AUDITORÍA DEL SISTEMA NACIONAL DE TOTALIZACIÓN

LUNES 09/11/15

PODER ELECTORAL

En el día de hoy, lunes 09 de noviembre de 2015, siendo las 09:00 a.m., encontrándonos reunidos en la sede del Consejo Nacional Electoral, ubicada en Plaza Venezuela, en la ciudad de Caracas, Distrito Capital, previa convocatoria, a los fines de llevar a cabo el evento de **AUDITORÍA DEL SISTEMA NACIONAL DE TOTALIZACIÓN**, para el venidero proceso Electoral Elecciones a la Asamblea Nacional 2015, a efectuarse el 06 de diciembre de 2015. Por la **Oficina Nacional de Participación Política**: Leonela Lanz Alvarez e Isa Mary Zabaleta; por la **Dirección General de Tecnología de la Información:** Franck Rodríguez; por la empresa **SMARTMATIC**: Frederick Faria; por los representantes de las **Organizaciones Con Fines Políticos: Partido Socialista Unido de Venezuela (PSUV)**: Marcos Oliveros; **Mesa De La Unidad Democrática (MUD):** Felix Arroyo, Javier Pose y María de Lourdes Ortega; por **Vanguardia Popular (VP):** Fidel Gil; por **Partido Comunista de Venezuela (PCV):** Roso Grimau y León Grimau; por **Nuevo Orden Social (NOS):** Luis Santos; por **Patria para Todos (PPT):** Oswaldo Zárraga y por los **Observadores Nacionales: Red de Observadores Electorales de Venezuela (ROEV):** Diana Koussan, **Fundación por un Pueblo Digno(FPPD):** Pedro Espinoza, **Observatorio Electoral Venezolano(OEV)**: Enrique Fernández, **Red de Observación Electoral de Asamblea de Educación (AE):** Abel Arce. En cumplimiento de las funciones constitucionales y legales, así como de la normativa emanada por el Consejo Nacional Electoral con la finalidad de brindar y proporcionar confianza, transparencia y seguridad, con motivo de las Elecciones a la Asamblea Nacional 2015.

Iniciado el acto el Ing. Franck Rodríguez, encargado del evento por la parte de la Dirección General de Tecnología de la Información del Consejo Nacional Electoral, dio la bienvenida a los presentes e informó la metodología de trabajo de la auditoria, seguidamente procedió a explicar lo siguiente:

Los Componentes de Aplicaciones del Sistema Nacional de Totalización:

- EMS (Election Management System)
- PEM (Party Endorsement Manager)
- SAES-LISTENER
- REIS (Real-Time Electoral Information System

Características Fundamentales Del Sistema Nacional de Totalización:

- Todas las aplicaciones que requieren interacción de usuario manejan seguridad basada en permisos.
- El sistema almacena registros de auditoría de todas las operaciones realizadas en cada módulo del sistema.

- Toda la comunicación (Cliente/Servidor) es realizada a través de canales seguros y cifrados usando SSL/TLS con certificados que contienen llaves asimétricas de 2048 bits.

Componentes Generales del SNT
Certificados SSL para Comunicación y Transmisión de Datos

- El CNE crea una Autoridad Certificadora para el Evento.
- La autoridad certificadora firma dos CA subalternas, una de Infraestructura, y otra de Máquina de Votación.
- La autoridad de Máquina de Votación se usa para firmar los certificados clientes de las máquinas de votación.
- El Resto de los Certificados usados en la Comunicación son firmados por la CA de Infraestructura.
- El día del evento el CNE genera el certificado de Transmisión, el cual es firmado por la Autoridad Certificadora de Infraestructura.
- Las Máquinas de Votación solo envían las Actas cifradas con la clave pública del certificado de transmisión del CNE.
- Las Máquinas de Votación y los Servidores sólo establecen comunicación con certificados que se encuentren en su cadena de confianza.

Se procedió a definir el EMS (Election Management System) y sus procesos generales: el cual es una aplicación que se utiliza para preparar una elección. Permite configurar y organizar la información, que posteriormente será utilizada por otras aplicaciones durante el transcurso del evento electoral; como los son el REIS y las máquinas de votación.

Se definió PEM, y sus procesos generales: que permite registrar las renuncias y sustituciones de candidatos llevadas a cabo por las organizaciones y grupos políticos previas a la elección para su reconocimiento en el proceso de totalización.

Se explicó el sistema **SAES-LISTENER:** siendo este un sistema que se encarga de recibir y procesar los paquetes de transmisión enviados por los dispositivos de votación, permitiendo que la información allí contenida pueda ser administrada y resguardada mediante distintos métodos de operación, lo que garantiza un canal de comunicación confiable entre los dispositivos de votación y los servidores de totalización, además del seguimiento de los paquetes transmitidos. Se explicó los **Procesos Generales del REIS Listener.** Seguidamente se detallaron los procesos de comunicación, paquete transmitidos por la MV, el proceso interno de recepción.

Se definió **REIS (Real-Time Electoral Information System),** sus procesos generales y características: El cual es una aplicación que se utiliza durante el transcurso de la elección y durante los procesos posteriores a la misma, que realiza la totalización, así como también permite emitir toda la documentación oficial requerida por el ente regulador (reportes, credenciales y certificados) para realizar la proclamación y publicación de los resultados.

Procesos Generales del REIS en todas sus fases

- Fase de Inicialización
- Fase de Recepción de Transmisiones.
- Fase de Totalización.
- Fase de Adjudicación.
- Fase de Publicación.
- Fase de Monitoreo

Seguidamente se procedió a mencionar y explicar las diferencias en el código fuente de las versiones de aplicaciones utilizadas en Elecciones Municipales 2013 hasta el día de hoy:

1.- Reemplazar Smartmatic Corp. por Smartmatic Intl. en bloques copyright al inicio de cada clase.
2.- Impedir Visualización de Queries Dinámicos.
3.- Corrección de bug: reiniciar flag para validar zips en cada ejecución de carga másiva.
4.- Corrección de bug: Al hacer carga masiva si algún campo tipo cadena de caracteres tenia la letra T o F, convertía esos campos a valores booleanos (true y false).
5.- Modificación de proceso post carga "Actualizar contiendas con votos múltiples" para que no tome en cuenta contiendas tipo lista.
6.- Se agrega nodo con centros de votación al archivo prog-units.xml.
7.- Permitir generación de archivos de remesa sin cargar los cargos.
8.- Reemplazar caracteres inválidos en nombre de archivo para PDF por el caracter '-'.
9.- Permitir usar corchetes angulares < y > en reportes dinámicos.
10.- Corrección de error al hacer búsqueda de electores en EMS.
11.- Corrección de error al ordenar opciones boletas en actas manuales.
12.- Agregar validaciones al generar archivos de máquina.
13.- Validación al crear grupo de contiendas.
14.- Optimización de búsquedas en BD.
15.- Optimizar rendimiento de archivos JS.
16.- Validación de grupos de contiendas al generar archivos election.xml, voting-device.xml y de experiencia de votación.
17.- Mejoras de rendimiento al hacer descarga masiva de documentos en REIS.
18.- Asociar un documento a una clase de contienda.
19.- Generación de archivos de ciudadanos desde EMS.
20.- Optimizaciones de rendimiento en asignación automática de opciones boletas y generación de IDs físicos de boletas.
21.- Optimizaciones rendimiento de carga másiva de electores.
22.- Modificar esquema de cifrado usado en la MV.
23.- Hacer configurable formato de campo identificación del elector.
24.- Transmisión de memorias abiertas.
25.- Transmisión de información de reemplazo de MV.
26.- Mensajes de logs al ingresar en funcionalidad de Carga de Contraseñas.
27.- Configuración de mostrar/ocultar funcionalidades de afis en EMS.
28.- Modificación de nombres de contadores en el xml del paquete de transmisión.
29.- Eliminar asociación de grupo de contiendas con grupo lógico de electores.

30.- Mostrar estadísticas de votantes correctamente en REIS al tener más de un grupo de contiendas.
31.- Mejoras de mensajes de logs.
32.- Documentación de código fuente.
33.- CRUD de Opción Boleta.
34.- Utilización de los zips de ciudadanos directamente en la MV.
35.- Impedir despliegue del servidor de recepción si detecta inconsistencias en sus diferentes validaciones.
36.- Bajar a la MV el total de electores por Grupo de Contienda.
37.- Validaciones de data biométrica.
38.- Generación de peticiones de REMESA a través de un archivo txt.
39.- Generación de data biométrica y listado de electores disponible en la generación de archivos de MV.
40.- Habilitación masiva de actas manuales.
41.- Corregir Log Duplicados en el listener.
42.- No aparecen todos los suplentes en el Acta de Adjudicación.

Como metodología de revisión de las diferentes aplicaciones, se decidió seguir el flujo normal de uso de los componentes, para esto, se llevaron a cabo las siguientes actividades:

- Revisión funcional de los distintos módulos del EMS.
- Descripción de los distintos procedimientos de generación de los productos electorales que genera la aplicación.
- Visualización de las funcionalidades con cambios desde las Elecciones Municipales 2013 y las nuevas implementaciones.
- Revisión funcional de PEM.
- Revisión del archivo XML de carga masiva de las renuncias y sustituciones de candidatos.
- Revisión funcional de la ejecución del Switch Maestro.
- Demostración funcional del proceso de recepción de las transmisiones de las máquinas de votación.

A continuación se generaron los hash de la plantilla de hash del código fuente de todas las aplicaciones y la herramienta de cálculo de hash JHashUtility, resultando:

HASH DE LA PLANTILLA DE HASH DEL CÓDIGO FUENTE:

Hash SHA256 Hexadecimal:
`166c1f4c32ce0b22e3fc2936c3eda31c8774da09efc3ad38f7f81b258121fd80`

HASH DE LA HERRAMIENTA DE CALCULO DE HASH JHashUtility.jar:

Hash SHA256 Hexadecimal:
`41c7d5df8ce8c96d2fbba175258d7714a5c248320c3138e9aba9398d9fbd6b83`

Durante toda la actividad, los representantes asistentes realizaron preguntas, las cuales fueron respondidas y aclaradas por los funcionarios técnicos del Consejo Nacional Electoral y SMARTMATIC.

Dándole cumplimiento a la normativa que regula esta materia y habiendo cumplido con todas las actividades establecidas en satisfactorias condiciones, con todo el personal asistente y no encontrándose objeción alguna, concluye el presente acto. Se levanta la presente acta, dejando expresa constancia de su transparencia, se firma en señal de aceptación y conformidad.

CONFORMES FIRMAN

POR LAS ORGANIZACIONES CON FINES POLÍTICOS:

PARTIDO SOCIALISTA UNIDO DE VENEZUELA (PSUV):

Marcos Oliveros
C.I.V-13.865.905

MESA DE LA UNIDAD DEMOCRATICA (MUD):

Félix Arroyo
C.I.V-3.230.961

Javier Pose
C.I.V-6.082.224

María de Lourdes Ortega
C.I.V-4.088.038

VANGUARDIA POPULAR (VP):

Fidel Gil
C.I.V-5.590.236

PARTIDO COMUNISTA DE VENEZUELA (PCV):

Roso Grimau
C.I.V-14.199.754

León Grimau
C.I.V-20.096.208

NUEVO ORDEN SOCIAL (NOS):

Luis Santos
C.I.V-1.846.936

PATRIA PARA TODO (PPT):

Oswaldo Zarraga
C.I.V-11.682.875

OBSERVADORES NACIONALES:

RED DE OBSERVADORES ELECTORALES DE VENEZUELA (ROEV):

Diana Koussan
C.I.V-16.368.589

FUNDACIÓN POR UN PUEBLO DIGNO (FPPD):

Pedro Espinoza
C.I.V-6.863.567

OBSERVATORIO ELECTORAL VENEZOLANO (OEV)

Enrique Fernández
C.I.V-13.284.083

RED DE OBSERVACIÓN ELECTORAL DE ASAMBLEA DE EDUCACION (AE):

Abel Arce
C.I.V-23.499.394

DIRECCIÓN GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN

Franck Rodríguez
C.I.V-15.794.239

REPRESENTANTE DE LA EMPRESA SMARTMATIC

Frederik Faria
C.I.V-16.303.512

OFICINA NACIONAL DE PARTICIPACIÓN POLÍTICA

Leonela Lanz Alvarez
C.I.V-6.130.674

Isa Mary Zabaleta
C.I.V-15.554.318