



En el día de hoy, jueves 02 de mayo de 2024, siendo las 9:00 a.m., encontrándose reunidos en la Sede del Consejo Nacional Electoral en Plaza Caracas, previa convocatoria, con el propósito de realizar la **AUDITORÍA DEL SOFTWARE DE MÁQUINA DE VOTACIÓN**, enmarcada en el Cronograma Electoral del Evento Elección Presidencial 2024, a realizarse el 28 de julio del presente año. Con la presencia en este acto de los representantes del CONSEJO DE EXPERTOS ELECTORALES DE LATINOAMERICA (**CEELA**), Nicanor Moscoso y Víctor Gastón Soto; de los funcionarios del Consejo Nacional Electoral: Dirección General de Tecnología de la Información y de la Oficina Nacional de Participación Política, de los Asesores Externos y con la participación de las Organizaciones con Fines Políticos Nacionales: PARTIDO SOCIALISTA UNIDO DE VENEZUELA (**PSUV**), MESA DE LA UNIDAD DEMOCRÁTICA (**MUD**), FUERZA VECINAL (**FV**), ACCIÓN DEMOCRÁTICA (**AD**), AVANZADA PROGRESISTA (**AP**), TENDENCIAS UNIFICADAS PARA ALCANZAR EL MOVIMIENTO DE ACCIÓN REVOLUCIONARIA (**TUPAMARO**), PARTIDO COMUNISTA DE VENEZUELA (**PCV**), ALIANZA DEL LÁPIZ PARTIDO POPULAR (**ALIANZA DEL LÁPIZ**), COMITÉ DE ORGANIZACIÓN POLÍTICA ELECTORAL INDEPENDIENTE (**COPEI**), ESPERANZA POR EL CAMBIO (**EL CAMBIO**), MOVIMIENTO SOMOS VENEZUELA (**MSV**), VOLUNTAD POPULAR ACTIVISTAS (**VPA**), PATRIA PARA TODOS (**PPT**), SOLUCIONES POR VENEZUELA (**SPV**), POR LA DEMOCRACIA SOCIAL (**PODEMOS**), UN NUEVO TIEMPO CONTIGO (**UNTC**), CAMBIEMOS MOVIMIENTO CIUDADANO (**CMC**), ORGANIZACIÓN RENOVADORA AUTÉNTICA (**ORA**), MOVIMIENTO REPUBLICANO (**MR**), BANDERA ROJA (**BR**), MOVIMIENTO PROGRESISTA DE VENEZUELA (**MPV**), MOVIMIENTO CENTRADOS EN LA GENTE (**CENTRADOS**), UNIDAD POPULAR VENEZOLANA (**UPV**), ALIANZA POLÍTICA ASAMBLEA RENOVACIÓN Y ESPERANZA (**AREPA**), PARTIDO FUTURO VENEZUELA (**PFV**), CONFEDERACIÓN NACIONAL DEMOCRÁTICA (**CONDE**), UNIDAD VISIÓN VENEZUELA (**UVV**) UNIÓN NACIONAL ELECTORAL (**UNE**) Y MOVIMIENTO PRIMERO JUSTICIA (**MPJ**).

Así mismo, con el acompañamiento a través de la plataforma de Video Conferencia Zoom de expertos electorales del Consejo del Expertos Electorales de Latinoamérica (CEELA): Alfredo Arévalo de Ecuador, Dania Veras de República Dominicana, Eugenio Chicas y Tito Bazán de El Salvador; del Observatorio de Pensamiento Estratégico para la Integración Regional (OPEIR): Marina Urrizola, Javier Juárez, Alejandra Outeda, Carlos López López, Diego Fernando Rubio y Carlos Soukiasian de Argentina; de la Comisión Electoral de Uganda: Welikhe Charles Wanditi y Muhammad Mubajje de Uganda; del Departamento de Elecciones y Límites: Roman Williams de Belice; por la Junta Suprema Electoral: Selcuk Kucukcetin de Turquía; de la Comisión Nacional de Elecciones: Turé Braima, Bari Mamadu Iai y Djalo Aliu de Guinea Bissau; por la Comisión Electoral de Zimbabue: Chirere Ocean, Shamba Noel, Mujaji Kudakwashe y Ngandini Charity de Zimbabue; de la Autoridad Independiente Para Elecciones (ISIE) Naim Nasri de la República Tunecina; de la

Comisión Electoral Nacional Independiente (CENI): Abdillah-Chabhane y Mshangama Monaward Ahmed de Comoras Por Venezuela, de la Fundación Proyecto Social, Claudia León Luna y por la Red de Observación Electoral de la Asamblea de Educación: Simón Andrés Bolívar.

Se da inicio al tercer día (03) de la Auditoría de Software de Máquinas de Votación, la cual está a cargo de los Especialistas Técnicos del CNE con la agenda que se detalla a continuación:

- Verificación de los códigos hash
- Módulo de escrutinio:
Proceso de cierre de votación
Validaciones
- Debug de módulo de escrutinio
- Módulo de transmisión:
Proceso de transmisión
Seguridad:
 - Algoritmo de cifrado de datos
 - Clave de cifrado
 - Vector de inicialización
- Validación de ADES
- Máquina de Reemplazo

Comenzó la jornada con la verificación del HASH de código fuente y de las bases de datos creadas durante la jornada 2 de la auditoría:

Código Fuente:

.\Hash_Codigo_Fuente_MV_2_0_14.sha256.txt,
U17KUp8IQzXqYnI7p+15TvnrYzb0zP5qdXMraAftdVs=, SHA-256, Base64

Bases de Datos

.\db01.db, lm5Vg8LjBK2Ldg1ZR4EHrvTorOAsfUA6dUMUS26knGQ=, SHA-256, Base64
.\db02.db, VnRGNMh47ImUubE+9LNYIcqZBh2YpvB5zllCK5w+ibo=, SHA-256, Base64
.\db03.db, kk6erCrxrHZ8oCNRbauCthIY5HgozRvZKvXBPJTT+el=, SHA-256, Base64
.\device.db, jHeE7dBcUJkwWCj5d9BELwd/inMjwPNqIHixzKiTPwM=, SHA-256, Base64
.\election.db, njx4iWki6mCPUD+pJeUORgW+mgaVyr7KROXHpK8xzA8=, SHA-256, Base64

[Handwritten signatures]

Módulo de Escrutinio

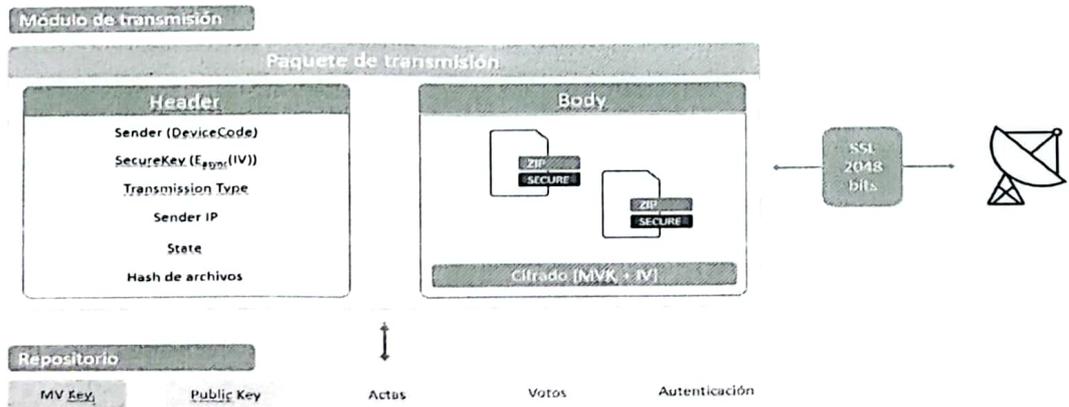
Se dio una descripción funcional del Módulo de Escrutinio en Máquina de Votación. Este módulo es el encargado de contar los votos para cada candidato y generar el ACTA de escrutinio para esa Máquina.

Para analizar el módulo de escrutinio se debe cerrar la elección, para cerrar la elección se deben ejecutar una serie de pasos, entre ellos cargar los miembros de mesa. Se verificó que los miembros de mesa pueden ser cargados en cualquier momento del día, y que pueden ser modificados hasta el momento de cierre de la elección. Se cerró la elección. Se verificó el funcionamiento de las funciones con debug de código fuente. La prueba se estableció con 14 votos, se verificaron los votos impresos, la función que realiza el conteo y la generación del acta.

Se revisaron los valores del acta impresa, se verificó que reflejaba el resultado correcto. Se verificaron los valores del acta en la base de datos. Se verificó la función que genera el código QR en el acta.

Módulo de Transmisión

Se dio una explicación funcional del módulo de transmisión. Se mostraron las funciones que arman el paquete de transmisión. Se analizaron las herramientas de protección de datos y se explicaron los protocolos de transmisión. Se mencionaron las medidas de seguridad implementadas para proteger el paquete y la transmisión, la única aplicación que puede descifrar el paquete es el sistema de recepción de mensajes incluido en el software de totalización. Se explicaron las validaciones que se realizan del lado del servidor de recepción.



Verificación de ADES

Se realizó una instalación de prueba, de una máquina en blanco para demostrar los mecanismos de verificación de datos de electores. Se revisaron las funciones intervinientes con DEBUG de

[Handwritten signatures]

[Handwritten signatures at the top of the page]

código fuente. El Archivo de electores o ADE es generado a partir del Tabla Mesa y contiene todos los electores que deben votar en esa Mesa. Este archivo se encuentra comprimido y cifrado con una clave única (una clave distinta por archivo), durante el proceso de inicialización de la máquina este archivo es descomprimido y los datos son colocados en un directorio en forma de archivos XML individuales (un archivo por elector, referenciado por número de cédula). Cada xml contiene los datos biográficos del elector, la foto que aparece en la pantalla del SAI y las huellas disponibles, adicionalmente cada archivo contiene una firma xml. Durante el chequeo de integridad se verifica que la firma de XML sea consistente con el certificado que posee la máquina. Este certificado es único y es generado por el CA (certification authority) del CNE. Como prueba de validación se modificó un valor a mano en uno de los archivos, al intentar inicializar la máquina esta no permite iniciar por detectar una inconsistencia en uno de los archivos de electores.

Máquina de reemplazo

Se dio una breve explicación de los mecanismos de recuperación previstos, la generación de máquinas de reemplazo y los procedimientos requeridos. Se verificaron las funciones que instalan el software, copian el contenido de la memoria removable a la memoria interna (Disco Duro Interno) e inicializan la máquina de reemplazo para convertirla en una principal. Se realizó el proceso completo y se verificó que la copia se realizó correctamente, se abrió la máquina y se constató que se encontraba en el mismo estado que había quedado la anterior (contenía los votos que había antes del cambio). Se cerró la elección y se verificaron las actas.

Se realizó una prueba para demostrar la integridad del voto:

Se autenticó un elector biométricamente, se habilitó la votación para ese elector, se seleccionó una opción boleta y se detuvo el código (simulando una falla de máquina). Se demostró que no se había registrado el voto ni el registro de sesión de autenticación exitosa.

Durante el desarrollo de la Auditoría, los representantes de las Organizaciones con Fines Políticos efectuaron preguntas y manifestaron dudas, las cuales fueron respondidas y aclaradas exhaustivamente por los Asesores Externos encargados de la Auditoría.

Dando cumplimiento con la normativa que regula esta materia con todo el personal asistente, se levanta la presente acta, dejándose expresa constancia de la transparencia del acto, se firma en señal de aceptación y conformidad.

[Vertical column of handwritten signatures on the right side of the page]

[Handwritten signatures at the bottom left of the page]

Por las Organizaciones con Fines Políticos Nacionales

Nº	ORGANIZACIÓN CON FINES POLÍTICOS	NOMBRE DEL REPRESENTANTE	CÉDULA DE IDENTIDAD	FIRMA
1	PARTIDO SOCIALISTA UNIDO DE VENEZUELA (PSUV)	OSCAR DUARTE	18764085	
2	MESA DE LA UNIDAD DEMOCRÁTICA (MUD)	ANA MORALES	12308110	
3	FUERZA VECINAL (FV)	MARCOS GIMÓN	14128991	
4	ACCIÓN DEMOCRÁTICA (AD)	JOSÉ PERAZA	2430901	
5	AVANZADA PROGRESISTA (AP)	RONALD ANGULO	23722977	
6	TENDENCIAS UNIFICADAS PARA ALCANZAR EL MOVIMIENTO DE ACCIÓN REVOLUCIONARIA (TUPAMARO)	DAYNIS MURILLO	14106460	
7	PARTIDO COMUNISTA DE VENEZUELA (PCV)	HUMBERTO ROMERO	5968632	
8	ALIANZA DEL LÁPIZ PARTIDO POPULAR (ALIANZA DEL LÁPIZ)	JOSÉ ALEJANDRO PÉREZ	124088113	
9	COMITÉ DE ORGANIZACIÓN POLÍTICA ELECTORAL INDEPENDIENTE (COPEI)	MILDREX FERNÁNDEZ	16460581	
10	ESPERANZA POR EL CAMBIO (EL CAMBIO)	JOSÉ DAVID VALBUENA	29816854	
11	MOVIMIENTO SOMOS VENEZUELA (MSV)	FABIOLA BRITO	22720579	
12	VOLUNTAD POPULAR ACTIVISTAS (VPA)	GELMARY FIGUEROA	12.210344	
13	PATRIA PARA TODOS (PPT)	OSWALDO ZARRAGA	11.682.875	
14	SOLUCIONES POR VENEZUELA (SPV)	NIROSQUI HERNÁNDEZ	14.125066	
15	POR LA DEMOCRACIA SOCIAL (PODEMOS)	ESDRAS OLIVARES	16407740	

Handwritten signatures and initials at the top of the page.

	ORGANIZACIÓN CON FINES POLÍTICOS	NOMBRE DEL REPRESENTANTE	CÉDULA DE IDENTIDAD	FIRMA
16	UN NUEVO TIEMPO CONTIGO (UNTC)	ANTONIO SILVA	9663887	[Signature]
17	CAMBIEMOS MOVIMIENTO CIUDADANO(CMC)	GILMARY HENRIQUEZ	27901089	[Signature]
18	ORGANIZACIÓN RENOVADORA AUTÉNTICA (ORA)	EDGAR GONZÁLEZ	18031258	[Signature]
19	MOVIMIENTO REPUBLICANO (MR)	ALONSO MALDONADO	7072076	[Signature]
20	BANDERA ROJA (BR)	JAVIER TORRES	10519873	[Signature]
21	MOVIMIENTO PROGRESISTA DE VENEZUELA (MPV)	JOSÉ GUILLERMO TIRADO	20588485	[Signature]
22	MOVIMIENTO CENTRADOS EN LA GENTE (CENTRADOS)	MARCEL CASTRO	11035937	[Signature]
23	UNIDAD POPULAR VENEZOLANA (UPV)	ERIKA ROJAS	1670801	[Signature]
24	ALIANZA POLÍTICA ASAMBLEA RENOVACIÓN Y ESPERANZA (AREPA)	FRITZ WAGNER	20028980	[Signature]
25	PARTIDO FUTURO VENEZUELA (PFV)	ARWIN QUEZADA	17155698	[Signature]
26	CONFEDERACIÓN NACIONAL DEMOCRÁTICA (CONDE)	JUAN AKKERMANS	14728710	[Signature]
27	UNIDAD VISIÓN VENEZUELA (UVV)	LUIS DE LOS SANTOS	24216434	[Signature]
28	UNIÓN NACIONAL ELECTORAL (UNE)	CARLOS SALAS	10546048	[Signature]
29	MOVIMIENTO PRIMERO JUSTICIA (MPJ)	CARLOS PARRA	18458840	[Signature]

Vertical handwritten notes and signatures on the left margin.

Vertical handwritten notes and signatures on the right margin.

Large handwritten signatures and initials at the bottom right of the page.

Handwritten signatures and marks at the bottom left.

Por el Consejo Nacional Electoral (CNE):

Dirección General de Tecnología de la Información:



Ing. Andrés Strubinger

Oficina Nacional de Participación Política:



Esp. Mayrett Torres



Dra. Jessica Rocco

Asesor Externo:



Lic. Hernán Sorell

Consejo de Expertos Electorales de Latinoamérica (CEELA)



Nicanor Moscoso
Presidente (CEELA)



Víctor Gastón Soto
Miembro (CEELA) Perú