



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

INFORME 2: Avance y Observaciones del sistema para voto con boleta única electrónica (BUE) al lunes 01/06/2015

El presente es un informe de avance anticipado que contiene información parcial con lo analizado por el equipo de auditores hasta el 1° de junio.

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 hasta la fecha 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.

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

Los principales auditores de los comicios siguen siendo tanto los fiscales de las agrupaciones políticas, como 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.

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.

Por otra parte, en algunos casos en que se considera de importancia, se remarca la necesidad de capacitar acerca determinadas cuestiones, ya sea a las autoridades de mesa o a la ciudadanía en general.

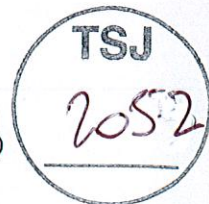
No fueron relevados los establecimientos de votación en cuanto a sus instalaciones eléctricas y la conectividad a internet. De todos modos, los equipos cuentan con baterías que, si están cargadas por completo, pueden permitir el normal funcionamiento aun ante la ausencia de energía eléctrica (ver Anexo 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.



- Los empleados de la empresa: operadores y administradores del sistema de escrutinio, personal de soporte técnico y coordinadores.

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

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.

Una solución posible es 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).

2. Al finalizar la impresión de un voto, el sistema le informa al votante cómo puede verificarlo. Esta pantalla no se puede llegar a leer en su totalidad; apenas está unos segundos y a continuación aparece nuevamente la pantalla inicial "Introduzca la Boleta Única Electrónica en la impresora" que invita 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, pasa completamente inadvertida.

Esto podría hacer pensar al elector que no llegó a tiempo a realizar la verificación de su voto o, simplemente, al no poder leer la pantalla, se olvide que existe 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.

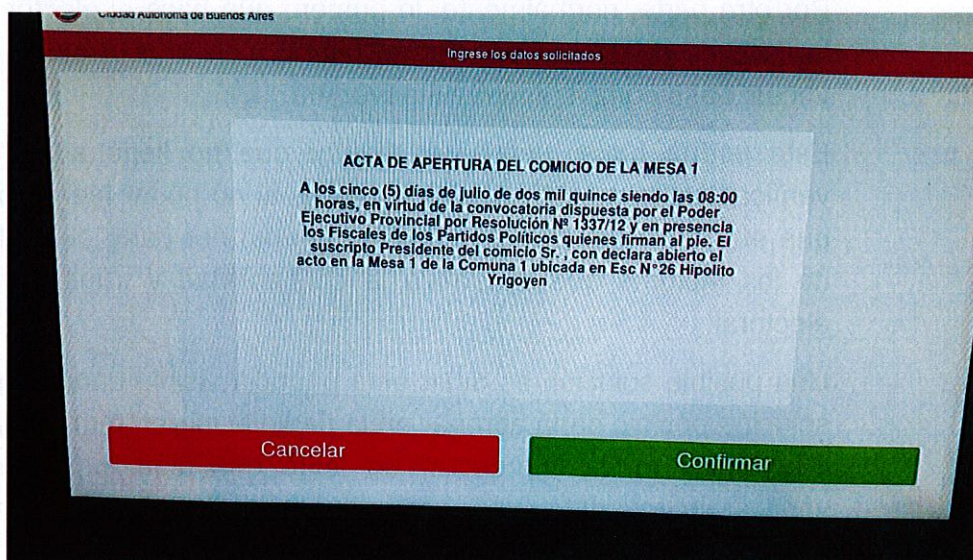
Una posible solución es dejar esta pantalla visible unos segundos más. Otra solución posible sería agregar en la pantalla inicial "Introduzca la Boleta Única Electrónica en la impresora" un texto que diga, por ejemplo, "No olvide verificar su voto al terminar de imprimirlo, apoyándolo en el lector" u otra frase a definir por el Tribunal.

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 le permita hacerlo aún sin modificar los números).
- b) No se controla 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.
- c) Si bien cuando se ingresa la hora y no los minutos o viceversa aparece un cartel indicando esto forzando a corregir el error, cuando no se ingresa ninguno de los dos campos, no aparece ningún cartel avisando de esto y permite seguir adelante asumiendo que la hora de apertura es 8:00 y la de cierre 18:00
- d) El sistema tampoco considera 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 (...)."



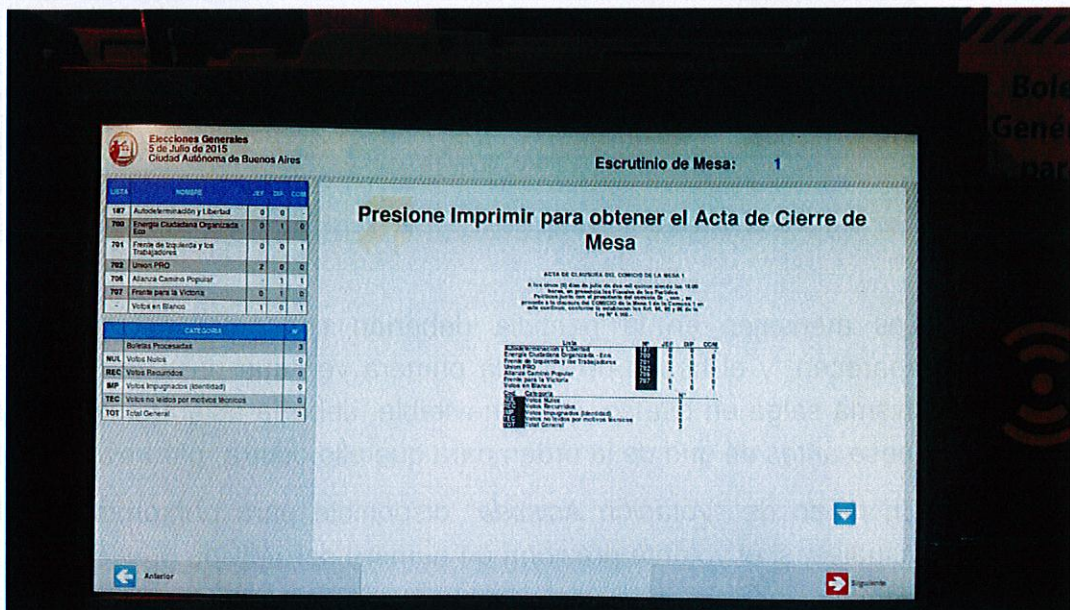
La implementación de estos controles son de bajo costo en relación a las ventajas de validar la información ingresada y evitar errores de tipeo u olvidos.



4. Cuando se está ingresando texto con los datos de las autoridades de mesa (nombre, apellido, documento), si el presidente cometió 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.

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

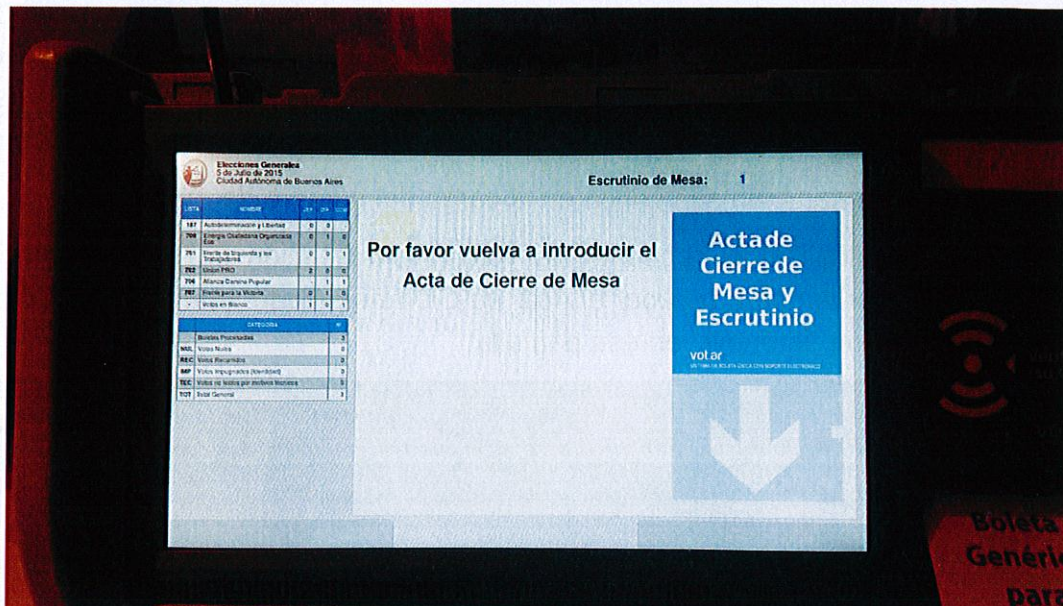


Más aún, si se presiona el botón “Siguiente”, el Acta de Cierre que está insertada en la impresora sale hacia abajo pero completamente vacía¹.

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.



A continuación aparece una pantalla solicitando se ingrese nuevamente el Acta:



Los mensajes en la pantalla deberían concordar con los botones que aparecen, y el hecho de que la primera vez que pasa el Acta de Cierre, la misma salga en blanco, si es inevitable, debería aclarársele al presidente de mesa *antes* de que de la orden para que ello ocurra, para evitar confundirlo.

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.

La solución adoptada en la última versión, 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.



Se recomienda que, en el caso de "Votación Asistida" el voto en blanco entre en el sorteo del orden como si fuese una agrupación más.

8. En el modo de "Votación Asistida" es imposible completar la selección ya que en el momento que el sistema debe emitir el título de la categoría correspondiente a *Miembros de la Junta Comunal*, el sistema deja de emitir audio por completo y el elector no tiene forma de continuar, aun cuando tuviera asistencia de alguien que estuviese mirando la pantalla.
9. Cuando el elector elige votar por lista completa, en la pantalla se muestran los datos de todas las agrupaciones, candidatos e imágenes pero no se muestra el número de la lista (sólo el nombre de la agrupación o alianza).

Si bien dicho número no es exigido por la Acordada 17 del Tribunal, esto no es consistente con las otras pantallas donde sí aparece el número de lista.

Luego de seleccionar la agrupación por nombre, en la siguiente pantalla de confirmación, aparece el número de la lista, y lo mismo ocurre cuando se elige votar por categoría: el sistema muestra el número de la lista junto con el nombre de la agrupación en cada una de las categorías.

En el modo de "Votación Asistida", no se escucha el número de la lista en ningún caso (ni votando por lista completa ni votando por categoría).

Además, cuando está eligiendo por categorías en dicho modo, el audio indica el cargo (la categoría) y para cada opción, el número que debe seleccionar y el nombre del candidato, pero **no** el nombre de la agrupación ni el número de lista a la que pertenece el candidato.

El sistema debería ser consistente con la información que brinda al elector en cada situación, ya sea mostrando *siempre* el número de lista o no haciéndolo nunca.

En el modo de "Votación Asistida" se debería *siempre* oír el nombre de la agrupación antes o después de cada candidato y que se oiga el número de lista debe depender de que el mismo se muestre o no en las pantallas normales.

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.

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.

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.

Asimismo, sería conveniente definir un salto mínimo para actualizar la información, ya sea en cantidad o porcentaje de mesas o votos escrutados o en tiempo. Por más que el sistema de transmisión y publicación permita una actualización casi permanente de la información, el público estaría viendo cambios constantemente y hasta los distintos medios de comunicación estarían brindando información distinta casi al mismo tiempo.

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 han sido recibidas y sin haber realizado el proceso de *testing* interno.

Algunas de las observaciones sobre funcionalidad que figuran en el presente informe, han aparecido recién en esta última versión recibida dos días antes de la presentación del presente informe de avance, con lo cual no hubo tiempo de informar a la empresa para que los solucione aun en los casos que fuese relativamente simple hacerlo.

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

Conclusiones

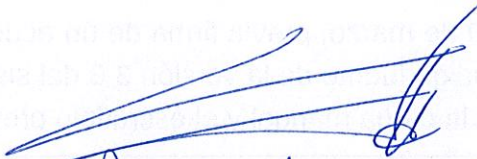
Ateniéndose al análisis de los componentes del sistema auditados (hardware, software, procedimientos), establecemos que es crucial para el correcto

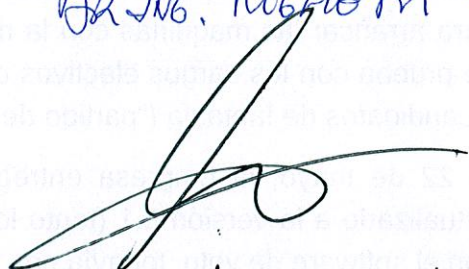


funcionamiento de dicho sistema en forma global que las autoridades de mesa, delegados judiciales y demás responsables de los comicios sigan los procedimientos aprobados por el Tribunal (Acordada 17/2015, Anexo II); y que el mecanismo de votación sea apropiadamente difundido para el conocimiento de los electores.

Dados los presupuestos del párrafo anterior, se determina que el sistema permite respetar los principios enunciados en el Artículo 24 del Anexo II de la Ley 4894.

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 el requerimiento de fiscalización por parte de las agrupaciones políticas.


Dr. Jue. Mariam C.B.


Lic. Marian Ansar

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, si no 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 mismo".

1. Fuente:

.../elecciones/msa/voto/gui/templates/js/ingreso_datos.js

Función/sección: pantalla_mesaypin, línea 147

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().

2. Fuentes: [.../elecciones/msa/voto/modulos/recuento.py](#)
[.../elecciones/msa/voto/modulos/totalizador.py](#)

Función/sección: get_campos_extra, líneas 299 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, False,
             "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 (el código en azul corresponde a lo que está sólo en `recuento.py` y el código en verde a lo que está sólo en `totalizador.py`). Por ejemplo en los archivos mencionados el contenido de una de las funciones se repite como contenido casi exacto de la primera mitad de la otra. 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 con los parámetros necesarios para reflejar la diferencia (en el caso del ejemplo el parámetro indicaría si son editables o no los valores de las listas especiales y si debe o no agregarse el campo COD_TOTAL al final).

3. Fuente: `.../elecciones/msa/core/data/candidaturas.py`

Función/sección: `full_dict`, líneas 337 a 338

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.



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

Función/sección: send_constants, líneas 630 a 634

Contenido aproximado:

```
def send_constants(self):  
    """Envía 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.

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

Función/sección: enviar() { ... guardar/permisos", línea 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.



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.

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 contenido². 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).

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 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 lavista 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

2 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.



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.

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.

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 voto³, debe ofrecerle su ayuda si el elector lo desea.

³ Esto puede ser necesario en los casos de electores de edad media o avanzada o con poco contacto con la tecnología en general.



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.

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.

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.

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) y que está siendo revisado en el contexto de los comicios generales.

La auditoría realizada hasta el momento 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 10hs 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 12hs donde se emitan 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 4 máquinas distintas instalando 2 con 1 batería y 2 con 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 2 baterías conseguían funcionar durante 12hs 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.

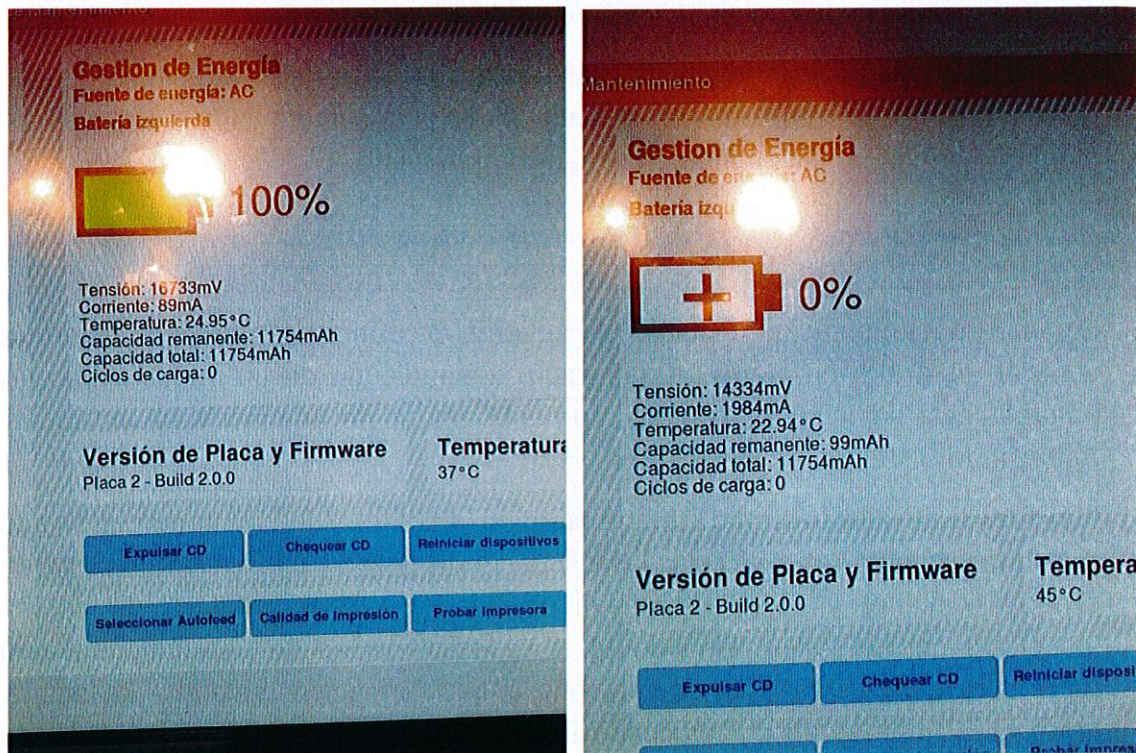
La carga se realiza cuando el equipo está conectado a la red eléctrica. A los efectos de adecuar las instalaciones eléctricas se detallan los valores medidos de corriente mediante una pinza amperométrica.

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.

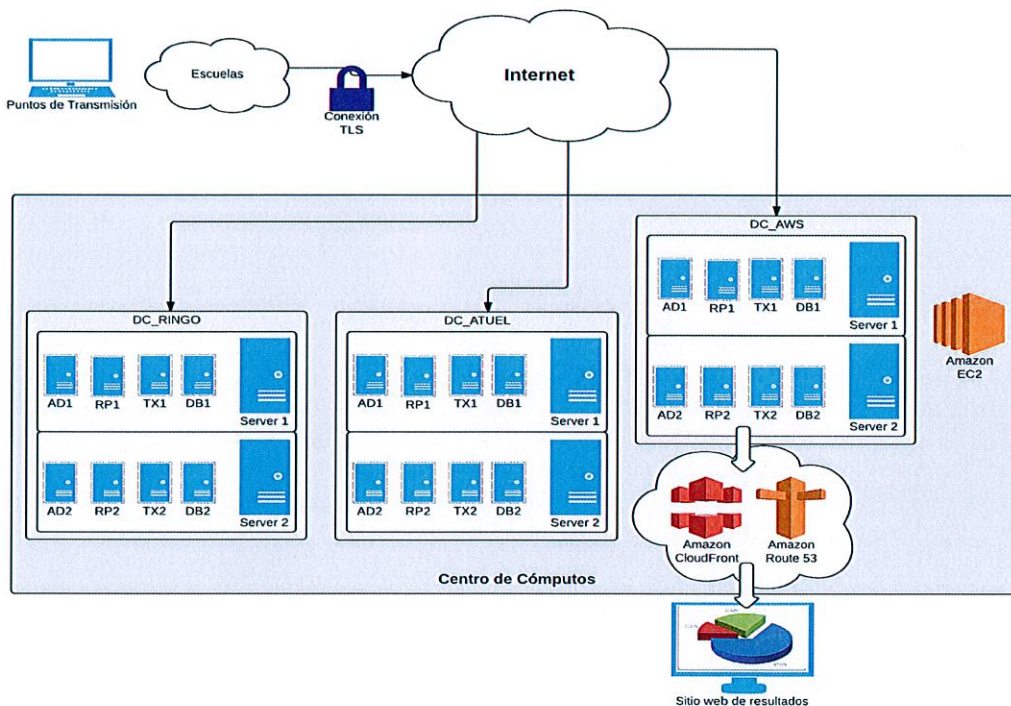
De todos modos, esta metodología es al menos igual de confiable (y en general más) que la utilizada hasta el presente con los métodos de votación manual donde se transmitían los resultados de las mesas por medio de faxes u otros mecanismos similares sin mayores validaciones de origen ni cifrado alguno.

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 replications asincrónicas nunca tardaron más de cuatro segundos.

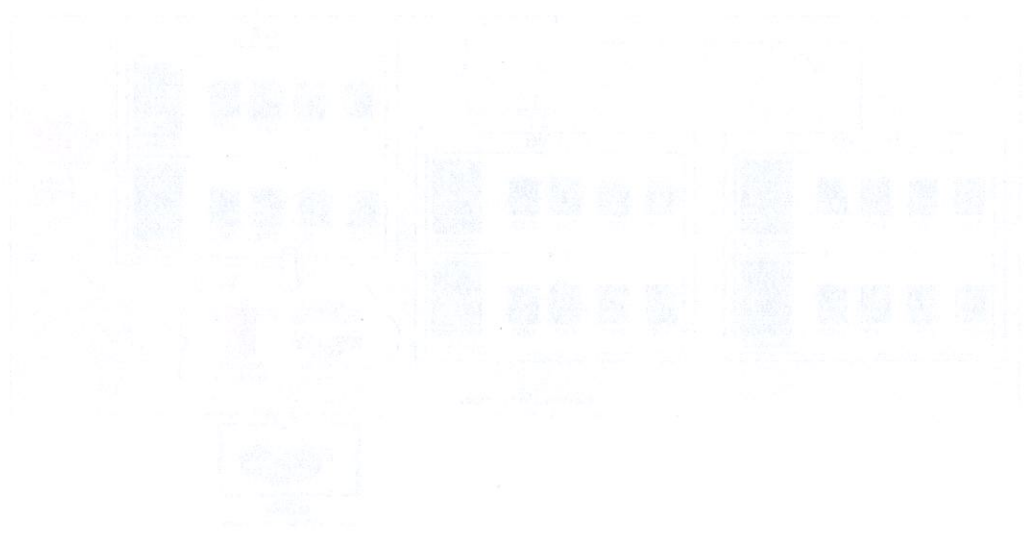


Las contingencias de campo, fallas en equipos, cuestiones de logística, etc. son monitoreadas con un sistema de operaciones que le permite a la empresa hacer un seguimiento caso por caso desde el centro de operaciones. El mismo sistema le permite mantenerse en contacto con actores relevantes del operativo.



Faint text at the top right of the page.

Main body of faint text, likely a letter or report, mostly illegible.



Faint text located below the architectural drawing.

Handwritten signatures and scribbles at the bottom left.

Faint text at the bottom right of the page.



Ciudad Autónoma de Buenos Aires, 1 de Junio del 2015

Dra. Alejandra Tadei

Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires


En cumplimiento de la actividades encuadrados dentro de la Orden de Asistencia Técnica (OAT 03-15) solicitada por Tribunal a la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires.

Y de acuerdo al cronograma previsto en la Adenda N° 1, se entrega en el día de la fecha el segundo informe de avance sobre la "Auditoría del escrutinio provisorio y de las tecnologías electrónicas que se implementen en la Ciudad Autónoma de Buenos Aires en el proceso electoral del año 2015."

Saluda Atte.


Prof. Dr. Claudio Enrique Righetti

Recibido el 1/6/15 a las 19:00 horas.


Dr. Roberto Asorey
Prosecretario Mayor
Secretaría Judicial en Asuntos Originarios
Tribunal Superior de Justicia
Ciudad Autónoma de Buenos Aires



Departamento de Computación, Facultad de Ciencias Exactas y Naturales
 Universidad de Buenos Aires
 Bahellón I - Ciudad Universitaria - (C1428EHA) - Buenos Aires - Argentina
 Tel: Fax: 54-11-4532-3333

Este documento es propiedad de la Universidad de Buenos Aires.

Facultad de Ciencias Exactas y Naturales

Departamento de Computación, Facultad de Ciencias Exactas y Naturales

Este documento es propiedad de la Universidad de Buenos Aires.


 Profesor Adjunto

Profesor Adjunto


Facultad de Ciencias Exactas y Naturales
 Departamento de Computación