# AUDITORíA DEL SISTEMA
# **BOLETA VOTO ELECTRÓNICO**

## ELECCIONES 2015 - CHACO

*INFORME Nº 1 – 10/09/2015*

Dirección de Servicios a Terceros
Secretaría de Extensión Universitaria
Facultad Regional Resistencia
Universidad Tecnológica Nacional

## CONTENIDO

# INTRODUCCIÓN

El presente informe surge como resultado del trabajo de auditoría realizado por pedido formal del Tribunal Electoral a la Universidad Tecnológica Nacional - Facultad Regional Resistencia y refrendado en convenio firmado el 7 de agosto de 2015 en el marco de las elecciones del 20 de septiembre de la provincia del Chaco y eventual segunda vuelta del 18 de octubre de 2015 si correspondiere.

# ALCANCE

El informe incluye los análisis realizados sobre los equipos y el software que se utilizarán para la impresión y grabación de la Boleta Voto Electrónico, el sistema de recuento, transmisión y recepción del escrutinio provisorio. El análisis incluye los siguientes procesos: apertura de mesas, selección de los candidatos en las distintas modalidades existentes, la impresión de la boleta y grabación del chip (generación de las Boletas Voto Electrónico), el recuento, trasmisión y recepción del escrutinio provisorio.

# TAREAS REALIZADAS

Para la realización de esta auditoría se conformaron tres equipos de trabajo, analizando en forma separada: Software, Hardware y Sistema de transmisión. También se han analizados los procesos involucrados durante la jornada electoral.

El equipo de auditores contó para su análisis con los siguientes elementos

**Documentación entregada por el Tribunal Electoral**

- Memoria Técnica Descriptiva
- Manual de Autoridades de Mesa
- Manual de Técnicos
- Plan de Proyecto
- Ley Nro. 4169

**Documentación entregada por MSA**

- Protocolo ARM ve 1.1
- Área de QA y Calidad Resumen de Procesos y Tipos de Test
- Características técnicas de los equipos de votación modelos P3 y P4 (2 documentos)
- Imagen ISO final del sistema denominada “Búfalo”
- Imagen ISO final del sistema denominada “Búfalo” auditable incluyendo código fuente y archivos de configuración
  - https://files.msa.com.ar/auditoria_chaco/voto-Chaco-generales-Produccion-Bufalo.iso
  - https://files.msa.com.ar/auditoria_chaco/voto-Chaco-generales-Auditable-Bufalo.iso
  - https://files.msa.com.ar/auditoria_chaco/voto-Chaco-generales-Auditable-Elefante.iso
  - https://files.msa.com.ar/auditoria_chaco/voto-Chaco-generales-Produccion-Elefante.iso

**Elementos entregados por MSA**

- Tres equipos de votación (dos equipos modelos P4, un equipo modelo P3)
- Credenciales de autoridades de mesa

- Credenciales para soporte técnico
- Tres sets con todas las boletas necesarias para la realización de todos los procesos
- DVD con la última versión de desarrollo del sistema
- DVD con el sistema de Transmisión y certificados necesarios para la realización de trasmisiones en un entorno de prueba

Además de la entrega de todos los elementos ya enumerados, se realizaron varias entrevistas tanto con el personal del Tribunal Electoral como con personal técnicos de la empresa MSA involucrados en el desarrollo y en los procesos involucrados en el sistema de boleta voto electrónico.

Nuestro primer contacto con el Sistema fue en un encuentro con el personal del Tribunal Electoral del Chaco, Adrián Poertela y Leandro Saltzer el día 19 de agosto del corriente año, donde se abordaron temas relativos a los procesos involucrados y distintos aspectos relacionados con la experiencia de uso de los usuarios finales del sistema.

El día 25 de agosto se realizó una jornada de trabajo en los laboratorios de la Universidad Tecnológica Nacional, Facultad Regional Resistencia, en la que participaron los equipos de auditoria y el encuentro con Sr. Claudio Denegad director de sistemas de la empresa MSA. En esa oportunidad se analizó el proceso electoral completo utilizando el sistema de boleta voto electrónico, y el Sr. Claudio Denega respondió las consultas presentadas por el equipo de auditores. También se habilitaron los canales de comunicación con el resto del equipo de trabajo de la empresa MSA.

El 1 de Septiembre, parte del equipo de Auditores, se trasladó a las oficinas de la empresa MSA en ciudad de Buenos Aires (Distrito Tecnológico), para desarrollar una agenda de trabajo conjunta, durante la cual se trabajó en el análisis profundo de cuestiones técnicas. En la misma participaron los siguientes técnicos de la empresa MSA: Ezequiel Chan (Gerencia TIC), Marcelo Fernández (Gerente de Tecnología), Felipe Lerena (Desarrollo), Sergio Angelini (Presidente), Jorge García (Hardware).

También participamos en las jornadas de capacitación, dirigida a los auxiliares técnicos, que fueron dictadas por Pablo Rojas y Alfonzo Ruiz los días 2, 3 y 4 de septiembre en el Domo del Centenario

# ANÁLISIS DE SOFTWARE

## Análisis Funcional del Software

Se realizó análisis funcional (interacción votante-máquina) y análisis de código fuente, analizado mediante pruebas de tipo funcional, teniendo como base el proceso normal de una votación con boleta común. Tratando de crear escenarios que se puedan llegar a suscitar el día de la votación, casos especiales. Haciendo test de tipo positivo-negativo (Funcionales).

Para los casos de prueba realizados, se recrearon escenarios diferentes, muy bien definidos incluyendo: apertura de mesa, voto normal, voto asistido, cierre de mesa, escrutinio.

## Análisis Técnico del Software

Se analizó el contenido del DVD utilizado para arrancar las máquinas de voto en su versión Búfalo, tanto el sistema de voto como el de transmisión.

Se realizó una revisión y análisis de la estructura de los directorios y los archivos que componen las distintas aplicaciones involucradas en el sistema, incluyendo revisiones de código fuente en cada caso.

También se analizó el código fuente del sistema (directorio App), el mismo está implementado en el lenguaje de programación Python.

Se analizaron los componentes utilizados por estas aplicaciones mirando los repositorios públicos de la empresa MSA.

https://github.com/MSA-Argentina/ojota
https://github.com/MSA-Argentina/zaguan
https://github.com/MSA-Argentina/Keyboard
https://github.com/MSA-Argentina/chancleta

Dentro del análisis del código se buscaron malas prácticas de programación que podrían llevar a comprometer la performance y la seguridad.

Se buscó dentro del código fuente del sistema operaciones de escritura en dispositivos de almacenamiento permanente y/o entradas o salidas de red.

La última versión entregadas por MSA bajo la denominación “Elefante” la cual correrá finalmente en las máquinas de voto para estas elecciones, fueron analizadas mediante la generación de diferencias con las versiones analizadas previamente (mediante la herramienta diff), realizando posteriormente todas las pruebas funcionales establecidas.

Este análisis del código fue acompañado con entrevistas a los con programadores de la empresa MSA donde se evacuaron dudas y se explicaron criterios de programación aplicados.

Mediante entrevistas con personal de MSA, también, se pudo analizar el hardware de los equipos, su integración con los componentes de software y su interacción.

## Observaciones

**Inicio y tiempos de respuesta del sistema**: Una vez insertado el DVD y encendido el equipo, este demora aproximadamente de 2 a 3 minutos cargar todo el software necesario para su funcionamiento. Si bien consideramos que el inicio del sistema es relativamente lento, se debe tener en cuenta que esto se debe a que utiliza un DVD para hacerlo, debiendo cargar todo el software en memoria. Una vez iniciado el sistema la operación normal es muy rápida y no presenta mayores inconvenientes, incluso después de horas de uso. El paso entre las diferentes pantallas es bastante fluido, no se evidencio en ningún momento un bloqueo o esperas demasiadas largas.

Durante el encendido de los equipos correspondiente al modelo P4 suele ocurrir en forma aleatoria que la pantalla quede en negro. Notamos que dicho incidente se soluciona reiniciando dicho equipos. Es recomendable instruir a los técnicos y autoridades de mesa al respecto.

**Almacenamiento**: El equipo no posee ningún sistema de almacenamiento permanente, no conserva datos entre votación y votación, no registra información del votante en ningún momento. Esto se ha verificado examinando el hardware y revisando el código fuente.

**Conectividad** Salvo en modo "Trasmisión" el equipo, no posee soporte para redes, por más que su interfaz de red esté disponible no es posible conectarse al equipo. Hemos verificado que el stock de red no está disponible.

**Boletas** Las boletas son muy resistentes y el poder usar el mismo tipo de boletas para casi todos las funcionalidades del sistema es admirable, simplifica mucho el trabajo. No hemos detectado problemas para la lectura ni para la escritura de boletas. No hemos detectado problemas para la impresión de las boletas Al estar correctamente doblada se bloquea la lectura del chip y esconde el voto impreso, al estar un poco abierta este bloqueo falla. Recomendamos que se recuerde a los votantes varias veces, cómo debe doblar la boleta para que su voto se mantenga secreto.

**Dispositivos para no videntes:** El sistema para personas no videntes es práctico y funciona muy bien, hemos realizado prácticas con los ojos vendados, pudiendo terminar el proceso sin problemas. Hemos notado que si uno selecciona una opción y no aprieta el numeral el sistema no informa o advierte sobre esa situación quedando en una espera indefinida. Recomendamos que si excedido un cierto tiempo el usuario no presiona ninguna tecla el sistema indique las instrucciones que permitan continuar con el proceso.

# ANÁLISIS DE HARDWARE

Se realizaron los controles y validaciones funcionales sobre los equipos de votación y escrutinio perteneciente a los modelos P3 y P4 que forman parte del parque destinados a estas elecciones. Además se realizaron análisis estructurales y de integridad, intentando reproducir y evidenciar los problemas y/o cuestionamientos existentes.

**Aspecto físico:** El equipo presenta un diseño robusto, sencillo y transportable. El único elemento que viene suelto con el equipo es el cable de alimentación, el cual viene en uno de los compartimientos

**Pantalla:** Analizando la pantalla se puede apreciar una buena visibilidad desde varios ángulos. La parte táctil demostró ser bastante fiable y solo en contados casos se tuvo que repetir la acción para que ocurra correctamente. Posee muy buena nitidez y contraste inclusive exponiéndola en una sala con mucha luz solar. La funcionalidad de alto contraste que posee maximiza aún más la capacidad de visualización.

**Impresora:** Su funcionamiento fue correcto no hubo ningún sobresalto. La calidad de impresión aun estando seleccionada la opción más baja fue, totalmente legible y entendible. La velocidad de impresión es muy buena.

**Lectura y grabado del chip RFID:** Se analizó la posibilidad de alterar de cualquier manera el contenido grabado en el chip RFID una vez impresa la boleta, y se ha podido comprobar que la información almacenada se encuentra legible (texto plano), y que una vez grabada dicho contenido es inalterable ya que todos y cada uno de los bloques de datos que conforman el chip son bloqueado "marcados como solo lectura". El comando concreto utilizado es LOCK que evita cualquier modificación sobre dichos bloques. Este hecho ha podido ser evidenciado en las pruebas realizadas. El resultado de nuestras pruebas condicen con las especificaciones técnicas que acompañan al chip utilizado.

**Alimentación eléctrica y baterías: ambos** modelos cuentan con una fuente de alimentación eléctrica de 220 v y dos baterías que en su conjunto brinda una autonomía de 11 hs aprox.

No existe indicador a simple vista del estado de carga las baterías en el equipo, en ninguno de los modelos que se utilizarán (P3 y P4). De modo tal que, conectando la máquina a la red de suministro eléctrico, no se encuentra ningún indicador ni luz LED que indique que el equipo se encuentra cargando o no, por ende tampoco se conoce cuando el equipo ha logrado completar la carga.

Es oportuno destacar que en el documento entregado bajo el nombre "Características técnicas del sistema.docx" se encuentra indicado en la especificación del equipo los siguientes detalles referentes a la carga de la batería. "Led´s indicadores de encendido/apagado y estado de carga de las baterías"

Con la credencial de técnico, una vez iniciado el proceso de votación, se puede acceder al menú de "Mantenimiento", donde se aprecia un menú con la gestión de la batería, donde se indican entre otros valores, la carga de cada una de las baterías.

En la visita a la empresa MSA, el personal indicó el modo de chequear el estado de carga de las baterías. El mismo consiste en abrir el compartimiento donde se encuentran alojadas las baterías, desajustar el velcro, tomar la batería y en el lateral se encontrarán cinco LED's junto a un pulsador. Al presionar el pulsador, se enciende la cantidad de LED's correspondientes al nivel de carga de la batería. Es decir, si se encienden dos de los cinco LED's, se estima que la carga de esa batería es de un 40%.

# ANÁLISIS DE PROCESOS

**Aspectos de seguridad:** El sistema se encuentra diseñado para ser ejecutado desde el DVD, sin almacenamiento alguno de información previa. Así mismo, en el momento en que se imprime una boleta, y va a dar comienzo a la elección de un nuevo votante, el sistema elimina toda información de la elección anterior. *Se ha identificado las porciones del código fuente en las cuales se realiza dicho procedimiento: archivo: app/msa/voto/controllers/voto.py, líneas 111, 432, 671*

Al igual que sucede en las elecciones tradicionales es fundamental la custodia de todo el material que conforma el sistema de boleta voto electrónico asegurándose que los equipos, las credenciales, las boletas los DVDs, etc. sean solo manipulados por el personal autorizado para hacerlo.

Se recomienda evitar la manipulación de aparatos electrónicos (celulares, tabletas, etc.) dentro del recinto de votación sobre todo cerca de las urnas y/o las máquinas de votación

**Planes de contingencia:** La empresa MSA implementará un sistema para monitorear todas las operaciones relativas al sistema de boleta voto electrónico el día de las elecciones lo que permitirá estar el tanto de cualquier contingencia y/o eventualidad que surja, como así también mantener contacto con los auxiliares técnicos desplegados en las escuelas.

**Transmisión de resultados**: el proceso de trasmisión de los resultados del escrutinio se realiza mediante la utilización de los mismos equipos utilizados para la impresión de boletas. Para ello se debe arrancar el equipo con un DVD diferente al usado para la emisión del voto, el cual contiene el "sistema de transmisión". Este sistema permite enlazar el equipo al centro de cómputo a través de internet.

Se observa en los equipos de votación a simple vista la existencia de un puerto de RED (Tipo RJ45), y puertos USB que podrían comprometer la seguridad de los mismos. Estos puertos se encuentran presentes con el objetivo de poder utilizar las mismas máquinas emisoras de votos como máquinas de transmisión. En este sentido hemos podido comprobar que durante la ejecución del sistema de votación tanto el puerto de RED como los puestos USB no están disponibles ya que el sistema no carga los módulos necesarios para su funcionamiento.

- **Integridad**: La Integridad de los resultados transmitidos por mesa, es verificable mediante una aplicación provista a los fiscales de cada partido. Así mismo el equipo de Auditoría, tendrá acceso durante el proceso a la base de datos que recepciona dichos datos.

- **Confidencialidad**: Los datos son transmitidos utilizando la tecnología HTTPS (protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP). A esto se incorpora la validación por parte del cliente mediante un certificado. Es decir, para que una transmisión pueda efectuarse, el técnico designado debe de proporcionar un certificado de cliente junto con su contraseña.

- **Disponibilidad**: la empresa demostró la evidencia acerca de la disponibilidad de 3 (tres) centros de datos, uno principal que recepciona los datos en situaciones normales, un segundo ubicado en las oficinas del tribunal electoral y un tercero disponible un una nube de terceros fuera del país (concretamente AWS Amazon Web Services). Si bien existen 3 centros de datos disponibles, la conmutación entre los mismos en caso de fallos, es manual y a discreción de la empresa MSA. En este sentido, se ha podido observar el centro de datos ubicado en el Tribunal Electoral. Se evidencia que se encuentran por duplicado los servidores físicos y switches de conectividad, y según la información proporcionada, los servidores alojan la misma información de manera duplicada.

**Conectividad:** Para el proceso de transmisión de los resultados del escrutinio, se requiere una conexión a internet. Teniendo en cuenta la realidad de la infraestructura tecnológica de los establecimientos escolares de la provincia, se sugiere reforzar los medios de contingencia para concretar el envío de los datos. Si bien lo indicado por la empresa MSA, el tráfico no es significativo, requiere mantener una conexión estable, y es importante tener en cuenta la deficiente cobertura de datos para los modem 3G que harían de contingencia, los cuales se hacen más notorios en el interior de la provincia.

Está previsto la realización de pruebas de conectividad en cada uno de los establecimientos donde se utilizara el sistema de boleta voto electrónico los días previos a los comicios de forma tal de testear el funcionamiento de las conexiones y de proveer todas las contingencias necesarias.

Durante la reunión mantenida en las oficinas de MSA el día martes 1 de Septiembre, se le recomendó coordinar con la empresa del estado provincial ECOM CHACO S.A, la conectividad necesaria en los puntos que se requiera.

# CONCLUSIONES

En función del análisis realizado por nuestros equipos de auditoría y teniendo en cuenta informes realizados anteriormente concluimos:

No existen problemas o inconvenientes que impidan el normal funcionamiento del sistema o que impliquen la violabilidad de las garantías constitucionales de los usuarios del mismo

Los procedimientos definidos para los comicios garantizan el desarrollo seguro de todas las actividades a realizarse, tanto para las jornadas previas de configuración y pruebas, como el mismo día de votación

La robustez del sistema radica en que la maquina solo imprime las boletas, sin llevar ningún tipo de registro de lo realizado, las cuales se convierten en votos válidos, recién, una vez ingresados en la urna. Esto permite

- Asegurar el anonimato del voto
- El hecho que los votos son impresos y grabados físicamente en una boleta para luego ser introducidos en una urna convencional permite comprobar fácilmente y en forma manual la voluntad del elector al mismo tiempo que puede ser fácilmente fiscalizado por las autoridades de

mesa y fiscales que participan en el proceso, permitiendo, en caso de algún percance o eventualidad realizar el escrutinio en forma manual

Como en una votación tradicional la integridad del voto es responsabilidad, en un principio del elector y una vez en la urna de las autoridades de mesa.

Es fundamental que todos los actores (votantes, autoridades de mesa, fiscales, delegados, etc.) tengan una acabado conocimiento sus funciones y responsabilidades para con el sistema de boleta voto electrónico