Prof. Claudio Enrique Righetti
Departamento de Computación – Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Pabellón I – Ciudad Universitaria – (C1428EGA) – Buenos Aires – Argentina
Tel./Fax:+54-11-4576-3359 - claudio@dc.uba.ar

OAT N° 03/15 – Auditoría de sistemas Elecciones 2015 – Ciudad de Buenos Aires

INFORME 4: Observaciones del sistema de voto con boleta única electrónica (BUE) para las elecciones generales al martes 23/06/2015

El presente informe es un compendio de todo lo revisado y actuado por la Auditoría hasta la fecha e incluye la información pertinente de los informes anteriores.

Se incluyen observaciones sobre el sistema y sobre su evolución a lo largo de la Auditoría.

Resumen ejecutivo

MSA, la empresa contratada por el Poder Ejecutivo, proveyó el código fuente, archivos de ejemplo de configuración, la documentación del código fuente y su uso y nombró un responsable técnico que evacuó las consultas a medida que se fueron realizando.

De las tareas de auditoría llevadas a cabo no se han detectado problemas graves, ni indicios de que las observaciones que se describen a continuación puedan causar inconvenientes insalvables el día de la elección. Muchas de las observaciones que se realizaron en informes anteriores, fueron solucionadas por la empresa en la versión final auditada.

El mayor resguardo del sistema consiste en los mecanismos de control existentes que son externos a la solución tecnológica, lo cual es facilitado por los procedimientos definidos en dicha solución.

Los principales custodios de los comicios siguen siendo tanto las autoridades de mesa y los delegados del Tribunal, como los fiscales de las agrupaciones políticas y los mismos electores.

La principal fortaleza del sistema radica en que las máquinas utilizadas para imprimir las BUE (Boleta Única Electrónica) no guardan información de la selección del elector. Una vez que las opciones elegidas se confirman, las mismas se imprimen y graban en la BUE y acto seguido, se borra de la memoria volátil de la máquina.

El propio elector puede comprobar físicamente en el momento el contenido de la BUE.

La máquina puede reiniciarse en cualquier momento o ser reemplazada por otra y esto no afecta el procedimiento ni invalida los votos impresos en la misma.

Las autoridades y fiscales del comicio pueden comprobar físicamente el contenido de las BUE (tanto impreso como la grabación digital) desde el momento de la apertura de la urna donde se depositan dichos soportes, tal cual ocurre en el sistema de voto tradicional.

Otra fortaleza importante es que el software que se ejecuta en dicha máquina no está en un medio interno de la máquina, si no que está en un soporte digital externo (DVD) que es generado bajo control de las autoridades y sellado hasta que lo recibe la autoridad de mesa. La máquina, sin dicho soporte, simplemente no puede hacer nada.

Alcance

La presente auditoría cubre los equipos y software utilizados para la impresión y grabación digital de la BUE a utilizarse para la emisión del voto, el recuento de votos de cada mesa, el sistema de transmisión y recepción de estos datos y el escrutinio provisorio.

No se audita el sistema de operaciones que la empresa utiliza para el seguimiento y control del operativo ni la capacitación de autoridades de mesa y ciudadanos.

De todos modos, dado que la empresa ha facilitado información y documentación acerca del sistema de operaciones, se hace referencia al mismo en determinados ítems.

Los establecimientos de votación fueron relevados por técnicos contratados por la empresa en lo relativo a sus instalaciones eléctricas y la conectividad a internet el día 20 de junio. Si bien esta auditoría no cuenta con los resultados de dicho relevamiento, los equipos cuentan con baterías que, si están cargadas por completo, pueden permitir el normal funcionamiento aun ante la ausencia de energía eléctrica (ver Anexo III). Con respecto a la conectividad, existen esquemas de contingencia que permiten la transmisión de datos por métodos alternativos (ver Anexo IV).

Aspectos funcionales del software

Llamamos aspectos funcionales del software a las características del mismo que son visibles por los usuarios o que determinan qué es lo que el usuario puede hacer y cómo.

Son usuarios del software:

- Los ciudadanos en general en su rol de electores y autoridades de mesa en las máquinas de votación.

- Las autoridades electorales que deben poder tomar decisiones sobre ciertos aspectos del proceso, así como sus delegados en los sitios de votación.
- Los partidos políticos en su rol de fiscales.

El software debe, en forma clara y eficiente, permitir a los usuarios realizar sus tareas. Debe proveer los mecanismos de control posibles para minimizar los errores provenientes del uso del mismo.

Observaciones sobre la funcionalidad y cambios introducidos luego de que las mismas hayan sido hechas

En esta sección se describen las observaciones realizadas a lo largo de todo el proceso de Auditoría. Cuando las observaciones han sido atendidas en versiones posteriores, se lo aclara a continuación con el título "**solución implementada**".

De la funcionalidad analizada se hacen las siguientes observaciones:

1. Las máquinas ordenan aleatoriamente las listas cada vez que el elector ingresa a la pantalla donde se muestran las listas. Si un elector pasa varias veces por esta pantalla, el orden de la misma será distinto cada vez. Esto podría confundir al ciudadano que recorra las pantallas más de una vez.

   La solución propuesta por esta auditoría en un informe anterior fue que el sorteo del orden de las listas se realice cada vez que ingresa un nuevo elector en el sistema (cuando se inserta una BUE en blanco) y se mantenga fijo hasta que ese elector haya confirmado toda su selección (hasta que imprima o retire la BUE).

   La **solución implementada** consiste en mostrar un recuadro azul sobre la elección realizada, de modo que si el elector vuelve a la pantalla, aunque la posición se vuelve a sortear, queda claro lo último que seleccionó.

   Esta auditoría considera que, dada la poca cantidad de listas que participan en este comicio, la solución implementada reduce las dificultades observadas en el informe anterior.

2. Al finalizar la impresión de un voto, el sistema le informa al votante cómo puede verificarlo. Esta pantalla no se podía llegar a leer en su totalidad; apenas estaba unos segundos y a continuación aparecía nuevamente la pantalla inicial "Introduzca la Boleta Única Electrónica en la impresora" que invitaba a iniciar una nueva votación.

   Por otra parte, normalmente, lo primero que hace el elector una vez impresa la BUE es girarla y leerla (en el papel), con lo cual dicha pantalla, muchas veces, pasaba completamente inadvertida.

Esto podría haber hecho pensar al elector que no llegó a tiempo a realizar la verificación de su voto o, simplemente, al no haber leído la pantalla, se olvidaba de que existía esa posibilidad. Verificar el voto por parte de cada votante es uno de los factores que ayudan a la confiabilidad y transparencia del proceso electoral.

Solución implementada: Siguiendo la sugerencia hecha por esta auditoría, se agregó un texto en la pantalla de bienvenida al elector recordándole que verifique su voto una vez impreso apoyándolo en el lector, con una indicación gráfica al respecto.

Esta auditoría considera que esta solución cubre la observación realizada.

3. En las pantallas de carga de datos para el Acta de Apertura y el Acta de Cierre:

   a) No se controla que los números de documento del Presidente y el Suplente sean diferentes. Si bien existe una mínima posibilidad de números repetidos (e.g. coincidencia entre Libreta Cívica y Libreta de Enrolamiento), estadísticamente, la posibilidad es muy baja y el sistema debería al menos hacerle notar a la autoridad de mesa que los números son iguales y ofrecerle modificarlos antes de avanzar (aunque, una vez notado esto, le permita hacerlo aún sin modificar los números).

      Si bien este comportamiento no se ha modificado, la posibilidad de cometer un error al registrar los documentos de las autoridades de mesa ya estaba presente cuando se realizaba el voto en papel, cuando las actas se confeccionaban completamente a mano.

   b) No se controlaba el rango horario. La hora de apertura no debería ser anterior a las 8:00 ni la hora de cierre debería ser anterior a las 18:00. El sistema debería al menos hacerle notar esto a la autoridad de la mesa.

      Solución implementada: El sistema ahora no permite cargar un horario de apertura anterior a las 8:00 ni un horario de cierre anterior a las 18:00 resolviendo la observación planteada.

   c) Si bien cuando se ingresaba la hora y no los minutos o viceversa aparecía un cartel indicando esto forzando a corregir el error, cuando no se ingresaba ninguno de los dos campos, no aparecía ningún cartel avisando de esto y permitía seguir adelante asumiendo que la hora de apertura era 8:00 y la de cierre era 18:00.

Solución implementada: El sistema ahora controla que los cambios hora y minutos estén ambos completos y nunca los completa automáticamente, resolviendo la observación planteada.

d) El sistema tampoco consideraba un error la ausencia de datos de autoridades de mesa por completo, permitiendo avanzar e imprimir un acta de apertura sin ningún dato de la autoridad de mesa, de hecho, generando un texto sin sentido:

"*El suscripto Presidente del comicio Sr. , con declara abierto el acto en la mesa XX (...).*"

Solución implementada: El sistema ahora controla que al menos una de las autoridades tenga los datos completos, y para cada autoridad en que se completa algún dato, se controla que estén todos los datos. Si se completara el dato de alguna autoridad y no la del presidente, luego de cargados se reconfiguran para que el primer suplente con datos cargados figure como presidente. Esto resuelve la observación planteada.

4. Cuando se está ingresando texto con los datos de las autoridades de mesa (nombre, apellido, documento), si el presidente comete un error omitiendo un carácter y lo descubre, puede tocar con el dedo para insertar el cursor en la posición donde desea continuar escribiendo; sin embargo, pese a que el cursor *aparece* en dicha posición, cuando utiliza el teclado en pantalla para ingresar texto, el texto se agrega al final y *no* en la posición del cursor.

   Esto también se verifica en la carga del número de mesa y PIN.

   Cambio implementado: En la versión actual, sigue ubicándose el cursor en el medio de un texto ingresado, y al presionar una tecla el cursor se ubica al final del texto donde también ubica la letra ingresada. La confusión que se genera es menor (porque el cursor se ve en el lugar donde se insertó la letra) pero todavía existe el problema de no permitir corregir textos largos sin necesidad de reescribir desde el error hasta el final (por ejemplo un apellido largo) y al mostrar inicialmente el cursor dentro del texto podría inducir al usuario a intentarlo varias veces. Cabe aclarar que la observación hace a la amigabilidad del sistema y no afecta su funcionamiento.

5. Al finalizar el recuento de votos, la indicación en pantalla decía: "*Presione Imprimir para obtener el Acta de Cierre de Mesa*", sin embargo, no había ningún botón "Imprimir" en esa pantalla.

   Luego, si se presionaba el botón "Siguiente", el Acta de Cierre que estaba insertada en la impresora salía hacia abajo, pero completamente vacía[1].

   A continuación aparecía una pantalla solicitando se ingrese nuevamente el Acta.

   En versiones anteriores se solicitaba la inserción de un Acta de Cierre de Mesa y Escrutinio en el momento de *comenzar* el escrutinio.

   Solución implementada: Se cambió la indicación "*Presione Imprimir(...)*" por "*Presione Siguiente(...)*" y se cambió el modo de funcionamiento del recuento y el sistema ahora no solicita que se inserte el Acta de Cierre sino hasta que finaliza el recuento y lo confirma. Estas soluciones evitan las confusiones mencionadas.

6. En modo de "*Votación Asistida*" disponible para personas con dificultades visuales, si el votante presiona un número pero olvida presionar la tecla "#" el sistema no le advierte de esa situación y se queda esperando indefinidamente. Luego de un tiempo de espera, el sistema debería volver a indicar las instrucciones necesarias para llevar a cabo la elección, o indicarle nuevamente que debe presionar la tecla "#" a continuación del número.

7. En el modo de "*Votación Asistida*", el voto en blanco siempre aparece como la última alternativa. En la versión anterior, el voto en blanco siempre aparecía como la opción "**0**". Se le informó a la empresa que esto permitía que una autoridad de mesa que estuviera asistiendo a alguien en este modo viendo la pantalla (este modo de asistencia está pensado para que ello sea posible) podría saber que un elector estaba votando en blanco.

   El **cambio adoptado** en la versión del 29 de mayo, poniendo el voto en blanco *siempre* como la última opción, no cambia mucho el secreto del mismo, ya que la cantidad de agrupaciones que se presentan para cada categoría es conocida. Este cambio se mantuvo en la versión final.

8. En el modo de "*Votación Asistida*" era imposible completar la selección ya que en el momento que el sistema debía emitir el título de la categoría correspondiente a *Miembros de la Junta Comunal*, el sistema dejaba de emitir audio por completo y el elector no tenía forma de continuar, aun cuando tuviera asistencia de alguien que estuviese mirando la pantalla.

---

1 Esto se observó en campo durante los comicios en la Provincia de Salta y el hecho de que el acta saliera vacía sorprendía y preocupaba a las autoridades de mesa.

Solución implementada: El problema ha sido resuelto y no es observable en la versión actual.

9. Cuando se estaba eligiendo por categorías en el modo de "*Votación Asistida*", el audio indicaba el cargo (la categoría) y para cada opción, el número que debía seleccionar y el nombre del candidato, pero ***no*** el nombre de la agrupación ni el número de lista a la que pertenece el candidato.

   Solución implementada: Se modificó el sistema y ahora, luego del nombre del candidato, se oye el nombre de la agrupación a la que pertenece.

10. Al seleccionar "*Versión de Demostración*" para utilización en la capacitación, el sistema solicita el número de Comuna (para poder mostrar las listas correctamente) y pasa al modo "demo". Sin embargo, dentro de este modo, no hay ningún indicio visual que muestre que se está en este modo y no en el modo de impresión de votos reales.

    Nueva observación: La empresa respondió al informe N°2 del 1 de junio diciendo que implementaría una modificación para que quien interactúa con la máquina pueda ver claramente que está en modo demo, sin embargo, esto no se observa en la versión actual.

    Si se ha definido que el modo "demo" no se utilizará y que las máquinas dedicadas a capacitación utilizarán un DVD diferente al que se utiliza en las máquinas de voto, DVD de las máquinas de voto debería tener completamente deshabilitada la opción del modo "demo".

    Además, en el modo "demo", la última versión del sistema *no imprime* las BUE de capacitación como lo hacía la versión anterior.

    Finalmente, en el modo "demo" no aparece la pantalla de verificación del voto, que es importante para capacitar al ciudadano en este aspecto. Si el modo "demo" no graba la información del voto en el chip RFID por cuestiones de seguridad, en el momento en que debería aparecer la pantalla de verificación del voto, debería aparecer una pantalla indicando que debería hacer esto, con una imagen de la BUE apoyada en el lector explicándole al ciudadano cómo hacerlo y como recordatorio al capacitador para que haga hincapié en esto.

    Solución implementada: Esta última parte (el recordatorio al elector para la verificación del voto) ha sido resuelta del mismo modo que la solución de la observación N° 2.

11. El módulo de reportes destinado a la web que muestra por internet los resultados parciales del escrutinio no tiene un tope o umbral mínimo de volumen para empezar a mostrar resultados. Con sólo 10 mesas escrutadas

puede mostrar resultados parciales. No se observa que haya un lugar donde la autoridad electoral competente pueda definir (en caso de que así se decida) un mínimo de cantidad (o porcentaje) de mesas escrutadas para permitir visualizar, ni una hora de comienzo, ni un control manual de "empezar a mostrar ahora".

En los comicios de la Provincia de Salta se comenzaron a mostrar datos con muy pocas mesas escrutadas. La autoridad de aplicación debería *a priori*, definir un piso de publicación razonable que podría estar indicado ya sea en número absoluto o porcentaje de mesas o votos escrutados, de modo tal de no mostrar al público un porcentaje poco relevante de votos.

Solución: La empresa respondió que se pueden establecer condiciones para el inicio de la publicación en base a la hora, una cantidad de mesas o un porcentaje de votos escrutados y que corresponde al órgano electoral o al responsable del escrutinio provisorio la decisión de utilizar dichos controles y que la Provincia de Salta decidió publicar a partir de la primer acta recibida.

Sin embargo, esta auditoría no encontró en el código dónde se solicitan o definen estos umbrales.

Mejoras observadas

En la última versión se introdujeron varias mejoras, algunas de las cuales se observan a continuación:

12. En diversas partes del sistema de voto se han observado aclaraciones, recordatorios y otras ayudas en las pantallas para el elector.
13. En la boleta impresa, se agrandó el tamaño de la tipografía, facilitando la lectura por parte del elector al verificar su voto, y de las autoridades de mesa y fiscales al contarlo.
14. En la boleta impresa se agregó un cartel señalando la posición del chip RFID (además del logo que ya existía anteriormente), con la leyenda "Verifique su voto" para recordarle al elector que lo haga y señalándole la ubicación.
15. En base a recomendaciones del Tribunal, y luego de conversaciones mantenidas entre el equipo de Auditores y la empresa, esta última introdujo una modificación en el funcionamiento del software de la máquina de votación en lo relativo al acceso que se logra con la credencial de técnico. Con esta modificación, para permitir al técnico cambiar el estado de la máquina, se requiere de la participación de la autoridad de mesa.

    En la nueva versión, una vez que la máquina está en funcionamiento en el modo de votación, la credencial de técnico no permite hacer nada (la misma

es ignorada cuando se acerca al lector). En este modo, la credencial de autoridad de mesa lleva a la pantalla de inicio; al volver apoyar la credencial de autoridad el sistema solicita o bien cargar el número de mesa con el PIN o apoyar el Acta de Apertura de la mesa para luego habilitar la pantalla del menú principal.

Recién en este instante, sólo en este menú, y estando presente la autoridad de mesa responsable con su credencial y el PIN correspondiente y/o el Acta de Apertura, el técnico puede acercar su credencial y tener acceso a la pantalla de mantenimiento que lo habilita a cambiar los parámetros operativos (que, de todos modos, no permiten modificar el funcionamiento básico de selección de listas o candidatos e impresión de las BUE).

Nuevas observaciones

16. Este comportamiento ya ocurría en versiones anteriores del sistema: Al seleccionar el voto por categorías hay, en cada pantalla, un título de pantalla que indica qué categoría se está eligiendo y que, además de darle información al elector, le permite a una autoridad de mesa que podría estar ayudándolo sin ver la pantalla a ubicarse en el programa.

    En el caso de la voto por lista completa, la pantalla no tiene título alguno. Si bien no es intrínsecamente necesario ya que es la única pantalla que verá antes de la de confirmación, un título que diga "voto por lista completa" o algo similar daría mayor consistencia y podría ser un punto de apoyo a quien esté ayudando al elector sin mirar la pantalla.

    Se recomienda estudiar estos cambios para el futuro. No se recomienda modificar la actual versión del software dado el escaso tiempo disponible para testear y validar las modificaciones.

17. Este comportamiento ya ocurría en versiones anteriores del sistema: Cuando en la pantalla de confirmación, luego de haber seleccionado todos los candidatos por cualquiera de los dos medios posibles, se presiona el botón azul "Modificar" para modificar una categoría, se muestra la pantalla correspondiente a la categoría con el candidato previamente seleccionado resaltado en azul.

    Podría ocurrir que el elector no sepa como "arrepentirse" y volver a la pantalla de confirmación (no notando que lo que debe hacer es volver a seleccionar el candidato que ya había seleccionado y que se encuentra resaltado en azul).

    Una solución posible sería agregar un botón verde que diga "Aceptar la selección" o similar cuando el candidato esté previamente seleccionado (el mismo botón podría existir cuando se vota por categorías y se han

completado todas). De todos modos, no se recomienda modificar la actual versión del software dado el escaso tiempo disponible para testear y validar las modificaciones.

18. Si el elector confirma su selección (aprieta el botón "imprimir") pero retira la BUE forzándola hacia arriba (mientras está el cartel que le indica que no lo haga), podrían pasar dos cosas diferentes:

    a) Que no haga tiempo a grabarse nada, en cuyo caso la BUE quedará completamente igual que cuando se insertó (en blanco, tanto el papel como el chip). Si el elector intenta introducir la boleta nuevamente en la máquina, podrá hacerlo sin inconvenientes.

    b) Que se haya grabado la información en el chip y no haya llegado a imprimirse nada (o casi nada). En este último caso, la información del voto está completa en el chip y no está impresa en el papel. Si el elector intenta introducir la boleta nuevamente en la máquina, verá en la pantalla lo que había seleccionado anteriormente (ya que está grabado en el chip), se expulsará automáticamente la BUE y no lo dejará generar un nuevo voto. El elector puede volver a la mesa, romper la BUE y solicitar una nueva.

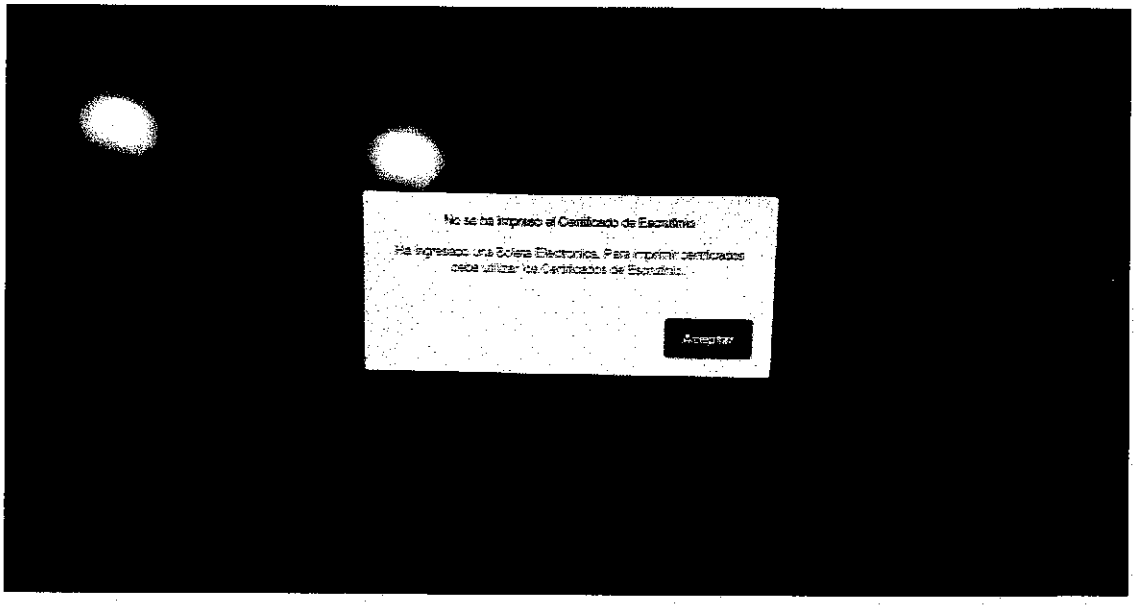
    Suponiendo que, en cualquiera de los dos casos, el elector lleve la BUE y la introduzca en la urna tal cual está (es decir, no intente usarla nuevamente), durante el recuento, al ver que la BUE está en blanco, el presidente de mesa no pasará la BUE por el lector y lo considerará un voto nulo que se agrega en la cuenta manualmente al final del recuento sin pasar por el lector.

19. Comuna 9: Dado que en esta Comuna la mecánica del voto es diferente, las máquinas de capacitación en los establecimientos de la misma deberían reflejar esto, con una consulta popular para que los electores no se sorprendan cuando vean la consulta en lugar de la pantalla de confirmación.

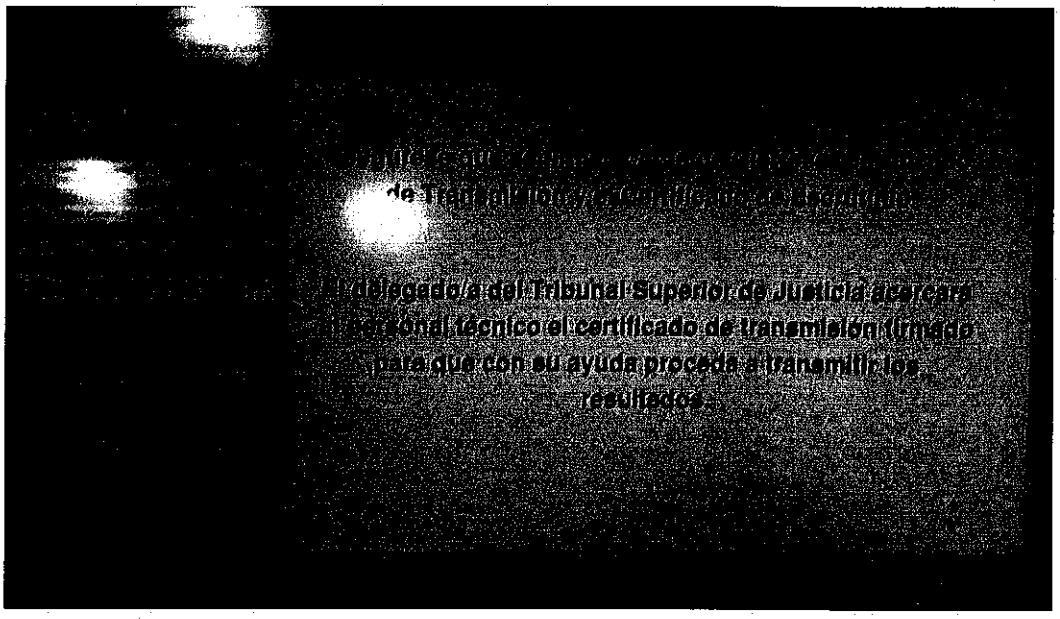
20. Una vez finalizado el escrutinio de la mesa, para imprimir los Certificados de Escrutinio para los fiscales, si se apoya el Acta de Cierre de Mesa y Escrutinio en el lector se ve, a la izquierda de la pantalla la tabla con el resultado del escrutinio y en el medio de la pantalla el código QR con la codificación de dichos datos.

a) En la parte superior de esta pantalla aparece un cartel que dice "Puede continuar introduciendo certificados de escrutinio para los fiscales que lo requieran", pero en la parte inferior aparece un cartel azul que dice "Listo para leer". Esto se presta a confusión.

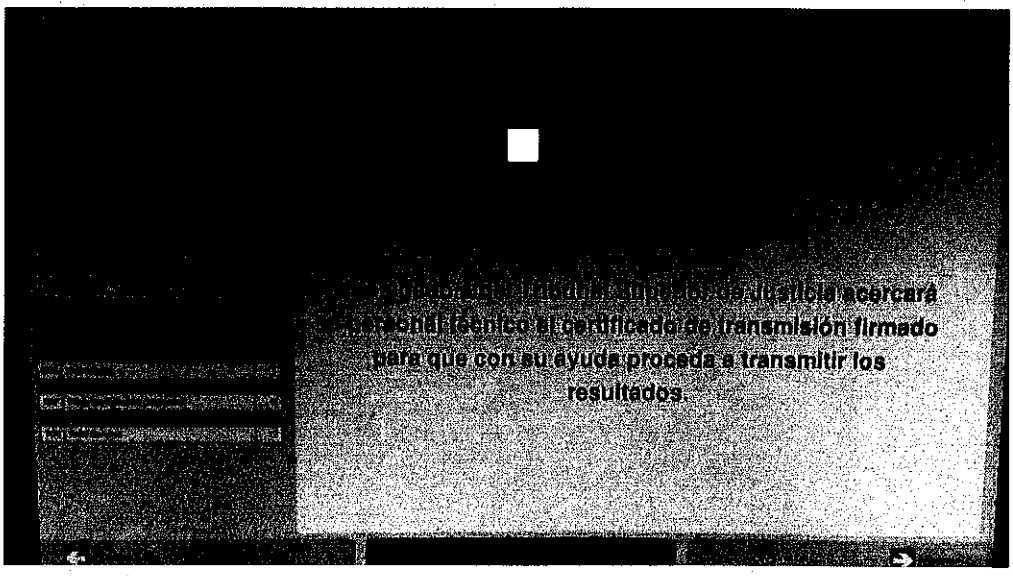
b) Si en lugar de introducir un Certificado de Escrutinio para fiscales (que la máquina reconoce por no tener chip RFID), se introduce un Acta o Boleta cualquiera (que sí tiene chip), el sistema la detecta, la expulsa y muestra un mensaje de error:



Luego de esto aparece un nuevo botón abajo a la izquierda de la pantalla con el texto "Salir", sin embargo, al presionarlo, se despliega un texto de ayuda:

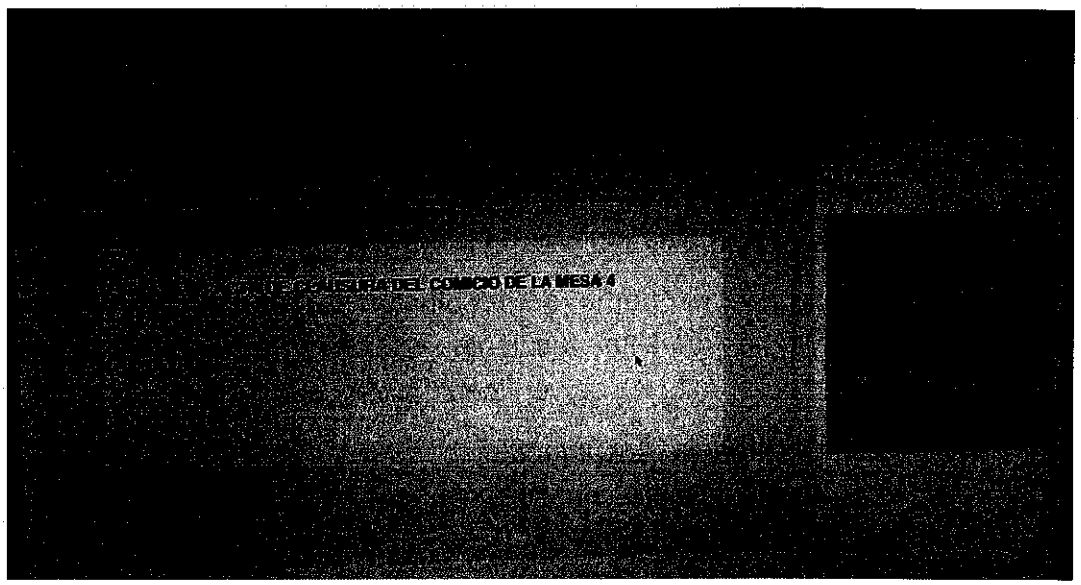


c) Si erróneamente se acerca el Acta de Cierre de Mesa y Escrutinio, aparece un cartel que advierte que no se ha impreso el Certificado de Escrutinio y aparece un nuevo botón con el texto "Ver QR". Si se presiona ese botón, la pantalla se oscurece:



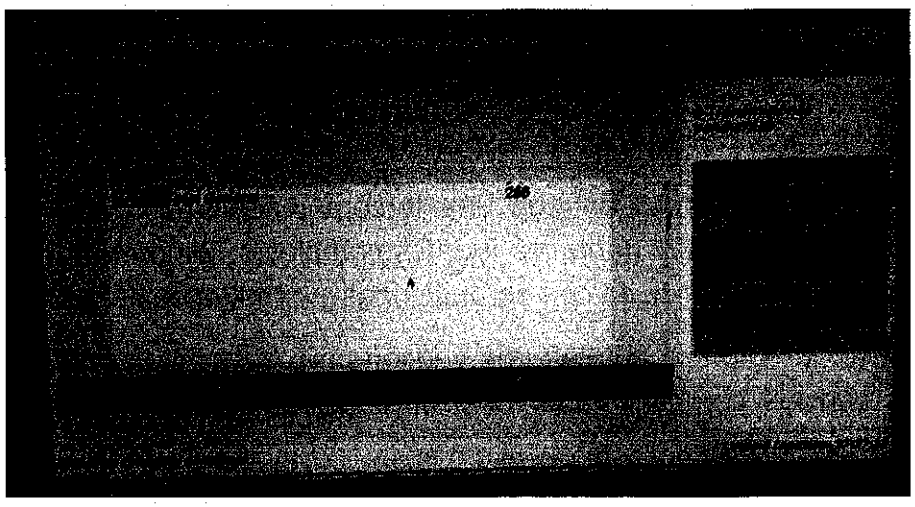
Si se vuelve a tocar la pantalla, el sistema continúa funcionando correctamente.

21. En la máquina de Transmisión, para el Delegado Judicial, cuando se acerca el Certificado de Transmisión al lector para verificar la lectura de los datos, sólo se aprecia el título del acta con un gran espacio en blanco debajo:



No se advierte inmediatamente que, a la derecha de la imagen, hay una barra de desplazamiento (*scroll bar*) y que, desplazando dicha barra recién aparecerán los datos del escrutinio de la mesa. Por otra parte, el desplazamiento de la imagen utilizando dicha barra es dificultoso con el dedo en la pantalla táctil.

22. En la pantalla de Transmisión, la posición de la barra de desplazamiento parece tener "memoria": Si al revisar el contenido de un certificado, el usuario se desplaza hacia abajo y lo deja así, y luego apoya un nuevo certificado, aparece el contenido del nuevo certificado pero desplazado hasta la posición en la que había quedado la barra de desplazamiento en el certificad anterior:



Código fuente auditado

MSA, la empresa contratada por el Poder Ejecutivo, proveyó el código fuente del sistema y el *firmware* de la máquina, archivos de ejemplo de configuración, la documentación del código fuente y su uso y nombró un responsable técnico que evacuó las consultas a medida que se fueron realizando.

Si bien las respuestas del responsable técnico fueron satisfactorias, no suplen por completo el hecho de que la documentación existente no es exhaustiva ni sigue plenamente las reglas del arte para documentar software.

Aun cuando el esquema de resolución de dudas interactivas por parte de un responsable o analista funcional estuviera a disposición permanente de los programadores, esto no es verificable por la auditoría.

Los defectos en la documentación representan un punto débil a observar en el software que dificulta no sólo la auditabilidad del mismo, si no también el mantenimiento y evolución.

El programa tampoco contiene casos de prueba automáticos. Si bien es común en las empresas que desarrollan software no incluir pruebas automáticas durante el desarrollo, incluirlas representa una ventaja apreciable porque minimiza la cantidad de errores de programación. Además los casos de prueba automáticos con alta cobertura de código es una parte importante de lo que hacen los programadores en las comunidades donde se comparte código, las pruebas automáticas son una señal de que se ha pensado el desarrollo para que otros puedan mirar, comprender y validar el código, ya sea para mejorar o cambiar su funcionalidad, corregirlo o auditarlo.

El 20 de marzo, previa firma de un acuerdo de confidencialidad, la empresa proveyó el código fuente de la versión 3.0 del sistema de voto, conjuntamente con el software para la carga manual y el escrutinio provisorio.

El 14 de abril, la empresa hizo entrega de dos máquinas de voto con sendos DVD para arrancar las máquinas con la misma versión del software y una base de datos de prueba con los cargos electivos de la Provincia de Salta y agrupaciones políticas y candidatos de fantasía ("partido de la música", "partido de los deportes", etc).

El 22 de mayo, la empresa entregó una tercera máquina de voto y el software actualizado a la versión 3.1 (tanto los fuentes completos como el DVD de arranque con el software de voto, todavía con agrupaciones y candidatos de fantasía.

El 29 de mayo, la empresa entregó una versión preliminar actualizada del software, ya cargada con los cargos y candidatos oficializados de la Ciudad Autónoma de

Buenos Aires, sin las imágenes oficiales ya que las mismas aún no habían sido recibidas y sin haber realizado el proceso de *testing* interno.

El 10 de junio la empresa entregó una versión con más testeo interno y el 17 de junio la versión preliminar definitiva (RC-1) que sólo podría aceptar cambios si se detectan errores graves antes de la grabación.

En el Anexo I se realizan algunas observaciones específicas sobre el código fuente que la presente auditoría entiende son significativas del sistema.

Máquinas de voto y escrutinio

Para evaluar el funcionamiento de las máquinas de voto y escrutinio en las tareas de apertura de mesa, emisión de votos, cierre de mesa y escrutinio, se seleccionó una muestra aleatoria para cada modelo de máquina[2]. Se revisaron las muestras y se catalogaron los posibles incidencias que pudieran encontrarse según su importancia:

- **ALTA**: son aquellas observaciones que puedan impactar en el resultado de la elección. Por ejemplo, cuando se observe que el voto impreso tiene datos distintos del voto grabado en el chip o de la selección que se hiciera en la pantalla o cuando el acta impresa tiene valores distintos de los grabados en el chip o de los votos efectivamente escrutados (incluidos los datos cargados para votos impugnados, nulos, recurridos, etc).
- **MEDIA**: son aquellas observaciones que dificultan el uso del sistema pero no afectarían el resultado del comicio. Por ejemplo: cuando se trabe la impresora o se cuelgue o deje de responder la máquina de modo que se entorpezca la operatoria, pero sin alterar los resultados o voluntad de los electores.
- **BAJA**: son observaciones que prácticamente son irrelevantes para el comicio. Por ejemplo: cuando faltase el encendido de alguna luz o se trabase la boleta de algún modo que se pudiera recuperar en el momento.

El siguiente cuadro refleja los resultados de las pruebas de controlar 1135 equipos sobre un total de 10200 máquinas fabricadas[3].

Modelo	Sin fallas	Fallas encontradas según su gravedad			Total revisadas	Total del lote
	OK	Baja	Media	Alta		
P2	128	129	29	0	286	3000

2 La empresa utilizará tres modelos de máquinas voto, similares entre sí, pero fabricados en distintos momentos y con algunas diferencias internas. Los modelos se identifican como **P2**, **P3** y **P4**.

3 El total de máquinas disponibles es menor, ya que algunas máquinas fueron apartadas previamente, ya sea debido a fallas o roturas detectadas en el proceso de control de calidad que aplica la empresa.

P3	231	39	22	0	292	1200
P4	479	22	56	0	557	6000

Antes de empezar los controles se calculó el tamaño de muestra mínimo de máquinas a revisar por lote que garantizara con una confianza del 95% que de no encontrar ninguna máquina con incidencias de importancia alta, la cantidad de equipos con ese tipo de fallas en el total del lote sea menor al 1%. Luego se seleccionó para cada modelo una muestra aleatoria de equipos y se procedió a controlar registrando las incidencias observadas.

Finalmente al no haber observado ningún error de importancia ALTA, se puede concluir (de acuerdo al diseño de la muestra), con un 95% de confianza, que el porcentaje de equipos con fallas en el lote correspondiente a cada modelo es menor al 1%.

Respecto de los errores de importancia MEDIA, la mayoría estuvieron relacionados con el uso de boletas que se habían curvado y que hicieron trabar las impresoras, y una proporción menor con diversas fallas en las que la máquina deja de responder. Cuando un equipo deja de responder en forma reiterada, se recomienda el cambio del equipo (calculamos el promedio menor a un 5%).

La mayoría de los errores de importancia BAJA están relacionados con fallas en las luces de encendido al lado de la tapa superior, que no afectan a la funcionalidad de voto y escrutinio.

Aspectos de seguridad

Las tareas de revisión de los aspectos de seguridad se centraron en los siguientes aspectos:

1. Lectura del contenido del chip del voto, desde el momento de ser grabado y antes de ser introducido en la urna (afecta la *privacidad* del voto[4]).
2. Modificación el contenido del chip de voto (afecta la *integridad* del voto[5]).
3. Alteración del contenido de la máquina de votación para que se comporte de una manera distinta a la especificada[6].

Análisis de los aspectos de seguridad

Se analizaron diversas posibilidades de *ataque* al sistema buscando puntos débiles factibles de ser vulnerados para luego comparar dicha "*vulnerabilidad*" con el

4 Ley 4894, Anexo II, Art. 24, inc. p
5 Ley 4894, Anexo II, Art. 24, inc. e
6 Ley 4894, Anexo II, Art. 24, inc. q

sistema de voto tradicional en papel con sobre y para analizar las medidas implementadas o implementables para mitigar o controlar dichas vulnerabilidades de modo tal que la misma ya no sea factible o su implementación no empeore el caso análogo en la elección tradicional con boleta de papel y sobre.

I. Lectura del contenido del chip del voto, desde el momento de ser grabado y antes de ser introducido en la urna

La lectura del contenido de la boleta podría violar el secreto del voto si la lectura se logra antes de meter la boleta en la urna de modo tal de saber cuál es el elector que votó con esa boleta. Entendemos que esto se puede realizar de dos maneras:

a) apoyando un celular moderno de tipo *smartphone* con soporte de NFC[7] (y software específico para esta tarea) a la boleta (o acercándolo a pocos centímetros de la misma). Dada la corta distancia necesaria para hacer esto[8], y el hecho de que la máquina está a la vista de las autoridades de mesa y fiscales, esta acción sería visible para dichas autoridades, los fiscales y el mismo elector, en especial si la operatoria se realiza en forma repetida;

b) usando una antena especial con un dispositivo tecnológico que lea la máquina en el momento en que se está realizando la grabación del chip. Esos equipos especiales requieren una antena de algunas decenas de centímetros de longitud. Para mitigar este problema hay que extremar los controles de los ambientes de votación para impedir que personal ajeno a la elección manipule dispositivos electrónicos en cercanía de las máquinas de votación. Se han publicados trabajos donde se podría, en un ambiente libre de obstáculos, detectar señales hasta 18 metros de distancia. Las experiencias que probaron decodificar la señal de la máquina de votar de MSA lograron resultados para decodificar la señal emitida a 30 centímetros; a distancias mayores, la señal era detectable pero no se pudo decodificar.

   Tanto en los casos prácticos ensayados, como en las publicaciones teóricas, la detección de las señales se realizó dentro del mismo recinto (sin paredes u otros obstáculos) y la decodificación sólo es posible si la señal proviene de una sola máquina.

---

7 NFC: Sigla de "*Near Field Communication*" que se puede traducir como "Comunicación de Campo Cercano". Es una tecnología que permite a teléfonos celulares y otros dispositivos conectarse entre sí utilizando comunicaciones de radiofrecuencia. Es posible utilizar esta tecnología para leer y escribir *chips* del tipo RFID desde un teléfono celular con soporte de dicha tecnología y software apropiado. El campo de acción de este mecanismo es usualmente menor a 10 centímetros, especialmente cuando la comunicación se realiza contra un *chip* RFID que no tiene alimentación propia.

8 Para poder hacer la lectura de la BUE vía NFC desde un *smartphone*, la boleta debe estar prácticamente apoyada sobre el mismo, ciertamente a una distancia bastante menor a los 10 centímetros y durante más de medio segundo, usualmente más de un segundo.

El instructivo en papel aprobado por la Resolución N° 131 incorpora instrucciones y advertencias para que las autoridades de mesa presten atención al uso de dispositivos electrónicos cuando los electores están emitiendo su voto, reduciendo de este modo los riesgos provenientes del uso de aparatos tecnológicos.

II. Modificación del contenido de la BUE

La modificación del voto, una vez emitido para reemplazar la información *impresa* en la BUE no es factible dado que la impresión es térmica y quema la superficie de la misma. No es posible modificar o *borrar* lo impreso.

Alterar el contenido del *chip* RFID para cambiar la información tampoco es factible porque los sectores utilizados para la grabación de la información son "*cerrados*" para que no puedan volver a escribirse. No se ha logrado modificar la información en *chips* que se hayan *cerrado* previamente.

Existe un tipo de *ataque* posible que sí podría hacerse consistente en *anular* la información contenida en el chip, impidiendo leer en el momento del escrutinio la información grabada. Para poder hacer esto se necesita un dispositivo que emita un pulso electromagnético fuerte. Se comprobó que las BUE son susceptibles a tal pulso utilizando un dispositivo casero. De todos modos este ataque no compromete el secreto del voto ni impide ejercer la voluntad del votante, generando un obstáculo (que no es insalvable) en el momento del escrutinio. Se recomienda tomar las mismas medidas para la observación anterior en relación al control de la presencia de personas ajenas o de personas manipulando dispositivos electrónicos en el área donde se encuentra la mesa de votación.

El instructivo en papel aprobado por la Resolución N° 131 incorpora instrucciones y advertencias para que las autoridades de mesa presten atención al uso de dispositivos electrónicos cuando los electores están emitiendo su voto y en cercanías de la urna.

III. Alteración del contenido de la máquina de votación para que se comporte de una manera distinta a la especificada

La máquina de votación tiene una serie de puntos débiles en relación a la falta de control de los dispositivos internos (que podrían estar validados por claves y certificados internos o adecuados niveles de permisos[9]). Para explotar cualquiera de esas debilidades se necesita acceder a la puerta superior, abrir el lector de DVD, cambiarlo por otro modificado especialmente y reiniciar el equipo. Esto hace que la

9
a) procesos internos que corren en la máquina de voto utilizando permisos de *root*,
b) puertos USB expuestos físicamente (pero bajo la tapa superior y apagados por software)
c) BIOS sin contraseña y ausencia de control de actualización de la misma
d) ausencia de control de la validez del sistema operativo
e) ausencia de control de la validez del firmware

custodia de la tapa superior de la máquina y tener la máquina a la vista de las autoridades de mesa durante todo el acto electoral sea la forma de controlar estas vulnerabilidades. Esta es una de las razones por las cuales se recomienda en el Anexo II cómo debe ser la disposición de la máquina de votación dentro del establecimiento.

De no controlarse la tapa superior de la máquina podría introducirse un DVD que cambie el comportamiento de la máquina de votación[10] pudiendo por ejemplo emitir votos distintos a los seleccionados o grabar información en el *chip* distinta de la impresa. Aún consiguiéndose esto, las anomalías en los votos son detectables en el momento de la verificación del voto o del proceso de escrutinio.

Otra cosa que podría hacerse es, además de cambiar el DVD, introducir un dispositivo USB con una memoria que registre los votos en orden o una antena que los transmita en el momento. Esto no es detectable por anomalías en el voto pero sí es detectable por la presencia física de un elemento extraño. De todos modos, para que el dispositivo USB funcione, también es necesario cambiar el DVD y reiniciar, o reiniciar y utilizar un teclado u otro dispositivo que lo emule (también conectado a un puerto USB) para permitir que la máquina cargue el sistema operativo desde el dispositivo USB en lugar del DVD.

Recomendamos que las autoridades de mesa custodien la tapa de la máquina cuando los electores se aproximan a la máquina (para verificar que no se abre la tapa) y que periódicamente revisen que no haya dispositivos agregados en los puertos USB.

Conclusiones sobre los aspectos de seguridad

Es importante que, del mismo modo que ocurre en los operativos de elecciones tradicionales, se custodien los materiales que se despliegan en los establecimientos para que los mismos no sean manipulados por extraños. A los materiales tradicionales (urnas, boletas, padrones, etc) ahora se agrega la custodia de las máquinas, BUEs, DVDs, credenciales y actas de apertura y cierre.

Similarmente a lo que ocurre en una votación en papel, el despliegue de dispositivos tecnológicos disimulados u ocultos, ubicados en lugares estratégicos podrían filmar o fotografiar los movimientos de los electores de una mesa violando el secreto del voto o introduciendo un mecanismo para verificar el cambio de su voluntad. Es por eso que el control de las instalaciones, del establecimiento y de las personas que tienen acceso al mismo sigue siendo igual de importante cuando se introducen aspectos tecnológicos durante la emisión del voto.

10 Para que este DVD funcione, sin embargo, es necesario reiniciar la máquina, lo cual emite una serie de pitidos y, por otra parte, demora en el orden de cinco (5) minutos, lo cual lo hace extremadamente difícil de realizar sin que sea advertidos por las autoridades o los fiscales.

Respecto de la custodia de la tapa superior de la máquina, el instructivo audiovisual aprobado por la Resolución N° 130 del Tribunal, así como el instructivo en papel aprobado por la Resolución N° 131 incorporan instrucciones y advertencias para que las autoridades de mesa presten atención a la misma toda vez que un elector u otra persona se encuentran frente a la máquina y que presten atención al uso indebido de teléfonos celulares y cámaras, reduciendo de este modo los riesgos observados.

Conclusiones

Ateniéndose al análisis de los componentes del sistema auditados (hardware, software, procedimientos), establecemos que es crucial para el correcto funcionamiento de dicho sistema en forma global que las autoridades de mesa, delegados judiciales y demás responsables de los comicios sigan los procedimientos aprobados por el Tribunal (Acordada 17/2015, Anexo II); y que el mecanismo de votación sea apropiadamente difundido para el conocimiento de los electores.

Entendemos que el instructivo audiovisual aprobado por la Resolución N° 130 y el instructivo en papel aprobado por la Resolución N° 131 del Tribunal son herramientas apropiadas para instruir a las autoridades de mesa en los procedimientos que tienen que cumplir durante el acto electoral.

Esta auditoría considera que el sistema permite respetar los principios enunciados en el Artículo 24 del Anexo II de la Ley 4894 (ver abajo).

En particular, el sistema es comprobable físicamente y la voluntad de los electores se puede verificar en forma completamente manual, sin la intervención del sistema, en casos extremos (aunque improbables) de fallas generalizadas o ante un requerimiento de fiscalización por parte de las agrupaciones políticas que se considere admisible.

Revisión detallada del Art. 24 del Anexo II de la Ley 4894

A continuación se incorpora el texto del artículo 24 del Anexo II de la Ley 4894. Los textos intercalados en *itálica* son las consideraciones de la auditoría respecto del cumplimiento del mismo.

Artículo 24. Principios aplicables a la incorporación de Tecnologías Electrónicas. Toda alternativa o solución tecnológica a incorporar en cualquiera de las etapas del procedimiento electoral debe contemplar y respetar los siguientes principios:

a) Accesibilidad para el/la votante: Que el sistema de operación sea de acceso inmediato, que no genere confusión y no contenga elementos que puedan inducir el voto o presentarse como barreras de acceso al sistema;

Consideramos que el sistema es accesible y no es confuso; también que no contiene elementos que puedan inducir el voto, de hecho, el orden de las listas y candidatos se decide aleatoriamente, con lo cual ni siquiera existe una preferencia posible de alguna opción en base a su ubicación relativa en la pantalla.

b) Auditable: tanto la solución tecnológica, como sus componentes de hardware y software debe ser abierta e íntegramente auditable antes, durante y posteriormente a su uso;

Consideramos que el sistema es auditable. La arquitectura de hardware es genérica, más allá de tener periféricos específicos, como ser una impresora térmica y un lector/grabador de RFID; aún estos periféricos están conectados utilizando componentes y protocolos estándar del mercado.

El sistema operativo utilizado para votar y transmitir datos es una de las implementaciones más populares de GNU/Linux (Ubuntu Linux) que es, de por sí, abierta y auditable.

El lenguaje utilizado para el desarrollo (Python) es abierto y los programas están almacenados en modo fuente, sin cifrado ni ofuscación alguna.

De todos modos se considera que sería una mejora cualitativamente sustancial que el software estuviera abierto (sea público) con mucha anticipación y que el código tenga documentación exhaustiva, casos de prueba incluidos en el fuente y se use alguna metodología de desarrollo que incluya cobertura de código en las pruebas.

c) Comprobable físicamente: la solución debe brindar mecanismos que permitan realizar el procedimiento en forma manual;

Los votos son impresos y grabados sobre un soporte físico (papel con un chip RFID) e introducidos físicamente en una urna tradicional, de manera tal que todo el procedimiento de recuento puede realizarse en forma completamente manual.

d) Robusto: debe comportarse razonablemente aún en circunstancias que no fueron anticipadas en los requerimientos;

El sistema mostró ser robusto, funcionando razonablemente bajo las hipótesis que esta auditoría se ha planteado.

e) Confiable: debe minimizar la probabilidad de ocurrencia de fallas, reuniendo condiciones que impidan alterar el resultado eleccionario, ya sea modificando el voto emitido o contabilizándose votos no válidos o no registrando votos válidos;

El sistema gira en torno a un procedimiento confiable preexistente (el de votación manual con boleta papel y sobre), construyendo sobre el mismo, aprovechando sus fortalezas y resolviendo algunas debilidades.

f) Simple: de modo tal que la instrucción a la ciudadanía sea mínima;

El sistema es simple, de todos modos, la instrucción a la ciudadanía debe existir, en particular, respecto de tener un rol de fiscalización individual por parte del elector.

g) Íntegro: la información debe mantenerse sin ninguna alteración;

La información se mantiene sin alteraciones que permitan modificar la voluntad de los electores siguiendo un procedimiento de resguardo similar al de la elección tradicional con boleta papel y sobre.

h) Eficiente: debe utilizar los recursos de manera económica y en relación adecuada entre el costo de implementación del Sistema y la prestación que se obtiene;

Esta auditoría no cuenta con información económica respecto de la solución, ni información respecto de los costos de una elección tradicional con boleta papel y sobre. El análisis de los aspectos económicos están fuera del alcance de la auditoría.

i) Estándar: debe estar formada por componentes de hardware y software basados en estándares tecnológicos;

La solución está conformada por componentes de hardware y software basados en estándares tecnológicos.

j) Documentado: debe incluir documentación técnica y de operación completa, consistente y sin ambigüedades;

La documentación de operación del sistema entregada es completa. Debe adecuarse aún a las últimas modificaciones implementadas.

La documentación técnica del desarrollo de software no es exhaustiva y no sigue plenamente las reglas del arte para documentar software.

k) Correcto: debe satisfacer las especificaciones y objetivos previstos;

El sistema cumple razonablemente con las especificaciones y objetivos detallados en el pliego de licitación al que tuvo acceso esta auditoría.

l) Interoperable: debe permitir acoplarse mediante soluciones estándares con los sistemas utilizados en otras etapas del procedimiento electoral;

Esta auditoría no cuenta con información acerca de sistemas utilizados en otras etapas del procedimiento electoral. Sin embargo, el sistema de consolidación y totalización de datos del escrutinio provisorio permite exportar la información en formatos estándar hacia otros sistemas. Asimismo es posible importar información desde otros sistemas, una vez que se detalle el formato y funcionalidad de la misma.

La tecnología de base de datos utilizada (motor relacional SQL) es estándar y el modelo de datos cuenta con documentación. La implementación en sí es abierta (PostgreSQL) con lo cual es técnicamente posible acoplarse con otros sistemas; para ello sería necesario hacer un desarrollo específico en los otros sistemas y en el de totalización.

m)Recuperable ante fallas: ante una falla total o parcial, debe estar nuevamente disponible en un tiempo razonablemente corto y sin pérdida de datos;

Los planes de contingencia revisados tanto para la emisión del voto, para la transmisión de resultados, para la totalización y la publicación del escrutinio provisorio permiten, operándolos adecuadamente, recuperar la operación de los mismos en un tiempo razonablemente corto y sin pérdida de datos, ya que la información de los votos se encuentra en las BUE y no dentro de las máquinas.

n) Evolucionable: debe permitir su modificación para satisfacer requerimientos futuros;

Esta auditoría no ha hecho estudios de futuros requerimientos, pero la historia del sistema y su utilización anterior en distintos procesos muestra una evolución en el pasado que se infiere puede continuar en el futuro. De todos modos, se ha detectado que algunas partes del sistema están programadas en forma antigua (sin respetar los estándares de la programación estructurada, por ejemplo) haciendo más difícil de lo necesario dicha evolución.

o) Escalable: de manera tal de prever el incremento en la cantidad de electores;

El sistema es escalable. El incremento en la cantidad de electores se reflejará en una necesidad de un mayor número de máquinas de voto. El sistema de transmisión y totalización de datos también escala fácilmente y los recursos que utiliza en su configuración para la cantidad actual de electores del Distrito es razonablemente modesta. El sistema de publicación del escrutinio

provisorio utiliza servicios en la nube que se ajustan dinámicamente a la demanda.

p) Privacidad, que respete el carácter secreto del sufragio y que sea imposible identificar bajo ningún concepto al emisor del voto;

El secreto del sufragio se mantiene del mismo modo que en la elección tradicional con boleta papel y sobre. Los votos sólo están en forma desagregada en el soporte físico (BUE) y no se cuentan hasta que no termina el sufragio. Los números de serie con que cuenta el chip RFID de la BUE son asignados por una entidad técnica ajena al Gobierno y a la empresa proveedora y no es factible asociar dicho número con el emisor del voto contenido en dicha BUE.

q) Seguridad informática, Proveer la máxima seguridad posible a fin de evitar eventuales instrucciones, intrusiones, o ataques por fuera del Sistema, debiendo preverse una protección y seguridad contra todo tipo de eventos, caídas o fallos del software, el hardware o de la red de energía eléctrica. Dicho sistema, no pueda ser manipulado por el administrador, salvo expresa autorización de la Autoridad de Aplicación; y

Las medidas de seguridad informática de las máquinas de voto permiten solucionar o controlar los puntos débiles analizados, en algunos casos se detectaron medidas adicionales que podrían tomarse para aumentar el nivel de seguridad utilizando múltiples medidas simultáneas (ver la sección Aspectos de seguridad y el Anexo II).

Las partes críticas del sistema, que son las incluidas dentro de la máquina de voto, no pueden ser alteradas dada la ausencia de disco rígido u otro tipo memoria persistente y dado que el sistema se encuentra grabado en un DVD de solo lectura, duplicado bajo el control del Tribunal, como se especifica en la Resolución N° 138.

Respecto de las partes del sistema almacenadas en servidores encargadas de la totalización final de los resultados, la autoridad de aplicación puede controlar el acceso de los administradores generando y haciendo custodia de las claves de los mismos y, de todos modos, el resultado de la totalización está abierto a la fiscalización por parte de los partidos políticos.

Las máquinas de voto cuentan con baterías que les permiten funcionar durante toda la jornada electoral (suponiendo que se encuentren completamente cargadas al inicio de la misma, ver el Anexo III) y, fuera de la eventual conexión a la red eléctrica, no cuentan con conectividad alguna. Los puertos USB y de red están desactivados en el DVD de arranque y las

máquinas no cuentan con capacidad de conexión inalámbrica (ver la sección Aspectos de seguridad).

Las comunicaciones entre las máquinas de transmisión y el centro de datos están cifradas y se realiza una autenticación cruzada (el cliente valida al servidor y el servidor valida al cliente). No se permite la transmisión de datos de escrutinio de mesas de un establecimiento desde la máquina de transmisión de otro establecimiento. No es posible computar más de una vez los datos correspondientes al escrutinio de una mesa en particular (ver la sección Transmisión de datos).

Según la documentación recibida de parte de la empresa, las instalaciones de los centros de datos cuentan con medidas de seguridad informática estándar adecuadas.

r) Capacitación in situ: Debe ser pasible de proveer una unidad de tecnología electrónica de emisión de sufragio por cada establecimiento de votación, a fin de facilitar el entrenamiento de los electores con igual tecnología a la utilizada en las mesas de emisión de sufragio.

Está prevista la utilización de máquinas de voto en cada establecimiento configuradas para capacitación. Esta configuración no permite que se emitan votos válidos en dichas máquinas.

Las modificaciones que se propongan deben garantizar el carácter secreto del voto y asegurar la accesibilidad, seguridad y transparencia del proceso electoral.

Anexos

Anexo I - Observaciones sobre el código fuente

A continuación se detallan observaciones, encontradas al revisar el código fuente del software, que son los puntos débiles detectados. Si bien no son errores en sí mismos podrían serlo en determinados contextos. Esta auditoría no se encuentra en la capacidad de afirmar o negar la posibilidad de estos errores dado el estado actual de la documentación del sistema.

Cada observación descrita es un representante de uno de los tipos de observaciones encontradas, es decir, *no son los únicos extractos de código observados, sino una **tipificación** de los mismos*.

Los errores encontrados en el código que son visibles desde el punto de vista funcional son reportados en la sección de "Aspectos funcionales del software".

1. **Fuente**:
   …/elecciones/msa/voto/gui/templates/js/ingreso_datos.js

   Función/sección/clase: pantalla_mesaypin, línea 151

   Contenido aproximado:

   ```
   inicializar_teclado(eval(callback_aceptar));
   ```

   Observación: el uso de **eval()** está desaconsejado por ser un punto vulnerable. No estamos en el peor escenario dado que el valor que recibe eval() en este caso es un valor constante que proviene del backend (de la función interaccion.py/set_pantalla). De todos modos el uso de eval() se considera un punto débil porque las condiciones del programa pueden cambiar durante el ciclo de vida del software (en futuros cambios o durante el mantenimiento del mismo).

   Otro inconveniente que presenta el uso de eval() está relacionado las prácticas de programación del equipo de desarrollo, cuando se permite el uso de prácticas desaconsejadas aumenta la probabilidad de introducir involuntariamente debilidades dentro del sistema.

   Posible solución: utilizar un módulo o un objeto local para almacenar las funciones que se desean invocar con este método; si fuera estrictamente necesario que las sean funciones se podría es utilizar la variable "window" para acceder al scope global junto con una "*white list*" de valores admitidos.

   ```
   if(whiteList[callback_aceptar]){
       inicializar_teclado(window[callback_aceptar]);
   ```

```
}
```

Aún sin la "*white list*" es preferible, en este caso, el uso de `window` sobre `eval()`.

Observación de la empresa: La empresa adujo que en el contexto específico en que se utilizó `eval()` no se corre riesgo de inyección de código.

Lo que se observa en la auditoría es que su utilización introduce una debilidad en el código fuente ya que, si el programador se equivoca en algún parámetro, no se podrá detectar sino luego de un testeo intensivo y, aún así, el error podría quedar oculto.

2. **Fuentes**: `…/elecciones/msa/voto/modulos/recuento.py`
`…/msa/voto/gui/test/web_server.py`

Función/sección/clase: `get_campos_extra`, líneas 290 a 311 y líneas 90 a 102 respectivamente

Contenido aproximado:

```
def get_campos_extra(self):
    campos_extra = []
    campos_extra.append({"codigo": "",
                 "titulo": _("boletas_procesadas"),
                 "editable": False,
                 "valor": sesion.recuento.boletas_contadas()})

    for lista in get_config("listas_especiales"):
        campos_extra.append(
          {"codigo": lista,
           "titulo": _("titulo_votos_%s" % lista[-3:]),
           "editable": True,
           "valor": sesion.recuento.listas_especiales[lista]})

    total = 0
    for campo in campos_extra:
        total += campo.get('valor', 0)
    campos_extra.append({"codigo": COD_TOTAL,
                         "titulo": _("total_general"),
                         "editable": False,
                         "valor": total})
    return campos_extra
```

Observación: Se observa **código repetido** en distintas partes de los fuentes. La función get_campos_extras está replicada idéntica en ambos fuentes. La duplicación de código es un punto débil en el mantenimiento del software y modificaciones de último momento porque podrían introducirse por error correcciones en una sola de las partes en casos donde deberían hacerse en varios haciendo que el programa funcione incoherentemente y teniendo que duplicarse las pruebas.

Posible solución: Cada vez que se utilice el mismo código, o código muy similar que tiene un objetivo común, utilizar una función, de ser necesario, con los parámetros necesarios para reflejar la diferencia.

3. **Fuente**: …/elecciones/msa/core/data/candidaturas.py

   Función/sección/clase: full_dict, líneas 341 a 342

   Contenido aproximado:

```
def full_dict(self, img_func=None, secundarios=True, suplentes=True,
              hijas=False):
```

   Observación: Se observan datos de configuración embebidos dentro del código como valores por defecto de parámetros. Esta debilidad se amplifica en el momento en que el programa debe ser configurado luego de que las autoridades electorales definen por ejemplo el diseño de las pantallas (si en los botones de selección deben verse simultáneamente los nombres de las agrupaciones y de los candidatos). La configuración del sistema que se halla dentro de los fuentes se encuentra diseminada en su mayoría en archivos llamados settings.py en las distintas carpetas del sistema, sin embargo hay mucha información de configuración fuera de ellos (como el caso de este ejemplo).

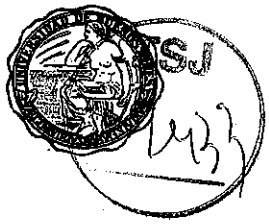
   Posible solución: Los parámetros de configuración deberían estar en un lugar unificado.

   Observación de la empresa: La empresa respondió que no se trata de configuraciones *propiamente dichas* y adujo cuestiones de *performance* para hacerlo de este modo. La auditoría opina que aunque no sean *propiamente dichas* estas configuraciones deberían tratarse del mismo modo que si lo fueran y ubicarlas todas en un lugar unificado.

4. **Fuente**: …/elecciones/msa/voto/controllers/voto.py

   Función/sección/clase: send_constants, líneas 627 a 631

   Contenido aproximado:



```
}
```

Aún sin la "*white list*" es preferible, en este caso, el uso de `window` sobre `eval()`.

Observación de la empresa: La empresa adujo que en el contexto específico en que se utilizó `eval()` no se corre riesgo de inyección de código.

Lo que se observa en la auditoría es que su utilización introduce una debilidad en el código fuente ya que, si el programador se equivoca en algún parámetro, no se podrá detectar sino luego de un testeo intensivo y, aún así, el error podría quedar oculto.

2. **Fuentes**: …/elecciones/msa/voto/modulos/recuento.py
…/msa/voto/gui/test/web_server.py

Función/sección/clase: `get_campos_extra`, líneas 290 a 311 y líneas 90 a 102 respectivamente

Contenido aproximado:

```
def get_campos_extra(self):
    campos_extra = []
    campos_extra.append({"codigo": "",
                 "titulo": _("boletas_procesadas"),
                 "editable": False,
                 "valor": sesion.recuento.boletas_contadas()})

    for lista in get_config("listas_especiales"):
        campos_extra.append(
          {"codigo": lista,
           "titulo": _("titulo_votos_%s" % lista[-3:]),
           "editable": True,
           "valor": sesion.recuento.listas_especiales[lista]})

    total = 0
    for campo in campos_extra:
        total += campo.get('valor', 0)
    campos_extra.append({"codigo": COD_TOTAL,
                         "titulo": _("total_general"),
                         "editable": False,
                         "valor": total})
    return campos_extra
```

Observación: Se observa **código repetido** en distintas partes de los fuentes. La función get_campos_extras está replicada idéntica en ambos fuentes. La duplicación de código es un punto débil en el mantenimiento del software y modificaciones de último momento porque podrían introducirse por error correcciones en una sola de las partes en casos donde deberían hacerse en varios haciendo que el programa funcione incoherentemente y teniendo que duplicarse las pruebas.

Posible solución: Cada vez que se utilice el mismo código, o código muy similar que tiene un objetivo común, utilizar una función, de ser necesario, con los parámetros necesarios para reflejar la diferencia.

3. **Fuente**: …/elecciones/msa/core/data/candidaturas.py

   Función/sección/clase: full_dict, líneas 341 a 342

   Contenido aproximado:

```
def full_dict(self, img_func=None, secundarios=True, suplentes=True,
              hijas=False):
```

   Observación: Se observan datos de configuración embebidos dentro del código como valores por defecto de parámetros. Esta debilidad se amplifica en el momento en que el programa debe ser configurado luego de que las autoridades electorales definen por ejemplo el diseño de las pantallas (si en los botones de selección deben verse simultáneamente los nombres de las agrupaciones y de los candidatos). La configuración del sistema que se halla dentro de los fuentes se encuentra diseminada en su mayoría en archivos llamados settings.py en las distintas carpetas del sistema, sin embargo hay mucha información de configuración fuera de ellos (como el caso de este ejemplo).

   Posible solución: Los parámetros de configuración deberían estar en un lugar unificado.

   Observación de la empresa: La empresa respondió que no se trata de configuraciones *propiamente dichas* y adujo cuestiones de *performance* para hacerlo de este modo. La auditoría opina que aunque no sean *propiamente dichas* estas configuraciones deberían tratarse del mismo modo que si lo fueran y ubicarlas todas en un lugar unificado.

4. **Fuente**: …/elecciones/msa/voto/controllers/voto.py

   Función/sección/clase: send_constants, líneas 627 a 631

   Contenido aproximado:

```
def send_constants(self):
    """Envia todas las constantes de la eleccion."""
    constants_dict = get_constants(self.sesion.mesa.codigo,
                                   self.sesion.mesa.comuna)
    self.send_command("set_constants", constants_dict)
```

Observación: Se observa dentro del código fuente el uso de denominaciones regionales como nombres de variables o nombre de parámetros. Esto representa una debilidad porque partes importantes del código fuente están preparadas para ser utilizadas en otras elecciones de otras jurisdicciones. Cosas similares se observan con la denominación de las categorías electorales (que están mezcladas dentro del código). Esto presenta una debilidad en el momento de hacer cambios y actualizaciones, y especialmente durante el *testing* porque pueden considerarse probadas y funcionando cosas que después de las actualizaciones jurisdiccionales no funcionan.

Posible solución: Utilizar nombres genéricos que no dependan de la situación regional para absolutamente todas las categorías, o niveles de separación geográfica, etc. Por ejemplo un parámetro que se refiera al primer nivel de la separación geográfica podría llamarse "`zona_nivel_1`", "`zona_nivel_2`" el siguiente, etc. Luego, en la configuración del sistema, se indicaría cuál es la denominación que usará el usuario para cada nivel de separación geográfica: *Comuna*, *Circuito*, etc.

Observación de la empresa: La empresa aduce que las denominaciones geográficas se utilizan en "pocos" lugares del código y que se utilizan para "evitar configuraciones regionales" sin explicar por qué las quiere evitar.

La auditoría observó que no son "pocos" los lugares del código donde se utilizan y que para "evitar configuraciones regionales" se introduce confusión ya que para las mismas entidades, a veces se utiliza un sistema jerárquico de árbol y otras veces los nombres específicos de las cosas directamente como nombres de variables o parámetros (por ejemplo en las ubicaciones), lo que debería evitarse más que dichas configuraciones regionales.

5. **Fuente**: `.../elecciones/msa/web/dashboard/static/js/funciones.js`

   Función/sección/clase: `enviar() { … guardar/permisos"`, líneas 203 a 207

   Contenido aproximado:

```
$.ajax({
```

```
            type: 'POST',
            url: url,
            data: data,
        });
```

Observación: la llamada a la función `ajax` se usa para guardar los nuevos permisos en la base de datos, pero no se recoge la respuesta ni el posible informe de error. Aún cuando aparenta no haber posibilidades de guardar datos inválidos (porque lo que se muestra en pantalla para seleccionar las opciones a grabar son siempre datos válidos) podría ocurrir una situación excepcional y si eso ocurriera el operador no se enteraría de la situación.

Posible solución: incluir en todas las llamadas ajax un par de funciones que muestren el resultado o la condición de error en la pantalla que hace la llamada al ajax.

Observación de la empresa: La empresa contestó que esto se observa en una aplicación de uso interno y que los errores los detecta el mismo equipo de personas que utiliza esta aplicación a través de los *logs* y que sería redundante controlar los errores a este nivel.

La auditoría encontró que este tipo de código no se encuentra solamente en las aplicaciones de uso interno. Existe el mismo problema en la aplicación de voto (ver punto 8 abajo).

6. **Fuente**: `.../elecciones/msa/voto/controllers/asistida.py`

   Función/sección/clase: `AsistenteCandidatos`, líneas 319 a 321

   Contenido aproximado:

```
if cod_categoria == "JEF":
    mensaje.append(self._("y"))
    mensaje.append(opcion['secundarios'][0]['texto_asistida'])
```

   Observación: Para identificar tipos de comportamiento o características comunes de algunas entidades se utilizan los códigos identificatorios de las entidades en vez de clasificarlas con atributos. Por ejemplo en el caso de la entidad "categorías", la categoría "Jefe de Gobierno" se distingue del resto en que tiene candidatos secundarios, en algunas partes el programa tiene un comportamiento específico para los casos donde hay candidatos secundarios. En todo el programa para identificarlos se compara el código de categoría con su código "`JEF`".

   Esta observación es una debilidad a la hora de auditar el código porque al encontrar un comportamiento específico basado en la identificación de un código

de entidad no queda claro cuál es la característica de la entidad la que determina ese comportamiento específico.

Posible solución: utilizar la orientación a objetos para modelar las entidades que tengan comportamientos específicos. Otra solución es agregar explícitamente un atributo (o campo) que señale el tipo para luego derivar los comportamientos específicos. Por ejemplo para las entidades "categorías" se podría agregar un atributo llamado "`con_secundarios`", luego dentro del código se reemplazarían las líneas del tipo:

```
cod_categoria = "JEF"
```

por:

```
categoria.con_secundarios = true
```

7. **Fuente**: …/`elecciones/msa/voto/controllers/interaccion.py`

Función/sección/clase: `ControllerInteraccion - cargar_datos_personales`, líneas 148 a 151

Contenido aproximado:

```
if self.modulo == MODULO_APERTURA:
 data['pattern_validacion_hora'] = "[0]?[8-9]|1[0-9]?|2[0-3]?"
else:
 data['pattern_validacion_hora'] = "1[8-9]?|2[0-3]?"
```

Observación: Se utiliza comparación de texto por patrones (expresiones regulares) para validar datos numéricos. Cuando se quieren validar rangos numéricos usar expresiones regulares es más difícil de programar y validar. Es una fuente probable de errores. La validación se realiza en dos lugares distintos del programa, se utiliza la expresión regular para el momento en que se está ingresando el dato (no mostrando como inválido el "1" y el "2" porque pueden ser el primer dígito de las horas de 10 a 23) y luego, antes de aceptar el valor se excluyen explícitamente el "1" y el "2"[11]. Eso introduce una nueva debilidad al esparcirse la configuración en distintas partes del código fuente.

Posible solución: utilizar rangos numéricos (un par de variables límite para cada variable a controlar: límite inferior de la hora de apertura, límite superior de la hora de apertura, límite inferior de la hora de cierre y límite superior de la hora de cierre). Separar los controles parciales (mientras se está ingresando) de los controles finales (después de ingresada). Además la configuración de esos controles no deberían estar dentro del código fuente sino como parte de la configuración general del acto eleccionario.

11 En el fuente …/`elecciones/msa/voto/gui/templates/js/ingreso_datos.js`, línea 370:
`var hora_invalida = $(".hora input").is(":invalid") || $("input[name='hora']").val() === "1";`

8. **Fuente**: .../elecciones/msa/voto/gui/templates/js/helpers.js

Función/sección/clase: get_template( ), líneas 62 a 74

Contenido aproximado:

```
$.ajax(url,
        …
        error: function(data, textStatus, jqXHR){
          console.log(textStatus);
          console.log(data);
        }
        …
);
```

Observación: La llamada a la función ajax se usa para traer las plantillas hacia la pantalla, pero si ocurriera una falla el informe este quedaría oculto. Aún cuando no parece probable que haya un error porque se está en un ambiente controlado podría ocurrir una situación excepcional y si eso ocurriera el usuario no se enteraría de la situación porque no se muestra un cartel indicando "que hubo un problema" y si se sugiere "reintentar la operación" o "reiniciar la máquina" o lo que sea más apropiado según el código de error recibido.

Posible solución: incluir en todas las llamadas ajax un par de funciones que muestren el resultado o la condición de error en la pantalla que hace la llamada al ajax.

Anexo II – Recomendaciones acerca de los procedimientos

Una de las principales fortalezas (si no la más importante) del sistema de voto con BUE objeto de la presente auditoría, consiste en que cada voto se mantiene en un soporte físico individual con la posibilidad de ser auditado fácilmente tanto por el elector como por las autoridades de mesa y los fiscales.

Para mantener esta fortaleza, es necesario el seguimiento de una serie de procedimientos por parte de todas las personas involucradas en las elecciones.

Si bien no está estrictamente dentro del alcance original de la presente auditoría, muchas de las dudas respecto de la seguridad y la confiabilidad del sistema se resuelven a través de la definición y el seguimiento de dichos procedimientos.

La única forma de asegurar la confiabilidad de los comicios con este sistema es, al igual que en el sistema tradicional de boletas preimpresas con sobres, que las autoridades de los comicios sepan los procedimientos que deben seguir y lo hagan.

Las siguientes recomendaciones se basan en el estudio del sistema, el hardware, el software y los procedimientos, así como de la experiencia de ver el sistema en funcionamiento durante los comicios para la elección de autoridades provinciales en la Provincia de Salta en mayo de 2015.

Estas recomendaciones fueron incorporadas en el Informe N°2, de fecha 1° de junio. Toda vez que se haya verificado la implementación de estas recomendaciones se lo notará en esta versión.

Disposición física de las mesas para autoridades y fiscales y las máquinas de voto

A diferencia del voto tradicional, no existe el cuarto oscuro. Es conveniente que las autoridades de mesa y los fiscales vean al elector mientras este opera la máquina de voto, pero sin tener la posibilidad de ver qué es lo que está votando.

Por ello, conviene que la(s) mesa(s) donde se ubican las autoridades y los fiscales se encuentre frente a la máquina y que la máquina esté dispuesta con la pantalla hacia el lado opuesto a donde están dichas autoridades.

En los establecimientos educativos donde normalmente se disponían las aulas como cuartos oscuros y las mesas de las autoridades en los pasillos fuera de dichas aulas, convendrá introducir las mesas en el aula cerca de la puerta y disponer la máquina en un ángulo opuesto a dichas mesas.

La pantalla de la máquina no debe ser visible, ni siquiera lateralmente, desde las mesas donde se dispongan las autoridades y fiscales, ni desde la puerta, ni desde ninguna ventana.

Al igual que en los cuartos oscuros en el sistema tradicional, se deberán tapar todos los vidrios que pudieran permitir la visión de la pantalla de la máquina, aunque sea lateralmente.

Si en un recinto se debiere ubicar más de una máquina de voto, ya sea para agilizar la votación en una mesa o porque se disponen múltiples mesas en el mismo recinto (por ejemplo, un gimnasio o un pasillo largo y ancho), las máquinas deberán estar dispuestas todas en la misma dirección, con las pantallas frente a una pared (o ventanas tapadas de modo tal que no se puedan ver desde afuera).

Las máquinas deberán estar dispuestas a una distancia tal que una persona votando o acercándose o alejándose de una máquina, no pueda ver la pantalla de la máquina que está a su lado en un ángulo tal que le permita ver su contenido[12]. En caso contrario, deberán instalarse divisores opacos ("biombos") entre las máquinas que impidan que una persona votando en una máquina o acercándose o alejándose de ella pueda ver la pantalla de la máquina a su lado.

El presidente de mesa debe también velar por la ausencia de elementos extraños al acto eleccionario en la mesa. Los fiscales no deberían tener elementos más allá de los indispensables para cumplir con su tarea y, si bien pueden tener un teléfono celular, no deberían estar usándolo todo el tiempo ni hacer actividades extrañas con el mismo.

Ni los fiscales ni los electores deben utilizar las cámaras de sus teléfonos celulares dentro del recinto de votación, ni durante el acto eleccionario ni durante el escrutinio.

Las autoridades de mesa deben supervisar que ni los electores ni los fiscales intenten realizar actividades extrañas sobre la máquina de voto (golpearla, abrir los compartimientos, apoyar o introducir elementos extraños, acercarle dispositivos electrónicos, etc).

Implementación: El instructivo audiovisual aprobado por la **Resolución N° 130** del Tribunal, así como el instructivo en papel aprobado por la **Resolución N° 131** incorporan instrucciones y advertencias para que las autoridades de mesa cumplan con las recomendaciones que les atañen de esta sección.

Responsabilidad sobre el arranque de la máquina de voto

Entre los materiales que recibe el presidente de mesa está el DVD con el software para arrancar la máquina de voto. La máquina es inútil sin este DVD ya que todo el

12 Se debe solicitar a la empresa proveedora cuál es la distancia mínima que debe haber entre dos máquinas con la pantalla a la misma altura para que esto suceda.

software que utiliza y los datos de los candidatos y cargos se encuentran en el mismo.

El DVD original deberá haber sido generado bajo supervisión del Tribunal y duplicado bajo control de personal idóneo a la vista de los fiscales de las agrupaciones políticas. El proceso de copiado debe ser auditado *in situ*.

Los DVDs así duplicados estarán ensobrados con un sello que se destruye al ser abierto. El presidente deberá verificar que el DVD que recibe con la urna y demás materiales está efectivamente dentro de un sobre completamente cerrado con dicho sello sin marca alguna de haber sido violado.

Es el presidente el responsable de arrancar el equipo utilizando dicho DVD al inicio de la jornada electoral y toda vez que sea necesario arrancar una máquina con la que se imprimirán votos para introducir en la urna correspondiente a su mesa, ya sea porque el equipo ha fallado y se ha debido reiniciar, ha sido reemplazado por otro o se hubiera agregado un equipo adicional a su mesa de votación.

De ser necesario, el presidente solicitará ayuda al Delegado Judicial, pero siempre verificará que la máquina arranque con un DVD que él mismo ha abierto.

Implementación: El protocolo dispuesto por el Tribunal en la **Resolución N° 138** cumple con las recomendaciones para la duplicación de los DVDs.

El instructivo audiovisual aprobado por la **Resolución N° 130** del Tribunal, así como el instructivo en papel aprobado por la **Resolución N° 131** incorporan instrucciones y advertencias para que las autoridades de mesa cumplan con las recomendaciones que les atañen de esta sección.

Acerca de las boletas, los troqueles y el secreto del voto

Las BUE consisten en una cartulina con un lado en blanco para imprimir el voto, un chip RFID para grabar la misma información impresa en formato digital, una pequeña lámina de metal que actúa como "jaula de Faraday" cuando está apoyada sobre dicho chip, impidiendo su lectura, y dos troqueles removibles con una serie de símbolos.

Cada símbolo de la serie tiene una mitad en un troquel y la otra mitad en el otro, y las series en las diversas BUE son diferentes entre sí.

La función de estos troqueles es que las autoridades de mesa y los fiscales puedan verificar que la BUE que se le entregó al elector es la misma que él imprimió por sí mismo e introducirá en la urna. Esta función es análoga a las firmas que ponían las autoridades y fiscales en los sobres que entregaban a los votantes en el sistema voto tradicional.

En particular, un objetivo es impedir que una persona concurra a votar con una BUE armada previamente por alguien más, o que verifique ante un tercero el contenido de su voto.

Cuando el presidente valida la identidad del elector, debe tomar una BUE cualquiera en blanco (eventualmente hasta podría darle a elegir al elector una entre varias); el presidente debe retirar el primer troquel y dejarlo junto con el documento del elector bajo su propia custodia.

Al entregarle la BUE para que vote, el presidente debería recomendarle que, una vez generado el voto, verifique que lo impreso coincida con su voluntad, y que acerque el chip de la BUE al lector para verificar que lo que aparece en pantalla es lo mismo que hay impreso, y doblar la BUE con el lado impreso hacia adentro para impedir su lectura por otras personas, dejando libre el segundo troquel.

Cuando el elector regresa luego de emitir su voto, si por cualquier motivo el elector alega que lo que está impreso no es lo que él quería votar (o que no coincidía lo impreso con lo grabado en el chip), ya sea porque el sistema no hizo lo que él deseaba, porque se equivocó al operarlo o porque se arrepintió, el presidente debe solicitarle al elector que destruya la BUE sin mostrar su contenido y debe darle una nueva BUE (otra vez guardando el primer troquel) para que el elector vuelva a la máquina para imprimir su voto.

Una vez que el elector se acerca de regreso a la mesa con su BUE plegada y conforme con el contenido, el presidente debe solicitarle que corte el segundo troquel y se lo entregue (*nadie* que no sea el elector debe tocar la BUE una vez impresa).

El presidente debe verificar que el segundo troquel coincide con el primero que él retuvo junto con el documento y recién ahí debe permitirle al elector introducir la BUE en la urna emitiendo *efectivamente*, su voto.

Si el presidente verifica que ambos troqueles *no* coinciden, entonces deberá solicitarle al elector que destruya la BUE y darle una nueva para volver a imprimir su voto.

Si el elector arrancó el segundo troquel sin la supervisión del presidente (por ejemplo, regresa de la máquina de voto con la BUE en una mano y el troquel en la otra), el presidente deberá solicitarle al elector que destruya la BUE y darle una nueva para volver a imprimir su voto.

Si el presidente observa que el elector regresa de la máquina de voto sin haber plegado la BUE y mostrando el lado impreso ya sea hacia la mesa con las autoridades y fiscales o hacia algún otro lugar donde haya personas que puedan

verlo, el presidente deberá solicitarle al elector que destruya la BUE y darle una nueva para volver a imprimir su voto.

Implementación: El instructivo audiovisual aprobado por la **Resolución N° 130** del Tribunal, así como el instructivo en papel aprobado por la **Resolución N° 131** incorporan instrucciones y advertencias para que las autoridades de mesa cumplan con la mayor parte de las recomendaciones que les atañen de esta sección.

Asistencia al elector

Al ser este un sistema novedoso para todos los electores, el mismo podría suscitar dificultades a la hora de emitir el voto.

Se recomienda, en primer lugar, que cuando el elector se acerque a la mesa se le recomiende, si es que no lo ha hecho, que se dirija a la máquina de capacitación con la que debería contar el establecimiento con el fin de capacitarse.

De todos modos, y aun cuando ya se haya capacitado en dicha máquina, o en el caso de que no haya podido hacerlo por cualquier motivo, si el presidente nota que el elector se encuentra desorientado frente a la máquina de voto[13], debe ofrecerle su ayuda si el elector lo desea.

En caso afirmativo, el presidente debería pararse frente al elector (es decir, viendo la parte de atrás de la máquina de voto) y tratar de guiarlo por las pantallas, explicándole lo que debería estar viendo y qué paso seguir, sin recomendar ninguna opción. Si no consigue siquiera saber qué pantalla está viendo, lo conveniente será solicitarle que retire la BUE de voto por arriba y que la inserte nuevamente, para ingresar en la primera opción ("voto por lista completa o voto por categorías") y desde allí guiarlo.

Cuando vea que la BUE se está imprimiendo, el presidente debería retirarse hacia atrás, evitando ver lo que se imprimió en la BUE y recomendándole al elector que primero verifique que lo que está impreso es lo que quiso votar; luego, que acerque la parte con el chip al lector y que verifique que lo que dice la pantalla es lo mismo que lo que está impreso (y es lo que quiso votar); finalmente, que le indique que doble la BUE ocultando el lado impreso y dejando libre el troquel que deberá cortar frente a la mesa.

Implementación: El instructivo audiovisual aprobado por la **Resolución N° 130** del Tribunal, así como el instructivo en papel aprobado por la **Resolución N° 131** incorporan instrucciones y advertencias para que las autoridades de mesa cumplan con la mayor parte de las recomendaciones que les atañen de esta sección.

13 Esto puede ser necesario en los casos de electores de edad media o avanzada o con poco contacto con la tecnología en general.

Modalidad de Voto Asistido para electores con discapacidad visual

Cuando se acerca a votar una persona con discapacidad visual, el presidente deberá solicitar al Delegado Judicial la plantilla y los auriculares para voto asistido y asistir a la persona durante el voto.

Si la persona tiene su propio par de auriculares, puede utilizarlos en lugar de los provistos por el Delegado (el conector que tiene la máquina en la parte superior es estándar).

El sistema está diseñado para que el presidente o quien asista a la persona pueda ver la pantalla para saber por qué paso de la selección está la persona, sin saber qué es lo que está votando.

Implementación: El instructivo en papel aprobado por la **Resolución N° 131** incorpora instrucciones para que las autoridades de mesa faciliten la votación de electores con discapacidad visual.

Voto asistido para personas con otras discapacidades

El Tribunal debería definir e informar quién y bajo qué condiciones puede asistir a un elector que tenga otra discapacidad, ya sea motriz o de otro tipo, que no le permita utilizar la máquina de voto por sí mismo.

Implementación: El instructivo en papel aprobado por la **Resolución N° 131** incorpora instrucciones para que las autoridades de mesa faciliten la votación de electores que requieren la asistencia de un acompañante.

Transmisión de datos

El proceso de transmisión de datos reemplaza al método de envío de resultados de las actas de escrutinio que en el pasado se hacían a través de los telegramas electorales.

Esta transmisión se realiza utilizando máquinas iguales a las que se utilizan para la impresión de votos, pero con un software diferente siguiendo los procedimientos establecidos en el Art. 8° del Anexo II de la Acordada 17/2015 del TSJ.

Dicho software también es provisto en un DVD para arrancar la máquina ya que, como se explicó anteriormente, la misma carece de memoria permanente para almacenar programas u otros datos.

En cada establecimiento hay una máquina de transmisión de datos.

El software de transmisión de datos permite conectar la máquina con los centros de totalización ya sea a través de internet o de la red celular de datos ("3G"). En dicho software se carga un certificado digital que identifica el centro de votación donde

está instalada la máquina de modo tal que el servidor de totalización valide el origen de la transmisión.

El servidor está configurado para sólo aceptar datos de mesas de un centro de votación utilizando el certificado digital correspondiente a dicho establecimiento. Asimismo, los servidores cuentan con certificados digitales que le garantizan a la máquina de transmisión que están comunicadas con un servidor legítimo.

La transmisión se inicia apoyando el Certificado de Transmisión de una mesa en el lector, la máquina lee el contenido e informa del mismo al servidor. El servidor valida que la mesa corresponde al centro de votación asociado al certificado digital de la máquina y que los datos de dicha mesa no han sido cargados aún.

De ser así, el servidor carga los datos recibidos en la base de datos y posteriormente le informa a la máquina de transmisión que los mismos han sido cargados.

Este proceso se realiza dos veces por cada mesa. Esto no parece ser necesario dados los controles internos de consistencia que contiene la información del Certificado de Transmisión, sin embargo el mecanismo parece estar presente por cuestiones históricas, emulando la "doble carga" que se realiza cuando el proceso se hace manualmente.

El software del servidor que se ocupa de totalizar, no permite que los datos de una mesa se contabilicen más de una vez.

El sistema de transmisión cuenta con mecanismos de transmisiones alternativas y contingencia descritos en el Anexo IV.

Auditabilidad del proceso de transmisión

A diferencia de los DVDs con el software utilizado para la votación, los DVDs para las máquinas de transmisión no pueden estar en sobres inviolables hasta el día del comicio ya que durante los días previos al comicio se realizan pruebas de transmisiones desde todos y cada uno de los centros de votación utilizando dicho software.

Si el Tribunal desea validar que se utilicen DVDs legítimos, el equipo de auditoría puede resguardar una copia válida unas semanas antes de los comicios y el Tribunal definir una cierta cantidad de DVDs de transmisión que se tomarán aleatoriamente luego de que se haya terminado el operativo en los centros de votación.

Un mecanismo posible es seleccionar aleatoriamente uno o dos establecimientos por Comuna, informarlo al cierre del comicio y que cuando termine la transmisión, el Delegado de dicho centro retire el DVD, lo introduzca en un sobre, lo selle y lo firme

en conjunto con los fiscales partidarios que se encuentren presentes y lo remita al Tribunal.

El equipo de auditoría validará durante las 48 horas posteriores al comicio que los DVDs seleccionados sean idénticos al que habían resguardado previamente.

Independientemente de esto, cabe remarcar que los datos transmitidos al centro de cómputos son auditables por los fiscales partidarios del mismo modo que siempre lo fueron ya que tendrán, como en el esquema manual, acceso a los datos totalizados por mesa.

Más aún, la empresa puso a libre disposición un software para dispositivos móviles con sistema Android que le permite a los fiscales leer los datos del código QR impreso en los Certificados de Escrutinio que reciben al finalizar cada escrutinio de mesa y pueden comparar la información de dicho certificado con la obtenida en el sistema de totalización disponible para los fiscales que desagrega la información a nivel de mesa facilitando la tarea de verificación de los datos cargados.

Totalización de resultados

El sistema de totalización de resultados es el mismo que se utilizó durante las PASO y que ya fuera auditado en su momento (ver Informe 1 de auditoría del 16 de abril) ha sido revisado en el contexto de los comicios generales.

La auditoría realizada muestra que los resultados totalizados por dicho sistema son confiables.

En dicho sistema, en lugar de utilizar los módulos de carga manual, se utilizan los módulos de carga automática vía web.

El sistema cuenta con mecanismos de contingencia descritos en el Anexo IV.

Anexo III - Alimentación eléctrica y baterías

La máquina de voto cuenta con una fuente para alimentación eléctrica con una tensión de 220V de corriente alterna (CA) que es la tensión normal domiciliaria en la República Argentina.

Asimismo cuenta con dos compartimentos para alojar sendas baterías que le permiten a la máquina funcionar sin conexión a la red eléctrica.

Cuando el equipo está conectado a la red de CA y las baterías están descargadas, el equipo las carga automáticamente.

Consumo de CA

El consumo máximo de una máquina de voto que se puede producir cuando está funcionando a pleno, imprimiendo y cargando ambas baterías (suponiendo que ambas estén completamente descargadas) es, en el peor de todos los casos, de 0.8 Amperes (A).

El consumo normal de una máquina conectada a la red de CA, con las baterías razonablemente cargadas, operando para votar, es del orden de 0.3 A.

Duración de las baterías

Las pruebas de duración de la batería se realizaron sobre dos metodologías de análisis:

1. Medición de los tiempos de servicio en simulacros de votación con escrutinio de 300 votos impresos y 10 horas de servicio
2. Medición de los parámetros internos de la batería, tensión, corriente, etc.

En virtud de los resultados obtenidos mediante la metodología 1 y las mediciones de carga y descarga de la metodología 2, podemos concluir que si las baterías son nuevas, no tienen fallas ni degradación por uso, alcanza con dos baterías que comiencen con el 100% de carga para el uso normal de 12 horas donde se impriman 300 BUEs y luego se haga el escrutinio de las 300 BUEs.

No pudiendo saber cuál será el estado de la carga de todo el conjunto de las baterías que dispone la empresa se recomienda definir un proceso de carga de las mismas el día previo a la jornada electoral, que las máquinas estén conectadas a la red eléctrica durante la elección y que se defina también un conjunto de baterías de reposición para las máquinas que no puedan conectarse a la red.

Todas las máquinas deberán contar con cable de conexión a la red eléctrica y deberá disponerse de todos los cables necesarios para que dichas máquinas puedan estar conectadas a dicha red estando en la ubicación que se utilizará

durante la votación, sin entorpecer la circulación de votantes, autoridades de mesa y fiscales.

Todas las máquinas deberán contar con baterías que deberán ser cargadas a pleno el día anterior a la elección.

En los casos en que no se pueda garantizar que la red eléctrica de un centro de votación pueda soportar la operación simultánea de todas las máquinas asignadas a dicho centro, incluyendo las de capacitación y transmisión de datos, las máquinas deberán contar con dos (2) baterías cargadas a pleno y deberá haber baterías de repuesto disponibles para casos fortuitos en que dichas baterías no alcancen para toda la jornada electoral.

Descripción de las pruebas realizadas con las baterías

1. Medición de los tiempos de servicio

Se hicieron una serie de pruebas durante la semana del 11 al 15 de mayo utilizando cuatro (4) máquinas distintas instalando dos (2) de ellas con una (1) batería y las otras dos (2) con dos (2) baterías, simulando el uso normal con 300 votos emitidos y 300 escrutados. La duración promedio por batería fue de 6:15hs. Las máquinas con dos (2) baterías conseguían funcionar durante 12 horas dejando una carga a veces inferior al 5% de remanente.

2. Medición de los parámetros internos de la batería

Según la información brindada por la empresa, las baterías son provistas por dos fabricantes distintos (*MinMax* y *Blaze Energy*), pero son todas iguales ya que son fabricadas de acuerdo a especificaciones del cliente. Las baterías son del tipo Li-Ion (iones de litio) y están construidas con celdas (Lithium-ion Cylindrical Cell).

El *pack* alcanza una tensión de funcionamiento de 14,8 Volts (Tensión Nominal) siendo la tensión de carga recomendada 16,8 Volts.

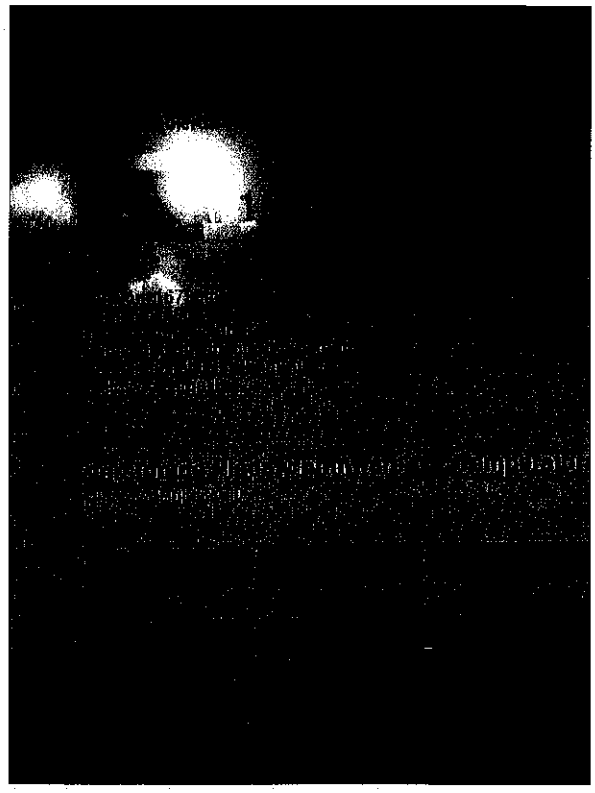
La carga se realiza cuando el equipo está conectado a la red eléctrica . A los efectos de adecuar las instalaciones eléctricas se detallan los valores medidos de corriente mediante una pinza amperométrica .

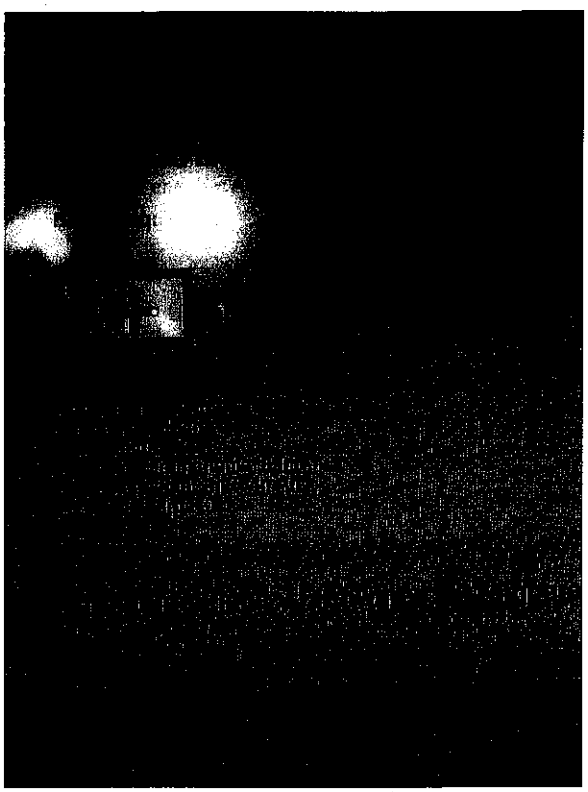
Con una batería totalmente descargada la corriente de 220 Volts alcanza los 0,3 Amper en el periodo de carga con la máquina encendida. Con dos baterías 0,6 Amper.

La condición es que ambas deben estar a un 100% de su carga (Tensión 16,7 Volts) antes de empezar la jornada de votación. Esta condición se logró en laboratorio para una batería descargada (0% de acuerdo a sistema monitoreo interno y tensión 13,3 Volts).

Según las pruebas que se llevaron a cabo utilizando dispositivos de medición externos a la máquina, se verificó que la pantalla que le permite al técnico visualizar los parámetros de tensión, corriente y temperatura se condice con las mediciones realizadas externamente con dichos dispositivos.

Ejemplos de pantallas de monitoreo de las baterías (accesibles a los técnicos):





Anexo IV – Planes de contingencia

La empresa presentó una pequeña memoria descriptiva de la arquitectura tecnológica utilizada para la transmisión de los datos desde los centros de votación, el escrutinio provisorio y la publicación de los resultados de dicho escrutinio, conjuntamente con los planes básicos de contingencia para esta arquitectura, así como el manejo de las contingencias de campo.

La documentación no cumple con las reglas del arte de una documentación de contingencia; de todos modos, el análisis de dicha documentación realizado hasta el momento brinda un escenario de confiabilidad razonable.

Transmisión de los certificados con datos de las mesas individuales desde los centros de votación

Según la documentación recibida, el esquema de transmisión desde los centros de votación está aún en etapa de definición, dependiendo de un relevamiento que la empresa está haciendo en conjunto con el Ministerio de Educación de la Ciudad y la Agencia de Sistemas de Información.

Idealmente se utilizará como método primario la conectividad a internet que ya tenga el establecimiento (en particular las escuelas de gestión pública que dependen del citado Ministerio) y como alternativa se pueden utilizar módems de datos con tecnología celular ("3G"). Finalmente, está la posibilidad de habilitar manualmente para cada centro, la posibilidad de enviar la información mediante la lectura del código QR impreso en el Certificado de Transmisión, utilizando un teléfono celular con cámara y una aplicación desarrollada *ad hoc* por la empresa.

Según la documentación de la empresa, el sistema utiliza certificados SSL para encriptar las comunicaciones vía internet y para autenticación. Por un lado, hay certificados en los servidores que le permiten a los equipos de transmisión de datos saber que le están enviando la información al servidor correcto, por el otro, hay certificados en los equipos de transmisión de datos en los centros de votación que le aseguran al servidor que el equipo está en determinado establecimiento y sólo acepta recibir de este equipo datos de las mesas de dicho establecimiento.

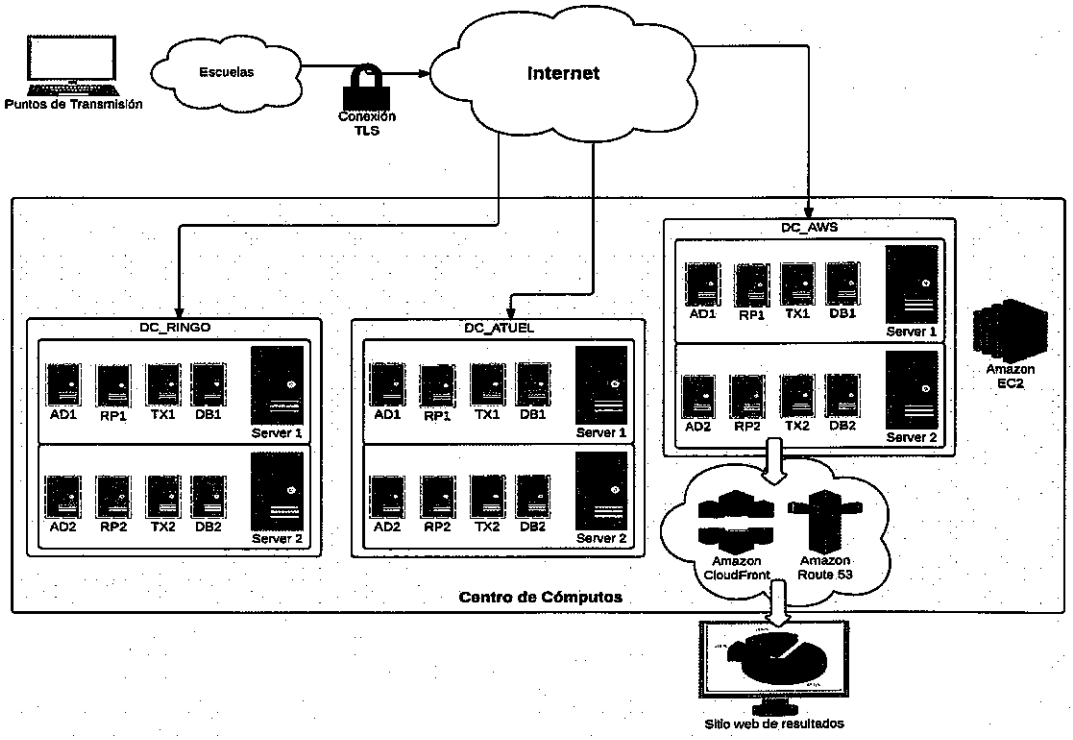
De todos modos, esta metodología es al menos igual de confiable (y en general más) que la utilizada hasta el presente con los métodos de votación manual donde se transmitían los resultados de las mesas por medio de faxes u otros mecanismos similares sin mayores validaciones de origen ni cifrado alguno.

Centro de consolidación del escrutinio provisorio

El esquema de redundancia y contingencia según la documentación provista es adecuado.

Se creará un único Centro de Cómputos "lógico" distribuido en tres Centros de Datos o *Data Centers* (DC), cada uno con al menos tres enlaces independientes a internet. Los mismos están ubicados respectivamente en iPlan (en la Ciudad de Buenos Aires), en las oficinas de la empresa (también en la Ciudad de Buenos Aires) y en Amazon Web Services (AWS), un proveedor global de servicios de cómputo en la "nube" (*cloud computing*); en este último caso, se utilizarán servicios en la región de São Paulo, Brasil, con *backup* en el estado de Virginia en Estados Unidos.

Cada DC contiene al menos dos servidores físicos y, dentro de cada uno de ellos, se ubican cuatro máquinas virtuales, cada una con un rol definido. La base de datos del DC que está recibiendo los datos se mantiene replicada en forma sincrónica entre ambos servidores físicos. Entre estos servidores y los que están en los otros DC, así como entre los servidores de los DC que no están recibiendo las transmisiones, las réplicas se realizan en forma asincrónica. La empresa informa que en las pruebas realizadas, las replicaciones asincrónicas nunca tardaron más de cuatro segundos.



Las contingencias de campo, fallas en equipos, cuestiones de logística, etc. son monitoreadas con un sistema de operaciones que le permite a la empresa hacer un seguimiento caso por caso desde el centro de operaciones. Este sistema operará desde un *call center* ubicado en el microcentro de la ciudad y le permite a la empresa mantenerse en contacto con actores relevantes del operativo.