicación denominada "VOTATEC", tiene la finalidad de:</p> <ol style="list-style-type: none"> 1. Registrar candidatos 2. Generar boleta electrónicas 3. Generar urnas genéricas 4. Cargar información a las urnas. <p>Aplicación Post-votación</p>	<p>Aplicación Pre-votación</p> <p>Cuenta con procedimiento para la generación de medios, el cual consiste en:</p> <p>Configurar un dispositivo USB con los datos de la elección de que se trate, (candidatos, partidos, logotipos, etc.)</p> <p>Aplicación Post-votación</p> <p>Cuenta con una aplicación que se divide en tres módulos, integrador,</p>	<p>Aplicación Pre-votación</p> <p>Se propone tomar la estructura de aplicación del Instituto Politécnico Nacional omitiendo la generación de códigos de barras para la activación de la urna, ya que resultaría un costo adicional la elaboración de los mismos en papel seguridad.</p> <p>Aplicación Post-votación</p> <p>Se propone tomar la estructura de aplicación del Instituto Politécnico</p>

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
	<p>datos postgress.</p> <p>4. Carga de los archivos de audio e imágenes de candidatos y partidos.</p> <p>5. Generar los archivos de configuración de cada urna.</p> <p>6. Realizar la integración de los resultados de la votación para Jefe de Gobierno, Jefes Delegacional y Diputados.</p> <p>7. Validar y recibir los datos provenientes de las Urnas Electrónicas de los distritos electorales (los datos son obtenidos de los dispositivos de almacenamiento USB).</p> <p>Aplicación Post-votación</p> <p>Desarrollaron otra aplicación denominada "Distrital", que cuenta con las siguientes funciones:</p> <p>1. Recepción y validación de los datos enviados por los operadores de la aplicación</p> <p>2. Los datos son obtenidos de los dispositivos USB instalados en las Urnas Electrónicas del distrito</p>	<p>3. Establecer las planillas electorales para los diferentes tipos de elección.</p> <p>4. El sistema permite generar reportes y consultas para que puedan ser corroborados por los partidos políticos involucrados en los comicios en turno.</p> <p>5. Una vez corroborados, se procede a empaquetar los datos en archivos únicos firmados digitalmente con GnuPG para asegurar su autenticidad y se copian a los dispositivos USB para posterior uso en la etapa de votación.</p> <p>Se establece en la URNA ELECTRÓNICA una imagen del sistema operativo depurado (solo lo necesario para la jornada electoral) y la aplicación de una electrónica (sin configurar).</p> <p>Aplicación Post-votación</p> <p>Desarrollaron otra aplicación denominada "Integrador" que se encontrará físicamente instalada en las oficinas de los distritos</p>	<p>En la misma aplicación denominada "VOTATEC", tiene la finalidad de:</p> <p>1. Envío y recepción de paquetes de elección.</p> <p>2. Publicación de votos.</p> <p>3. Almacenamiento de paquetes de elección.</p> <p>La aplicación esta desarrollada en lenguaje Java.</p>	<p>estadística y transmisión. Están desarrollados en java Software Development Kit j2sdk1.4.2, y se requiere la clave de acceso de cada partido político para ingresar al sistema (al menos 5), al momento de integrar la información del dispositivo USB se realiza una validación con respecto al número de serie.</p>	Nacional.



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
	<p>electoral.</p> <p>3. Realizar totalizaciones progresivas de los votos que reciben, dependiendo del tipo de elección de que se trate.</p> <p>4. Obtener los archivos de votación y de auditoría de los Distritos Electorales.</p> <p>5. Visualización de los resultados para cada tipo de elección por distrito, sección, casilla, etc.</p> <p>6. Realizar la transmisión de los resultados a la sede central, sincronizado con la aplicación MARU.</p> <p>Ambas aplicaciones están desarrolladas en lenguaje C.</p>	<p>electorales y se encarga de:</p> <p>1. Leer los archivos de los votos, descifrarlos y mostrarlos en pantalla.</p> <p>2. Transmitir los archivos de los votos electorales y bitácoras al equipo integrador que está instalado en las oficinas centrales del IEDF.</p> <p>3. Corroborar la integridad de los datos.</p> <p>4. Administrar los archivos transmitidos y por transmitir, así como los archivos que necesitan ser retransmitidos por errores de comunicación (Revisión de checksum y firma digital)</p> <p>5. Entre otras características de consultas y reportes parciales.</p> <p>Ambas aplicaciones están desarrolladas en lenguaje Java con clases Swing para la interfaz de usuario. Para almacenar los datos se utiliza el manejador de bases de datos Sql Server.</p>			



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
4. Aplicación de la Urna	<p>La aplicación se denomina "ASVEL" (Administrador de Sesiones de Voto Electrónico) y tiene las siguientes funciones:</p> <ol style="list-style-type: none"> 1. Activar y configurar la urna a través de código de barras. 2. Verificación de los componentes e impresión del resultado del diagnóstico. 3. Imprimir las actas de urna vacía. 4. Autenticar electores y funcionarios a través de los códigos de barras. 5. Emitir sonidos para el apoyo a débiles visuales. 6. Habilitar la urna para votación a través de código de barras. 7. Verificar el tiempo de emisión del voto que no supere el tiempo configurado en la aplicación MARU. 8. Permitir al funcionario de casilla habilitar la urna a los electores que no han terminado de emitir su voto para todas las elecciones, a 	<p>La aplicación genera planillas de configuración de la urna de manera dinámica y genera los siguientes archivos:</p> <ol style="list-style-type: none"> 1. Archivo de votos 2. Archivos de bitácoras de operación de la urna electrónica. 3. Actas de apertura y cierre. <p>Utiliza una clave de usuario y contraseña para inicializar y cerrar la urna.</p> <p>Realiza la verificación de los componentes.</p> <p>Imprime las actas de urna vacía.</p> <p>El proceso de votación no cuenta con restricciones de tiempo para la emisión del voto.</p> <p>Utiliza audio y un teclado braille para el apoyo a débiles visuales.</p> <p>Al cerrar la votación se cifran y se copian los datos al dispositivo USB.</p>	<p>La aplicación se denomina "UVETEC", la cual cuenta con dos módulos: administración y votación. El módulo de administración realiza las siguientes funciones:</p> <ol style="list-style-type: none"> 1. Prueba de funcionamiento de componentes. 2. Impresión de las actas de inicio. 3. Activación del módulo de votación. <p>El módulo de votación permite la emisión del voto por cada elector.</p> <p>Esta aplicación esta desarrollada en lenguaje C con librerías de GTK.</p>	<p>Esta desarrollada en lenguaje C con librerías QT Designer 3.2. La aplicación realiza la verificación de componentes: procesador, memoria, video, audio y medios de almacenamiento; el funcionario sólo tiene contacto hasta la prueba de sonido. Posteriormente, realiza la impresión de las actas de urna vacía y del diagnóstico de componentes. Al momento que la urna es activada se muestran las boletas simulando unas pestañas y puede operar a través de una mascarilla braille diseñada para cada tipo de elección y cuenta con sonidos. Al finalizar la jornada realiza el cierre a través de un código de barras de administrador, se generan las actas de resultados y realiza una copia interna del archivo generado. La urna queda deshabilitada pero no se apaga.</p>	<p>Se propone tomar la funcionalidad de la aplicación desarrollada por el Instituto Politécnico Nacional, incluyendo utilización de estados propuestos por la Universidad Nacional Autónoma de México y utilizando las pantallas gráficas de la aplicación desarrollada por la universidad Autónoma Metropolitana</p>



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
	<p>través del código de barras del funcionario.</p> <p>9. Realizar el cierre a través del código de barras y utilizando parámetros configurables en el sistema.</p> <p>10. Contabilizar los votos emitidos en las elecciones.</p> <p>11. Imprimir las actas de resultados.</p> <p>12. Generar el archivo de resultados y copiar el archivo de resultados y el archivo de log en un dispositivo extraíble USB.</p> <p>13. Al momento de generar el archivo de resultados la urna se deshabilita y se apaga y sólo puede ser encendida para efectos de auditoría.</p> <p>Esta aplicación esta desarrollada en lenguaje C++ con librerías de QT.</p>	<p>La aplicación esta basada en estados, es decir, cuando inician la urna no pueden realizar auditoría sino hasta que haya concluido la votación.</p> <p>La aplicación de la urna electrónica esta desarrollada con lenguaje C y bibliotecas gráficas GTK+.</p>			

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
4. Sistema de alimentación, batería	Circuito Diseñado por el propio Instituto Politécnico Nacional, el cual realiza conmutación de carga-alimentación-batería por medio de modulación de corriente, con alimentación independiente para impresora, cargador y placa base, el sistema cuenta con protección contra retorno de corriente.	Circuito Diseñado por la Universidad Nacional Autónoma de México, el cual realiza conmutación de carga-alimentación-batería por medio de relevador mecánico, con alimentación independiente para impresora, cargador y placa base.	Utilizan una batería comercial N-Charge Power Center, desarrollada por la empresa Valence Technology, Inc.	Circuito Diseñado por la UAM realizando conmutación de carga-alimentación-batería por medio de modulación de corriente, con alimentación independiente para impresora, cargador, placa base, sistema de control de activación.	Se propone tomar el dispositivo de carga del Instituto Politécnico Nacional que es el más compacto y cuenta con los cálculos detallados del consumo de corriente. En todas las propuestas la batería tiene similar tamaño y peso, con la excepción de la propuesta por el ITESM que es un costo más elevado.
5. Diseño de carcasa	Las carcasas serán construidas por medio de procesos de inyección de plástico en siete piezas: 1. Base, 2. Cubierta abatible exterior, 3. Cubierta de la pantalla de LCD, 4. Cubierta abatible del hardware y batería, 5. Contenedor de la impresora, 6. Cubierta abatible de acceso a la impresora y rollo de papel, 7. Contenedor de los votos. Peso total de la urna electrónica 9.5Kg incluyendo todos los componente y batería. El diseño de la carcasa permite el apilamiento. Incluye un arnés para conexiones externas de red, USB y sonido.	Todos los dispositivos y elementos que constituyen la urna están encapsulados en un solo paralelepípedo de 32 X 48 X 9cm. Esta diseñada ergonómicamente para que se puedan manipular la pantalla "touch screen" y los controles colocados en la parte inferior. Para su almacenamiento se puede apilar tanto horizontalmente como verticalmente. Esta desarrollado con plástico y PET, diseñado con características de seguridad, ergonomía, facilidad de uso, facilidad de transportación y almacenaje.	Cuenta con monitor con posiciones que permite ajustar a voluntad y reducir el espacio envolvente a la hora de almacenarla. La estructura del gabinete es su propio embalaje, esto permite que cada urna pueda ser tomada como una unidad y así generar estructuras mayores para poder apilarlas.	La carcasa se integra por dos partes: activador y urna. Ambos componentes permanecen unidos mientras se encuentran almacenados y para su traslado del centro de votación son separados por los funcionarios de casilla. La inclinación de la pantalla es ajustable. El material para la fabricación de la cubierta es desecho, recuperado de la basura. Además el diseño de la urna incluye una plantilla braille, como apoyo para débiles visuales.	Se propone tomar el diseño del Instituto Politécnico Nacional, ya que tiene mayor facilidad de manejo y propone combinar con la propuesta de la Universidad Autónoma Metropolitana, el cual es a través de materiales reciclados e incluir botones para discapacitados tomar la propuesta de la Universidad Nacional Autónoma de México.



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
7. Logística de operación de la urna y preparación previa y posterior a la jornada	<p>Pre-votación</p> <ul style="list-style-type: none"> ▪ Cargar de los listados de los números de serie de los dispositivos USB que serán utilizados en la elección en la aplicación MARU. ▪ Cargar de los catálogos para la elección en la base de datos Postgres. ▪ Generar todas las llaves públicas de las aplicaciones. ▪ Realizar la generación e impresión de los códigos de barra. ▪ Realizar la carga del sistema operativo en cada urna. ▪ Realizar la carga de la aplicación genérica en cada urna. ▪ Generar los dispositivos USB con los archivos de configuración de acuerdo a la sección y casilla. 	<p>Pre-votación</p> <ul style="list-style-type: none"> ▪ Realizar la carga de la base de datos con los datos correspondientes a los partidos, candidatos y formulas de elección y seleccionando los archivos binarios que contienen las indicaciones auditivas, logotipos de los partidos y fotografías de los candidatos. ▪ Hacer la compilación cruzada del Kernel del SO ▪ Realizar la compilación cruzada de la aplicación de la urna. ▪ Cargar el SO en la Urna. ▪ Cargar la aplicación en la urna. ▪ Cargar la USB genérica por distrito con todos sus datos (a partir de los cuales se personaliza para la sección y casilla específica). 	<p>Pre-votación</p> <ul style="list-style-type: none"> ▪ Realizar la carga de la base de datos de candidatos y partidos. ▪ Realizar la generación de boletas electrónicas ▪ Realizar la generación de Urnas ▪ Definir a los funcionarios de Casilla ▪ Crear las firmas electrónicas para funcionarios de casilla ▪ Realizar la carga de Urnas <ul style="list-style-type: none"> ▪ Verificación del estado de la memoria USB ▪ Generación del acta de creación de urna ▪ Impresión del acta de creación de urna ▪ Imprimir las firmas electrónicas de funcionarios de casilla correspondiente. ▪ Realizar el Empaquetamiento y lacrado de Actas, Firmas y Memoria USB ▪ Enviar las urnas y actas empaquetadas a la casilla 	<p>Pre-votación</p> <ul style="list-style-type: none"> ▪ Carga de los listados de los dispositivos USB y los dispositivos Bluetooth que serán utilizados en la elección en la aplicación del Generador de medios y la carga de los catálogos para la elección. ▪ Generación e impresión de los CUV (Códigos únicos de votación). ▪ Generación de claves de acceso para partidos políticos que serán ocupados para activar la aplicación de post-votación. ▪ Realizar la carga del Sistema operativo a través de flash card. ▪ En la propuesta se considera la carga del listado nominal en el identificador, por lo que se requiere se configure y se instale en cada uno de los identificadores (personalizado). 	<p>La propuesta es :</p> <p>Pre-votación</p> <ul style="list-style-type: none"> ▪ Realizar la carga de la base de datos con la información candidatos, partidos y formula de elección. ▪ Realizar la carga de los archivos binarios correspondientes a fotos de los candidatos emblemas de partidos políticos ▪ Revisión de Código fuente aplicaciones y Sistema Operativo ▪ Realizar la compilación de aplicaciones ante partidos políticos y funcionarios involucrados. ▪ Generación de firmas por partidos políticos y funcionarios involucrados. ▪ Realizar la carga de las baterías ▪ Generar los dispositivos USB con los datos para la configuración de las urnas. ▪ Realizar la carga del sistema



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
	<ul style="list-style-type: none"> ▪ Verificación y validación de la correcta operación de la batería. <p>Post-votación</p> <ul style="list-style-type: none"> ▪ Recepción de los dispositivos USB en el equipo Distrital. ▪ Recepción de las urnas 	<p>Post-votación</p> <ul style="list-style-type: none"> ▪ Recepción de las USB con los datos correspondientes a la elección. ▪ Almacenamiento de las urnas. 	<p>Post-votación</p> <ul style="list-style-type: none"> ▪ Recepción de los paquetes electorales en la sede distrital. ▪ Obtención de los dispositivos USB. ▪ Almacenamiento de los paquetes electorales 	<ul style="list-style-type: none"> ▪ Configurar los GPS para que cada urna pueda ser encendida en la fecha y hora correspondiente. ▪ Realizar el lacrado de urnas con las etiquetas propuestas. ▪ Realizar y verificar la carga de las baterías. <p>Post-votación</p> <ul style="list-style-type: none"> ▪ Recepción de los dispositivos USB ▪ Activación de la aplicación con las claves de cada uno de los partidos políticos ▪ Recepción de las urnas 	<p>operativo y de la aplicación genérica.</p> <ul style="list-style-type: none"> ▪ Verificación de la carga de urnas. ▪ Realizar el lacrado de urnas electrónicas ante partidos políticos y funcionarios involucrados. ▪ Remitir las urnas a las sedes distritales. <p>Post-votación</p> <ul style="list-style-type: none"> ▪ Recepción de los paquetes electorales en la sede distrital ▪ Recepción de las urnas ▪ Revisión del lacrado de las urnas ▪ Obtención de los dispositivos USB. ▪ Almacenamiento de paquetes electorales <p>Se deben contemplar los métodos y lugares de almacenamiento de urnas, teniendo en cuenta que algunas contienen baterías de plomo-ácido. Así mismo se debe preparar la for</p>

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
					de carga de las baterías, ya que, en forma masiva, requiere un gran consumo de corriente.
3. Contingencia	<p>Cualquier falla en la urna electrónica amerita ser cambiada por una urna de contingencia, en la cual se inserta el dispositivo USB que fue extraído de la urna que falló. Se enciende la urna y se continúa con la operación normal.</p> <p>Nota: El archivo de log no se transfiere a la urna de contingencia sólo el archivo de votos.</p>	<p>Cualquier falla en la urna electrónica amerita ser cambiada por una urna de contingencia, en la cual se inserta el dispositivo USB que fue extraído de la urna que falló. Se enciende la urna y se continúa con la operación normal.</p> <p>Nota: El archivo de log no se transfiere a la urna de contingencia sólo el archivo de votos.</p>	No consideran contingencias.	No consideran contingencias.	Se propone tomar el procedimiento de contingencia del Instituto Politécnico Nacional y la Unidad de Informática incluirá otros procedimientos de contingencia referentes a recuperación de datos, recepción y transmisión de datos.
9. Identificación del votante	Método tradicional	Método tradicional	Método tradicional	Es una aplicación en C++, en donde se propone que la credencial de elector sea leída por el lector de cinta magnética. El ciudadano es buscado a través de un método binario en la lista nominal que corresponde a la casilla y se realiza la verificación si el elector existe en la lista nominal, si ya ejerció su voto, si no ha votado pero si le proporcionó el código de barras para activar la urna y si el elector no ha votado	Se propone utilizar un dispositivo para identificación del elector a través de un lector infrarrojo que permita visualizar fotografía y datos generales del elector y guarde un registro que indique si el elector ya emitió su voto o no. Por lo tanto, la Unidad de Informática propone utilizar un dispositivo para la identificación de los electores basada en la credencial para votar con fotografía.



INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

SECRETARÍA EJECUTIVA

UNIDAD DE INFORMÁTICA

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
10. Activación de la urna	Se lleva a cabo por medio de un lector de código de barras integrado a la urna electrónica.	Se realiza con una contraseña de acceso, que es proporcionada por los funcionarios de casilla. Están implementando un sistema de activación (en fase de desarrollo) con PIC's (circuitos integrados de Microchip Technology Inc.), que pertenece a la categoría de los microcontroladores es decir, aquellos componentes que integran en un único dispositivo todos los circuitos necesarios para realizar un completo sistema digital programable.	Se realiza por medio de un dispositivo adicional que puede controlar hasta 8 urnas por medio de Radio Frecuencia, con semáforos para cada urna. El dispositivo activador integra un circuito electrónico controlado por un microprocesador (8051) con un transmisor-receptor por cada urna; adicionalmente requiere un circuito transmisor-receptor en cada urna, conectado a través del puerto serial.	Es a través de bluetooth el cual se sincroniza con la urna para aceptar solo el código de barras que ha sido leído en el activador. Posteriormente, ese código de barras es leído y aceptado por la urna para su activación. La comunicación es por una banda de frecuencia abierta ISM (médico-científica internacional), con rangos que van de los 2.400 Mhz a los 2.500 Mhz. El dispositivo Bluetooth utiliza un sistema FH/TDD (salto de frecuencia/división de tiempo duplex). El bluetooth permite dar seguimiento al proceso de votación, ya que la aplicación contiene un simulador de semáforo.	Se propone tomar el mecanismo de la Universidad Nacional Autónoma de México ya que el activador debe ser un sistema que sólo requiera operar un botón para habilitar la urna, ya sea de manera remota o conectada a través de cables.

Componente	Instituciones educativas				Integración
	Instituto Politécnico Nacional	Universidad Nacional Autónoma de México	Instituto Tecnológico y de Estudios Superiores de Monterrey	Universidad Autónoma Metropolitana	
11. Instalación de la urna (Interacción del funcionario de casilla con la urna el día de la elección)	<p>Se realiza el borrado y la instalación del sistema operativo a través de la función de arranque por medio de Compact Flash.</p> <p>Realiza una instalación de sistema operativo y posteriormente de la aplicación de urna genérica.</p> <p>El funcionario inserta el dispositivo USB y el proceso de configuración se inicia hasta que se lee el código de barras del funcionario.</p>	<p>Se realiza el borrado y la instalación del sistema operativo a través de la función de arranque por medio de red.</p> <p>Realiza una instalación de sistema operativo y aplicación de urna conjuntamente.</p> <p>Se personaliza la urna electrónica seleccionando los datos de una sección en específico y un tipo de casilla y presionando una clave de acceso.</p>	<p>Se realiza el borrado y la instalación del sistema operativo a través de la función de arranque por medio de la red.</p> <p>Se copia la aplicación al dispositivo USB y se carga en la urna.</p>	<p>Se realiza el borrado y la instalación del sistema operativo a través de la función de arranque por medio de Compact Flash.</p> <p>Realiza una instalación de sistema operativo y posteriormente de aplicación de urna genérica</p> <p>El funcionario inserta el dispositivo USB en la urna y se inicia el proceso de instalación con la búsqueda de la información en la USB y copia los archivos para la configuración. No hay ningún mecanismo para instalar la urna.</p>	<p>Se propone realizar la carga del sistema operativo y de la aplicación genérica conjuntamente.</p> <p>Posteriormente, realizar la instalación a través de una llave que permita el arranque y configuración de la urna.</p>