Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema:

Incorporación de las TIC en el Sistema Electoral Argentino

Título:

Voto Electrónico en Argentina

Autor: Ing. Gustavo Antonio Sánchez

Tutor del Trabajo Final: Lic. Graciela Pataro

Año: 2011

Cohorte: 2010

Resumen

La incorporación de las nuevas tecnologías en los procesos electorales es una realidad que debe analizarse desde distintos enfoques aún cuando el Código Nacional Electoral no lo contemple todavía.

La emisión y el registro del sufragio por medios electrónicos implica no sólo un gran cambio cultural en nuestra aún incipiente democracia, sino un profundo análisis de los métodos de aplicación que garanticen, entre otras, la confidencialidad, integridad y disponibilidad de los datos electorales.

El objetivo del presente trabajo es analizar las posibilidades de incorporación de las TIC en el sistema electoral argentino, en base a las distintas alternativas que pueden ser empleadas en la actualidad y a las experiencias llevadas a cabo en el ámbito nacional.

Para ello, primero se hará una descripción de los sistemas actuales de aplicación de las TIC a los procesos de captura y recuento de los sufragios:

- Sistema de recuento automático
- Sistema de registro electrónico directo
- Sistema de votación a distancia

Luego se analizarán las distintas experiencias de voto electrónico llevadas a cabo en Argentina en los últimos años conjuntamente con las distintas posturas vertidas por los distintos autores, teniendo en consideración los siguientes aspectos:

- Confidencialidad:
    - Secreto del voto.
    - Aspectos legales y éticos.
- Integridad:
    - Auditoría del hardware y del software.
    - Seguridad del sistema operativo y de las aplicaciones.

    - Proceso de inseminación del software.
    - Encripción de datos electorales.
- Disponibilidad:
    - Consolidación de los datos electorales.
    - Rapidez en la obtención de los resultados.

Finalmente, teniendo en cuenta las ventajas y desventajas de los distintos sistemas y los resultados de las experiencias mencionadas, se buscará analizar todo lo expuesto a fin de llegar a determinar las posibilidades de aplicación de las TIC al sistema electoral argentino.

Tabla de contenidos

1. Sistemas de captura y recuento de sufragios

Los diferentes autores coinciden en clasificar los sistemas de captura y recuento de sufragios en dos grandes grupos, los presenciales y los no presenciales.

En el primer grupo encontramos aquellos sistemas en donde quien emite su voto debe hacerse presente en los lugares de votación, estos son, los sistemas de recuento automático y los sistemas de registro electrónico directo.

En el segundo grupo, los sistemas permiten que el voto se realice en forma remota sin la necesidad de trasladarse a los sitios de votación, son los sistemas de votación a distancia.

Beatriz Busaniche y Federico Heinz en [1; pág. 21], describen en forma pormenorizada, cada uno de los sistemas mencionados. A continuación se transcriben partes de esta obra.

1.1. Sistemas de recuento automático

Los primeros sistemas de esta clase datan del siglo XIX, cuando se comenzaron a implementar en la ciudad de Nueva York mediante tarjetas perforadas. Actualmente, la mayoría de los sistemas de este tipo se basan en el reconocimiento óptico de marcas hechas por el votante sobre la boleta, ya sea en forma directa o a través de una máquina de marcar boletas. Entre los años 1994 y 2003, Venezuela utilizó sistemas de este tipo, basados en un sistema de boletas impresas en papel con un espacio rellenado por el elector y posteriormente contabilizados mediante un sistema de reconocimiento óptico de caracteres.

En principio, estos sistemas resuelven el problema más álgido de la incorporación de tecnología al sufragio: al mantener el principio de que la voluntad del elector se expresa en un trozo de papel anónimo, se desacopla el acto de emisión de voto (que debe ser inauditable) del acto del escrutinio (que debe ser auditable en todos sus detalles). De esta manera es posible construir un sistema en el cual todos los resultados en los que la informática está involucrada

pueden ser auditados independientemente de los dispositivos usados y el software en sí, mediante el simple recurso de realizar un recuento manual.

Aún así, la aplicabilidad de estos mecanismos no puede tomarse en forma aislada, sino en el contexto del sistema completo del cual forman parte. Es posible tomar muchas decisiones respecto del sistema como un todo que pueden anular total o parcialmente las ventajas del mecanismo.

Un elemento que no puede faltar en la aplicación de sistemas de recuento automático es la auditoría manual de los resultados arrojados por una porción estadísticamente significativa de las máquinas usadas, seleccionadas al azar luego del acto eleccionario. De lo contrario, una programación maliciosa del software de tabulación de votos podría alterar los resultados sin ser detectada.

Estos sistemas pierden una porción importante de sus ventajas cuando la boleta no es marcada a mano por el elector. Las máquinas de marcar boletas vuelven a introducir en el sistema muchos de los problemas asociados con las máquinas de registro directo. Si bien permiten que el votante verifique que las marcas en la boleta se correspondan con sus elecciones, suponen un doble trabajo para el votante (elegir por un lado, controlar por otro), lo que aumenta la probabilidad de que el elector no realice concienzudamente el control. Esto hace factible el mismo ataque que se puede hacer en las máquinas de RED[1]: introducir código que intente adulterar la intención del votante, pero abandonar el intento si el votante rechaza la boleta. De esta manera se pueden secuestrar los votos de todos aquellos ciudadanos que no sean lo suficientemente cuidadosos. También ponen en riesgo el anonimato del voto, toda vez que la máquina de marcar boletas podría agregar, además de las manchas legítimas, algunas que pasen por “suciedad” pero en realidad codifiquen información que permita reconstruir la secuencia de emisión de los votos.

Otro mecanismo que reduce la utilidad de estos dispositivos es el de pasar la boleta por un escáner antes de introducirla en la urna, en vez de hacerlo al abrir ésta. Esto no solo aumenta los costos (requiere un escáner por mesa, mientras que de otro modo puede utilizarse el mismo escáner para varias de ellas), sino que potencialmente permite registrar la secuencia en la que se emitieron los votos, y así reconstruir la relación de cada votante con su voto.

Una crítica común a este tipo de mecanismo señala la dificultad que presentan en el caso de elecciones complejas, en particular cuando se realiza una elección para múltiples cargos en múltiples niveles de distrito. En una elección en la cual, por ejemplo, se deba elegir concejales de la ciudad, intendente, legisladores provinciales, legisladores nacionales,

[1] Las máquinas RED se describen en el apartado 1.2

gobernadores y presidente, la magnitud de la boleta dificulta al votante el marcado de todas las opciones, así como su posterior lectura detallada. Sin embargo esto es más una crítica de las elecciones complejas que del sistema de recuento automático en sí: mientras más compleja es una elección, más difícil es votar en ella y contar los votos. La "solución" a este problema ofrecida por los sistemas RED consiste, básicamente, en barrerlo bajo la alfombra: como en ellos es imposible contar a mano los votos, disfrazan el vicio de virtud declarando que es una tarea "innecesaria".

Otra crítica común de estos mecanismos, e igualmente inmerecida, es la que objeta la facilidad con la que se puede alterar o anular un voto mediante el agregado de marcas por parte de quienes realizan el escrutinio. Si bien la factibilidad del ataque es real, es exactamente la misma que con cualquier sistema basado en papel, que a su vez es mejor que la de cualquier sistema completamente electrónico: mientras que las boletas pueden ser alteradas, esto debe ser hecho individualmente con cada boleta, y el impacto de una persona corrupta se circunscribe a las boletas bajo su custodia. En el sistema electrónico, en cambio, una única persona corrupta tiene el potencial de infectar un gran número de máquinas, comprometiendo de esa manera incluso la integridad de votos en masa, incluyendo los de mesas cuyos fiscales actúen de buena fe.

1.2. Sistemas de registro electrónico directo

Los sistemas RED o DRE son aquellos que más se corresponden con el imaginario popular de las "urnas electrónicas". Representan, además, el modelo preferido de la mayoría de las empresas que participan de este mercado. Las urnas electrónicas utilizadas en Brasil, así como en varios estados de EEUU o en las últimas elecciones de Venezuela pertenecen a esta clase.

Los sistemas RED se caracterizan por realizar simultáneamente el registro y la tabulación del voto mediante un dispositivo informático que es operado directamente por el votante mediante un teclado, una botonera especial, o una pantalla táctil. Algunos sistemas de RED ofrecen además ayudas para personas con algún tipo de discapacidad, por ejemplo mediante una interfaz de audio para superar las dificultades visuales. A diferencia de los sistemas de recuento automático, en los que el soporte fundamental del voto es la boleta marcada por el ciudadano, en las máquinas RED el registro se realiza directamente en la memoria del dispositivo.

Muchos proveedores de equipamiento señalan como una ventaja del sistema el hecho de que permite "independizar del papel" a la elección. Por lo general, recomiendan no usar la

opción ofrecida por algunos modelos de máquinas RED de usar impresoras similares a las que funcionan dentro de las cajas registradoras para generar una cinta de auditoría, argumentando que “desnaturaliza el voto electrónico”. En todo caso, las máquinas RED no usan el papel emitido para sus resultados, sino que se basan enteramente en los registros presentes en su memoria.

Los sistemas RED pueden configurarse de tal modo que permitan al usuario corregir sus opciones y hasta votar en blanco, pero no permiten invalidar el voto ni cometer errores clásicos que resultan en la anulación del voto.

Los sistemas RED suelen ser también los preferidos por aquellos que trabajan en las elecciones, porque son los que más trabajo les ahorran: no hay boletas que custodiar, el recuento de votos es inmediato, y no hay riesgo de que un nuevo recuento de votos arroje una diferencia con el anterior: la máquina obtendrá siempre el mismo resultado, independientemente de si éste refleja la voluntad de aquellos que la usaron para votar o no.

En esta preferencia se hace evidente un punto de tensión entre los intereses de los ciudadanos (que necesitan que el resultado refleje sus elecciones) y los de quienes están encargados de conducirlo (quienes desean terminar la tarea con la mayor rapidez y el menor esfuerzo posible, descargando tanta responsabilidad como se pueda por eventuales errores o actos de corrupción).

1.3. Sistemas de votación a distancia

Son mecanismos para emitir el sufragio desde una computadora común conectada a la red de redes, permitiendo que los sufragantes emitan su voluntad desde sus propios domicilios, desde puntos públicos de acceso, e incluso desde el extranjero. Existen variantes de estos sistemas que permiten emitir el voto no sólo desde una computadora personal, sino eventualmente también desde un teléfono celular o un sistema de televisión digital.

Uno de los desafíos más grandes que enfrenta este tipo de sistemas es la identificación del votante, que es imprescindible para asegurar varias propiedades importantes de mecanismo, tales como evitar que alguien vote más de una vez o en nombre de otra persona, o que voten personas que no están habilitadas para hacerlo. Este problema suele resolverse mediante una clave unívoca y personal, que puede incluir elementos físicos de autenticación tales como la posesión de una tarjeta de identificación criptográfica o un generador de claves pseudoaleatorias.

Aún con los métodos de autenticación más sofisticados, no queda claro que sea posible reconciliarlos con los requerimientos de identificación exigidos por la ley, que por lo general requieren la verificación de documentos de identidad por parte de autoridades electorales. Un problema adicional asociado al de la identificación es que obligan a la máquina que reciba el voto tenga conocimiento de quién los está emitiendo. Esto ofrece un punto único de ataque para quien quiera violar el secreto del voto: basta con obtener la información almacenada en el servidor del sistema de votos para averiguar cómo votó cada persona que lo usó.

Los proponentes de estos sistemas señalan que se prestan a ser usados en lugares en los que la participación en las elecciones no es obligatoria y está permitido votar por correo. El argumento es sólido, en el sentido de que es un sistema que puede ser usado en contextos en los que la experiencia muestra que el riesgo de fraude es bajo.

Es interesante señalar que hay experiencias exitosas de uso de votación a distancia en ciertos ámbitos específicos, en particular en aquellos en los que los participantes tienen un grado alto de familiaridad y acceso a recursos informáticos y está ausente la exigencia de anonimato. El proyecto Debian, por ejemplo, un proyecto comunitario de desarrollo de software integrado por personas de todo el mundo que no tienen oportunidad de encontrarse para votar, utiliza voto a distancia como una herramienta cotidiana, con excelentes resultados. El sistema es robusto, justo y difícil de engañar, pero solo funciona gracias al hecho de que el voto no es secreto.

2. Distintas experiencias de voto electrónico en Argentina

Las distintas experiencias de voto electrónico en Argentina a excepción de las recientes elecciones provinciales en la provincia de Salta el pasado 10 de Abril de 2011, han sido de muy bajo impacto en el contexto global de los respectivos actos eleccionarios en las que tuvieron lugar.

Debido a ello después de casi 8 años desde la primera prueba piloto en la provincia de Buenos Aires, el voto electrónico no forma parte vinculante de los procesos electorales en la Argentina.

A partir de las diferentes fuentes consultadas se describirán a continuación en orden cronológico, los principales acontecimientos relacionados con las experiencias de voto electrónico llevadas a cabo hasta el presente:

- 14 de Septiembre de 2003

  En la provincia de Buenos Aires en la VII sección electoral se lleva a cabo una prueba piloto solo para mesas de extranjeros para un total de 336 electores habilitados. Se utilizaron dispositivos de registro electrónico directo sin impresión de comprobantes de voto, los electores no tenían posibilidad de auditar su elección.

- 26 de Octubre de 2003

  En la ciudad de Ushuaia se lleva a cabo la elección municipal incluyendo el padrón completo, 36.158 electores habilitados. Se utilizaron dispositivos de registro electrónico directo donde solo el 23% contaban con la funcionalidad de impresión de comprobantes de voto, por lo que una porción de los electores contaron con la posibilidad de validar su elección.

- 23 de Octubre de 2005

En la ciudad de autónoma de Buenos Aires se lleva a cabo una prueba piloto no vinculante donde en algunos recintos de votación, los electores fueron invitados a participar voluntariamente. Se sometieron a prueba 4 modelos diferentes de captura y procesamiento de votos:

1) Lector óptico de boleta individual (LOB): mediante el cual las boletas impresas elegidas son ingresadas individualmente por el elector en un escáner, que lee y muestra la elección y luego de ser validada ingresa a una urna cerrada para un eventual recuento posterior y queda registrado en una unidad de almacenamiento.
2) Registro electrónico con almacenamiento digital externo (REA): el elector recibe una tarjeta magnética en el momento de identificarse ante las autoridades de la mesa de votación y con ella ingresa al cuarto oscuro para introducirla en la máquina de votación. Luego de realizar la elección de candidatos, ésta queda grabada en la tarjeta que es devuelta al elector por la máquina. Para finalizar el elector introduce la tarjeta en una segunda máquina que se encuentra en la mesa de votación, que la lee y registra el voto. La tarjeta es depositada automáticamente dentro de una urna cerrada para una eventual verificación del sufragio.
3) Lector óptico de planilla de selección múltiple (LOP): el elector recibe al momento de identificarse en la mesa de votación, una planilla o boleta única junto con un marcador especial. En el cuarto oscuro registrará su elección rellenando en la boleta, los espacios reservados a tal fin junto a cada una de las opciones. Finalmente en la mesa de votación, ingresará la boleta en un escáner que validará las marcas, registrará electrónicamente la elección y depositará la boleta en una urna cerrada para un posible recuento manual.
4) Registro electrónico con verificación impresa (REV): estas máquinas son del tipo RED descriptas en el capítulo anterior con

el agregado de una impresora que imprime un comprobante de voto con la elección del elector para su verificación a través de un visor. Al ser validado, el comprobante es almacenado en una urna cerrada con fines de auditoría.

- 13 de Septiembre de 2007

  En la ciudad de Ushuaia se resuelve no repetir la experiencia de voto electrónico porque no se llega a un acuerdo con la empresa proveedora de las máquinas utilizadas en la elección anterior para colocar impresoras de comprobantes de voto en todas ellas. Otros oferentes de la licitación fueron desestimados por costos elevados. Se vuelve al sistema tradicional de votación.

- 28 de Octubre de 2007

  En la provincia de Buenos Aires en los partidos e Berisso, San Martín, San Isidro y Vicente López, se lleva a cabo una prueba piloto solo para mesas de extranjeros para un total de 37.155 electores habilitados de los cuales solo asisten 3.320. Se utilizaron dispositivos de registro electrónico directo sin impresión de comprobantes de voto, los electores no tenían posibilidad de auditar su elección.

- 16 de Diciembre de 2007

  En la ciudad de Las Grutas, se realiza una prueba piloto no vinculante en las elecciones municipales con máquinas de votación de registro electrónico directo. Se registran muchos inconvenientes: en las dos mesas femeninas las votantes no pudieron votar porque no figuraban en el padrón cargado en las máquinas, debieron votar en otras mesas mediante el voto tradicional; en una mesa masculina se terminó el papel para la impresión de votos y se procedió a su apertura sin los debidos controles quedando expuestos los votos anteriores y en otra

mesa masculina, al finalizar el acto eleccionario, se imprimieron los totales en cero, debiéndose contar los votos en forma manual.

- Julio de 2008

  En la ciudad de Las Grutas, debido a todos los problemas que se registraron durante la prueba piloto del año anterior, el concejo deliberante local, deroga la ordenanza que autorizó el uso de urnas electrónicas.

- 28 de Marzo de 2010

  En la ciudad de Pinamar, se lleva a cabo la elección a intendente mediante la utilización de máquinas de registro electrónico directo con impresión de comprobantes de voto.

- 5 de Septiembre de 2010

  En la ciudad de Marcos Juarez, se lleva a cabo la elección de autoridades municipales mediante la utilización de máquinas de registro electrónico directo sin impresión de comprobantes de voto. Esta elección fue considerada como prueba piloto para las elecciones provinciales de 2011, pero dado que los resultados no fueron satisfactorios, no pudieron impulsarse los cambios necesarios en la legislación electoral provincial y los próximos comicios se realizarán de la forma tradicional.

- 10 de Abril de 2011

  En la provincia de Salta se lleva a cabo la elección de autoridades provinciales donde el 33% del electorado utiliza máquinas del tipo de recuento automático de boletas de voto electrónico. Estas máquinas tienen dos funcionalidades diferentes. Durante el acto eleccionario, el elector introduce el ella una boleta de voto electrónico “en blanco”, que le es entregada en la mesa de votación al momento de

identificarse. Esta boleta posee un dispositivo RFID. La máquina comprueba que el dispositivo RFID no contenga ninguna información y presenta en una pantalla táctil, todas las opciones al elector. Completados los pasos de elección de candidatos y luego de confirmar su elección, el elector retira de la máquina la boleta de voto electrónico con su voto impreso y grabado en el dispositivo RFID. El elector, puede verificar que en la boleta quedó correctamente registrado su voto visualizando la impresión en la misma y apoyando el dispositivo RFID en el lector de la máquina de votación visualizando en la pantalla táctil lo mismo que está impreso en ella. Luego de verificar su voto, el elector introduce la boleta en una urna cerrada ubicada en la mesa de votación para su posterior recuento al finalizar el acto eleccionario. Para realizar el escrutinio, la máquina se comporta como un lector y tabulador de los sufragios contenidos en las boletas. Para ello, las autoridades de mesa pasan por el lector cada una de las boletas y al mismo tiempo que se contabilizan automáticamente, la máquina muestra en la pantalla lo mismo que está impreso en ellas para su control.

Como puede observarse en la descripción precedente, ninguna de las pruebas realizadas ha dado origen a una continuidad de utilización de métodos de elección por medio del voto electrónico. Entre los principales motivos pueden encontrarse: que los resultados de las pruebas no fueron satisfactorios, que el costo de las propuestas es elevado o simplemente no hubo determinación para continuar con las pruebas.

Una explicación a la falta de continuidad mencionada podría ser que todas las pruebas fueron intentos aislados. Alejandro Tullio en [7; pág. 58], sobre este tema refiere lo siguiente:

La introducción del voto electrónico debiera realizarse de forma gradual, a través de la implementación de un Plan Estratégico de largo plazo que contemple la posibilidad de realizar

diversas pruebas piloto con distintos prototipos. Se trata de un tema muy sensible y que sería fácil de interpretar como un acto arbitrario.

Una parte muy importante de la implementación del voto electrónico y que hasta el momento viene estando ausente en todas las pruebas realizadas y que en la implementación de un Plan Estratégico, debe significar el primer paso, es la materialización de padrones electorales actualizados y actualizables de manera permanente mediante la incorporación de las TIC.

Los diferentes autores consultados, consideran de fundamental importancia contar con padrones electorales genuinos y depurados que puedan garantizar la ausencia de históricos cuestionamientos como la existencia de electores fallecidos, errores en la documentación registrada, domicilios no actualizados, etc.

Al respecto, Patricio Lorente en [1; pág. 85], menciona lo siguiente:

… El desarrollo de mejores padrones y con mayor nivel de actualización es una necesidad más apremiante que la incorporación de urnas electrónicas. Un padrón más exacto facilitaría el rediseño de circuitos electorales más pequeños, acercando el lugar de votación al ciudadano. En la provincia de Buenos Aires la mayor parte de los circuitos electorales se mantienen igual desde hace más de cincuenta años. Muchas áreas rurales que por su escasa población daban lugar a circuitos electorales muy extensos se han transformado en áreas urbanas desde hace décadas sin que se haya modificado la geografía electoral; hoy tienen padrones de decenas de miles de lectores que deben movilizarse a sitios de votación alejados de su hogar.

Por su parte, María Inés Tula, en [7; pág. 30], refiere lo siguiente:

… Es altamente recomendable que el cambio del sistema de votación manual por un de tipo electrónico esté precedido por la modernización en la producción, verificación, y manejo de documentación básica utilizada en el acto electoral. Este proceso facilitará la incorporación gradual de nueva tecnología. Por otra parte, y específicamente para el caso argentino, la conformación de los registros electorales con bases computarizadas permitirá la “limpieza” de éstos, es decir, la actualización permanente de las altas, defunciones y cambios de domicilio y, en consecuencia, terminará con distorsiones tales como los “padrones inflados”.

Eduardo Pasalacqua, en [7; pág. 83], aporta lo siguiente:

… cualquier intento de reforma, mejora o modernización electoral no puede prescindir, bajo riesgo de terminar en un frustrante fiasco, del imprescindible cambio sustantivo en la confección, emisión, mantenimiento, actualización y depuración de los padrones.

3. Consideraciones de seguridad

A continuación se desarrollarán algunos aspectos de seguridad que, según los distintos autores, deben tenerse en cuenta para evaluar la incorporación de tecnología en los procesos electorales.

3.1. Confidencialidad

El secreto del voto es uno de los principales atributos del método de elección contemplado en la legislación vigente y por lo tanto una característica que debe garantizarse a lo largo de todo el proceso electoral.

Cualquier sistema de elección debe garantizar que no es posible establecer la relación entre voto y elector. Para ello, la verificación de identidad del elector debe efectuarse en la forma manual tradicional, o en dispositivos totalmente aislados de los de votación.

Esta característica está presente en los sistemas de lectura óptica de marcas en boletas pre-impresas o en los sistemas de boletas de voto electrónico. No obstante, es importante asegurar que no es posible reconstruir el orden de lectura de las boletas en los primeros y que no se imprime o graba ninguna información de secuencia en los segundos.

Posteriormente veremos que en los sistemas de boleta de voto electrónico se requiere grabar junto con la elección del votante, un número único aleatorio para control de duplicidad durante el recuento de sufragios.

En relación a este tema, Pedro A. Dourado de Rezende, uno de los principales referentes sobre voto electrónico en Brasil, en [1; pág. 97], aporta lo siguiente:

> En elecciones secretas, en las cuales la identidad del votante no puede ser vinculada a su voto durante la votación ni durante el escrutinio, la eficacia del proceso de fiscalización se torna sensible al soporte que registra materialmente cada voto. En consecuencia, si el proceso

de votación electrónica desmaterializa el voto, registrándolo –a cada voto o a sus sumas parciales– sólo digitalmente, la eficacia de cualquier proceso de fiscalización se ve anulada. Anulada en el sentido de que cualquier medida para detectar o impedir fraudes de origen interno (colusiones entre un organizador y alguna candidatura) servirá también para proteger a los defraudadores externos, fiscales de candidaturas empeñados en sabotear (anular una elección perdida) o subvertir la fiscalización (contaminar el sistema con mecanismos de fraude). Al mismo tiempo, cualquier medida para detectar o impedir sabotaje o subversión del resultado final en la fiscalización protegerá también a los defraudadores de origen interno que tengan privilegios de acceso para programar, controlar u operar el sistema. Se trata de la incongruente lucha ente espías y contra-espías, que une los sentidos legítimos e ilegítimos de la seguridad.

Quien como ciudadano no se preocupa por el riesgo de que la seguridad legítima sea, bajo algún pretexto, arrollada por la ilegítima, no valora la democracia o, en el fondo, no la acepta. Y quien, como científico, desee estudiar sus mecanismos, debe separar tal conocimiento y creencias de los problemas y límites inherentes a los mismos. Así fue que el estudio científico de esos límites alcanzó un marco importante con la tesis de doctorado de la Dra. Rebecca Mercuri, defendida en la Universidad de Pensilvania (EUA) en el año 2000. Su tesis muestra que la inviolabilidad del secreto del voto y la garantía del correcto escrutinio –garantía que niega el segundo sentido de más arriba– son propiedades excluyentes en los sistemas puramente electrónicos. En otras palabras: en una elección procesada sólo electrónicamente, es imposible asegurar a la vez el secreto del voto y la corrección del escrutinio, pues en ella tales protecciones son como fases opuestas de una misma moneda. Moneda que corresponde al sistema electrónico puro, cuyo valor corresponde al proceso electoral que el sistema ejecuta, pero moneda que no se puede “girar” durante una elección para poder ver sus dos lados, pues el proceso es ejecutado sin posibilidad de auditoría.

El peso de estos argumentos científicos pasó a reflejarse, bajo presión de movimientos civiles fortalecidos por la dudosa ética de los proveedores de sistemas electrónicos puros, en la legislación electoral norteamericana. Entre marzo de 2004 y mayo de 2005, 14 estados federales aprobaron leyes que obligaban a las máquinas electrónicas de votación a emitir un voto impreso y verificable por el elector, para mantener o recuperar capacidad de auditoría del proceso electoral anterior a las computadoras. Hoy[2] 19 estados ya tienen leyes de este tipo aprobadas, 3 están esperando ser sancionadas, 17 tienen proyectos en trámite y solamente 12 no ven problemas en usar máquinas del tipo que Brasil usa hoy[3]. Por otro lado, en el Congreso están siendo tramitadas hoy casi una decena de proyectos exigiendo el voto impreso verificable por el elector como parte del principio federal de organización democrática en los EEUU. La

[2] Año 2008

[3] Las máquinas utilizadas por Brasil son del tipo RED

idea no es, ingenuamente, la de acabar con los fraudes, pero sí la de hacer que sus posibles formas sean más difíciles, costosas y arriesgadas en igual medida, exponiéndolas al riesgo de ser comprobadas a tiempo y por electores comunes, incluso aquellos que no tienen doctorados en seguridad informática.

Por su parte el Dr. Alejandro Prince, en [3; pág. 13], aporta lo siguiente:

Los sistemas de voto electrónico deben garantizar el anonimato, la privacidad y la no coerción al momento de emitir el sufragio. Es decir, los ciudadanos deben poder votar en total libertad y privacidad, sin que su identidad pueda ser vinculada al voto. La forma más práctica de garantizarlo consiste en separar –física y electrónicamente– el registro de votantes del proceso de recolección.

En este sentido un modelo destacado es el que se emplea en Bélgica donde el votante se identifica en la mesa y recibe la tarjeta magnética; con ésta se dirige a la cabina de votación, vota, y deposita la tarjeta en la urna. En el caso brasilero ocurre lo contrario, ya que la identificación del elector y la votación son realizadas en la misma urna, levantando sospechas sobre la quiebra del anonimato.

Ingo Boltz y Federico Centeno Lappas, en [7; pág. 292], refieren sobre el secreto del voto lo siguiente:

El carácter secreto del voto es la garantía de protección de la libre decisión del elector. En argentina, este principio también se introdujo con la Ley Sáenz Peña y está garantizado por el Colegio Electoral Nacional, que prevé una pena de tres meses a tres años a quien utilizare medios tendientes a violar el secreto del sufragio (artículo 141). También constituye una obligación guardar el secreto del voto durante toda la jornada electoral. Se prevé una pena de uno a dieciocho meses de prisión para quien revelase su voto en el momento de emitirlo (artículo 142).

El secreto del voto guarda estrecha relación con el requisito técnico de la *privacidad* del acto electoral, que se refiere a que no puedan conocerse las preferencias electorales de los votantes. Este punto es de suma importancia ya que está íntimamente ligado con las viejas prácticas clientelares como la compra y venta de votos. Según Cranor (1996), “[…] los ciudadanos pueden vender sus votos si son capaces de mostrar al comprador que han efectivamente votado de acuerdo a la voluntad de éste. De igual manera, aquellos que utilizan la extorsión como método para forzar el sufragio de los ciudadanos no tienen éxito si no tienen una prueba física de ello”.

En relación a la compra y venta de sufragios aportan lo siguiente:

… La ausencia de un comprobante físico del sufragio podría mejorar la privacidad o secreto del voto dado que, en su mayoría, el esquema para la compra y venta de los sufragios o los mecanismos conocidos de coerción requieren de una prueba (se marca el sobre donde se introduce el voto, o bien, se usan boletas distribuidas previamente por el puntero). En definitiva, la idea es poder identificar al ciudadano con su voto, pero si no hay comprobante físico es cierto que este esquema se rompe. Así, con un sistema de votación electrónica *correctamente diseñado*, es imposible conectar a un votante con su voto y, en consecuencia, la votación electrónica podría considerarse más secreta que la tradicional.

Como hemos visto hasta aquí, la manera más segura de garantizar el secreto del voto es no vincular en el proceso de voto electrónico las instancias de identificación del votante con la de emisión del sufragio. Esto podría resolverse manteniendo la identificación del votante en la forma manual tradicional en la mesa de votación, no registrando ningún dato que refiera orden u hora de votación.

Por otro lado, la ausencia de un comprobante físico del voto, si bien garantiza la imposibilidad de identificar el voto con el votante, anula completamente la posibilidad de auditar el acto eleccionario lo cual podría ayudar a la concreción de numerosos fraudes.

Es imprescindible entonces, contar con un comprobante físico del sufragio para permitir auditar el acto eleccionario y al mismo tiempo para que el votante pueda comprobar que su elección fue correctamente capturada y registrada.

Cabe aclarar, que bajo ningún aspecto se considera apropiada la emisión de un “recibo” para el elector como comprobante de su voto, similar al que entrega un cajero automático, ya que este podría servir como elemento de prueba para la compra o venta de sufragios.

Las consideraciones expuestas en este capítulo pueden verse sintetizadas en lo que Michael Ian Shamos [6], planteó como los mandamientos a tener en cuenta para evaluar cualquier sistema de voto electrónico:

I. Se deben mantener secretas las opciones de cada uno de los votantes.

II. Se debe permitir que cada votante vote una sola vez, y sólo para aquellos cargos para los que está en condiciones de emitir su voto.
III. No debe permitirse ninguna alteración ni manipulación del sistema de votación ni el intercambio de votos por dinero.
IV. Se debe informar con exactitud de todos los votos.
V. El sistema de votación deberá permanecer en funcionamiento y operable a lo largo de cada elección.
VI. Se deberá mantener un comprobante de auditoría para detectar violaciones contra los mandamientos II al IV, pero ese comprobante no debe violar el mandamiento I.

Según el autor, los tres primeros mandamientos son los fundamentales, mientras que los restantes pueden admitir alguna flexibilidad, en la medida que no cambien el resultado de la elección.

3.2. Integridad

Otro atributo de importancia que debe tenerse en cuenta para la aplicación de las TIC en los procesos electorales es el correcto registro y contabilización de los sufragios y la posibilidad de auditar los resultados.

Para poder verificar el correcto registro y contabilización de los sufragios es determinante poder efectuar controles previos tanto del hardware como del software, a fin de detectar y corregir diferentes errores.

En relación a las verificaciones sobre el software es interesante la opinión de Alfredo Daniel Rezinovsky de la Facultad de Ingeniería de la Universidad Nacional de Cuyo, en [1; pág. 70]:

> … Las computadoras fallan y son vulnerables, todos lo sabemos. Sistemas hechos por empresas con 30 años de experiencia en sistemas operativos fallan y son vulnerados pocos días después de salir a la venta. Incluso en sistemas de código abierto se descubren a veces fallas que llevan años en los programas. El atractivo de atacar un sistema de voto electrónico hace además que las medidas de seguridad a las que estamos acostumbrados sean obsoletas. La teoría de control de calidad de software explica que sólo podemos garantizar que hay fallas si las encontramos, pero no podemos garantizar la ausencia de las mismas al no encontrarlas.

Si en lugar de fallas se trata de vulnerabilidades intencionales encontrarlas se hace aún más difícil.

Recientemente se han detectado fallas en sistemas de voto electrónico usados en EEUU por los cuales algunos votos “desaparecían” al trasladar los datos. Estas fallas estuvieron ahí durante más de 10 años y nadie las vio. Y lo que es peor aún, nunca vamos a saber cuántos ni cuáles votos se perdieron en elecciones reales usando esos equipos.

Por último añade:

¿Se puede hacer sistemas de voto electrónicos seguros? Probablemente sí. ¿Puede alguien verificar que lo son? No. Esa incertidumbre hace que se pierda completamente el control por parte del votante, por parte de los auditores y por parte de los técnicos...

También se destaca el aporte realizado por Ingo Boltz y Federico Centeno Lappas en [7; pág. 299]:

Asegurar que el software funcione con “exactitud” no es un problema exclusivo del voto electrónico, sino que existe una amplia gama de operaciones tales como bancarias, bursátiles, comerciales, turísticas, etcétera, que lo hacen bajo esta modalidad, es decir, aplicando tecnología. Si este funciona incorrectamente, podría ocasionar graves consecuencias para los negocios que se desarrollan y es, precisamente, con el objeto de evitar estos problemas que las industrias se aseguran de que su software funciones de manera confiable, mediante un cuidadoso diseño y proceso de auditoría.

El diseño de un software que funcione correctamente y no tenga errores es un arte en sí mismo, sobre el que se han escrito numerosos libros que escapan a los límites de este trabajo. No obstante ello, existen ciertos lineamientos estandarizados respecto de la elaboración de programación sólida, como las normas ISO/IEC 90003:2004. Lo importante a destacar aquí es que cada organización que labora software para elecciones y pretenda elaborar un producto de alta calidad desde el comienzo, debería contar con severos y agudos procesos de revisión que incluyan varias pruebas del software.

Al respecto, es importante destacar que hasta el software diseñado con el mayor de los cuidados es susceptible de contener errores y puntos débiles que puedan ser percibidos y usados por los *hackers*. Aún más, los buenos procesos de programación no protegen contra las manipulaciones intencionales llevadas a cabo por personas internas al proyecto como, por ejemplo, un empleado descontento que programe una disfunción para así dañar o humillar a su empleador, o un programador corrupto que alterando el software bancario transfiera fondos de

otras personas a su cuenta personal. Estas irregularidades pueden ser advertidas sólo con una profunda auditoría del software.

En una auditoría de esta clase, expertos en programación externos (que no sean los programadores que se encuentran trabajando en el software) examinan el programa (más específicamente el código fuente) buscando errores, fallas de seguridad y manipulaciones intencionales. En caso de encontrar algo, describen estos errores y envían el software nuevamente a los programadores, a fin de que éstos solucionen las fallas detectadas. Una vez que se han realizado estas correcciones, el software es auditado nuevamente y en el caso de que se detecten los mismos errores u otros nuevos, se lo devuelve otra vez para su tratamiento. Solo cuando no se encuentran más errores, fallas de seguridad o irregularidades, el software es certificado como correcto y seguro.

El procedimiento de auditar un software es una tarea dificultosa y si a esto se le suma la complejidad de los programas de los sistemas de votación electrónica debido a su gran magnitud, la tarea es doblemente dificultosa. Por ejemplo, el sistema de votación electrónica AccuVote TS, elaborado por la compañía estadounidense Diebold, contiene aproximadamente 285.000 líneas de código fuente (RABA, 2004); el sistema de Diebold/Procomp utilizado en Brasil contiene 3 millones de líneas de código fuente (Rezende, 2004). La localización de errores en semejante cantidad de datos es como buscar una aguja en un enorme pajar. Como si esto fuera poco, un programador mal intencionado podría trabajar escondiendo y camuflando todas sus manipulaciones, lo que dificulta doblemente la tarea de encontrar el *malware*.

Dada esta gran dificultad es que muchos expertos afirman que un auditor nunca puede garantizar en un ciento por ciento la seguridad del software que ha verificado. Ken Thompson, un veterano en seguridad informática, señala por ejemplo, “nunca puede uno fiarse de un código que no ha sido escrito por uno mismo […] ninguna verificación o escrutinio que se realice a nivel de las fuentes, por más rigurosa que sea, lo protegerá a uno de utilizar códigos no fiables […] un código maligno, bien instalado y escondido será casi imposible de detectar” (Thompson, 1984). Coinciden con esta afirmación, Neumann (1993) y Mercuri (1993, 1995), otros dos prestigiosos especialistas en votación electrónica.

En el mejor de los casos, los auditores requerirán para su trabajo mayor disponibilidad de tiempo y acceso libre y completo a todo el código fuente, a fin de llevar a cabo su tarea con la mayor eficiencia y eficacia posible.

Como corolario, el precio a pagar por el uso de máquinas de votación electrónica trae una indefectible pérdida de transparencia en el proceso electoral: ni una auditoría exhaustiva, ni el control por parte de observadores garantiza la seguridad del software. La transparencia deja de ser un atributo custodiado por cada elector, como ocurre con el sistema de voto tradicional

manual, pasando a depender exclusivamente de la capacidad y buenas intenciones de un reducido grupo de expertos.

Los autores citados precedentemente aportan conceptos adicionales, en [7; pág. 301], sobre la fiabilidad del software de los sistemas de votación electrónica.

Una elección significa un reparto institucional del poder, por lo tanto, ganar una elección representa una tentación muy fuerte para adulterar el software a fin de "inclinar la balanza" a favor.

Respecto de este punto, Neumann (1995) sostiene: "Las oportunidades para alterar las elecciones [electrónicas] son ilimitadas, incluyendo la instalación de trampas y caballos de Troya –simples juegos de niños para vendedores y funcionarios electorales con el conocimiento suficiente– […] el fraude puede tener lugar aún sin cambios en los códigos fuente; por lo tanto, el análisis de los códigos no es suficiente para garantizar la ausencia de caballos de Troya". Mercuri (2002) concuerda con Neumann, y señala que "[ningún] análisis que se haga del sistema antes, durante o después de las elecciones, no importa su profundidad, [es] suficiente para asegurar que dichos problemas [tales como: el fraude, la falla de los equipos o la programación errónea] no tuvieron ni tendrán lugar. Esto se debe, en parte, a la tarea de por sí insoluble de que los programas basados en computadoras no cuenten con características adicionales desconocidas".

Como hemos visto ya, no solo las auditorías no son 100% efectivas sino que hay muchos otros posibles ataques al sistema de votación que pueden alterar a un sistema ya auditado. Las auditorías de software no protegen contra este tipo de acciones, lo que nos permite concluir que *por sí mismas no son suficientes* para garantizar seguridad ni transparencia en las elecciones con urnas electrónicas.

Una manera de contrarrestar este defecto es *verificando* los resultados del sufragio electrónico y para esto se necesita un registro de la votación que se genere *independientemente* del sistema electrónico. De esta manera, si el sistema de votación electrónica ha sido manipulado, se podrá comparar ambos resultados (el que arroja la urna electrónica con el registro independiente).

A diferencia de lo que ocurre con el sistema tradicional, donde el recuento de los votos es manual y, en consecuencia, susceptible de comprobación (ante la duda sobre los resultados finales puede solicitarse a la autoridad competente un nuevo recuento de los votos), en la

votación electrónica con sistema RED no hay boletas impresas (aunque han empezado a incorporarlas) y, por lo tanto, no queda registro físico de su sufragio.

Ahora bien, si la máquina hace un registro inexacto del voto (ya sea por error o manipulación) éste no puede ser corregido por el elector dado que desconoce lo que está ocurriendo con su sufragio. Los *bits* erróneos almacenados dentro de la computadora resultan anónimos porque el votante no puede demostrar cómo votó. Por lo tanto, el voto defectuoso será contabilizado sin posibilidad de verificación o corrección.

Finalmente, en [7; pág. 302], los autores fundamentan la importancia de contar con un comprobante de votación que permita auditar los resultados electorales:

Aceptar la posibilidad de que nunca se podrá estar 100% seguro de que el sistema registrará con exactitud la elección de un votante, es aceptar un sistema que viola uno de los principios fundamentales de las elecciones democráticas, como es su integridad. Para salvar este problema, se propone la necesidad de que haya un comprobante de votación que sirva como control en caso de que se hayan detectado errores o manipulaciones y se requiera un segundo recuento de votos.

El comprobante de votación VVPT (Voter Verified Paper Trail), conocido también como Método Mercuri en alusión a su creadora, Rebecca Mercuri, tiene como fin agregar a los sistemas de votación electrónica la posibilidad de comprobación y de otorgar mayor transparencia a través de boletas impresas pero, al mismo tiempo, tratando de evitar las debilidades del sistema en lo que respecta a privacidad.

En sus propias palabras: “La combinación de falta de estándares, los vacíos legislativos, el secreto comercial, los problemas en el uso, la privacidad, la seguridad, y otros asuntos inherentes a las computadoras resultan en una extraña mentalidad de ‘confía en nosotros’. La transparencia es esencial durante este proceso, no sólo a fines de hacer posible la auditoría, sino también para mejorar la confianza de los votantes. Esto puede ser alcanzado, de manera muy sencilla, mediante la utilización de comprobantes de votación que puedan ser posteriormente utilizados en los recuentos”.

Un sistema de voto electrónico con VVPT Mercuri está equipado con una impresora. Luego de que el votante haya seleccionado su voto (ya sea mediante tacto sobre una pantalla o presionando un teclado) la impresora emite un comprobante que señala la selección efectuada por el elector. Si está de acuerdo, lo confirma y esta boleta cae en una urna sellada en donde quedará como prueba en caso de ser necesario para recuento posterior. Si, por el contrario,

observa que no es lo que marcó, puede cancelarlo y el comprobante es impreso con una nota que lo identifica como “no válido” y también cae en la misma urna. El voto electrónico de este elector también se cancela y puede volver a sufragar. Solo cuando el votante confirma lo indicado por el comprobante se contabiliza el voto.

Es importante destacar que durante todo este proceso el elector puede ver su sufragio (a través de un vidrio que cubre la urna externa) pero no tocarlo ni llevárselo con él (evitando también la compra/venta de votos a partir de la prueba física del voto) (Mercuri, 2002).

En el caso de que surgieran dudas luego de una elección, las urnas selladas pueden ser abiertas y se puede efectuar un recuento paralelo manual. Como el votante ha visto *con sus propios ojos* el comprobante y ha confirmado su validez, éste será la mejor representación de su voluntad y tendrá prioridad sobre el voto digital.

La combinación de buenos procesos de desarrollo de software, auditorías profundas y detalladas, juntamente con un comprobante de votación que sirva como medio para verificar los resultados de los comicios pueden proveer un nivel relativamente alto de transparencia. La presencia de estos tres aspectos debería ser exigida junto con otras medidas de seguridad más tradicionales y, en este caso, las elecciones electrónicas podrían ser consideradas más seguras.

La particularidad de los sistemas desarrollados para voto electrónico, a diferencia de otros radica en que los errores y vulnerabilidades detectados posteriormente a su utilización en un acontecimiento real, si bien pueden ser corregidos para una próxima utilización, poco puede hacerse en relación al acto eleccionario concluido.

Por un momento imaginemos el impacto negativo que tendría sobre los sistemas de voto electrónico, la situación en donde los resultados del escrutinio provisorio, por el voto electrónico, difieren del escrutinio definitivo de tal manera que los candidatos que resultaron ganadores de la elección fueran otros que los indicados inicialmente. Muy probablemente podría ocurrir lo que determinó que el gobierno de Holanda el 16 de Mayo de 2008, tomara la decisión de retornar a los sistemas tradicionales de votación con boletas de papel para lectura de marcas. Esto fue debido a que las fallas y errores presentados por los sistemas de voto electrónico del tipo de registro electrónico directo utilizados hasta ese momento determinaron la pérdida de confiabilidad en los mismos. Situaciones

similares se podrían presentar en otros países de Europa como Alemania Francia e Irlanda [10].

Algunos autores han tratado de determinar algún criterio para medir la confiabilidad de los sistemas de voto electrónico. Al respecto un grupo de trabajo de especialistas convocado por el instituto NIST en 2006 concluyó que no conocían ningún criterio medible para determinar la confiabilidad de dichos sistemas. Posteriormente en 2007, acordaron definir un criterio que resulta adecuado: un sistema de voto electrónico es confiable si el resultado correcto de la elección es independiente del software utilizado.

En relación a este criterio, Federico Heinz en [1; pág. 91], aporta lo siguiente:

> A lo que el NIST se refiere con “independencia del software” no es a la construcción de urnas que se comportarán correctamente sin importar si el programa contiene errores o código malicioso (lo que sería imposible), sino de urnas que ofrezcan un mecanismo que permita calcular el resultado sin necesidad de recurrir al software. En otras palabras, una urna que lleve la contabilidad doble de los votos: una interna, digital, que es la que el software usa para calcular sus resultados, y otra externa, analógica y legible por seres humanos sin asistencia técnica, que permite hacer un recuento independiente a mano.
>
> Esta posibilidad es la que nos permite verificar, aún luego de realizado el comicio, si la urna se comportó correctamente o no: basta con tomar un muestreo aleatorio estadísticamente significativo de todas las urnas, y hacer un recuento manual. Si el resultado de todas las urnas auditadas es correcto, entonces podemos asegurar con alto grado de confianza que el resultado en todas las demás también debe haberlo sido. De lo contrario, debemos descartar el resultado calculado automáticamente, y recontar todos los votos a mano. Afortunadamente, y a diferencia del caso de la urna electrónica sin registro paralelo, este recuento puede ser engorroso, pero al menos es factible.
>
> Un ejemplo de tal sistema son los dispositivos de automatización del escrutinio, aquellos en los que el votante hace marcas sobre una boleta de papel que deposita en una urna, que los fiscales luego abren y recuentan pasando las boletas por la máquina. En este caso, las boletas de papel ofrecen un mecanismo alternativo de recuento. Otro ejemplo son las urnas electrónicas provistas de impresoras de boletas, en las que la boleta impresa también ofrece un respaldo razonable para el recuento, pero aquí hay que hacer la salvedad de que,

dado que en éstas es la urna misma la que produce las boletas, existen posibilidades de ataque de demostrada eficacia en las que la urna facilita la vinculación de cada votante con su voto, o en las que la misma urna invalida boletas correspondientes a votos genuinos y emite votos falsos para reemplazarlos.

Al respecto es posible concluir que el criterio de independencia del software implica utilizar el equipamiento de voto electrónico como un dispositivo que facilite la contabilización de los votos pero la confiabilidad del sistema continúe depositada en la posibilidad del recuento manual.

Otra etapa importante luego de la validación del software es la que corresponde a la distribución o inseminación del software.

La importancia de esta etapa radica en inseminar, en todas las máquinas de votación, copias idénticas del software validado para lo cual podrían emplearse métodos tradicionales de auditoría o emplear algunos mecanismos de seguridad.

En el primer caso, los partidos políticos designan a fiscales informáticos para que junto con especialistas de universidades nacionales y de organismos veedores electorales soliciten a la autoridad electoral la selección al azar de una determinada cantidad de máquinas para su análisis antes del inicio del acto electoral. También podría repetirse esta operatoria con otro grupo de máquinas al concluir el acto electoral.

Como mecanismo de seguridad para proteger el software previamente validado contra posibles alteraciones, es posible utilizar técnicas de firma digital para asegurar tanto la integridad como la certificación de origen.

3.3. Disponibilidad

Una vez concluido el acto electoral, se debe proceder a contabilizar los votos, los cuales, dependiendo del sistema, podrán obtenerse directamente de los registros de las máquinas de votación, del recuento automático o del

recuento manual. En los últimos dos casos se consideran únicamente sistemas de recuento automático con impresión de comprobantes de voto o de boletas de voto electrónico.

A los efectos de considerar situaciones que requieran hacer frente a una contingencia, aquellos sistemas donde el recuento de los votos se realiza al concluir el acto electoral, presentan una ventaja considerable frente a los que llevan el recuento durante éste. Una falla que impida el normal funcionamiento de una máquina de votación de este último tipo, derivará indefectiblemente en la realización de un recuento manual de los votos. Por otro lado, en los sistemas mencionados en primer lugar, podría considerarse la posibilidad de repetir el recuento de los sufragios en forma automática tantas veces como lo estimen necesario las autoridades de mesa, ya que las máquinas solo funcionarían como un soporte para facilitar el recuento y registro de los votos.

En cualquiera de los casos, se podrá contar con totales por mesa electoral tanto en formato digital como en papel.

Para la transmisión de los datos en formato digital se podrán emplear esquemas de firma digital a fin de resguardar su integridad. Por lo tanto, para la transmisión de esos datos podrán emplearse diferentes vínculos sin importar la seguridad de los mismos, pudiendo utilizarse desde HTTPS o VPN hasta el envío de correo electrónico utilizando dispositivos móviles.

3.4. Consolidación

En relación a la consolidación de los resultados de las distintas mesas electorales, se deberán concentrar en una única sede del Comando Nacional Electoral a fin de evitar posibles manipulaciones de los datos, el cual deberá contar con planes de contingencia a fin de asegurar la disponibilidad de la información a todos los interesados.

Para garantizar la transparencia en el proceso de consolidación de datos, se deberá facilitar la verificación de los datos registrados a nivel de cada mesa de votación, a fin de que cada autoridad de mesa y cada fiscal partidario puedan auditar dichos datos con los obtenidos al finalizar la contabilización y cuyo respaldo impreso obtuvieron de las máquinas de votación.

Una vez auditados los resultados de todas mesas electorales, restará validar los resultados totales por distrito, para lo cual bastará con que los partidos políticos y los organismos nacionales de fiscalización, puedan bajar estos resultados a sus respectivos sistemas de consolidación de datos electorales y luego de procesarlos los comparen con los resultados totales informados por el Comando Nacional Electoral.

El sistema de consolidación de datos electorales deberá brindar información en tiempo real sobre el estado del escrutinio a fin de que pueda ser seguido por la población en general. Muestra de ello fueron los últimos procesos electorales en los cuales fue posible acceder vía Internet a distintos niveles de información.

4. Conclusiones

Antes de comenzar a analizar las ventajas y desventajas de los distintos sistemas y los resultados de las experiencias electorales de voto electrónico en nuestro país, para determinar las posibilidades de aplicación de las TIC a nuestro sistema electoral, es importante tener presente que en Argentina no se han producido los problemas de fraude generalizado que en Brasil, Paraguay y Ecuador produjeron el desgaste y el descrédito del sistema tradicional de emisión del voto y derivaron en la implementación del voto electrónico.

En tal sentido, María Inés Tula en [7; pág. 27] señala que:

…, a diferencia de otros países latinoamericanos, en la Argentina las experiencias de aplicación de voto electrónico y los debates en torno de su adopción generalizada no se produjeron en un contexto de comicios viciados o cuestionados que reclamaba una imperiosa necesidad de cambio…

Asimismo, Alejandro Tullio en [7; pág. 50] aporta lo siguiente:

… la decisión de cambiar el sistema de votación hacia mecanismos electrónicos debe apuntar a mejorar un sistema cuyo rendimiento objetivo es altamente aceptable. Nuestro país[4] no enfrenta los problemas que hicieron necesario el voto electrónico en Brasil o Paraguay, o lo hacen deseable en Ecuador.

En relación al descreimiento y desconfianza en los procesos electorales tradicionales de los países de la región, que motivaron cambios profundos en la legislación vigente e impulsaron como parte del mismo la aplicación del voto electrónico, es importante destacar la encuesta publicada en 1998 y mencionada por María Inés Tula en [7; pág. 23] en la que en países como Chile, Uruguay y Argentina las elecciones eran consideradas “limpias” por el 68% o más y “fraudulentas” por menos del 19% de los encuestados. Como contraste, en países como Brasil, Venezuela, México y Paraguay las elecciones eran

[4] Argentina

consideradas “limpias” por menos de 23% y “fraudulentas” por más del 69% de los encuestados.

Al respecto, María Inés Tula en [7, pág. 25] señala:

> Para marcar el contraste, cabe señalar que en los países que hacia los años noventa registraban los niveles más bajos de cuestionamiento hacia las elecciones, como Uruguay y Chile, no se introdujeron reformas relativas a los órganos de administración y control de los comicios, ni tampoco se adoptaron mecanismos electrónicos de votación (aunque sí se efectuaron cambios en los procesos de transmisión de resultados preliminares).
>
> En pocas palabras, en las democracias latinoamericanas las presentaciones de voto electrónico tuvieron como escenario común un contexto de descreimiento y desconfianza generalizados hacia las consultas electorales. Las reformas políticas que incluían entre sus principales puntos la adopción del voto electrónico sirvieron así para mostrar una fuerte señal de cambio, un claro y enérgico gesto de las autoridades públicas orientado hacia el objetivo de que las elecciones ganasen en credibilidad y confiabilidad, que se imponía a cualquier otro tipo de cálculo respecto de los costos y riesgos que implicaba tal operación. Pero más allá de esta particular situación, en otros países de la región –claramente en Chile y Uruguay–, las iniciativas pro voto electrónico no existieron o bien no lograron una adhesión significativa ni entre la dirigencia política ni entre organizaciones de la sociedad civil.

Por lo tanto, la implementación del voto electrónico en nuestro país, al igual que en Chile y Uruguay, no puede verse como la solución a problemas que hasta el momento no se han manifestado de manera generalizada.

Solo con la aplicación gradual de un Plan Estratégico de largo plazo que se adecúe a nuestra realidad y que contemple únicamente las actuales necesidades de mejora de nuestro sistema electoral, se podría evitar el fracaso de la aplicación de las TIC como viene ocurriendo en algunos países de Europa.

En tal sentido, la primera etapa de aplicación de las TIC debería ser sin lugar a dudas, la creación de un sistema de confección y mantenimiento de padrones electorales que asegure contar en todo momento y en tiempo real de información actualizada, confiable y auditable por los distintos partidos políticos y fundamentalmente por el propio ciudadano. Cualquier implementación al

respecto debería facilitar el cumplimiento del mandamiento de Shamos que refiere que cada votante debe votar una sola vez, y sólo para aquellos cargos para los que está en condiciones de emitir su voto.

La situación actual de padrones no actualizados con datos poco confiables, los que solo pueden consultarse en breves períodos previos a los actos eleccionarios, solo conduce a los típicos reclamos como: existencia de ciudadanos fallecidos o sorprendentemente longevos, números de documento erróneos o duplicados, falta de actualización de tipos de documento y de domicilios, solo para mencionar algunos.

En una etapa posterior, podrían mejorarse los métodos de identificación de los ciudadanos, utilizando desde la lectura óptica de los números de documento, por ejemplo con caracteres OCR, código de barras o código UPCODE, hasta el empleo de métodos biométricos como lectura de huellas dactilares, reconocimiento facial, de retina, de la palma de la mano, entre otros.

Solo después de avanzar en la aplicación de las TIC sobre los padrones electorales se podría iniciar el proceso de incorporación de tecnología informática al acto eleccionario propiamente dicho.

A partir de esta instancia, se debería tener en cuenta que habría que cambiar el actual sistema de boletas pre impresas ya que las mismas no poseen ningún elemento que permita su lectura o captura. Este cambio tendría un significativo impacto ya que haría frente a uno de los problemas ampliamente denunciados en los últimos actos electorales como es la sustracción de boletas pre impresas de los cuartos oscuros, dando lugar, en algunos casos, a que los ciudadanos no pudieran ejercer su voluntad de elegir libremente a los candidatos.

Para comenzar, se deberían establecer algunas premisas a tener en cuenta para determinar cómo y de qué manera se incorporarían las TIC, teniendo presentes algunos de los mandamientos que Michael Ian Shamos planteó en 1993, indicados en el capítulo Confidencialidad del presente trabajo.

En primer lugar se debería mantener en todo momento una separación entre voto y votante, por lo que se debería dejar de lado cualquier equipamiento que pueda fijar o reconstruir, por algún método, esta relación.

Otro elemento a tener en cuenta es que en ningún caso el elector debería conservar y retirar del lugar de votación comprobante alguno que pueda indicar su elección, aún cuando éste podría considerarse como una forma de auditoría del registro de su voto. Un tipo de comprobante como el indicado podría dar lugar a manipulación o compra de votos.

Con el fin de permitir auditar los resultados electorales, se debería contar con un respaldo impreso del voto emitido por el elector, el cual debería poder ser verificado y validado antes de ser entregado o depositado en la urna ya sea en forma manual o automática.

De esta manera se descartarían todos aquellos dispositivos del tipo de registro electrónico directo que no emiten comprobantes de voto. Asimismo, con el fin de facilitar su lectura tanto por parte de los votantes como por las autoridades de la mesa electoral, se considerarían poco apropiados aquellos equipamientos que entregan comprobantes impresos en tiras de papel similares a los que entregan los cajeros automáticos.

Con el objeto de facilitar el acceso a los sistemas de votación de personas con capacidades diferentes, éstos deberían contar con accesorios tales como auriculares, teclados Braille y soportes con identificación Braille para boletas pre impresas con espacios reservados para marcas.

Para analizar otros casos, como el de personas con movilidad reducida y que no puedan llegar hasta los lugares de votación, se debería tener en cuenta lo establecido en el Código Electoral Nacional de Argentina [2] que en su artículo 86 dice lo siguiente:

> … Los electores podrán votar únicamente en la mesa receptora de votos en cuya lista figuren asentados…

Por su parte, el artículo 94 establece que:

… Las personas que tuvieren imposibilidad concreta para efectuar todos o algunos de los movimientos propios para sufragar, serán acompañados por el presidente de la mesa al cuarto oscuro, donde a solas con el ciudadano elector, colaborará con los pasos necesarios hasta la introducción del voto, en la medida que la discapacidad lo requiera.

Finalmente el artículo 12 enumera quienes quedan exentos de la obligación de votar, entre los que se citan:

… d) Los enfermos o imposibilitados por fuerza mayor, suficientemente comprobada, que les impida asistir al acto…

Como se puede ver, la legislación actual considera los casos de personas con movilidad reducida pero como se trata de un acto que requiere de la presencia física del elector, no contempla la posibilidad de que emitan su voto aquellas personas que no puedan movilizarse hasta el lugar de votación establecido.

Una manera de tener en cuenta la recomendación del NIST referida a la independencia del software indicada en el capítulo Integridad del presente trabajo, podría ser la de realizar el conteo o tabulación de los sufragios luego del cierre de los comicios, y no durante el desarrollo de los mismos. De esta forma, el dispositivo electrónico solo se utilizaría para agilizar el proceso de contabilización de votos, pudiendo repetirse esta operación las veces que se requiera, teniendo como requerimiento de control evitar la doble imputación de un mismo comprobante o boleta. Para lo cual, cada comprobante o boleta debería tener un número único y aleatorio pre impreso o grabado en el momento de registrar el voto, que evite un doble conteo, pero que no permita vincular el voto con el votante.

Teniendo en cuenta las distintas premisas y las actuales particularidades de nuestro sistema electoral, se considera apropiado implementar en una primera etapa dispositivos de contabilización como los indicados en el párrafo anterior. Estos podrían ser del tipo de lectura óptica o RFID. En el primer caso

se utilizarían boletas únicas pre impresas con espacios reservados para que el votante realice las marcas correspondientes a su elección. En el segundo caso se utilizarían dispositivos como los empleados en Salta en las últimas elecciones provinciales, y mencionados en el capítulo Distintas experiencias de voto electrónico en Argentina del presente trabajo.

Con el fin de hacer frente a los problemas de lectura a distancia de las boletas de voto electrónico con etiquetas RFID, se deberían considerar las etiquetas del tipo pasivo y de baja frecuencia que operan en 124 KHz, 125 KHz o 135 KHz, cuyo rango de lectura máximo, establecido por los estándares de la industria, es de 30 centímetros [11], no obstante, también se tendrían que emplear esquemas de firma digital por mesa electoral con lo cual la lectura a distancia no revelaría ninguna información en claro respecto del voto.

Como resultado de la contabilización de votos, se obtendrían los totales por mesa tanto en formato digital como un respaldo en papel el cual serviría como soporte de control en el caso de requerirse una auditoría o contabilización manual.

Para la transmisión de los datos en formato digital se podrían emplear esquemas de firma digital a fin de resguardar su integridad.

Finalmente, para garantizar el éxito de la implementación del Plan Estratégico a largo, una vez consolidada esta primera etapa, se estaría en condiciones de continuar investigando la incorporación de nuevas TIC al Sistema Electoral Argentino.

5. Bibliografía

1. Busaniche, B. Heinz, F. y Rezinovsky, A., Voto Electrónico. Los riesgos de una ilusión, Fundación Vía Libre, Córdoba, 2008.
2. Código Electoral Nacional, ley 19.945 del 19 de Noviembre de 1972 y sus modificatorias, http://infoleg.mecon.gov.ar/infolegInternet/anexos/15000-19999/19442/texact.htm, 19 de junio de 2011.
3. Prince, Alejandro, Consideraciones, aportes y experiencias para el Voto electrónico en Argentina, Prince & Cooke, Buenos Aires, 2005.
4. Saltman, Roy G., Computer, Freedom and Privacy Conference, Burlingame, CA, Marzo de 1993 – Assuring Accuracy, Integrity and Security in National Elections: The Role of the U.S. Congress, Computer Professionals For Social Responsibility Organization, http://cpsr.org/prevsite/conferences/cfp93/saltman.html, 7 de enero de 2011.
5. Schneier, Bruce, Essays and Op Eds by Category: Elections, http://www.schneier.com/essays-elections.html, 28 de Octubre de 2010.
6. Shamos, Michael Ian, Computer, Freedom and Privacy Conference, Burlingame, CA, Marzo de 1993 – Electronic Voting Evaluating the Threat, Computer Professionals For Social Responsibility Organization, http://cpsr.org/prevsite/conferences/cfp93/shamos.html, 7 de enero de 2011.
7. Tula, M. I. (Coordinadora), Voto Electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales, Ariel Ciencia Política, Buenos Aires, 2005.
8. Tula, M. I., Voto Electrónico: Algunos principios generales para su aplicación, Documento de Políticas Públicas Nro. 31, CIPPEC, Buenos Aires, 2006.

9. Tula, M. I. y Bertotto, A., Pautas para la observación electoral en experiencias de voto electrónico, Documento de Políticas Públicas Nro. 32, CIPPEC, Buenos Aires, 2007.
10. The Netherlands return to paper ballots and red pencils, http://wijvertrouwenstemcomputersniet.nl/English, 7 de Enero de 2011.
11. The RFID Journal, http://www.rfidjournal.com, 19 de junio de 2011.