



**UACH**  
UNIVERSIDAD AUTÓNOMA DE  
**CHIHUAHUA**

**Reporte de la auditoría  
al Sistema de Cómputo de las Urnas Electrónicas  
para el proceso del  
Plebiscito 2019**

**22 de noviembre de 2019  
Chihuahua, Chih.**



**INSTITUTO ESTATAL ELECTORAL  
CHIHUAHUA**

**Audidores:**

**José Rómulo Barrón Hernández**

**Víctor Alonso Domínguez Ríos**

**Arión Ehécatl Juárez Menchaca**

*[Handwritten signatures in blue ink]*

# Contenido

Contenido	2
I. Introducción	3
II. Revisión del código y bases de datos	4
Resultados de la revisión de código y base de datos	11
III. Pruebas funcionales de caja negra.	13
Generación de archivos para habilitar urnas.	13
Emisión de votos	16
Cierre de la votación en la urna	22
Concentración de resultados	24
Generación de hash SHA-256 y SHA-512	26
Resultados de las pruebas funcionales de caja negra	27
IV. Revisión del hash del sistema de cómputo en las urnas electrónicas	28
Resultados de las pruebas de revisión de hash	32
V. Conclusiones	33



# I. Introducción

Con el objetivo de realizar las pruebas funcionales de caja negra, caja blanca, y verificación de hash a los sistemas de cómputo a utilizarse en el plebiscito 2019 en la ciudad de Chihuahua, se llevó a cabo una serie de reuniones de trabajo donde se realizó en primera instancia una revisión al código del sistema y un análisis a la base de datos que concentrará los votos emitidos en la jornada, asimismo, se realizó un simulacro de votación en 4 urnas dispuestas por el Instituto Estatal Electoral (IEE) de Chihuahua para las pruebas funcionales de caja negra, en las cuales se realizó el proceso de carga de la urna, la apertura, proceso de votación, cierre de urna, exportación de archivo con los votos y concentración de resultados. Por último, se comprobó que los programas cargados en las urnas electrónicas fueran los mismos presentados para las pruebas funcionales, dando con esto mayor certidumbre al proceso que se llevará a cabo el 24 de noviembre de 2019.

A handwritten signature in blue ink, consisting of several loops and a horizontal line at the bottom.

## II. Revisión del código y bases de datos

Parte de la auditoría se llevó a cabo el día 15 de noviembre del 2019, iniciando con una parte pruebas de caja negra, donde la funcionalidad se verifica sin tomar en cuenta la estructura interna de código, detalles de implementación o escenarios de ejecución internos en el software.

Esta revisión se llevó a cabo en el Módulo de Administración, en el Sistema de Voto Electrónico, Bases de Datos y en el Sistema Concentrador de Resultados.

En el módulo de administración se revisaron las opciones que le aparecerán al usuario, en este caso contempla 3; SI, NO y DESEO ANULAR MI VOTO, como se muestra en la Imagen 2.1.

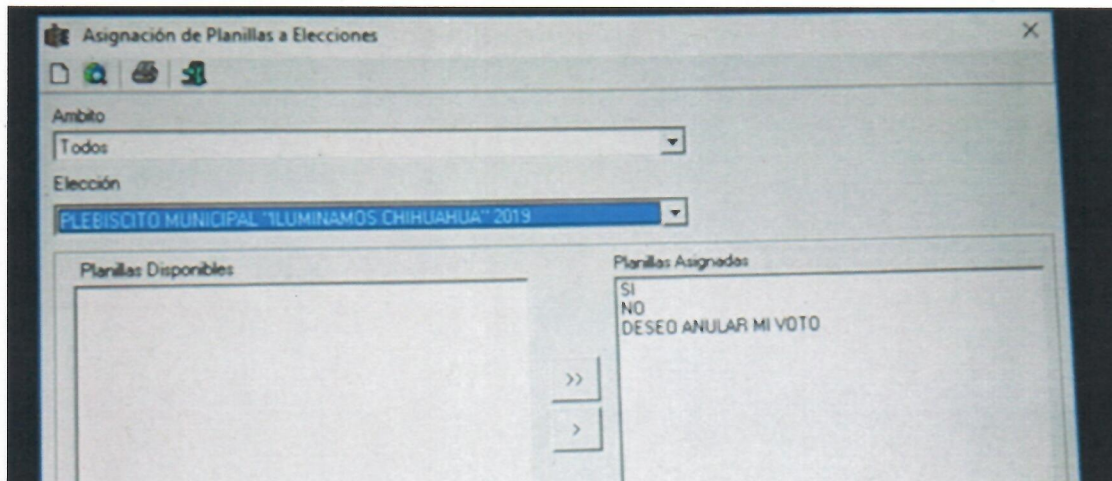


Imagen 1.1. Configuración de opciones para mostrar en pantalla de votación.

Debido a que existen variantes en las urnas electrónicas, se genera una plantilla horizontal o vertical según sea el tipo, manejando esta configuración en la parte de la administración del sistema (Imagen 2.2).

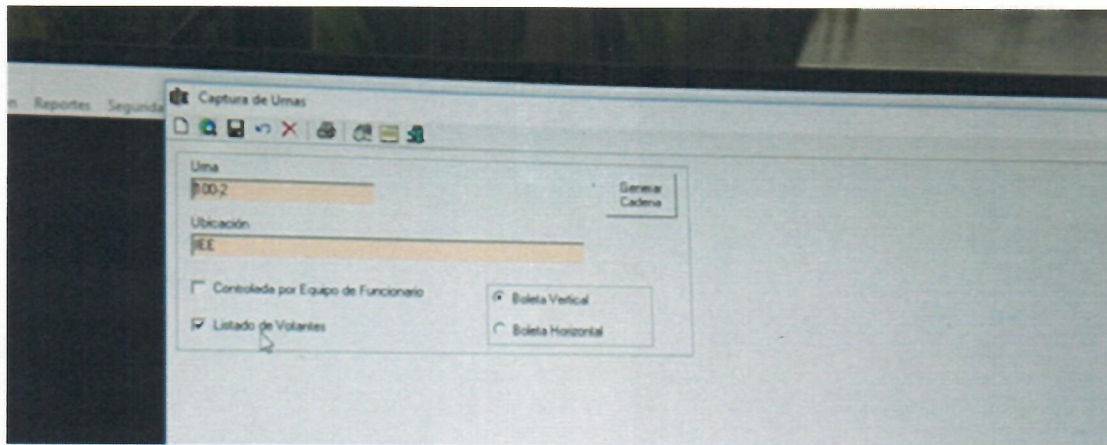


Imagen 2.2. Configuración de presentación de la boleta en pantalla de la urna.

La pantalla que se mostrará a los habitantes de la ciudad de Chihuahua muestra la consulta, dando las 3 opciones mencionadas anteriormente, SI, NO y DESEO ANULAR MI VOTO como se muestra en la Imagen 2.3.

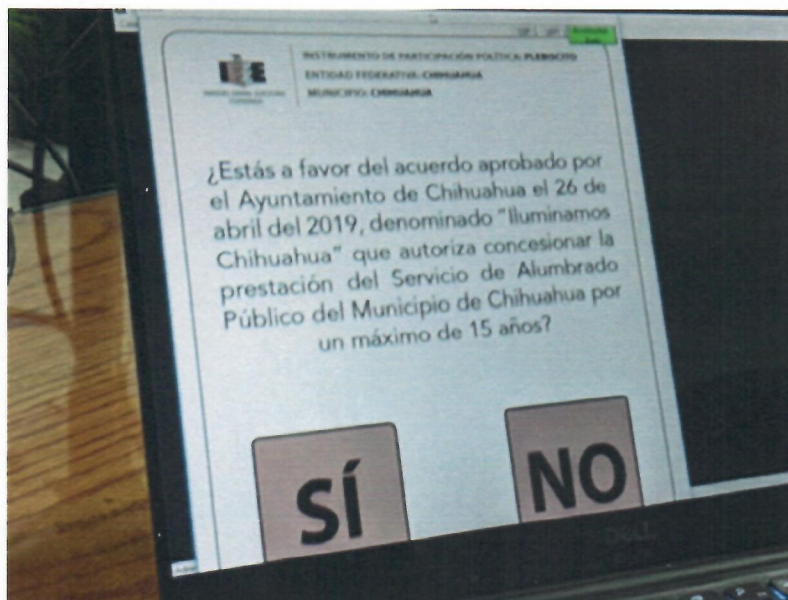


Imagen 2.3. Formato de presentación de consulta vertical

Lo siguiente a verificar son las tarjetas de privilegios dentro del sistema, para ello se imprimen con un código de barras (Imagen 2.4), que será leído por el sistema, dentro de las opciones se cuenta con la "Clave" para inicializar la urna, supervisor para cuestiones de supervisión, "código de salida" para si una persona quiere salir de la

votación sin elegir las opciones que se le presentan. Esto garantiza que los usuarios de las urnas no puedan realizar movimientos sin el consentimiento de los encargados de las urnas.

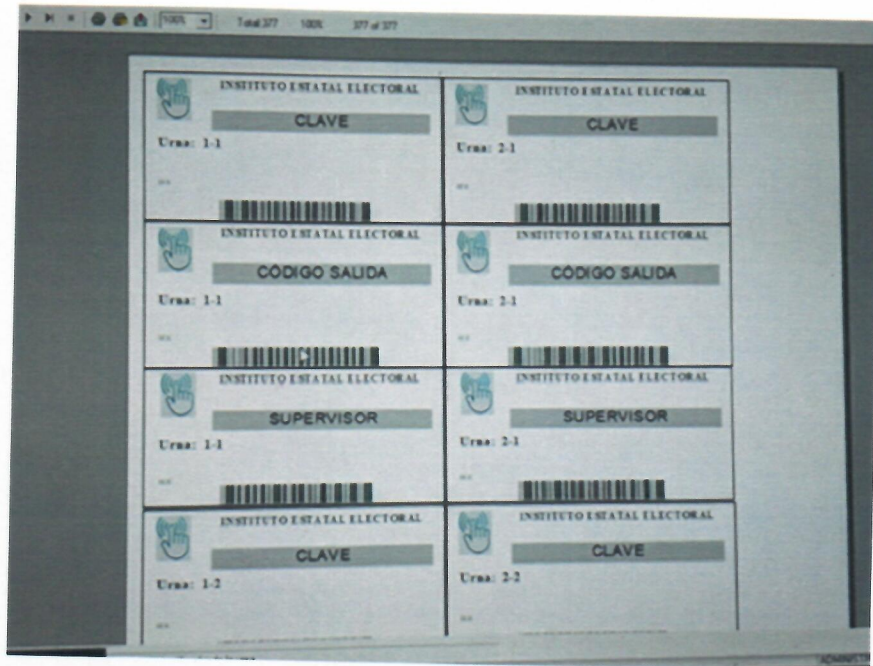


Imagen 2.4. Tarjetas de permisos dentro del sistema de voto

*[Handwritten signatures in blue ink]*

El sistema tiene una serie de configuraciones para el sistema de votación, entre las configuraciones tiene la opción de habilitar la captura de la credencial de elector de manera manual, en caso de que el lector no pueda reconocerlo como se puede apreciar en la Imagen 2.5.

Configuración de Opciones del Sistema

Datos de la Institución

Nombre de la Institución  
INSTITUTO ESTATAL ELECTORAL

Dirección  
CONOCIDO

Municipio  
CHIHUAHUA

Localidad  
CHIHUAHUA

Opciones del Sistema

Registro de Planillas

Validar un solo cargo por planilla

Validar que un elector sea integrante solo de una planilla

Validar que las planillas tengan completos los cargos

Fecha Elección  
15/11/2019

Desplegar en boleta de votación

Desplegar el Nombre de las Planillas

Desplegar las Siglas de las Planillas

Imprimir en Reportes

Desplegar el Nombre de las Planillas

Desplegar las Siglas de las Planillas

Impresión de comprobante

Imprimir Comprobante

No Imprimir Comprobante

Nombre de la Planilla

Siglas de la Planilla

Imprimir grupo de votación

Pantalla Inicio de Votación

Mostrar Datos del Votante

Mostrar última activación

Poder Iniciar con Clave Manual

No

Opcional

Visible Inicio

Controlada por Mesa

Título Mostrar Datos DATOS DEL CIUDADANO

Voz

Habilitar Voz

Voz al seleccionar una opción y cambio de página

Cierre de Urna

Total por Elección

Total por Elección por Grupo

Temas

Base de Datos

Versión BD  
2019.10

Escriba el Nombre de la Escuela

*[Handwritten signature]*

*[Handwritten signature]*

*[Handwritten signature]*

Imagen 2.5. Configuraciones del sistema

Asimismo, se observa la captura manual de votos de la urna en caso de que la carga del archivo o generación de este tuviera algún problema, una vez capturado manualmente, ya no permite la carga por archivo (Imagen 2.6).

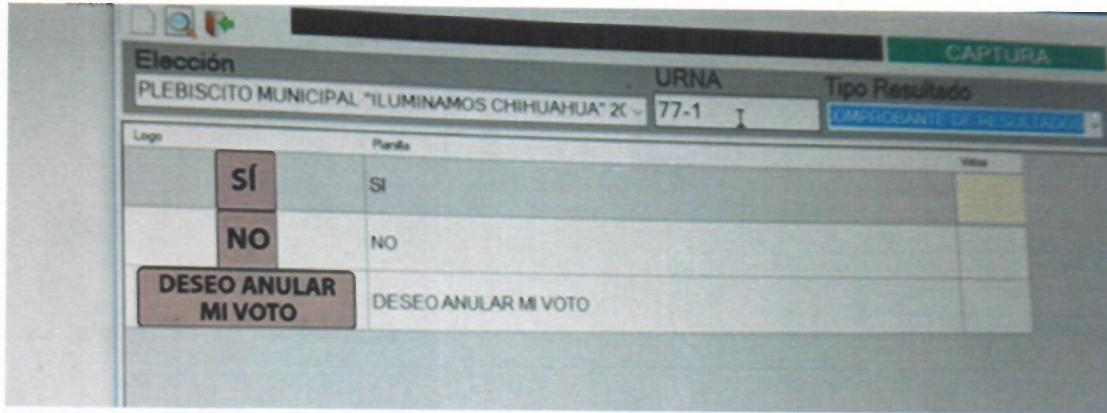


Imagen 2.6. Captura de los resultados de la urna de manera manual.

Una vez revisada las opciones de configuración, se procedió a las pruebas funcionales de caja negra y caja blanca del sistema de votación que usarán los ciudadanos. Se da inicio a la urna generando el archivo que será cargado (Imagen 2.7).

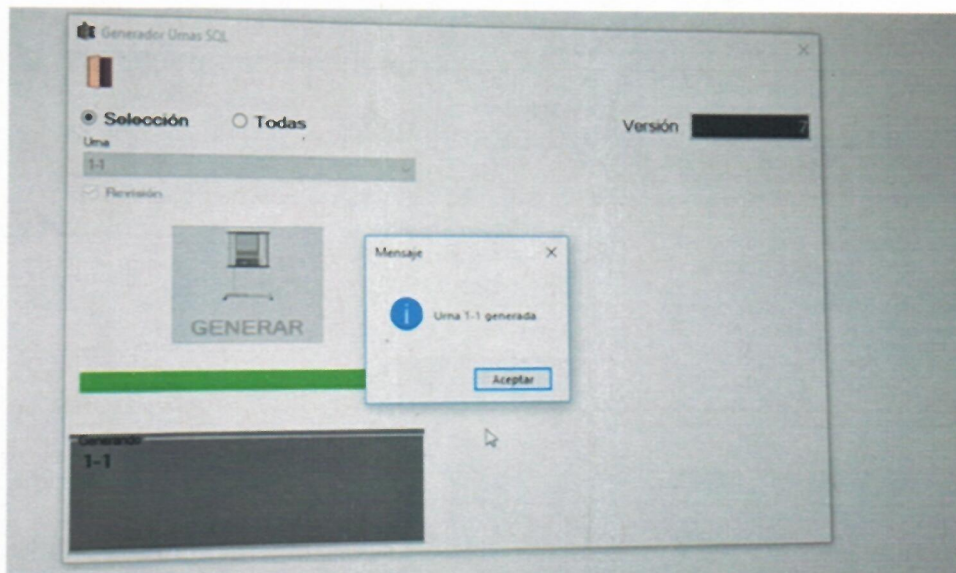


Imagen 2.7. Generación de archivo de inicio de la urna electrónica.

El archivo se encuentra encriptado (Imagen 8) para garantizar que no sea modificado antes de ser cargado en la urna.

*Handwritten signature in blue ink, possibly 'JP'.*



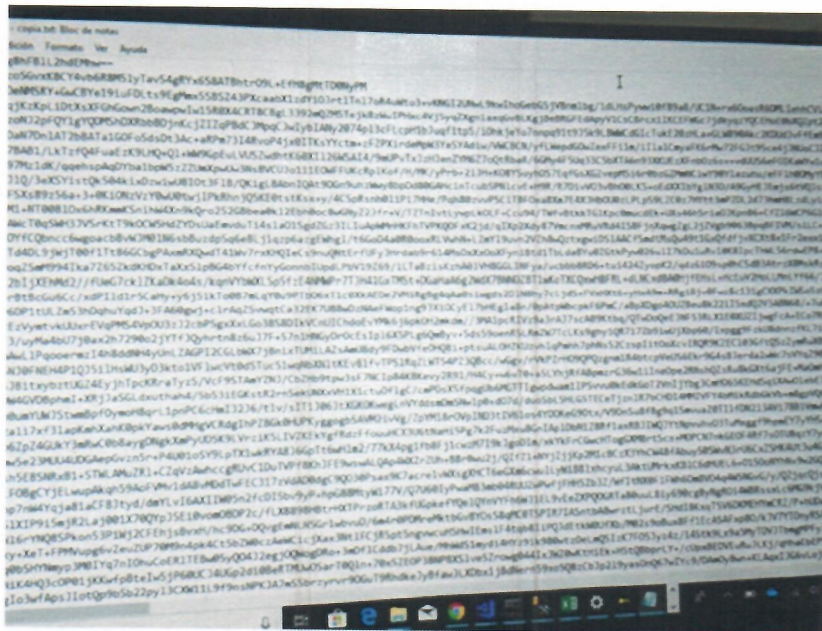


Imagen 2.8. Archivo de carga de urna encriptado.

En la Imagen 2.9 se muestra una de las urnas a utilizar en el plebiscito de 2019, con una configuración vertical.



Imagen 2.9. Urna electrónica en configuración vertical.

*[Handwritten signatures and initials in blue ink, including a large signature and the initials 'JP' at the bottom.]*

Una vez cargado el archivo, se procede a habilitar la urna, se tiene que verificar las secciones que le correspondan a la urna, como se muestra en la imagen 2.10.

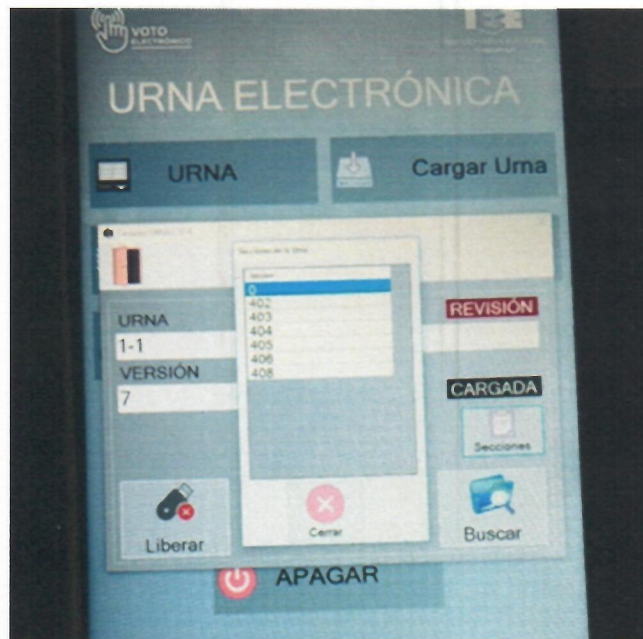


Imagen 2.10. Verificación de secciones que corresponden a la urna

Se verifica que la votación esté en ceros (Imagen 2.12), revisando también la base de datos comprobando que las tablas correspondientes a los registros de votación también estén vacías (Imagen 2.13).

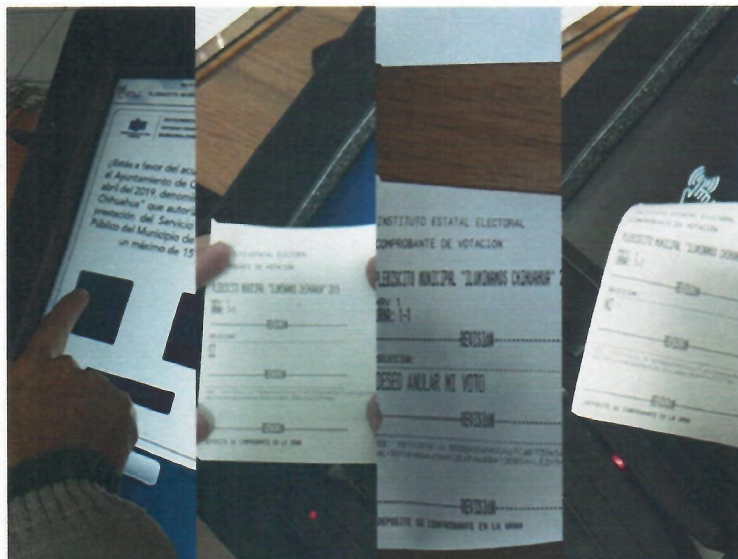


Imagen 2.11. Impresión de votos emitidos.

*[Handwritten signature]*  
*[Handwritten signature]*  
*[Handwritten signature]*

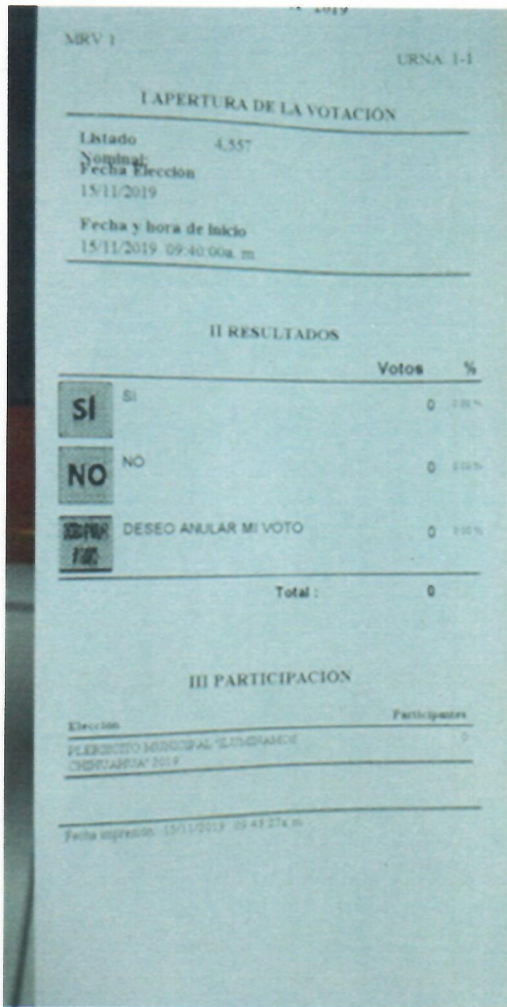


Imagen 2.12. Inicio de la votación en ceros.

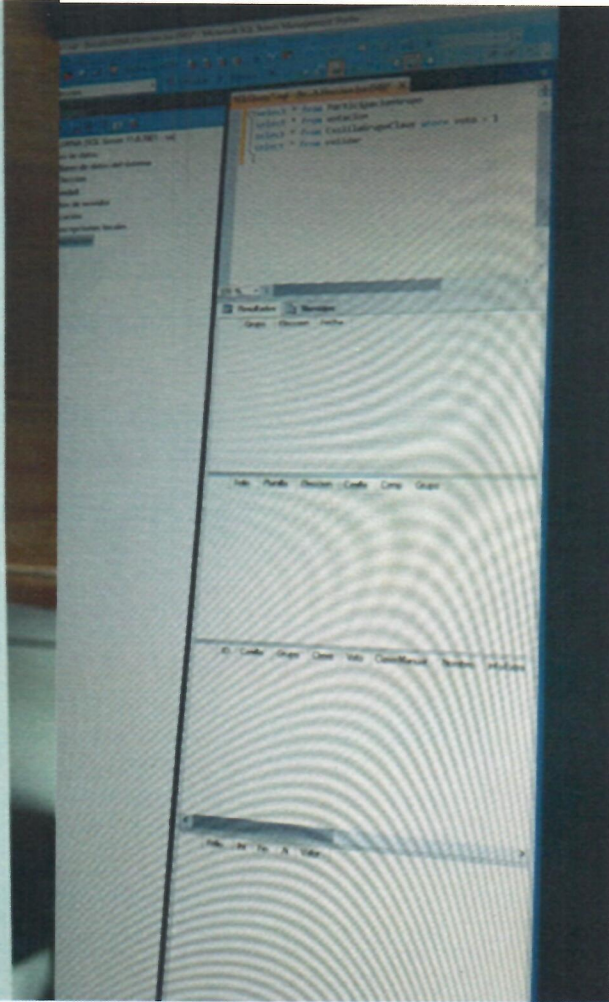


Imagen 2.13. Base de datos sin registros

*[Handwritten signatures in blue ink]*

## Resultados de la revisión de código y base de datos

- El sistema cumple los requerimientos para la emisión del voto por parte de los ciudadanos, almacenándolos en la base de datos local de cada urna, para posteriormente hacer la unión de todas las bases para el conteo total del plebiscito.
- Se garantiza la secrecía del voto con el sistema, ya que se verificó que no hubiera registro en las bases de datos de quien emite cada voto tanto en el código del programa como en sus bases de datos, y a su vez se verifica que no hubiera desencadenadores que pudieran afectar la confiabilidad del sistema.

- Para garantizar una mayor secrecía, se solicita al IEE deshabilitar el log que trae por default el manejador de base de datos, en el cual se puede tener un registro de la hora en que se realizó cada inserción a la base de datos.
- Debido a que las urnas no cuentan con conexión de red, puede haber duplicidad de votos en la sección (aunque esto es complicado debido a que hay una persona encargada de verificar si ya emitió su voto), por lo que se recomienda para actualizaciones futuras tener una comunicación al menos de manera local entre las urnas de la sección para garantizar el proceso.
- Asimismo, se hace mención que, aunque no forma parte del sistema de cómputo, la necesidad de poner a las urnas un mecanismo que impida ver la posición en la pantalla que selecciona el usuario, conociendo con esto la selección de su votación.
- Se encuentra una vulnerabilidad en la forma de extraer la información de la urna una vez realizada la votación, el hecho de tener que utilizar una USB para posteriormente pasarla a otra computadora, implica tener un alto control del proceso, se encuentra aun así que la información está encriptada para una mayor seguridad.
- Se debe tener una revisión de que la base de datos sea la misma en todos los equipos, ya que se detectó que, si hay una actualización de la base de datos y al no estar en red, se tiene que actualizar manualmente en todos los equipos.



### III. Pruebas funcionales de caja negra.

En las pruebas funcionales de caja negra, se enfoca solamente en las entradas y salidas del sistema, sin preocuparse en tener conocimiento de la estructura interna del programa de software. Para obtener el detalle de cuáles deben ser esas entradas y salidas, se tiene que basar en los requerimientos de software y especificaciones funcionales.

Para la prueba de caja negra, se contó con cuatro urnas de distintos modelos, de las cuales 3 modelos cuentan con Windows 10 como Sistema Operativo, y un modelo con Windows 7 (imagen 3.1). El sistema para la votación fue desarrollado en Visual Basic y la base de datos con Microsoft SQL Server Express 2012.



Imagen 3.1. Modelos de urnas disponibles para el plebiscito 2019

#### Generación de archivos para habilitar urnas.

Como inicio de las pruebas funcionales, se verificó la generación de archivos de cada urna, donde carga la lista nominal que le corresponde (imagen 3.2), este archivo se

*[Handwritten signatures in blue ink]*

encuentra encriptado para una mayor seguridad. Paso siguiente fue cargar desde la urna correspondiente el archivo que se encuentra ya localizado en una memoria USB (imagen 3.3).

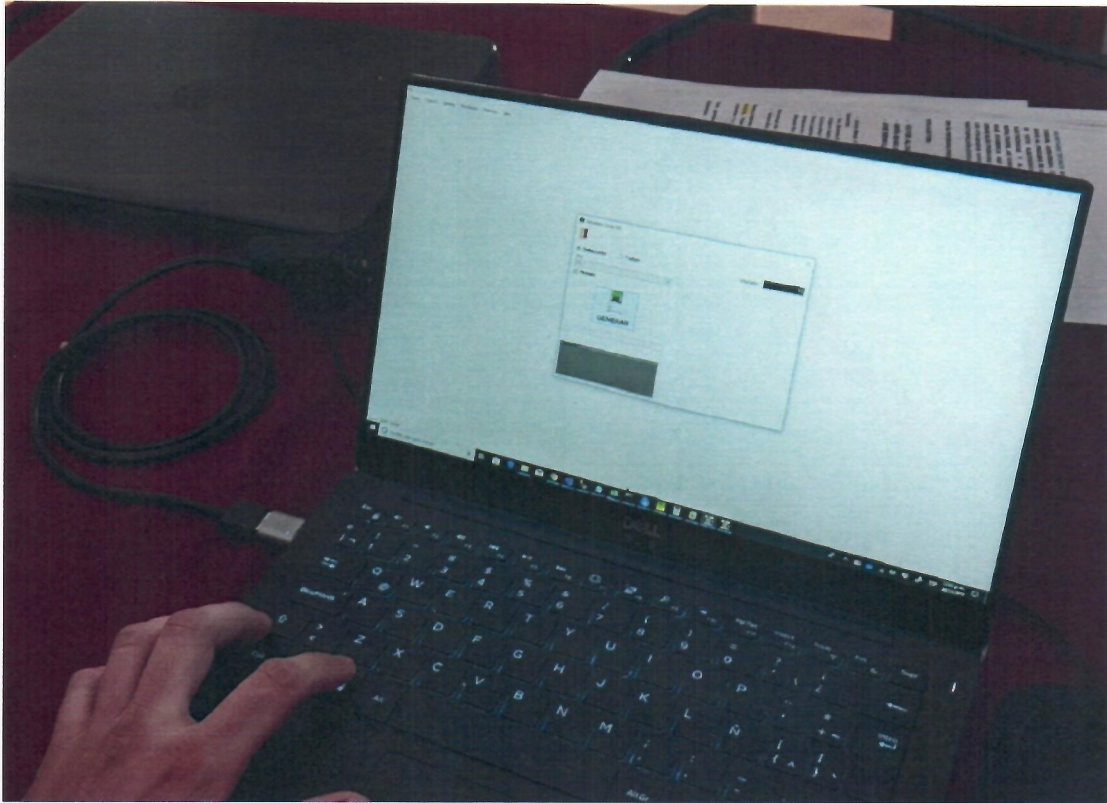


Imagen 3.2. Carga de archivo con la generación de datos para las urnas electrónicas

*[Handwritten signature]*  
*[Handwritten signature]*  
*[Handwritten signature]*

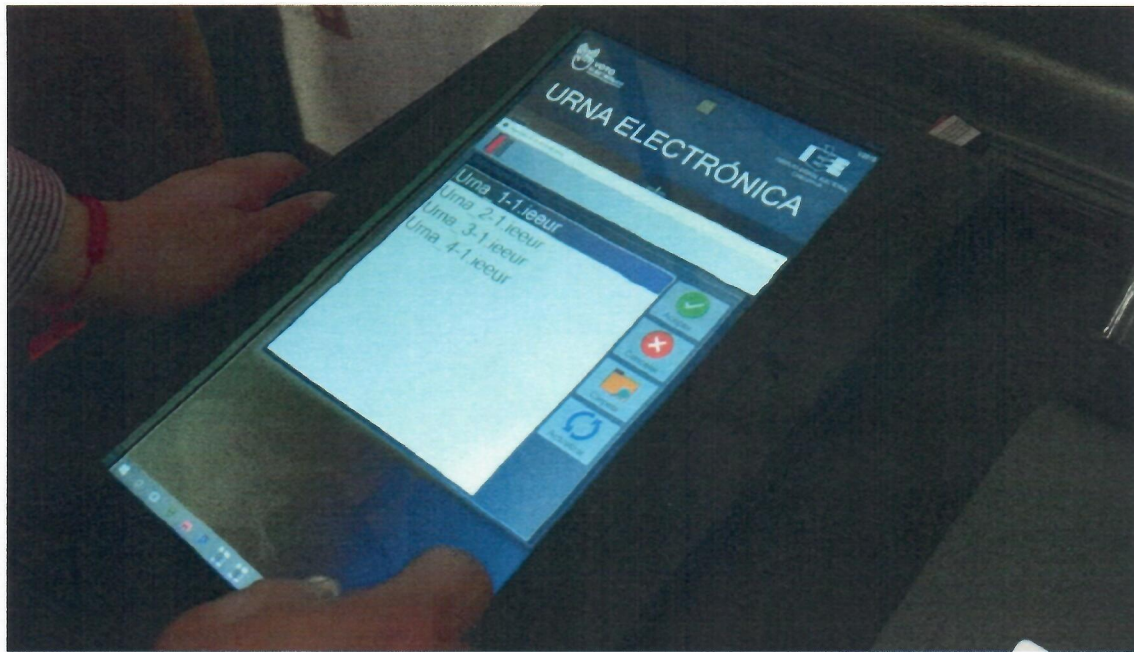


Imagen 3.3. Selección del archivo correspondiente a la urna para la carga e inicio de la urna

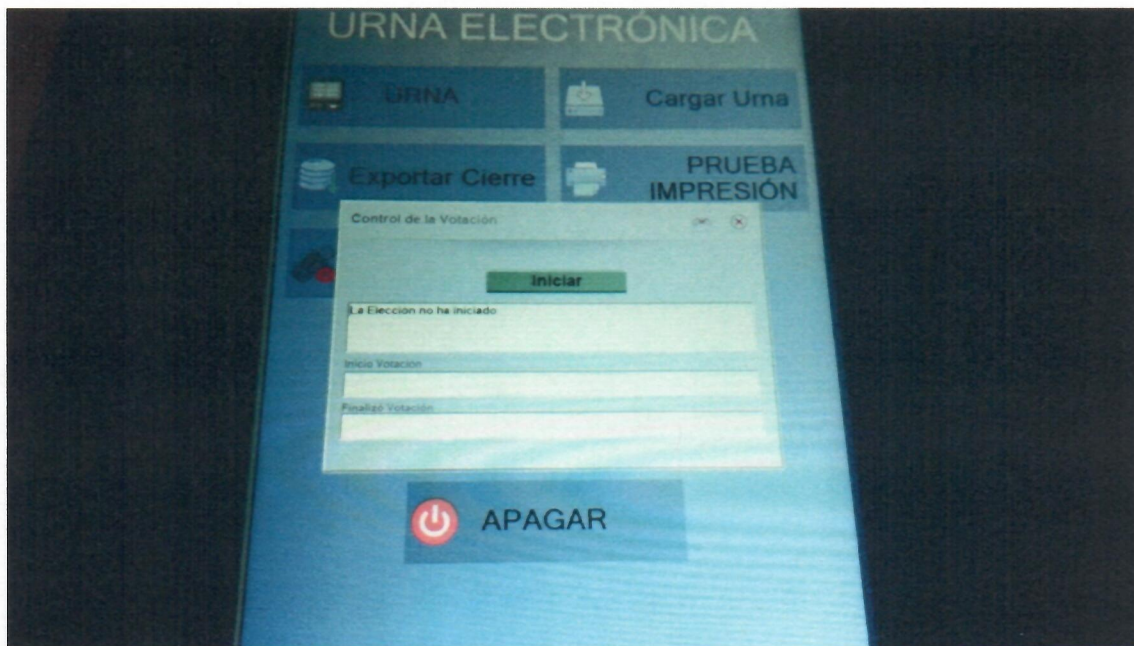


Imagen3. 4. Proceso de inicio de la votación

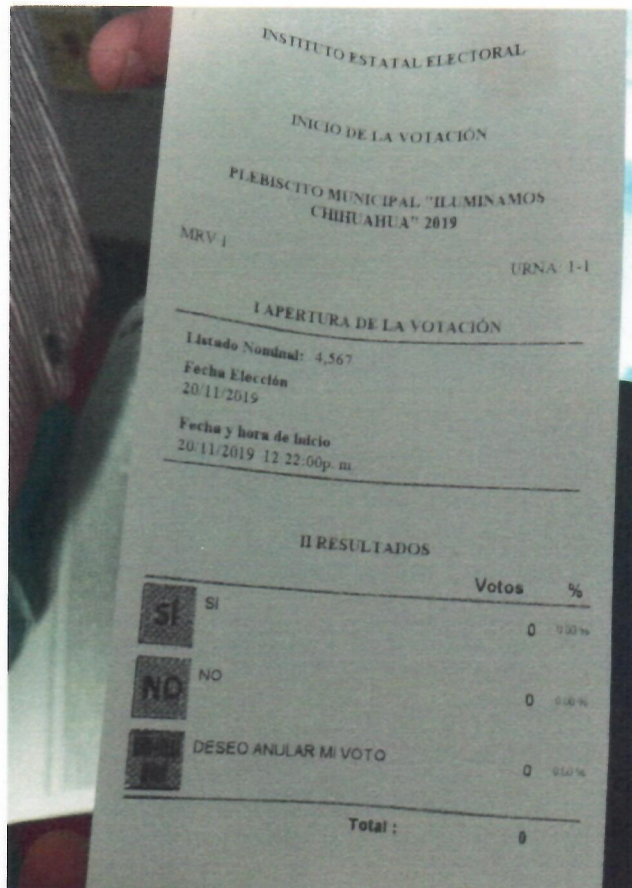


Imagen 3.5. Reporte de resultados en ceros para iniciar el proceso de votación

Este proceso de carga da inicio a las bases de datos para que el sistema de votación inicie en ceros, como se muestra en la imagen 3.4 y 3.5. Esta acción de verificar que las votaciones en las urnas inician en cero se realizó en los 4 modelos disponibles para las pruebas.

## Emisión de votos

Una vez verificado que el reporte muestra ceros las 3 opciones disponibles (SI, NO, DESEO ANULAR MI VOTO), se da inicio a la votación, introduciendo el OCR de la credencial elector. Se realiza este proceso en cada urna disponible, como resultado, en la primera urna se introducen 4 votos con la opción SI, 3 con la opción No y 3 con la opción DESEO ANULAR MI VOTO, en la imagen 3.6 se observa el registro manual y en la imagen 3.7 el reporte que imprime el sistema con los resultados.

*[Handwritten signatures in blue ink]*



INSTITUTO ESTADAL ELECTORAL CHIHUAHUA  
 AUDITORIA VOTO ELECTRÓNICO  
 RESULTADOS DE LA VOTACIÓN POR URNA  
 UACH CHIHUAHUA

FECHA: 20/11/2019  
 HORA: 12:10pm

**URNA 1**

											TOTAL	
SI	✓	✓	✓	✓								4
NO	✓	✓	✓									3
NULO	✓	✓	✓									3

Imagen 3.6. Registro manual de los votos emitidos en la urna 1

INSTITUTO ESTADAL ELECTORAL CHIHUAHUA 2019  
 MRV 1  
 I CIERRE DE LA VOTACIÓN

Fecha Elección: 20/11/2019  
 Fecha y hora de cierre: 20/11/2019 12:31:00p. m.

**II RESULTADOS**

	Votos	%
<b>SI</b> SI	4	40%
<b>NO</b> NO	3	30%
<b>DESEO ANULAR MI VOTO</b>	3	30%
<b>Total:</b>	10	

**III PARTICIPACIÓN**

Imagen 3.7. Reporte de votos de la urna 1

Se observa entonces que los votos que reporta el sistema son los mismos que se emitieron como prueba de caja negra para la urna 1. En la imagen 3.8 se observan los votos contabilizados manualmente y por sistema. Este mismo procedimiento se realiza en las urnas 2 (imagen 3.9), 3 (imagen 3.10) y 4 (imagen 3.11).

**AUDITORIA VOTO RESULTADOS DE LA VOTACION**

**INSTITUTO ESTADAL ELECTORAL** **UACH CHIHUAHUA**

**CIERRE DE LA VOTACION**

PLEBISCITO MUNICIPAL "ILUMINAMOS CHIHUAHUA" 2019

CHA: 20/11/2019  
ORA: 12:10pm

MRE: 1 URNA: 1-1

**I CIERRE DE LA VOTACION**

**URNA**

Fecha Eleccion: 20/11/2019  
Fecha y hora de cierre: 20/11/2019 12:31:00pm

**II RESULTADOS**

	Votos	%
SI	4	40.00%
NO	3	30.00%
DESEO ANULAR MI VOTO	3	30.00%
<b>Total</b>	<b>10</b>	

**III PARTICIPACION**

Electores: Participantes:

**TOTAL**

4  
3  
3

Imagen 3.8. Comparación de votos en la urna 1

*[Handwritten signatures and initials in blue ink]*

**INSTITUTO ESTADAL ELECTORAL**  
**AUDITORIA VOTO E**  
**RESULTADOS DE LA VOT**

**UACH**  
**CHIHUAHUA**

**INSTITUTO ESTADAL ELECTORAL**  
**CIERRE DE LA VOTACION**  
**PLEBISCITO MUNICIPAL "ILUMINAMOS CHIHUAHUA" 2019**

MRV 2 URNA 2-1  
 CHA: 20/11/2019  
 ORA: 12:38 pm

**I CIERRE DE LA VOTACION**

Fecha Eleccion: 20/11/2019  
 Fecha y hora de cierre: 20/11/2019 12:39:00p.m.

**II RESULTADOS**

	Votos	%
SI	3	37.50%
NO	4	50.00%
DESEO ANULAR MI VOTO	1	12.50%
<b>Total</b>	<b>8</b>	

**III PARTICIPACION**

Elecciones: PLEBISCITO MUNICIPAL "ILUMINAMOS CHIHUAHUA" 2019  
 Participantes: 8

**URNA 2**

SI: [✓] [✓] [✓] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

NO: [✓] [✓] [✓] [✓] [ ] [ ] [ ] [ ] [ ] [ ]

NULO: [✓] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

**TOTAL**

SI: 3  
 NO: 4  
 DESEO ANULAR MI VOTO: 1

Imagen 3.9. Comparación de votos en la urna 2

**INSTITUTO ESTADAL ELECTORAL**  
**AUDITORIA VOTO E**  
**RESULTADOS DE LA VOT**

**UACH**  
**CHIHUAHUA**

**INSTITUTO ESTADAL ELECTORAL**  
**CIERRE DE LA VOTACION**  
**PLEBISCITO MUNICIPAL "ILUMINAMOS CHIHUAHUA" 2019**

MRV 3 URNA 3-1  
 CHA: 20/11/2019  
 ORA: 12:45 pm

**I CIERRE DE LA VOTACION**

Fecha Eleccion: 20/11/2019  
 Fecha y hora de cierre: 20/11/2019 12:46:00p.m.

**II RESULTADOS**

	Votos	%
SI	0	0.00%
NO	6	100.00%
DESEO ANULAR MI VOTO	0	0.00%
<b>Total</b>	<b>6</b>	

**III PARTICIPACION**

Elecciones: PLEBISCITO MUNICIPAL "ILUMINAMOS CHIHUAHUA" 2019  
 Participantes: 6

**URNA 3**

SI: [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

NO: [✓] [✓] [✓] [✓] [✓] [✓] [ ] [ ] [ ] [ ]

NULO: [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

**TOTAL**

SI: 0  
 NO: 6  
 DESEO ANULAR MI VOTO: 0

Imagen 3.10. Comparación de votos en la urna 3

*[Handwritten signatures and scribbles in blue ink]*

**AUDITORIA VOTO ELE**  
**RESULTADOS DE LA VOTAC**

INSTITUTO ESTATAL ELECTORAL

CIERRE DE LA VOTACIÓN

PLEBISCITO MUNICIPAL "ILUMINAMOS CHIHUAHUA" 2019

MRV 4 URNA: 4-1

20/11/2019

**URNA 4**

SI: [6 checkmarks]

NO: [5 checkmarks]

NULO: [0 checkmarks]

**II RESULTADOS**

	Votos	%
SI	7	58.3%
NO	5	41.7%
DESEO ANULAR MI VOTO	0	0%
<b>Total</b>	<b>12</b>	

**III PARTICIPACIÓN**

Fecha Elección: 20/11/2019  
Fecha y hora de cierre: 20/11/2019 12:55:59p. m.

**TOTAL**

7

5

0

Imagen 3.11. Comparación de votos en la urna 4

Asimismo, en cada voto emitido el sistema imprime el comprobante, para ser depositado en la urna de manera física, en las imágenes de la 3.12 a la 3.19 se observa los comprobantes obtenidos de la votación de la urna 2

INSTITUTO ESTATAL ELECTORAL  
COMPROBANTE DE VOTACIÓN  
PLEBISCITO MUNICIPAL "ILUMINAMOS CHIHUAHUA"  
MRV 2  
URNA 2-1

REVISIÓN

SELECCIÓN

DESEO ANULAR MI VOTO

REVISIÓN

REVISIÓN

DEPOSITE SU COMPROBANTE EN LA URNA

INSTITUTO ESTATAL ELECTORAL  
COMPROBANTE DE VOTACIÓN  
PLEBISCITO MUNICIPAL "ILUMINAMOS CHIHUAHUA"  
MRV 2  
URNA 2-1

REVISIÓN

SELECCIÓN

SI

REVISIÓN

REVISIÓN

DEPOSITE SU COMPROBANTE EN LA URNA

Imagen 3.12 y 3.13. Voto emitido en la urna 2

*[Handwritten signature]*

*[Handwritten signature]*

*[Handwritten signature]*

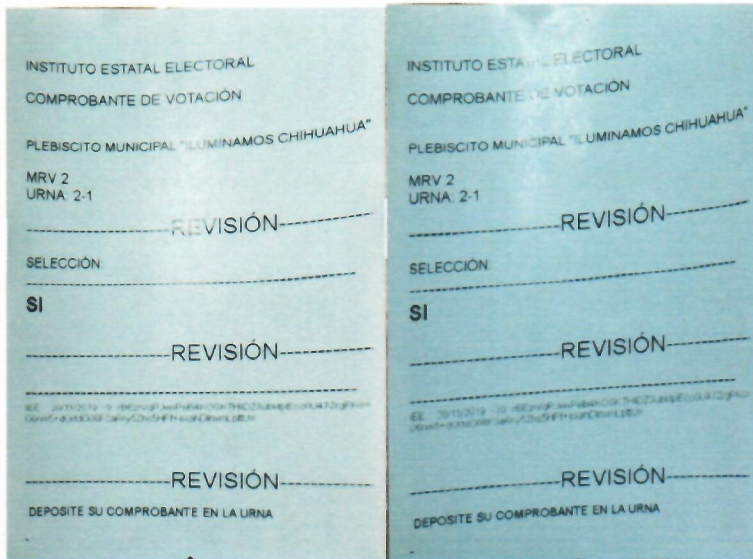


Imagen 3.14 y 3.15. Voto emitido en la urna 2

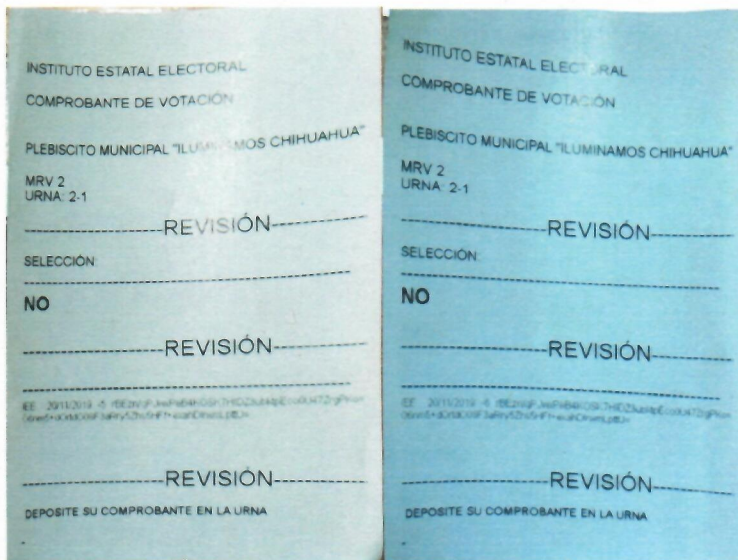


Imagen 3.16 y 3.17. Voto emitido en la urna 2

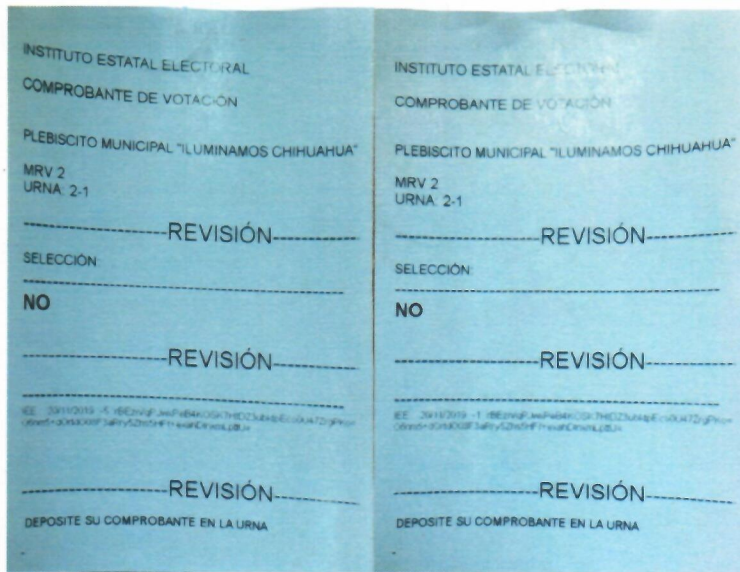


Imagen 3.18 y 3.19. Voto emitido en la urna 2

### Cierre de la votación en la urna

Posterior a la emisión de votos en cada urna, se procedió al cierre de las mismas, para ello se requiere de una clave que se ingresa mediante la lectura de una tarjeta con código de barras (imagen 3.20), después imprime los resultados que se vieron en las imágenes 3.8, 3.9, 3.10 y 3.11.



Imagen 3.20. Lectura de tarjeta con clave mediante lector de código de barras

*[Handwritten signature]*  
*[Handwritten signature]*  
*[Handwritten signature]*

Se verifica que una vez cerrada la urna, no permita seguir recibiendo los votos, comprobando que sólo deja imprimir o exportar los resultados como se muestra en la imagen 3.21.



Imagen 3.21. Exportación de resultados de la urna

En el cierre, al final el sistema imprime un resumen de votos recibidos en la urna, a continuación, en la imagen 3.22 un ejemplo del reporte.

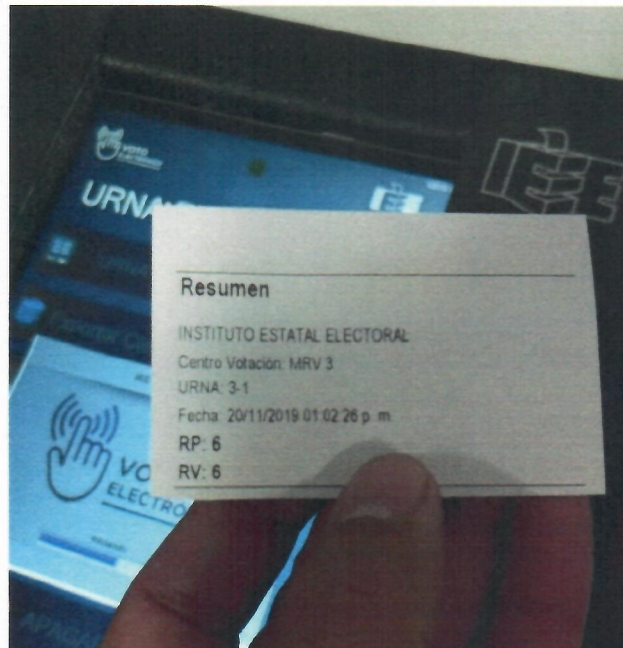


Imagen 3.22. Resumen del cierre de urna

*[Handwritten signatures in blue ink]*

## Concentración de resultados

La concentración de resultados se lleva a cabo mediante la exportación de los resultados de cada urna, se concentraron en una memoria flash con conexión USB previamente revisada para que estuviera sin archivos adicionales. El sistema de concentración de resultados lee de la memoria los archivos y se reflejan en el sistema como se observa en la imagen 3.23.

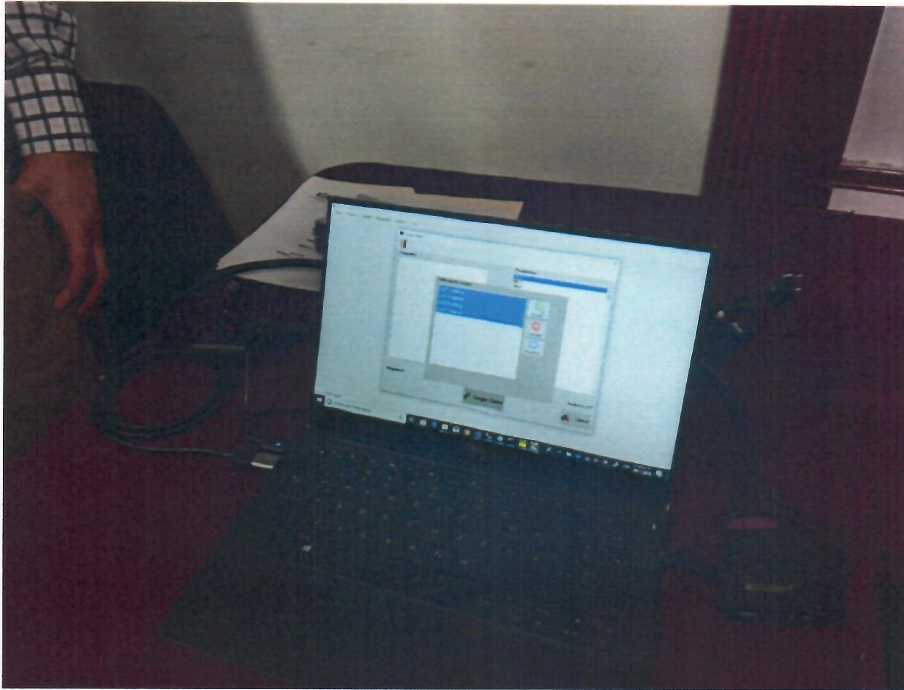


Imagen 3.23. Lectura de archivos en la memoria flash

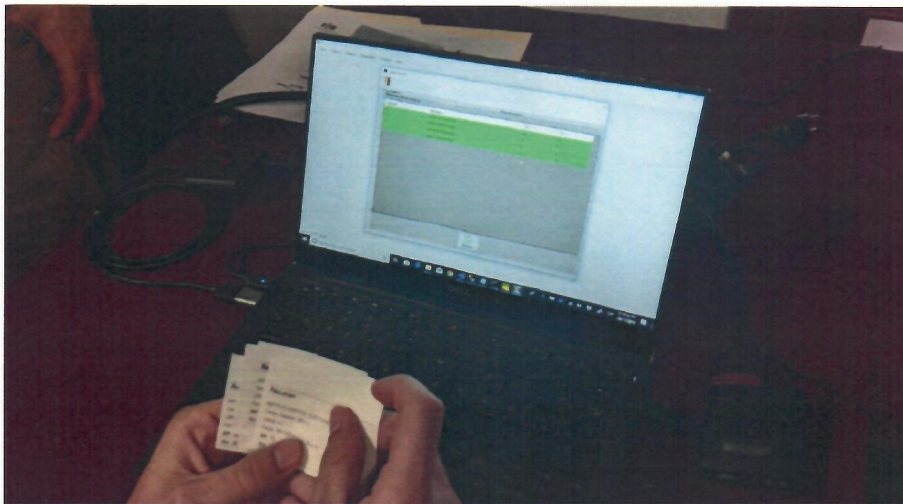


Imagen 3.24. Lectura de votación concentrados

*[Handwritten signatures in blue ink]*



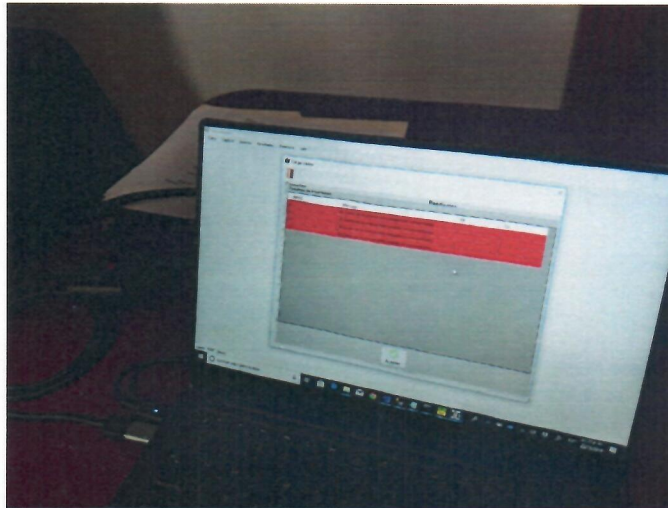


Imagen 3.25. Error al cargar archivos nuevamente

Se verifica que no se puedan cargar nuevamente los archivos para no duplicar votos, la imagen 3.25 muestra que detecta que ya se habían cargado y muestra un error resaltando las casillas en rojo. Se realiza la prueba también si cambiando el nombre al archivo no lo detecta como diferente casilla, sin embargo, el resultado fue el mismo, marca con rojo que ya había sido capturada.

Para completar las opciones de lectura de resultados, se procedió a realizar una captura manual en el sistema, que significa que por alguna razón falló la urna y se tuvieron que contar los votos de manera manual con los comprobantes impresos, para esto se elige capturar 24 votos para SÍ, 12 para No y 5 para DESEO ANULAR MI VOTO. Los resultados finales se mostraron como se observa en la imagen 3.26.

*[Handwritten signature]*  
*[Handwritten signature]*  
*[Handwritten signature]*

INE			RESULTADOS POR URNA				
INSTRUMENTO DIGITAL ELECTRONICO							
MRV	URNA	Tipo Resultado	Total	SI	NO	NULO	
1	MRV 1	1-1	CONCENTRACION DIGITAL	10	4	3	3
1	MRV 2	2-1	CONCENTRACION DIGITAL	8	3	4	1
1	MRV 3	3-1	CONCENTRACION DIGITAL	8	0	6	0
1	MRV 4	4-1	CONCENTRACION DIGITAL	12	7	3	0
1	MRV 5	5-1	COMPROBANTE DE RESULTADOS	24	12	7	5
<b>Totales</b>				<b>68</b>	<b>26</b>	<b>25</b>	<b>8</b>
URNAS 5 de 377							

Imagen 3.26. Resultados obtenidos del concentrador de votos

## Generación de hash SHA-256 y SHA-512

Las funciones Hash, también conocidas como funciones resumen son funciones que, utilizando un algoritmo matemático, transforman un conjunto de datos en un código alfanumérico con una longitud fija. Da igual la cantidad de datos que se utilice, el código resultante tendrá siempre el mismo número de caracteres<sup>1</sup>. Entonces se realizó la generación de los hash para el sistema de votación de las urnas y del concentrador de votos, en los formatos de hash 256 y de 512 para comprobar que sean los mismos que se utilizarán el día de la votación.

A continuación, se presentan los hash resultantes de los sistemas auditados, cabe mencionar que existen dos versiones para las urnas, ya que unas cuentan con Windows 10 y otras con Windows 7, los cuales se establecen en la siguiente imagen (imagen 3.27). Asimismo, en la imagen 3.28 se muestra el proceso de extracción del hash.

### ANEXO 1

Aplicación	Versión	SHA256	SHA512
Urna2019 exe	2019.10	C3D3F9F8D 147BBCD5A 336BC7CC5 876C65E639 0156C197AA A87C675461 E817C59	8C104FFCD84647246942FDF937737 B9A38C9E3E9F650525D7F4C377E1 5CCB0C558BE8F8F6087657E1B75B F831082BF612CC46126F4C04C985 B31B4910F6D96DA
Urna2019 exe	2019.10 Win 7	D58345E9D4 D7E4900208 F5ACD7AB2 3103614F4A 2563E327FA 3A514BB4A6 5FEE0	7E87DEDF9DAC647C7A6270B5A12 CA84774B9D8C24655F7840964D355 26A1670A30CC9E7BCC4A7E36BEB C714F66220821968FB4F0918E0E0F 356C5B698677AB1F
Concentrador exe	2019.10	06E98C5C6 C57B674AC 5B7ECC36A BA1DD0CC8 9A69EC509 CC24CFFC2 FB656E085E	7E24E64C4792B2614FF43743EEA78 CD0F9412DFB605B10142BAD6681D 0AD7D57CF73946181BD20319666E 3926DE56E4DA63E2DECC15407AB 55F0668777917ED1

Imagen 3.27. Documentación de los hash SHA256 y SHA512 obtenidos

<sup>1</sup> Gonzalo García-Valdecasas. (2019, 27 agosto). ¿Qué son las funciones Hash y para que se utilizan? Recuperado 22 noviembre, 2019, de <https://www.cysae.com/funciones-hash-cadena-bloques-blockchain/>

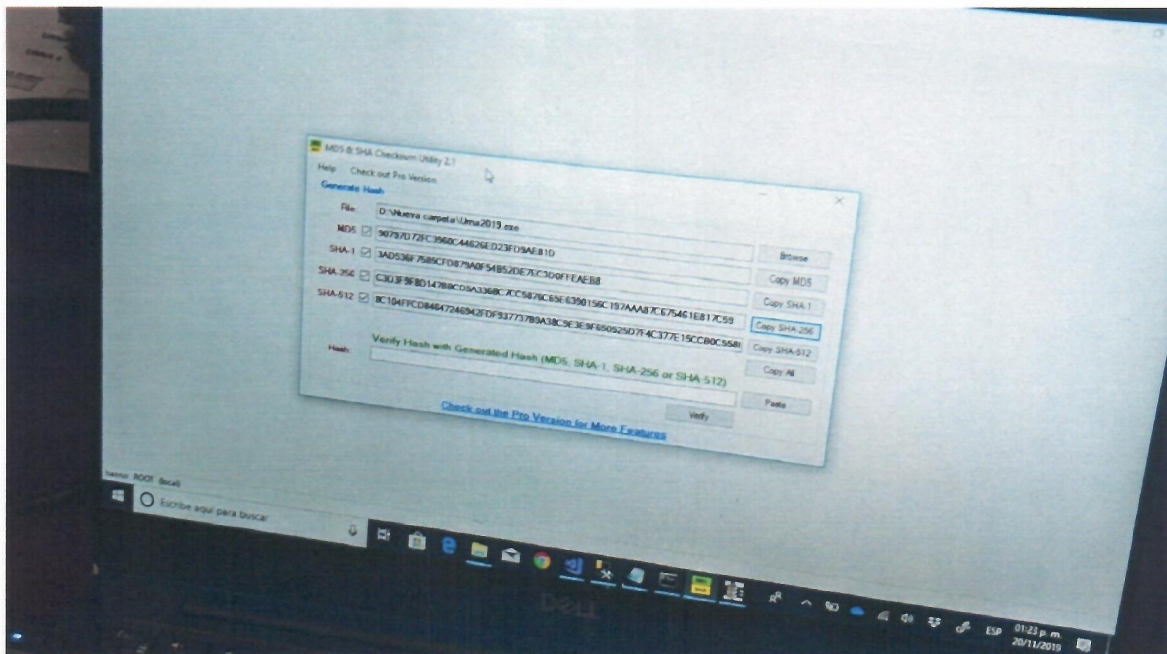


Imagen 3.28. Proceso de extracción del hash

## Resultados de las pruebas funcionales de caja negra

- El proceso de las pruebas funcionales se llevó de manera adecuada con la presencia de observadores del proceso.
- Se desarrolló el simulacro de votación, se realizó desde la carga de información a la urna, apertura de la misma, el proceso de introducir votos de manera aleatoria, cierre de las urnas y concentración de resultados.
- Los resultados obtenidos por el sistema coincidieron con los trabajados de manera manual.
- Se generan los hash de las urnas electrónicas con dos versiones, una con el sistema operativo Windows 7, y otras con Windows 10, por lo que se tienen que verificar según su versión en las urnas que se utilizarán en el plebiscito.
- Se genera el hash del sistema concentrador de datos, a utilizarse el día de las votaciones.

*[Handwritten signatures in blue ink]*

## IV. Revisión del hash del sistema de cómputo en las urnas electrónicas

Para la revisión del hash, se realizó en el momento en que cargaron los datos de votación a las urnas electrónicas, en este proceso, se genera de cada urna un archivo encriptado que será leído únicamente en la que corresponde, después se sellaron las urnas para evitar manipulación posterior a la carga. Es así que, en este proceso, se eligió de manera aleatoria 24 urnas de las 360 disponibles para comparar el hash SHA-256 y SHA-512 mediante una aplicación que permite la comparación de los mismos. Se cuenta entonces con el código que se generó el día 20 de noviembre en las pruebas funcionales de caja negra, y se compara con los que se obtienen el 21 de noviembre, día que se cargan los archivos.

A continuación, se presenta en la tabla 4.1 las urnas elegidas y si hubo coincidencia de los hash mencionados anteriormente.

No.	Identificador	Urna	Sistema Operativo	Coincidencia?
1	MRV001	1	WINDOWS 7	SI
2	MRV020	2	WINDOWS 10	SI
3	MRV020	1	WINDOWS 10	SI
4	MRV040	1	WINDOWS 10	SI
5	MRV040	2	WINDOWS 10	SI
6	MRV048	1	WINDOWS 10	SI
7	MRV048	2	WINDOWS 10	SI
8	MRV061	2	WINDOWS 7	SI
9	MRV076	2	WINDOWS 7	SI
10	MRV052	1	WINDOWS 10	SI
11	MRV053	2	WINDOWS 10	SI
12	MRV054	2	WINDOWS 10	SI
13	MRV159	2	WINDOWS 7	SI
14	MRV160	2	WINDOWS 7	SI



15	MRV154	2	WINDOWS 7	SI
16	MRV153	2	WINDOWS 7	SI
17	MRV188	1	WINDOWS 10	SI
18	MRV187	1	WINDOWS 10	SI
19	MRV182	1	WINDOWS 10	SI
20	MRV183	1	WINDOWS 10	SI
21	MRV185	1	WINDOWS 10	SI
22	MRV184	1	WINDOWS 10	SI
23	MRV179	1	WINDOWS 10	SI
24	MRV180	1	WINDOWS 10	SI

Tabla 4.1. Urnas elegidas aleatoriamente para la verificación de coincidencia del hash

Como se puede observar en la tabla, se contaba con dos versiones del sistema operativo Windows, la versión de Windows 7 y la de Windows 10, esto debido a que algunos equipos no soportan el sistema operativo más reciente de Microsoft, se optó por instalar el último soportado que cumpliera con el funcionamiento del sistema. Por lo tanto, como se observa en la imagen 3.27, se contaba con un hash para la versión de Windows 10 y otro para la versión de Windows 7. Las imágenes 4.1 y 4.2 muestra la comparación vía sistema de los hash.

*[Handwritten signatures and marks in blue ink]*

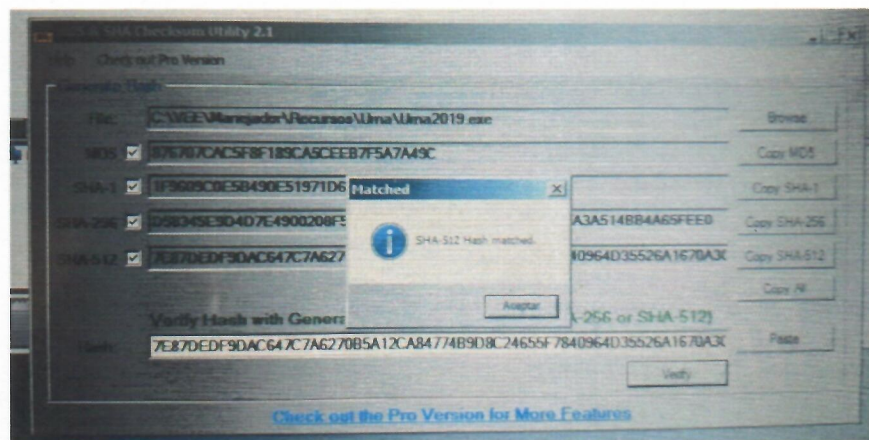


Imagen 4.1. Programa de verificación de hash

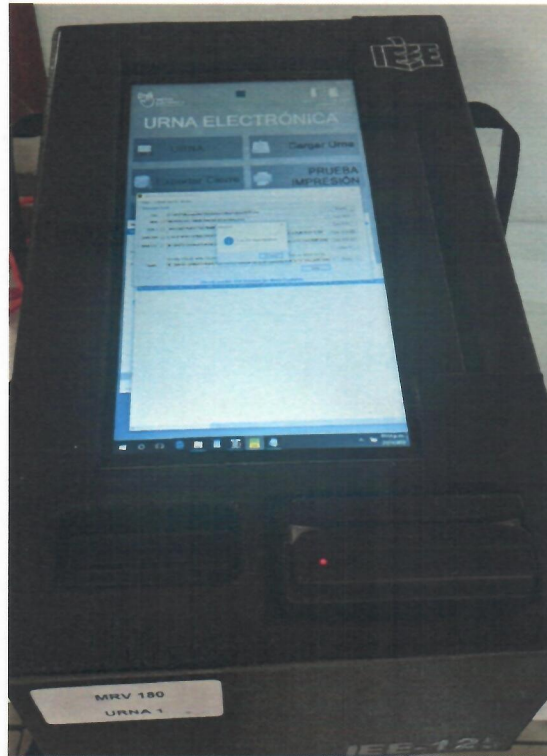


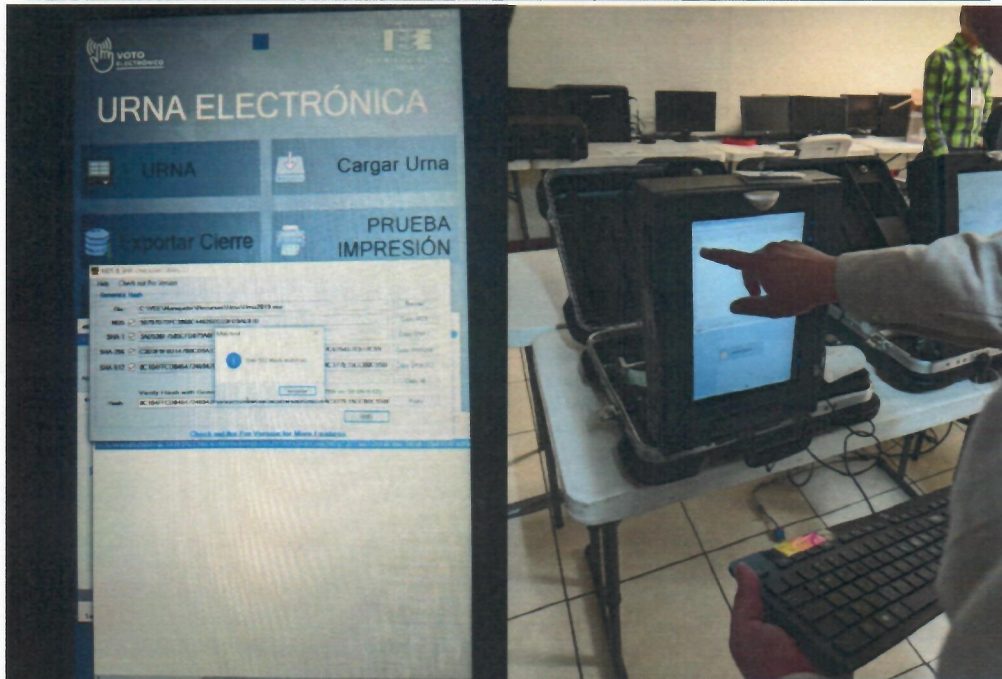
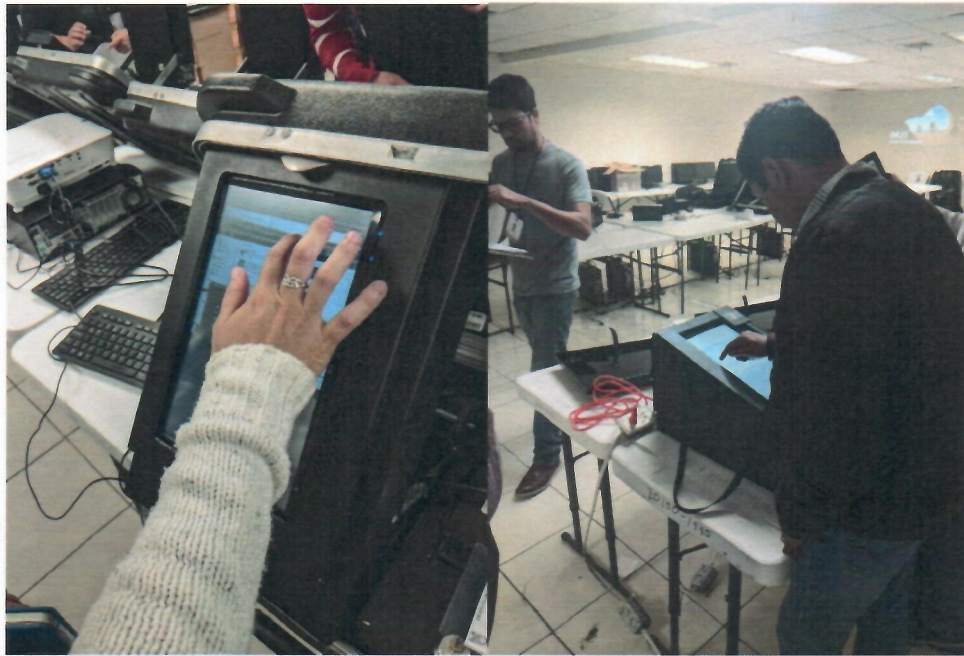
Imagen 4.2. Ejecución de revisión de hash en la urna electrónica

La revisión del tercer hash de la imagen 3.27, se realizará el día de la votación antes de concentrar los datos, para corroborar que el que están usando es el mismo que se presentó en las pruebas funcionales de caja negra.

A continuación, una serie de imágenes donde se realiza este proceso de revisión de hash.



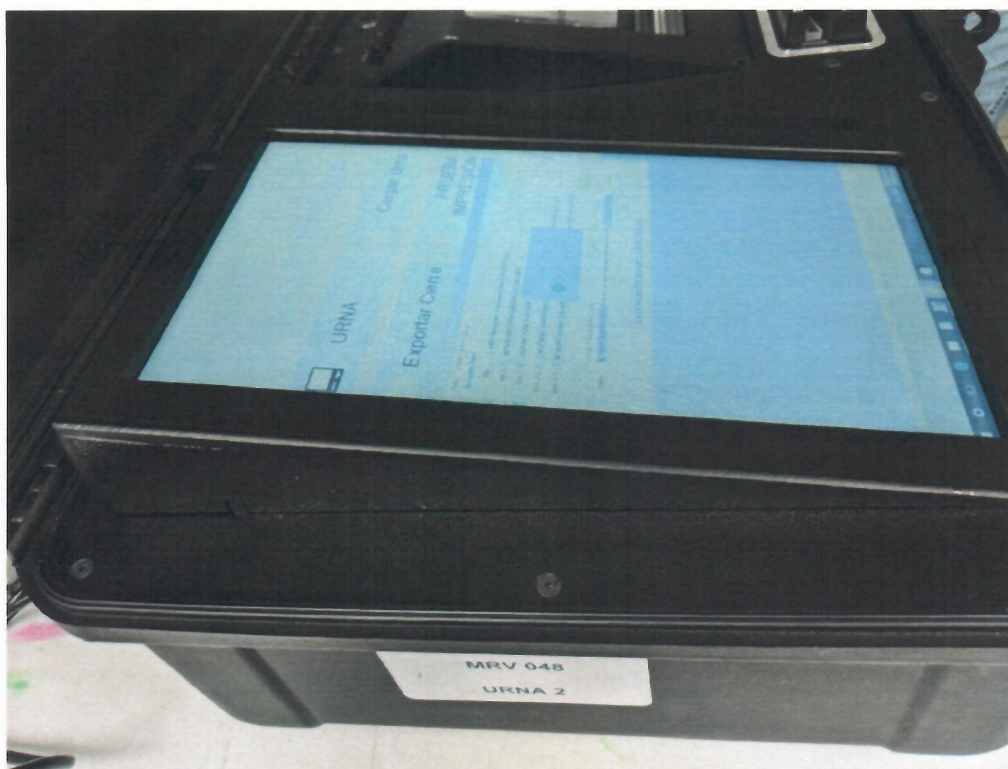
*[Handwritten signature]*  
*[Handwritten signature]*  
*[Handwritten signature]*



*[Handwritten signature]*

*[Handwritten signature]*

*[Handwritten signature]*



*[Handwritten signature]*  
*[Handwritten signature]*  
*[Handwritten signature]*

## Resultados de las pruebas de revisión de hash

- El desarrollo de la carga de datos para la ejecución de las urnas se llevó de manera fluida, permitiendo hacer el análisis de comparación de hash a 24 urnas electrónicas.
- Todas las urnas revisadas de manera aleatoria coincidieron con el hash generado en las pruebas funcionales de caja negra, tanto en la versión de Windows 7 como en las de la versión de Windows 8.

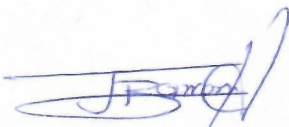


## V. Conclusiones

La auditoría de pruebas funcionales de caja negra, de caja blanca y comparación de hash se llevó sin contratiempos ni detección de vulnerabilidades que impidan su utilización en el proceso de votación del plebiscito del 24 de noviembre de 2019. El sistema cuenta con medidas de seguridad que dan certeza al proceso como lo es la encriptación de la base de datos, así como de los archivos que se transfieren mediante memorias flash, sin embargo, este movimiento de información no es del todo adecuado, por lo que se sugiere que en futuros usos de las urnas electrónicas se realice mediante una conexión de red, que permita una transferencia de datos de manera más segura.

La comprobación de los hash corroboró que los sistemas utilizados en las urnas que recibirán las votaciones de los ciudadanos de Chihuahua, es el mismo que fue auditado el 20 de noviembre del presente año.

Por último, se establece el cumplimiento en gran medida de la secrecía del voto, comprobando que no existen desencadenadores que puedan modificar el resultado en la base de datos.



**L.I. José Rómulo Barrón Hernández**



**Dr. Víctor Alonso Domínguez Ríos**



**M.I. Arión Ehécatl Juárez Menchaca**