GST

AUDITORÍA TÉCNICA REALIZADA AL SISTEMA DE VOTO AUTOMATIZADO (SVA) PARA LAS ELECCIONES PRESIDENCIALES 2006 EN VENEZUELA

M. Torre *, F. Gil *, M. Cañas *, L. González *, M Wilhelm *, F. Salinas *

*** Grupo de Seguimiento Técnico (GST)**
mtorre@usb.ve
fgil@usb.ve
macanas@cantv.net
leopoldog@cantv.net
blake00@gmail.com
salinasfer25@gmail.com

RESUMEN

Este trabajo, elaborado por el Grupo de Seguimiento Técnico (GST), presenta una breve descripción de las actividades técnicas y puntos de atención recolectados por los integrantes de este grupo durante las actividades de Revisión Técnica de todo el Sistema de Votación Automatizada (SVA) implantado por el Consejo Nacional Electoral (CNE) para el conteo y escrutinio de las elecciones presidenciales de Diciembre de 2006 en la República Bolivariana de Venezuela. Se presentan algunas conclusiones y recomendaciones a tomar en cuenta para la realización de auditorías técnicas de futuros procesos electorales automatizados.

El GST ha participado en las revisiones técnicas del SVA de los dos últimos eventos electorales, dando soporte técnico especializado a través de los actores políticos participantes en dichos eventos.

PALABRAS-CLAVE

Auditoría Técnica, Revisión Técnica, Sistema de Votación Automatizada, Elecciones, Sistema de Autenticación de Votantes.

1. GRUPO DE SEGUIMIENTO TÉCNICO (GST)

El Grupo de Seguimiento Técnico (GST) es una agrupación de carácter netamente técnica, sin filiación política partidista alguna. Está conformado por profesionales y técnicos en computación, electrónica y telecomunicaciones, quienes voluntariamente ceden su tiempo y esfuerzo para el estudio, análisis, evaluación y auditoría del sistema automatizado de votación en Venezuela, sin retribución económica alguna. En este momento, cuenta con aproximadamente 15 personas, y no tiene acceso a recursos ni financiamiento alguno de parte de entrs públicos o privados.

2. ACTIVIDADES DE PREPARACIÓN PREVIA AL INICIO DE AUDITORÍA

2.1. PREPARACIÓN INICIAL

Antes del inicio del período de auditoría previsto por el Consejo Nacional Electoral (CNE) para las elecciones presidenciales 2006, el grupo de trabajo de GST realizó la recolección de toda la información obtenida de labores de revisión de procesos eleccionarios anteriores en los que este organismo había aplicado el Sistema de Votación Automatizadas (SVA), en especial del proceso correspondiente a las elecciones parlamentarias venezolanas del 4 de Diciembre de 2005.

Al culminar la recolección de datos disponibles hasta ese momento, se elaboró un diagrama de interconexión entre los distintos componentes que integran el SVA, el cual se muestra en la Figura 1.

En este diagrama, se identificaron adicionalmente procesos que deben ocurrir antes del evento electoral, a la vez que muestra los bloques que constituyen el sistema en el momento de su operación durante el día de los comicios.

En el diagrama se identifican los siguientes procesos:

a. Creación del “Padrón Electoral” a partir del corte del Registro Electoral que se actualiza permanentemente en la República Bolivariana de Venezuela.

b. Creación de las Tabla-Mesa y de los Cuadernos de Votación para cada Centro de Votación, con base al Padrón Electoral

c. Fabricación, creación de los programas, configuración y particularización de las Máquinas de Votación (MV).

d. Fabricación, creación de los programas, configuración y particularización de las Máquinas de Acopio (MA).

e. Transmisión de las MV y MA al Sistema de Totalización (ST) a través de la Infraestructura de Telecomunicaciones.

f. Procesamiento de la información electoral por medio del Sistema de Totalización (ST).

g. Recolección, procesamiento y respuesta del Sistema de Autenticación de Votantes (SAV) o Sistema de Identificación Biométrica.

Es importante destacar que los proceso a. y b. señalados anteriormente no fueron parte de la revisión técnica realizada por el GST.

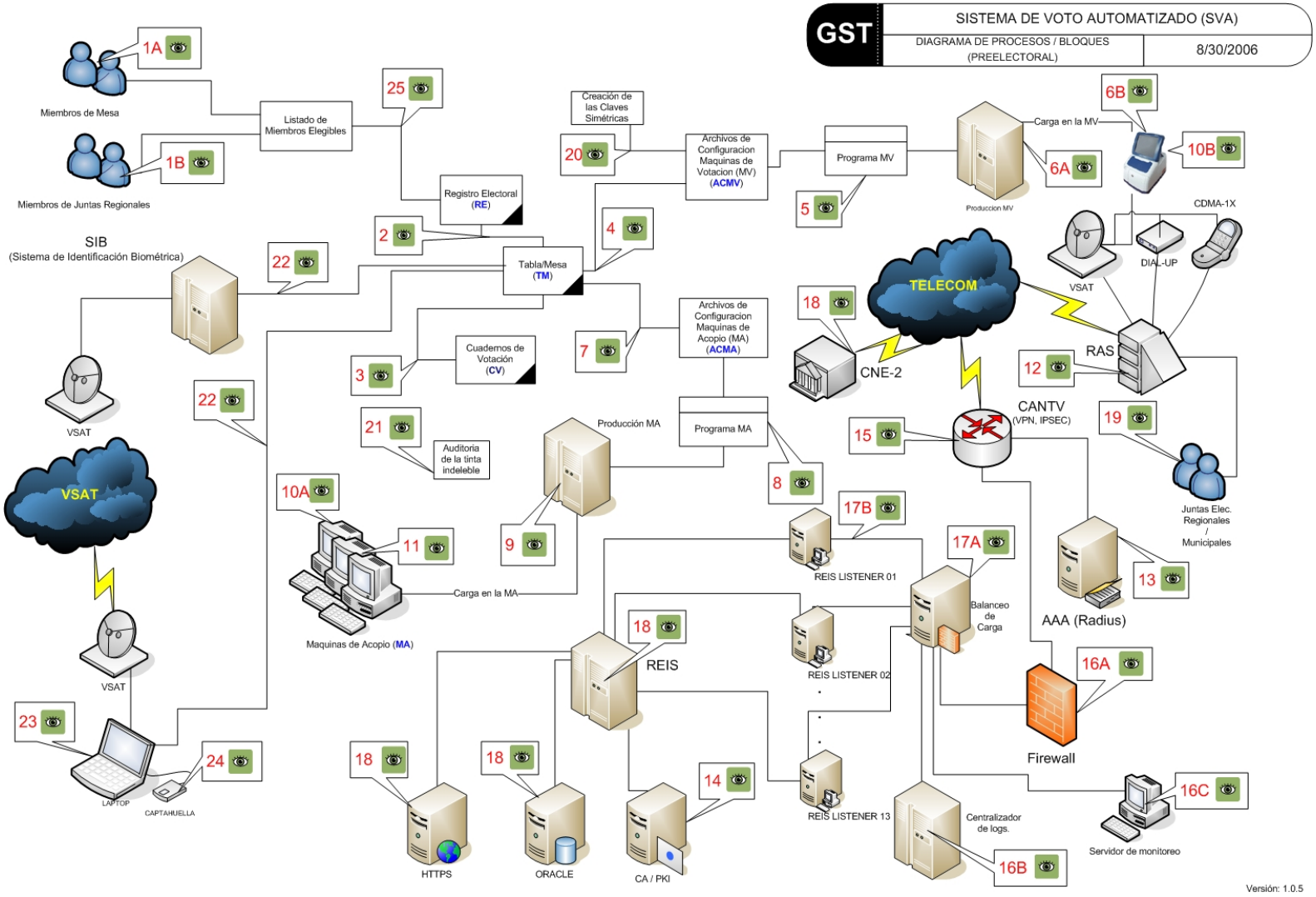

Figura 1: Diagrama de Procesos/Bloques del SAV (basado en información recolectada antes de las Elecciones Presidenciales 2006)

En el diagrama se detectaron todos aquellos puntos que se consideraron “críticos” y que por lo tanto requerían atención especial durante las actividades de auditoría. Estos puntos están destacados en el diagrama con iconos correspondiente a un “ojo”, junto con un número que identifica cada punto crítico de forma individual.

Con base en este diagrama, se realizaron dos actividades previas al inicio del período de la auditoría del SAV. Estas actividades fueron: La elaboración de un Plan de Auditoría, y la creación de una lista de todas las dudas y preguntas que surgieron durante la preparación del diagrama de Procesos/Bloques presentado en la Figura 1.

2.2. PLANES DE AUDITORÍA

El GST se dividió en varios grupos técnicos, con el fin de trabajar en paralelo en los distintos subsistemas que integran el SAV. Estos subsistemas son:

a. Máquinas de Votación (MV)
b. Infraestructura de Telecomunicaciones (IT)
c. Sistema de Totalización (ST)
d. Sistema de Autenticación del Votante (SAV)

Cada uno de los grupos redactó un Plan de Auditoría (GST[1], 2006), con los puntos más críticos a analizar en cada subsistema, y la acción a tomar para mitigar el riesgo en cada punto crítico. Las actividades de elaboración de los planes de auditoría conllevaron un esfuerzo de todo el grupo de más de 4 meses.

2.3. PREGUNTAS AL CNE

Durante la elaboración de los Planes de Auditoría, surgieron una serie de dudas técnicas y procedimentales que debían ser despejadas por el CNE una vez se iniciaran

las actividades de auditoría. Se elaboraron un total de 95 preguntas (GST[2], 2006), las cuales fueron entregadas al CNE tanto en forma escrita, como en forma electrónica a través de un sitio en Internet que el CNE dispuso especialmente para que los expertos acreditados ante el organismo electoral por los partidos políticos participantes en la contienda electoral, plantearan sus inquietudes técnicas acerca del SVA. Aunque durante las actividades de revisión técnica permitidas por el CNE se respondieron varias de las preguntas, ni el CNE ni SmartMatic (empresa proveedora de las MV y el ST) respondieron jamás formalmente a las preguntas formuladas por el GST a través de los mecanismos formales establecidos para ello por el organismo electoral.

3. ACTIVIDADES DE AUDITORÍA

Las actividades de Auditoría, tal como el CNE quiso denominar al proceso de Revisión Técnica que efectivamente se realizó, se iniciaron el día 10 de Octubre de 2006. Tanto el CNE como SmartMatic comenzaron las actividades mediante la realización de una presentación global del SVA, indicando muy superficialmente cada uno de sus componentes y la arquitectura del sistema. El contenido de presentación fue propuesto por el CNE, limitándose exclusivamente a los puntos por ellos sugeridos. Solo en las rondas de preguntas fue que se pudo obtener mas información que la expresada en las presentaciones, quedando sin respuestas muchas de las preguntas formuladas por el GST.

En general, las actividades de revisión técnicas realizadas por el GST se suscribieron exclusivamente a los equipos electrónicos, aplicaciones de software y procedimientos computacionales del SVA. El GST no tuvo participación en otros componentes no automatizados del SVA.

Durante el desarrollo de todas las actividades que el CNE permitió ejecutar por los técnicos acreditados ante el organismo electoral por los partidos políticos participantes en la contienda electoral, los miembros del GST pudieron constatar que este proceso en

realidad no podría ser considerado como una Auditoría Técnica, dado que a los participantes acreditados no se les permitió el tipo de libertades normalmente asociadas al trabajo de un Auditor (acceso a toda la información, discrecionalidad mínima aceptable para la definición de los protocolos de auditoría, etc.). Por ello, se insiste en que cuando en este documento se utiliza la palabra "Auditoría", en realidad se hace referencia a una Revisión Técnica restringida por las condiciones limitantes impuestas por el CNE para este propósito.

3.1. AUDITORIA DE LAS MAQUINAS DE VOTACION

El 17 de Octubre se iniciaron las actividades de auditoría de las MV. Se inició con la revisión de los programas que corren en estas máquinas. Con respecto a las actividades de auditoría correspondiente al software de las MV, las pruebas y actividades realizadas se pueden resumir en las siguientes:

a. Se realizó una revisión muy exhaustiva del software de la MV. Sin embargo, esta revisión se realizó sobre un PC convencional y no sobre una MV propiamente dicha, debido a que para revisar la programación se requería una herramienta de desarrollo y depuración (Microsoft Visual Studio 2003) que no puede ser ejecutada en el Hardware de una MV. El grupo auditor aceptó este método debido a que una MV es esencialmente un PC estándar, y puede ejecutar los mismos programas (en este caso Windows XP y Windows .NET framework).
b. Se repitió, junto con el personal tanto de SmartMatic como del CNE, el procedimiento de creación de los programas que corren tanto en la MV como en las Máquinas de Acopio (esta última es la que SmartMatic/CNE denominan Counter-Transmission-Station, o CTS). El procedimiento de creación de estas aplicaciones es muy importante debido a que en las mismas debe "introducirse" claves de encriptación que fueron generadas precisamente en los días de la auditoría, en forma conjunta por los distintos participantes en tal auditoría.

c. Es muy importante destacar que se elaboró, de común acuerdo entre las partes, un procedimiento de respaldo y verificación de integridad de todas las aplicaciones de la MV, a fin de que cada nuevo día de actividades se comenzaba con las mismas aplicaciones que se habían terminado de auditar el día anterior, con la garantía que tales aplicaciones no habían sido modificadas en el transcurso de la noche. Este procedimiento se puso en práctica todos los días en que se extendió el proceso de auditoría, a fin de garantizar que las aplicaciones no fueran alteradas durante las actividades.

d. Una vez creadas las aplicaciones con las claves de encriptación generadas en forma conjunta por los participantes, se revisó el software de la MV, paso a paso. Se puso especial énfasis en los algoritmos de encriptación y uso de claves simétricas y asimétricas tanto para la data que es transmitida por la MV hacia el ST como la data que es almacenada tanto en la MV como el "pendrive" (memoria removible) de la máquina.

e. Se revisó detenidamente el algoritmo de "mezclado" en la escritura de la información electoral en la unidad de almacenamiento de la MV, cuyo fin es garantizar que no quedan rastros de "secuencialidad" o "marca de tiempo" en los archivos de votos almacenados. Es importante destacar que, durante la auditoría realizada en el evento electoral de Diciembre de 2005 se determinó que el software de las MV existía un "error informático" que podía ser utilizado para determinar la secuencia de los votos almacenados en dichas máquinas. Este error fue corregido por SmartMatic para el SVA correspondiente a las elecciones presidenciales de Diciembre de 2006.

f. Únicamente se realizó la revisión de la aplicación que corre en la MV; no se realizó la revisión exhaustiva de la aplicación que corre en las máquinas CTS, ni las otras aplicaciones que fabrican las MVs ni las que producen los "pendrives" en forma masiva. Tampoco se revisó la infraestructura denominada SCADAUtil, la cual sirve para hacer una comprobación de la configuración de todas las MV antes de su traslado.

g. Se aclararon cómo son los procedimientos de contingencia para el reemplazo de las MV por las denominadas “maquinas de contingencia”. Sin embargo, no se revisó detalladamente los procedimientos correspondientes a la creación de “pendrives de contingencia”.

h. Cada MV utiliza una clave única por MV, creada en el momento de la instalación de la máquina para la encriptación de la información en la memoria de la misma MV. Sin embargo, para la transmisión de datos se utiliza otra clave única, pero creada previamente por SmartMatic. Esta clave de transmisión, aunque está bien resguardada, puede ser obtenida por el personal de CNE y/o SmartMatic que tengan acceso a esa información.

i. Se solicitó en múltiples oportunidades la lista completa de TODAS las MV y CTS en poder tanto del CNE como de SmartMatic, incluyendo serial individual y ubicación física de cada MV. Sin embargo, nunca se obtuvo respuesta a este requerimiento.

j. Se solicitó en múltiples oportunidades, tanto al CNE como a SmartMatic, los procedimientos escritos para el desarrollo, manipulación, control de calidad, implantación y despliegue de las aplicaciones de software que se estuvieron revisando durante las auditorías. Jamás se obtuvo esa información.

k. Se solicitó igualmente los nombres y roles de cada una de las personas que participan en el movimiento, manipulación y verificación del software de las MV. No se obtuvo esta información.

l. Nunca se pudo realizar una auditoría efectiva del Hardware de la MV. El GST construyó una herramienta de hardware/software a través de un “pendrive”, para determinar los componentes que están instalados en una MV. Sin embargo, esta herramienta fue sólo parcialmente efectiva, dado que sólo se pudo usar en un tipo de máquina, y usar en conjunto con un “pendrive” de SmartMatic en el otro tipo de máquina. No obstante, la prueba que se pudo hacer no arrojo ningún resultado sospechoso.

m. Se solicito al CNE la revisión exhaustiva de una muestra del 1% de los archivos de configuración de las MV. Sin embargo, esta solicitud no fue atendida por el CNE.

3.2. AUDITORIA DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES.

El 20 y 21 de Octubre se llevaron a cabo las actividades de auditoría del Sistema de Infraestructura. Se inició con una exposición de parte del CNE explicando en qué consistía la plataforma de Telecomunicaciones a utilizar en el evento del 3D.
Con respecto a las actividades de auditoría del Sistema de Infraestructura, se pueden emitir los comentarios que aparecen a continuación.

3.2.1. SISTEMA DE TRANSMISIÓN DE DATOS CANTV

El CNE realizó una presentación sobre el Sistema de Infraestructura. La misma estuvo dividida en bloques, empezando por la red WAN, red LAN, Seguridad, Certificados Digitales y Base de Datos.

La empresa CANTV (Compañía Anónima Nacional Teléfonos de Venezuela) fue la empresa encargada de transmitir la data almacenada en cada MV hacia el Sistema de Totalización. Es importante destacar que para la fecha de las elecciones de Diciembre de 2006 CANTV era una empresa privada administrada por Verizon. En Marzo 2007, el gobierno venezolano estatizó esta empresa y se encarga de su administración. La CANTV dispone de una red conformada por teléfonos fijos, teléfonos celulares y sistema satelital. Se instaló una red la cual daría servicio a 4200 centros de votación a través de líneas fijas con redundancia celular y 3000 centros a través de líneas celulares. El resto de los Centros donde no existe infraestructura de telecomunicaciones las memorias “pendrives” son llevadas a un Centro de Acopio donde son transmitidas vía satelital al Sistema de Totalización (ST) a través de las Máquinas de Acopio (MA).

Únicamente hubo servicio satelital a 15 centros de acopio. Las actas de los Centros con votación manual o del extranjero son llevadas al CNE en Caracas donde son transcritas y transmitidas al ST.

CANTV/CNE elaboraron en conjunto una lista blanca de números telefónicos tanto celulares como fijos que están autorizados a nivel del servidor de acceso de datos (RAS Server) a conectarse al sistema de totalización. Se informó que sólo estos números estarían habilitados para conectarse al ST. No se dio información de cuantos RAS Server se utilizaría. La información en cuanto a la responsabilidad de la configuración de los RAS Server entre CANTV y el CNE no quedó muy bien definida. La razón para no suministrar esta información fue que CANTV y CNE serían los únicos que tendrían potestad para configurar equipos donde se solicitaran “login” y “password” y por lo tanto la seguridad estaría garantizada.

CANTV tuvo tres niveles de seguridad implementados. Uno era la línea telefónica con su respectiva central relacionada la cual era registrada en la “lista blanca” la cual permite que sólo los números autorizados pueden establecer llamadas a través de la central y hacia los RAS Servers. De existir un número no autorizado la central lo rechaza e inhabilita la comunicación a través de este número. El segundo nivel de seguridad era el servidor AAA Radius, el cual chequea el dominio de la MV’s y si la misma esta habilitada en este servidor. El último nivel de seguridad era el RAS Server. Lo importante de este esquema de seguridad es que en cada una de las etapas se estarían registrando las transacciones por lo que sería fácilmente auditable.

De acuerdo con la arquitectura propuesta, los intentos de llamada antes del cierre del proceso electoral no podrían llegar hasta el ST por cuanto el Firewall no lo permitiría. Todas las MV estarían programadas para discar como primera opción un número fijo único a través de la línea conectada al puerto RJ11. Si después de dos intentos no se lograse esta conectar de esta manera, la MV intentaría vía el puerto celular. Si tampoco logra comunicarse de esta manera, la MV intentaría el puerto de datos RJ45. Este ciclo

se repetiría el número de veces que sea necesario hasta que se lograse la comunicación y transmisión efectiva del acta.

Existen dos Centros de Totalización. Uno en el CNE, Centro 1, y otro alterno en la esquina del Chorro, Centro 2. Si todo marchase bien en el Centro 1 todas las llamadas de las MV a través de líneas fijas, celulares o satelitales llegarían al Centro 1. Si por alguna razón el Centro 1 entrase en contingencia se ejecutaría un proceso entre CANTV y CNE para el desvío de todas las llamadas hacia el Centro 2.

Para el evento electoral, CANTV dispuso de dos salas de monitoreo. Una fue el COR (Centro de Operación Regional) el cual se encuentra ubicado en los Palos Grandes, Caracas, y desde donde se puede controlar y monitorear toda la Red. Aquí sólo labora personal de CANTV, la supervisión del CUFAN (Comando Unificado de la Fuerza Armada Nacional) y la DISIP (Dirección de los Servicios de Inteligencia y Prevención). Desde este centro se monitoreó el estado de la red destinada a la transmisión de datos del CNE. La otra sala fue el CET (Centro de Telecomunicaciones) ubicada en San Martín, Caracas. En el CET existe dos salas de Monitoreo paralelas, una bajo supervisión de CANTV y la otra bajo supervisión de CONATEL y CNE. En el CET también se localizó personal de SmartMatic, CUFAN, Aerocav (Empresa de transporte terrestre) y CANTV. En la sala, SmartMatic contó aquí con una herramienta para el monitoreo de las MV's cuando ellas se conectan con la ST y hacen efectiva la descarga de la data. CANTV se podía conectar a la ST a través de un router el cual es administrado exclusivamente por ellos. SmartMatic también contó con un "Call Center" donde los técnicos de Smartmatic en el campo reportaron los problemas de las MV y desde donde se recibieron instrucciones técnicas de cómo proceder cuando el CNE autoriza el reemplazo de una MV o un "pendrive".

Desde el punto de vista de arquitectura, el sistema de transmisión de datos es bastante seguro, donde sólo tendría cabida las MV's que están autorizadas y de igual manera sólo podrían usarse números de teléfono que están en la "lista blanca". No se tiene

información exacta de cuantos sitios vía satélite transmitieron dado que no se pudo confirmar esta información.

Es importante destacar que CANTV firmó un Acuerdo de Nivel de Servicio (SLA en inglés), donde se detallan todas y cada una de las áreas de trabajo, actividades, responsabilidades, tiempos de respuesta, etc., para la operación y monitoreo de la Red antes, durante y después del día de las elecciones. El GST realizó la solicitud al CNE de este contrato, pero este requerimiento jamás fue respondido por el organismo electoral.

3.2.2. ACCIONES DE AUDITORÍA EN EL SISTEMA DE TELECOMUNICACIONES DURANTE EL DÍA DE LAS ELECCIONES

Se ubicaron testigos del GST en las dos salas anteriormente mencionadas. En el COR se pudo tener de antemano información sobre intentos de transmisión fuera de hora y también sobre el comportamiento de la red a la hora de cierre de mesas y comienzo del proceso de transmisión de datos. En CET de igual manera se destacaron equipos de observación para tener información referente a instalación de MV's dado que SmartMatic tuvo allí su centro de atención. De igual manera a la hora de inicio de transmisión de datos SmartMatic contó en este sitio con una herramienta de monitoreo que permitiría saber cuales centros habían transmitido exitosamente (a través del numero de teléfono). De igual manera en la sala de Totalización se contó con testigos que estuvieron atentos al comportamiento de la plataforma de infraestructura. Es posible afirmar que en todos los sitios antes mencionados no se observó ninguna anomalía con respecto a la transmisión de datos el día de las elecciones, la cual comenzó aproximadamente a las 4:30 pm. cuando desde el Centro de Totalización del CNE se dio la autorización de abrir el firewall.

4. AUDITORÍA DEL SISTEMA DE TOTALIZACIÓN

El 25 de Octubre se iniciaron las actividades de auditoría correspondientes al Sistema de Totalización (ST). Se inició con la explicación global de cómo funciona el sistema, y cuántas aplicaciones se ejecutan durante el proceso. Posteriormente, se procedió a revisar cada uno de los componentes que integran el Sistema, que se resumen en los siguientes:

a. Sistema REIS (RealTime Election Information System)
b. Sistema REIS Receptor (REIS listener)
c. Sistema manejador de Base de Datos Oracle

Durante las actividades de auditoría, las cuales se extendieron por un período de 3 semanas. Se revisaron detalladamente cada uno de estos subsistemas. En los tres casos, se procedió a firmar digitalmente cada uno de ellos, con herramientas que fueron provistas por el mismo grupo auditor.

Después de estas actividades de auditoría sobre el ST, se pueden realizar los siguientes comentarios:

a. Se revisó exhaustivamente el procesamiento de cada acta de votación que llega al ST, y cómo cada acta es clasificada, según haya sido retransmitida automática o manualmente.
b. Se revisaron los procedimientos de manejador de base de datos para procesar las actas recibidas y su almacenamiento en las Bases de Datos del Sistema.
c. Se revisaron los procedimientos de elaboración de pantallas e informes de escrutinio a través del Sistema REIS.
d. No se revisó el subsistema correspondiente al EMS (Endowment Management System), que es el que realiza la configuración inicial del sistema ST y es el que genera las claves de encriptación de transmisión tanto a las MV como a las CTS.

e. Se solicitó en múltiples oportunidades, tanto al CNE como a SmartMatic, los procedimientos escritos para el desarrollo, manipulación, control de calidad, implantación y despliegue de las aplicaciones de software que se estuvieron revisando durante las auditorías. Jamás se obtuvo esa información.

f. Se solicitó igualmente los nombres y roles de cada una de las personas que participan en el movimiento, manipulación y verificación del software del ST. Jamás se obtuvo esta información.

g. Se revisó muy superficialmente los archivos de configuración de las aplicaciones que sirven de soporte para el sistema, tal como el JBOSS middleware.

h. Se propuso (y de hecho se realizó) la incorporación de una nueva facilidad en el Sistema REIS, en el cual, en cualquier momento después de la emisión de un boletín parcial, se emita un listado con todos los códigos de las actas válidas que fueron tomadas en cuenta para el mencionado boletín. Se logró el compromiso de que esta información fuera suministrada a los partidos políticos para que con sus copias de actas pudieran verificar los resultados contenidos en el boletín parcial en el mismo momento de su emisión por parte del CNE.

i. De las actividades de auditoría, se detectaron otras aplicaciones que se ejecutan en el ST y de las que no se tenía idea que existían en este sistema, y por ello no tenían planteado Plan de auditoría. Estas aplicaciones son: El Sistema IDS (Detección de Intrusos), el Snort (detección de intrusos en la Red LAN) y el Pluto (detección de lectura / escritura de archivos).

j. Se realizó una auditoría poco completa a los elementos de control de acceso a red, como son el RADIUS Server, el FIREWALL y los DIALADMIN. Se dispuso de muy poco tiempo para realizar la revisión de estos subsistemas, además de que el grupo no disponía de un plan de auditoría específico para la revisión de estos equipos.

k. Jamás se pudo revisar el Servidor de Autoridad de Certificados (CA), ni se pudo determinar si estaba efectivamente aislado de la red LAN o de cualquier otra Red.

4.1. AUDITORIA DEL SISTEMA DE AUTENTICACION DE VOTANTES (CAPTAHUELLAS)

La auditoría del Sistema de Autenticación de Votantes (SAV) o Sistema Captahuellas se inició el día 10 de Noviembre de 2006. Las actividades se extendieron por una semana. El grupo conformado por CNE y la empresa Cogent Systems realizaron una explicación funcional en qué consiste el SAV.

Se realizó una revisión medianamente exhaustiva de la aplicación que se ejecuta en el laptop que acompaña el captahuellas. No se realizó revisión alguna, ni jamás se vio correr la aplicación correspondiente a los servidores de captahuellas.

Es importante destacar que este SAV sólo se instaló en 8 Estados, cubriendo cerca del 48% de los votantes.

De esta auditoría se puede comentar lo siguiente;

a. Al igual que los demás subsistemas, existe una total carencia de procedimientos escritos para el control de personal y roles que tienen acceso y manipulan el software y el hardware del sistema. Se desconocen cuántas y cuáles personas tienen clave de acceso a los distintos sistemas, y cuál es el procedimiento de entrega y remoción de tales claves.
b. El sistema únicamente puede ser efectivo para el caso de que llegue el impostor de una persona que ya haya votado anteriormente, y cuya huella esté almacenada en la base de datos local en el laptop. Los Laptops sólo tienen la data correspondiente al Estado donde se encuentra el Centro de Votación.
c. El sistema SAV no justifica en absoluto la transmisión de la huella hacia un centro de computación. La justificación no está basada en la autenticación del

votante, y crea sospechas de que esta información pueda ser utilizada con fines de ventaja política por parte del gobierno.

d. A nivel de infraestructura física, el centro de computación del SAV comparte las mismas instalaciones en lo que respecta a piso falso en sala de máquinas, sistemas de control de incendio, electricidad, equipos de acondicionamiento de aire, etc., con otras instituciones del estado (Gobierno e Institutos, Universidad Bolivariana, PDVSA), comprometiendo la seguridad de la información que se almacena en este sistema, lo que obviamente constituye un elemento más de desconfianza respecto a qué otro uso se puede realizar con la información biométrica de los votantes que allí se procesa y recolecta.

5. AUDITORIA DEL 3 DE DICIEMBRE DE 2006.

El 3 de diciembre de 2006, un grupo de auditores del GST y de la Organización No Gubernamental “Ojo Electoral” participaron en las actividades de auditoría previos al inicio de la votación, durante el proceso de votación y durante el proceso de escrutinio.

Se realizó un procedimiento de pruebas, diseñado exclusivamente por el personal del GST, y se ejecutaron las mismas a medida que pasaba el evento electoral (GST[3], 2006).
Es importante destacar que todas las pruebas seleccionadas por los auditores (y con el visto bueno tanto del personal de CNE como de SmartMatic) fueron pasadas satisfactoriamente y dentro de los plazos de tiempo establecidos. No se detectaron anomalías sustanciales durante el período de recepción de actas electrónicas ni durante el proceso de escrutinio.

6. CONCLUSIONES Y RECOMENDACIONES

El trabajo realizado por el Grupo de Seguimiento Técnico (GST) comprendió el esfuerzo de un importante grupo de profesionales y técnicos, que dedicaron desinteresadamente su tiempo para la labor descrita en este trabajo. De esta labor, el GST elaboró una serie de conclusiones y recomendaciones las cuales se transcriben a continuación:

a. El GST nunca realizó una auditoría al Sistema de Votación Automatizada, desde el punto de vista formal. Durante las actividades programadas se realizaron una serie de pruebas, conducidas por el CNE, en la que se le permitió al grupo auditor participar principalmente como observador. Sin embargo, en algunas ocasiones, el grupo auditor realizó sugerencias de pruebas específicas que, después de enconadas discusiones, fueron aceptadas por el CNE y realizadas como parte de las actividades de auditoría. Pese a que el CNE accedió a cambiar ligeramente el cronograma de actividades de auditoría para algunos

puntos específicos detectados en el plan de auditoría, la amplia mayoría de tales planes no pudieron ser llevados a la práctica, debido a que el CNE no aceptó cambios sustanciales en la agenda.

b. Es importante recalcar que todas las actividades de revisión realizadas por el GST se suscribieron única y específicamente en aquellos equipos electrónicos, programas y procedimientos computacionales del Sistema de Votación Automatizada (SVA). El GST no participó en las auditorías de los componentes "no automatizados" del SVA, cuyo correcto funcionamiento y transparencia también son esenciales para garantizar la voluntad popular de los electores.

c. El GST antes del inicio de las actividades, y durante el desenvolvimiento de las mismas, remitió al CNE una gran cantidad de preguntas técnicas que jamás fueron formalmente respondidas por el ente electoral. Esto influyó negativamente sobre la efectividad en la realización de las auditorías. No obstante, muchas de las preguntas fueron verbalmente respondidas tanto por el personal del CNE como por el personal de SmartMatic durante el transcurso de las pruebas.

d. La auditoría técnica realizada al Sistema de Votación Automatizada de Venezuela por el GST, no pudo evaluar y auditar con la rigurosidad deseada todos los subsistemas que componen el mismo. Existen muchos componentes del Sistema que no pudieron ser evaluados y auditados. Las razones por la que no se pudieron evaluar algunos subsistemas se resumen a continuación:

    - El GST no tenía conocimiento previo de la existencia de algunos subsistemas, tales como: el Sistema Servidor de Base de Datos Relacional ("DB Cluster"), el Sistema de Detección de Intrusos (IDS), el sistema de Generación de Reportes de Software ("Report Log")" y el Sistema de Gerencia de Red ("Network Management System"), dado que ni el CNE ni SmartMatic proporcionaron información detallada de estos componentes antes del inicio de las actividades de auditoría, ni respondieron a las preguntas remitidas por el GST previo a dichas

actividades. Esto hubiera llevado a que el GST conociera la existencia de estos subsistemas y se preparara correctamente para evaluarlos;

- No se pudieron realizar los planes de auditoría elaborados previamente por el GST, dado que el CNE no aceptó la aplicación de los mismos. Las actividades se restringieron a las previamente programadas por el CNE, por lo que no se pudo efectuar una labor de auditoría efectiva a los componentes del SVA.

e. Sin embargo, dentro de los límites impuestos por la agenda del CNE, se pudo realizar una evaluación exhaustiva de varios componentes importantes del sistema, entre los cuales se encuentran las aplicaciones (software) dentro de las Máquinas de Votación (MV) y las aplicaciones (software) en el Sistema de Totalización (ST). En los subsistemas evaluados, dentro de los límites de lo que se pudo analizar, no se encontraron anomalías o fallas en el sistema.

f. El GST realizó un análisis del sistema de seguridad en el almacenamiento de datos electorales dentro de las Máquinas de Votación, encontrando que se trata de un sistema robusto y seguro. No obstante, la seguridad en la transmisión de datos, aún teniendo un alto nivel de seguridad, posee algunas debilidades que el GST considera que deben ser auditadas exhaustivamente. Entre estas debilidades, se encuentran las siguientes:

- Algunas claves de encriptación utilizadas por la transmisión de datos desde las MVs hasta el ST son generadas previamente por el personal de SmartMatic y el CNE. Esto conlleva un riesgo inherente a través del personal que tiene acceso a tales claves.

- No se pudo realizar una auditoría a los servidores de Autenticación de Certificados del sistema, ni se pudo garantizar que estos servidores estén plenamente protegidos ni resguardados contra el acceso no controlado de personal de SmartMatic, CNE u otros organismos oficiales.

Estas debilidades pueden comprometer la seguridad en la transmisión de datos desde las MV hasta el ST.

g. El GST (ni ningún otro auditor) no tuvo acceso a la documentación formal del Sistema de Votación Automatizada. Se solicitaron los manuales del Sistema, Diagramas de Comunicaciones, Documentos de Diseño Funcional. Manuales de Operación y Mantenimiento, Memoria Descriptiva etc., y el CNE no entregó tales documentos a pesar de respondió a este requerimiento. Es esencial que el grupo auditor tenga acceso a los documentos y manuales del sistema antes del inicio de las actividades de auditoría.

h. El GST, en reiteradas oportunidades, solicitó los Manuales de Procedimientos para la Operación del Sistema de Votación Automatizada. Se exigieron los manuales que describen los siguientes procedimientos :

- Normas y procedimientos para la asignación de usuarios con acceso al sistema de computación.
- Normas y procedimientos para la creación y revocación de palabras clave de los usuarios del sistema;
- Normas y procedimientos para la creación y revocación de palabras clave de las Máquinas de Votación y Máquinas de Acopio ;
- Normas y procedimientos para la asignación de los roles y capacidades específicas de cada uno de los usuarios;
- Normas y procedimientos de acceso a las salas donde se encuentran los equipos de computación y telecomunicaciones;
- Normas y procedimientos de acceso a los depósitos en donde se almacenan las Máquinas de Votación y Máquinas de Acopio;
- Normas y procedimientos de manejo y traslado de las Máquinas de Votación a los Centros de Votación;

- Normas y Procedimientos para la programación y configuración de las Máquinas de Votación y Máquinas de Acopio antes del evento electoral;
- Normas y Procedimientos de control de inventario de las Máquinas de Votación y Máquinas de Acopio;

En general, se solicitó que el CNE entregara el Sistema de Gestión de Calidad de SVA. Ni el CNE ni SmartMatic jamás respondieron (formal o informalmente) a esta solicitud de información. Se desconoce si tales documentos realmente existen. La evaluación exhaustiva de estas normas y procedimientos, y la verificación de su práctico cumplimiento es esencial para el éxito de la auditoría técnica del sistema, ya que puede dar luces sobre la efectividad en la administración del SVA.

i. No se pudo realizar ni siquiera una revisión mínima aceptable para el Sistema de Autenticación del Votante. Sin embargo, con lo poco que se pudo ver, este sistema demostró que no realiza las labores para lo que fue diseñado, dado que no puede garantizar que un elector vote una sola vez.

j. El CNE, en general, impuso severas limitaciones en tiempo, espacio y acceso para la debida revisión de los sistemas que constituyen el SVA. Sin embargo, es importante destacar la buena disposición del personal técnico tanto de SmartMatic como del CNE, en mostrar y explicar detalladamente los componentes a los que el GST tuvo acceso durante las actividades de auditoría. Este personal siempre mantuvo un trato cordial y atento para con los auditores, y las discusiones generadas durante las labores de auditoría siempre se desenvolvieron con cordialidad dentro de un plano netamente técnico.

k. En general, los Sistemas de Votación Automatizada son sistemas de alta complejidad técnica, que involucran una profunda integración de varias disciplinas tecnológicas, tales como computación, electrónica, seguridad y telecomunicaciones, entre otras. Además envuelven complejos sistemas logísticos para la configuración, despliegue, operación y repliegue del sistema para cada evento electoral. Realizar la auditoría técnica de un sistema de esta

magnitud requiere de un grupo de técnicos y profesionales altamente calificado, y a dedicación exclusiva, con el debido entrenamiento para realizar auditorías en este tipo de sistemas electorales.

l. Es muy importante señalar, que aunque se hizo una revisión técnica de varios aspectos del SVA, los resultados obtenidos de esta revisión no pueden ser utilizados como aval para procesos electorales pasados, ni tampoco pueden ser trasladados a elecciones futuras. Siempre se debe auditar completa y exhaustivamente todo el SVA antes de cada evento electoral.

m. Por otro lado, dado el vertiginoso avance de la tecnología informática y electrónica, los riesgos y vulnerabilidades se incrementan exponencialmente, por lo que la revisión de sistemas, software, hardware, protocolos, roles y procedimientos debe ser cada vez más exhaustiva y detallada.

n. El GST que participó en las auditorías técnicas de las Elecciones Presidenciales 2006, aunque está conformado por personal calificado, trabajó en forma voluntaria, cediendo su tiempo sin remuneración alguna, a tiempo parcial. Además, el número de participantes del GST que trabajó en estas auditorías fue insuficiente para cubrir la evaluación de todos los subsistemas que componen el SVA, y emitir resultados con un nivel aceptable.

o. Para que los electores puedan tener confianza en un Sistema de Votación Automatizada, es esencial que se realice un proceso de auditoría exhaustiva de todo el sistema, tanto a nivel técnico, administrativo como a nivel procedimental, que sea realizado por un personal política y financieramente independiente de las instituciones gubernamentales. Este personal debe poseer suficientes recursos (humanos y económicos), y tener pleno acceso a todos los componentes del SVA a fin de poder completar una auditoría con el nivel adecuado. Los resultados de esta auditoría deberán ser transmitidos a los actores políticos, a las ONGs y al electorado, a fin de brindar la confianza necesaria en el proceso electoral.

p. El Sistema de Votación Automatizada debe, en todo caso, proporcionar mecanismos de auditoría en “caliente”, en las que en el mismo día del acto electoral, pueda verificarse manualmente y en forma rápida, el resultado emitido por el Sistema. Estos mecanismos, además de corroborar el resultado automatizado, deben tener vinculación legal en el caso de que se presenten disparidades.

q. Es importante destacar que uno de los logros mas importantes del proceso de “auditorías” llevado a cabo por el GST fue el conseguir cerrar la “traza de papel” al lograr el informe sobre las actas que componen un boletín de resultado parcial de las elecciones, tal como se indica en el punto h de la sección 4 de este trabajo. La traza de papel permite a los actores políticos verificar que todas las actas electorales que componen un boletín parcial puedan ser verificadas contra las copias de las actas obtenidas en las mesas de votación. Si bien el CNE efectivamente entregó este informe de actas en formato digital, el objetivo de la “traza de papel’ no se logró en las Elecciones Presidenciales 2006, debido a problemas en el funcionamiento del sistema que los actores políticos diseñaron e implantaron para tal fin.

r. Otro importante logro fue la entrega, por parte del CNE, de Discos Compactos (CD) con toda la información correspondiente a las bitácoras (logs) que generan las aplicaciones que se ejecutan en el Sistema de Totalización.

s. Para el éxito y transparencia del proceso electoral, más allá de las auditorías técnicas a todo el SVA, es esencial contar con testigos electorales en todas las mesas de votación el día del evento, y obtener una copia del acta de cierre que imprime la MV. De igual manera, se deben realizar auditorías post-electorales al Sistema a fin de verificar que el sistema fue limpio y transparente.

t. Una importante conclusión de este proceso es que, aunque se realicen múltiples y exhaustivas auditorías a un Sistema de Votación Automatizada, jamás se puede garantizar 100% la transparencia y exactitud de dicho sistema para el momento del evento electoral. Pero se puede diseñar el Sistema de manera que

genere la información necesaria para que los distintos factores políticos puedan corroborar los resultados, contrastándolo con la información proveniente de los testigos electorales presentes en cada una de las mesas de votación. Es sólo así que se puede confiar plenamente en el funcionamiento de un sistema automatizado de votación. Por supuesto, esto no exime de manera alguna la extrema importancia de las auditorías técnicas al sistema.

u. Si no se cuenta con testigos electorales en las mesas y con la copia de las actas que emiten las MV no es posible avalar que el resultado que emite el ST sea completamente cierto. Es importante para los actores políticos contar con un sistema para la suma rápida de los resultados de las actas a fin de poder tener certeza de los resultados automatizados que emite el SVA.

v. Es esencial que se pueda obtener y analizar, para futuros procesos electorales en las que se utilice el SVA, una copia del Acuerdo de Nivel de Servicio (SLA), a fin de elaborar los Planes de Auditoría adecuados, realizar las revisiones técnicas a toda la infraestructura de telecomunicaciones y planificar la presencia de especialistas en las áreas críticas del sistema el día de los comicios. La auditoría del Sistema de Infraestructura de Telecomunicaciones es de vital importancia para futuros procesos electorales, más aún con la reciente estatización de la empresa CANTV.

BIBLIOGRAFÍA

1. GST, *Planes de Auditoría elaborados para la Auditoría del Sistema de Votación Automatizado del Consejo Nacional Electoral – Elecciones Presidenciales 2006,* Agosto 2006.
2. GST, *Lista de Preguntas Técnicas relacionadas con el Sistema de Votación Automatizado (SVA) y el Sistema de Autenticación del Votante (SAV), enviados al Consejo Nacional Electoral (CNE) – Elecciones Presidenciales 2006*, Septiembre 2006.

3. GST, *Resultados de las Revisiones Técnicas realizadas durante el día de las Elecciones Presidenciales 2006*, Enero 2007.
4. IIDH/CAPEL, *Informe Técnico Auditoría Internacional del Registro Electoral República Bolivariana de Venezuela*, 2005
5. COGENT SYSTEMS, *One Voter One Vote*, 2005