



En el día de hoy, jueves 15 de octubre de 2020, siendo las 9:00 a.m., encontrándose reunidos en la carpa del Consejo Nacional Electoral, sede Plaza Caracas, previa convocatoria, con el propósito de realizar la **Auditoría del Software de Máquina de Votación**, establecida en el cronograma de las **Elecciones a la Asamblea Nacional 2020**. Con la presencia en este acto de los funcionarios del Consejo Nacional Electoral: **Dirección General de Tecnología de la Información** y **Oficina Nacional de Participación Política**. Con los especialistas técnicos: **Asesores Externos**. Con la participación presencial de las **Organizaciones con Fines Políticos Nacionales**: Partido Socialista Unido de Venezuela (**PSUV**), Alianza para el Cambio (**APC**), Avanzada Progresista (**AP**), Comité de Organización Política Electoral Independiente (**COPEI**), Movimiento al Socialismo (**MAS**), Partido Comunista de Venezuela (**PCV**), Soluciones por Venezuela (**SPV**), Unidad Popular Venezolana (**UPV**) y Venezuela Unida (**VU**); por las **Organizaciones Indígenas Nacionales**: Consejo Nacional Indio de Venezuela (**CONIVE**) y Asociación Civil Cátedra Guaicaipuro (**C. GUAICAIPURO**).

Se dio inicio al día cuarto (4º) de la actividad, la cual estuvo a cargo de los Especialistas Técnicos del CNE y Asesores Externos, realizando las actividades siguientes:

Se revisó y verificó el hash del código fuente del software de máquina de votación.

Acto seguido, se procedió a la revisión del código fuente del Módulo de Seguridad, a solicitud de los representantes de las organizaciones participantes, en el cual se aplican los mecanismos para garantizar la integridad y confiabilidad de los datos, así como el secreto del voto. Los datos son cifrados con claves divididas entre el organismo electoral y las organizaciones participantes de manera que, el único que conoce la clave es el software de máquina de votación.

En este Módulo de Seguridad se revisaron los aspectos siguientes:

- Las claves de seguridad: la clave compartida y la clave principal. Se revisó cómo están protegidas estas claves dentro del software de máquina de votación y además se revisó en qué parte del software de máquina de votación se utilizan.
- Asociación de las bases de datos: se revisó cómo las bases de datos se asocian al momento de instalación del software de máquina de votación, lo cual evita que se pueda cambiar o manipular la información, una vez instalada la máquina.

- Seguridad de las bases de datos: se revisó cómo se obtiene la información desde las bases de datos, usando las claves que corresponden a cada base de datos (Clave compartida y clave principal).
- HMAC en voter session: se revisó cómo se calcula el código HMAC en cada voter session. Adicionalmente, se revisó cómo se calcula el código HMAC para los archivos de huellas de los electores que son capturados en el proceso de autenticación.
- Archivo de Electores (ADE's): se revisó cómo se verifica la integridad de los archivos de los ciudadanos en el proceso de inicialización de la máquina, lo cual evita que se pueda cambiar o manipular la información de los ciudadanos, una vez instalada la máquina.
- Transmisión: se revisó la parte de transmisión, cómo se crea y se cifra el paquete que se transmite al Centro Nacional de Totalización; adicionalmente, se verificó que los procesos de cifrado dentro del software de máquina de votación utilizan algoritmos estándar de cifrado.
- Actas de Escrutinio: se revisó cómo se calcula el código HMAC de la información que se muestra en el código QR del acta.

Durante esta jornada, los representantes de las organizaciones participantes realizaron preguntas hacia los técnicos especialistas electorales, sobre los módulos sometidos a análisis del software de máquina de votación, las cuales fueron respondidas a satisfacción de los mismos.

El representante auditor de la organización con fines políticos Avanzada Progresista (**AP**), consignó un escrito con observaciones relativas a los módulos sometidos a la revisión el día de hoy, la cual espera sea respondido lo más oportunamente por la unidad ejecutora del CNE que corresponda. Este escrito se anexa y forma parte de esta acta.

Para este acto, a través de la plataforma de video conferencia zoom, se contó con la participación siguiente: por la organización con fines políticos nacional: Esperanza por el Cambio (**EL CAMBIO**): Luis Rengifo; por el **Consejo de Expertos Electorales de Latinoamérica (CEELA)**: Alfredo Arévalo (Ecuador), Augusto Aguilar (Honduras), Eugenio Chicas (El Salvador), Gastón Soto (Perú), Guillermo Reyes (Colombia), Jessica Plua López (Ecuador), Nicanor Moscoso (Ecuador) y Tito Antonio Bazán (Ecuador); por los **Expertos Electorales de la República de Argentina**: Marina Urrizola, y por la **Comisión Electoral de Sudáfrica**: Mlugisi Kelemba.

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.

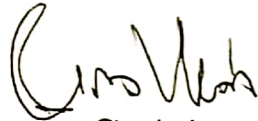
The image shows several handwritten signatures in black ink, arranged horizontally. From left to right, there are approximately seven distinct signatures, some appearing to be initials or full names in cursive script. The signatures are placed below the text of the act, indicating the signatories' approval.

Por las Organizaciones con Fines Políticos Nacionales:


Partido Socialista Unido de Venezuela (PSUV):

  
José Pino  
C.I. V- 11380294

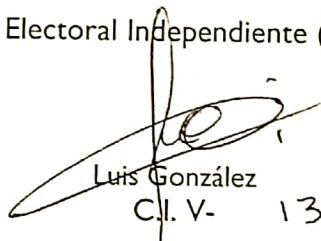
Alianza para el Cambio (APC):

  
Ciro León  
C.I. V- 74.533009.


Avanzada Progresista (AP):

  
Jaime Parada  
C.I. V- 15194678


Comité de Organización Política Electoral Independiente (COPEI):

  
Luis González  
C.I. V- 13284115.


Movimiento al Socialismo (MAS):

  
Homero Rodríguez  
C.I. V- 2708802.

Partido Comunista de Venezuela (PCV):

  
Junior Sumosa  
C.I. V- 17078200

Soluciones por Venezuela (SPV):

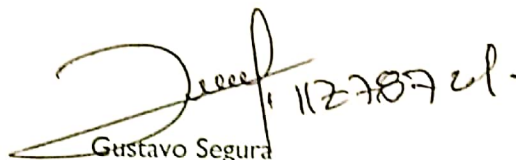
  
Félix González  
C.I. V- 25880312

Unidad Popular Venezolana (UPV):



Evelyn Barboza León  
C.I. V- 12213136.

Venezuela Unida (VU):



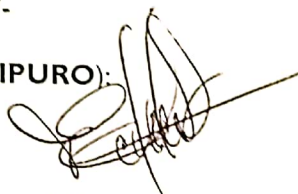
Gustavo Segura  
C.I. V-

**Por las Organizaciones Indígenas Nacionales:**

Consejo Nacional Indio de Venezuela (CONIVE):

Raúl Tempo  
C.I. V-

Asociación Civil Cátedra Guaicaipuro (C. GUAICAIPURO):



Emmanuel Avendaño  
C.I.V- 16.554.873.

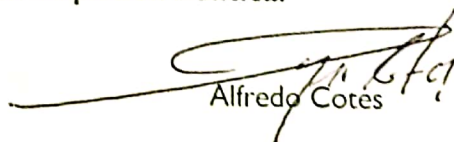
**Por el Consejo Nacional Electoral (CNE):**

Dirección General de Tecnología de la Información:



Andrés Strubinger

Oficina Nacional de Participación Política:



Alfredo Cotés

Asesores Externos:



Ángel Elía



PODER ELECTORAL

ELECCIONES A LA ASAMBLEA NACIONAL 2020

Fecha 15/10 2020

ORGANIZACION CON FINES POLITICOS:			AVANZADA PROGRESISTA		
REPRESENTANTE:			JAIME PARADA		
<input type="checkbox"/> Observación		<input checked="" type="checkbox"/> Solicitud		<input type="checkbox"/> Sugerencia	
① INCLUIR EN EL ACTA DE ESCRUTINIO LA INFORMACIÓN CORRESPONDIENTE A LOS "MATCH" Y "NO MATCH" DEL SISTEMA DE AUTENTICACIÓN.					
② DE ACUERDO A LO DISCUTIDO EN LA SESIÓN DE AUDITORÍA DEL DÍA MIÉRCOLES 14/10, PROPORCIONAR LISTADOS CON LA DESCRIPCIÓN Y NOMBRE DE CADA PARÁMETRO QUE ESTÁ INCLUIDO EN LOS ARCHIVOS DE CONFIGURACIÓN QUE SERÁN AUDITADOS.					
③ DE ACUERDO A LO DISCUTIDO EN LA SESIÓN DE AUDITORÍA DEL DÍA MIÉRCOLES 14/10, PROPORCIONAR LA DESCRIPCIÓN Y FORMATO DEL "QR" QUE VENDRÁ IMPRESO EN EL ACTA DE ESCRUTINIO.					
④ DE ACUERDO A LO DISCUTIDO EN LA SESIÓN DE AUDITORÍA DEL DÍA JUEVES 15/10, PROPORCIONAR UN FLUJOGRAMA DE TODO EL PROCESO DE OFUSCAMIENTO DE VARIABLES EN MEMORIA Y MANEJO CRIPTOGRAFICO PRESENTADO.					
⑤ PROPORCIONAR CUALES ES EL PROCEDIMIENTO OFICIAL PARA HABILITAR VOTANTES CUYA HUELLA DACTILAR: ① NO COINCIDE, ② NO POSEE HUELLA POR CUALQUIER RAZÓN, O ③ LA HUELLA NO SE ENCUENTRA REGISTRADA EN EL SISTEMA DE AUTENTICACIÓN; Y CUALES SON LOS LÍMITES PARA PERMITIR VOTAR POR ESTAS VÍAS.					

Firma:

N°CI:

13194678

Oficina Nacional de Participación Política  
Dirección de Relaciones con las Organizaciones con Fines Políticos  
Dirección General de Tecnología de la Información